



MINISTÉRIO DO MEIO AMBIENTE
INSTITUTO CHICO MENDES DE CONSERVAÇÃO DA BIODIVERSIDADE
GABINETE DA PRESIDÊNCIA
EQSW 103/104, Bloco "C", Complexo Administrativo - Bloco C - Bairro Setor Sudoeste - Brasília
Telefone: (61) 2028-9011/9013

PORTARIA ICMBIO Nº 670, DE 10 DE AGOSTO DE 2022

Instituir a Política de Segurança da Informação - POSIN - no âmbito do Instituto Chico Mendes de Conservação da Biodiversidade. (Processo nº 02070.000752/2013-03).

O PRESIDENTE SUBSTITUTO DO INSTITUTO CHICO MENDES DE CONSERVAÇÃO DA BIODIVERSIDADE - ICMBio, no uso das competências atribuídas pelo artigo 24 do Decreto nº. 10.234, de 11 de fevereiro de 2020, designado pela Portaria GM/MMA nº 185, de 11 de julho de 2022, publicada no Diário Oficial da União de 12 de julho de 2022, Seção 2, pág. 54;

RESOLVE:

CAPÍTULO I
DO ESCOPO

Art. 1º Instituir a Política de Segurança da Informação - POSIN, que estabelece os princípios e diretrizes estratégicas para assegurar a disponibilidade, integridade, autenticidade e confiabilidade de dados, informações e documentos do ICMBio, contra ameaças e vulnerabilidades, de modo a preservar os ativos de informação institucional.

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

Art. 3º Esta POSIN e demais normas e procedimentos complementares aplicam-se à todas as unidades da estrutura organizacional do ICMBio, aos servidores e, no que couber, a colaboradores e demais usuários dos recursos de tecnologia da informação, seja em ambientes virtuais ou físicos abrangendo:

I - a segurança cibernética;

II - a segurança física e a proteção de dados organizacionais; e

III - as ações destinadas a assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação.

Art. 4º A presente Política de Segurança da Informação tem por fundamento as seguintes referências legais e normativas:

I - Decreto nº 9.637, de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação, e altera o Decreto nº 2.295, de 4 de agosto de 1997, que regulamenta o disposto no art. 24,

nº 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional;

II - Decreto nº 10.641, de 2 de março de 2021, que altera o Decreto nº 9.637, de 26 de dezembro de 2018;

III - Decreto nº 10.332, de 28 de abril de 2020, que Institui a Estratégia de Governo Digital para o período de 2020 a 2022, no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional e dá outras providências;

IV - Decreto nº 10.996, de 14 de março de 2022, que Altera o Decreto nº 10.332, de 28 de abril de 2020, que institui a Estratégia de Governo Digital para o período de 2020 a 2022, no âmbito dos órgãos e das entidades da administração pública federal

fundacional.- Decreto nº 10.222/2020, de 05 de fevereiro de 2020, que aprova a Estratégia Nacional de Segurança Cibernética;

V - Decreto nº 10.748, de 16 de julho de 2021, que institui a Rede Federal de Gestão de Incidentes Cibernéticos;

VI

- Instrução Normativa nº 1, de 27 de maio de 2020, do Gabinete de Segurança Institucional da Presidência da República, que dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal;

VII - Instrução Normativa GSI/PR nº 3, de 28 de maio de 2021 que dispõe sobre os processos relacionados à gestão de segurança da informação nos órgãos e nas entidades da administração pública federal;

VIII - Instrução Normativa GSI/PR nº 5, de 31 de agosto de 2021 que dispõe sobre os requisitos mínimos de segurança da informação para utilização de soluções de computação em nuvem pelos órgãos e pelas entidades da administração pública federal;

IX - Instrução Normativa GSI/PR nº 6, de 23 de dezembro de 2021 que estabelece diretrizes de segurança da informação para o uso seguro de mídias sociais nos órgãos e nas entidades da administração pública federal;

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

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

XII - Lei nº 9.983, de 14 de julho de 2000, que altera o Decreto-Lei

nº 2.848, de 7 de dezembro de 1940 - Código Penal e dá outras providências;

XIII -Lei nº 13.709/2018, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais;

XIV - Norma Complementar nº 05/IN01/DSIC/GSIPR, de 14 de agosto de 2009, do Departamento de Segurança da Informação e Comunicações da Presidência da República, que disciplina a criação de Equipes de Tratamento e Respostas a Incidentes em Redes Computacionais - ETIR nos órgãos e entidades da Administração Pública Federal;

XV - Norma Complementar nº 07/IN01/DSIC/GSIPR, de 15 julho de 2014, do Departamento de Segurança da Informação e Comunicações da Presidência da República, que estabelece diretrizes para a implementação de controles de acesso à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta;

XVI-Norma Complementar nº 08/IN01/DSIC/GSIPR, de 14 de agosto de 2010, do Departamento de Segurança da Informação e Comunicações da República, que estabelece as Diretrizes para o Uso de Dispositivos Móveis nos Aspectos relativos à Segurança da Informação e Comunicações nos órgãos e entidades da Administração Pública Federal;

XVII - Norma Complementar nº 12/IN01/DSIC/GSIPR, de 30 de janeiro de 2012, que estabelece diretrizes para o Uso de Dispositivos Móveis nos Aspectos relativos à Segurança da Informação e Comunicações nos órgãos e entidades da Administração Pública Federal;

XVIII - Norma Complementar nº 21/IN01/DSIC/GSIPR, de 08 de outubro de 2014, que estabelece as Diretrizes para o Registro de Eventos, Coleta e Preservação de Evidências de Incidentes de Segurança em Redes nos órgãos e entidades da Administração Pública Federal, direta e indireta;

XIX - Norma Técnica ABNT NBR ISO/IEC 27001:2013, que especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação dentro do contexto da organização;

- Norma Técnica ABNT NBR ISO/IEC 27002:2013, que fornece diretrizes para práticas de gestão de segurança da informação;

XXI - Norma Técnica ISO/IEC 27000:2018, que especifica conceitos e definições relacionados às normas de segurança da informação;

XXII - Portaria GSI/PR nº 93/2019, de 18 de outubro de 2021, que aprova o Glossário de Segurança da Informação;

XXIII - Portaria nº 271, de 27 de dezembro de 2013, que dispõe sobre normas a serem adotadas na elaboração e expedição de atos administrativos, no âmbito do Instituto Chico Mendes de conservação da Biodiversidade;

XXIV - Portaria nº 255, de 1º de abril de 2020, institui a Política de Gestão de Riscos e Integridade no âmbito do Instituto Chico Mendes de Conservação da Biodiversidade -ICMBio;

XXIII - Portaria Conjunta Nº 266, de 17 de junho de 2020, que institui o Planejamento Estratégico Integrado do Ministério do Meio Ambiente de suas Entidades Vinculadas 2020-2023;

CAPÍTULO II DOS CONCEITOS E DEFINIÇÕES

Art. 5º. Para efeitos desta POSIN, fica estabelecido o significado dos seguintes termos e expressões

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

II - **AGENTE PÚBLICO** 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 - **ALTA ADMINISTRAÇÃO** : para efeitos desta política, considera-se alta administração os ocupantes do cargo da Presidência e das Diretorias;

IV - **AMEAÇA**: conjunto de fatores externos ou causa potencial de um incidente indesejado, são agentes ou condições causadoras de incidentes contra ativos, em que são exploradas as vulnerabilidades, ocasionando perda de confidencialidade, integridade ou disponibilidade que pode resultar em dano para um sistema ou organização;

V - **ATIVIDADE**: ação ou conjunto de ações executados por um órgão ou entidade, ou em seu nome, que produzem ou suportem um ou mais produtos ou serviços;

VI - **ATIVIDADE CRÍTICA** - atividade que deve ser executada visando garantir a consecução de produtos e serviços fundamentais do órgão ou entidade, de forma a atingir os objetivos mais importantes e sensíveis ao tempo;

VII - **ATIVIDADE MALICIOSA** - qualquer atividade que infrinja a política de segurança de uma instituição ou que atente contra a segurança de um sistema

VIII - **ATIVO**: tudo que tenha valor para a organização, material ou não;

IX - **ATIVO DE REDE** - equipamento que centraliza, interliga, roteia, comuta, transmite ou concentra dados em uma rede de computadores;

X - **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;

XI - **ATOS INTERNACIONAIS**: vide tratados internacionais;

XII - **ATUALIZAÇÃO AUTOMÁTICA**: atualizações que são feitas no dispositivo ou sistema, sem a interferência do usuário, inclusive, em alguns casos, sem notificação ao usuário;

XIII - **ATUALIZAÇÃO AUTOMATIZADA**: fornece aos usuários a habilidade de aprovar, autorizar e rejeitar uma atualização. Em alguns casos, o usuário pode necessitar ter o controle de como e quando as atualizações serão implementadas, em função de horário de funcionamento, limite de consumo de dados da conexão, padronização do ambiente, garantia de disponibilidade, entre outros aspectos;

XIV - **AUDITORIA**: processo de exame cuidadoso e sistemático das atividades desenvolvidas, cujo objetivo é averiguar se elas estão de acordo com as disposições planejadas e estabelecidas previamente, se foram implementadas com eficácia e se estão adequadas e em conformidade à consecução dos objetivos;

XV - **AUTENTICAÇÃO**: processo que busca verificar a identidade digital de uma entidade de um sistema, no momento em que ela requisita acesso a esse sistema. O processo é realizado por meio de regras preestabelecidas, geralmente pela comparação das credenciais apresentadas pela entidade com outras já pré-definidas no sistema, reconhecendo como

verdadeiras ou legítimas as partes envolvidas em um processo;

XVI - AUTENTICAÇÃO DE DOIS FATORES (2 FACTOR AUTHENTICATION): processo de segurança que exige que os usuários forneçam dois meios de identificação antes de acessarem suas contas;

XVII - 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 (aferrível 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);

XVIII - AUTENTICIDADE: propriedade pela qual se assegura que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, equipamento, sistema, órgão ou entidade;

XIX - AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD): órgão da administração pública federal responsável por zelar, implementar e fiscalizar o cumprimento da Lei nº 13.709, de 14 de agosto de 2018;

XX - AUTORIZAÇÃO: processo que ocorre após a autenticação e que tem a função de diferenciar os privilégios atribuídos ao usuário que foi autenticado. Os atributos de autorização normalmente são definidos em grupos mantidos em uma base de dados centralizada, sendo que cada usuário herda as características do grupo a que ele pertence; portanto, autorização é o direito ou a permissão de acesso a um recurso de um sistema;

XXI - AVALIAÇÃO DE CONFORMIDADE DE SEGURANÇA DA INFORMAÇÃO: exame sistemático do grau de atendimento dos requisitos relativos à segurança da informação com legislações específicas;

XXII - AVALIAÇÃO DE RISCOS: processo de comparar o risco estimado com critérios de risco predefinidos para determinar a importância do risco;

XXIII - BACKDOOR: qualquer mecanismo inserido no sistema, intencionalmente ou acidentalmente, com o objetivo de permitir o acesso não documentado ao sistema ou aos seus dados;

XXIV - BACKEND AS A SERVICE(BaaS) - serviço de computação em nuvem que serve como middleware. Fornece aos desenvolvedores uma forma para conectar suas aplicações mobile e web a serviços na nuvem, a partir de interface de programação de aplicações (API) e de kit de desenvolvimento de software(SDK), abstraindo completamente a infraestrutura do lado do servidor;

XXV - BACKUP: conjunto de procedimentos que permitem salvar os dados de um sistema computacional, garantindo guarda, proteção e recuperação. Tem a fidelidade ao original assegurada. Esse termo também é utilizado para identificar a mídia em que a cópia é realizada;

XXVI - BANCO DE DADOS: coleção de dados inter-relacionados, representando informações sobre um domínio específico. São coleções organizadas de dados que se relacionam, a fim de criar algum sentido (informação) e de dar mais eficiência durante uma consulta ou a geração de informações ou conhecimento;

XXVII - BANCO DE DADOS PESSOAIS: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;

XXVIII

- BIA: sigla de business impact analysis (análise de impacto de negócios);

XXIX - BIG DATA: conjuntos de dados extremamente amplos e que, por este motivo, necessitam de ferramentas especialmente preparadas para lidar com grandes volumes, de forma que toda e qualquer informação nesses meios possa ser encontrada, analisada e aproveitada em tempo hábil;

XXX - BIOMETRIA: verificação da identidade de um indivíduo por meio de uma característica física ou BLACKLIST - lista de itens aos quais é negado o acesso a certos recursos, sistemas ou protocolos. Utilizar uma blacklist para controle de acesso significa garantir o acesso a todas entidades exceto àquelas incluídas na blacklist;

XXXI - BLINDAGEM: também chamada de hardening, trata-se de um processo de mapeamento das ameaças, mitigação dos riscos e execução das atividades corretivas, com foco em infraestrutura, com o principal objetivo de torná-la preparada para enfrentar tentativas de ataque;

XXXII -BLOCKCHAIN: base de dados que mantém um conjunto de registros que crescem continuamente. Novos registros são apenas adicionados à cadeia existente, sem que nenhum registro seja apagado;

XXXIII

- BLOQUEIO: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados;

XXXIV

- BLOQUEIO DE ACESSO: processo que tem por finalidade suspender temporariamente o acesso;

XXXV -BOT: tipo de malware que, além de incluir funcionalidades de worms, dispõe de mecanismos de comunicação com o invasor, os quais permitem que o computador infectado seja controlado remotamente. O processo de infecção e propagação do bot é similar ao do worm, ou seja, o bot é capaz de se propagar automaticamente, explorando vulnerabilidades existentes em programas instalados em computadores;

XXXVI

- BOTNET: rede formada por diversos computadores zumbis (infectados com bots). Permite potencializar as ações danosas executadas pelos bots e ser usada em ataques de negação de serviço, esquemas de fraude, envio de spam, entre outros;

XXXVII

- BRING YOUR OWN DEVICE(BYOD): trata-se de uma política de segurança de uma organização, que permite que os dispositivos pessoais dos funcionários sejam usados nas atividades corporativas. Uma política BYOD estabelece limitações e restrições sobre se um dispositivo pessoal (como um notebook, smartphone ou tablet) pode ou não ser conectado pela rede corporativa;

XXXVIII

- CAVALO DE TRÓIA: tipo de malware que, além de executar funções para as quais foi aparentemente projetado, também executa outras funções normalmente maliciosas e sem o conhecimento do usuário;

XXXIX

- CERT DIVISION: vide computer emergency response team division;

XL - CERTIFICAÇÃO: atesta a validade de um documento ou entidade;

XLI - CERTIFICAÇÃO DE POSTO DE CONTROLE: comprovação da conformidade dos requisitos técnicos mínimos, verificados por ocasião de uma inspeção de segurança

XLII - CERTIFICAÇÃO PROFISSIONAL: processo acordado pelas representações dos setores especializados, pelo qual se identifica, avalia e valida formalmente os conhecimentos, saberes, competências, habilidades e aptidões profissionais desenvolvidos em programas educacionais ou por experiência de trabalho, com o objetivo de promover o acesso, a

permanência e a progressão profissional;

XLIII - CERTIFICADO: documento assinado de forma criptografada, destinado a assegurar para outros a identidade do terminal que utiliza o certificado. Um certificado é considerado confiável quando for assinado por outro certificado confiável, como uma autoridade de certificação, ou se ele próprio é um certificado confiável, pertence a uma cadeia de confiança reconhecida;

XLIV - CERTIFICADO DE CONFORMIDADE: garantia formal de que um produto ou serviço, devidamente identificado, está em conformidade com uma norma legal;

XLV - CERTIFICADO DIGITAL: conjunto de dados de computador, gerados por uma autoridade certificadora, em observância à recomendação internacional ITU-T X.509 que se destina a registrar, de forma única, exclusiva e intransferível, a relação existente entre uma chave criptográfica e uma pessoa física, jurídica, máquina ou aplicação;

XLVI - CHAVE CRIPTOGRÁFICA: valor que trabalha com um algoritmo criptográfico para cifração ou decifração;

XLVII - CIFRAÇÃO: ato de codificar sinais de linguagem em claro, mediante uso de algoritmo criptográfico simétrico ou assimétrico, com o intuito de transformá-los em sinais ininteligíveis para pessoas não autorizadas a conhecê-la;

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

XLIX - CLICKJACKING: técnica maliciosa em que uma vítima é induzida a clicar em URL, botão ou outro objeto de tela que ela não tenha percebido e nem pretendido clicar. O clickjacking pode ser realizado de muitas maneiras, uma delas seria carregar uma página web, de forma transparente, atrás de outra página visível, de forma que os links e objetos para clicar são apenas fachadas; ou seja, quando o usuário clicar em um link aparentemente óbvio, ele na verdade, estará selecionando o link de uma página oculta

L - CLOUD BROKER: indivíduo ou organização que oferece consultoria, medeia e facilita a seleção de soluções de computação em nuvem em nome de uma organização. Um cloud broker serve como um terceiro entre um provedor de serviço de nuvem (PSN) e uma organização que contrata serviços de computação em nuvem. Para as infraestruturas de multi-nuvem, o cloud broker proporciona uma visão mais centralizada de todos os fornecedores e soluções, o que auxilia no gerenciamento dos recursos disponíveis e também dos custos. Em geral, consideram-se quatro tipos de cloud broker: a) serviços de agregação, que garantem a interoperabilidade entre diversos provedores de serviço de nuvem, por meio da agregação de todos os serviços contratados em uma única interface; b) serviços de integração, que adicionam valor automatizando fluxos de trabalho em ambientes híbridos, por meio de uma única orquestração, para melhorar o desempenho e reduzir o risco de negócios; c) serviços de personalização (ou customização), que modificam os serviços de nuvem existentes, a fim de atender às necessidades dos negócios da contratante, podendo inclusive desenvolver recursos adicionais para executar corretamente os serviços desejados; d) serviços de arbitragem, fornecendo flexibilidade ao contratante por intermédio da oferta de vários serviços semelhantes para avaliação e seleção;

LI - CLOUD JACKING: forma de ataque cibernético em que hackers infiltram-se nos programas e nos sistemas armazenados em ambiente de computação em nuvem, a fim de utilizar esses recursos para minerar criptomoedas;

LII - CÓDIGO DE INDEXAÇÃO: código alfanumérico que indexa documento com informação classificada em qualquer grau de sigilo;

LIII - CÓDIGO MALICIOSO: programa, ou parte de um programa de computador, projetado especificamente para atentar contra a segurança de um sistema computacional, normalmente por meio de exploração de alguma vulnerabilidade de sistema;

LIV -

Colaborador: pessoa que atua nos processos laborais do Instituto, independentemente de qual seja o vínculo institucional,

LV - COLETA DE EVIDÊNCIAS DE SEGURANÇA EM REDES COMPUTACIONAIS: processo de obtenção de itens físicos que contém uma potencial evidência, mediante a utilização de metodologia e de ferramentas adequadas. Esse processo inclui a aquisição, ou seja, a geração das cópias das mídias ou a coleta de dados que contenham evidências do incidente;

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

LVII - COMITÊ DE SEGURANÇA DA INFORMAÇÃO (CSIN): grupo de pessoas com a responsabilidade de assessorar a implementação das ações de segurança da informação no âmbito do ICMBio;

LVIII - COMITÊ GESTOR DE SEGURANÇA DA INFORMAÇÃO: instituído pelo Decreto nº 9.637, de 26 de dezembro de 2018, com atribuição de assessorar o Gabinete de Segurança Institucional da Presidência da República (GSI/PR) nas atividades relacionadas à segurança da informação;

LIX - COMITÊ GESTOR DA ICP BRASIL: vinculado à Casa Civil da Presidência da República, possui como principal competência determinar as políticas que a AC-Raiz executará. É composto por cinco representantes da sociedade civil, integrantes de alguns setores afetos ao tema e representantes de órgãos da administração pública federal;

LX - COMMON VULNERABILITIES AND EXPOSURES(CVE): banco de dados on-line de ataques, explorações e comprometimento de segurança. É mantido pela MITRE Corporation em benefício do público. Ele inclui quaisquer ataques e abusos conhecidos, sobre qualquer tipo de sistema computacional ou produto de software. Muitas vezes, novos ataques e explorações são documentados em um CVE muito antes do fornecedor admitir o problema ou liberar uma atualização ou patch para resolver a situação. O link para o CVE é <https://cve.mitre.org>;

LXI - COMPUTER EMERGENCY RESPONSE TEAM DIVISION(CERT DIVISION): divisão do Software Engineering Institute (SEI), que se trata de um centro de pesquisa e desenvolvimento financiado pelo governo federal dos Estados Unidos sem fins lucrativos. O CERT pesquisa ameaças cibernéticas que impactam o desenvolvimento e utilização de software e a segurança na Internet, publica pesquisas e informações sobre suas descobertas e trabalha com empresas e governo para melhorar a segurança do software e da Internet como um todo;

LXII - COMPUTAÇÃO EM NUVEM: modelo de fornecimento e entrega de tecnologia de informação que permite acesso conveniente e sob demanda a um conjunto de recursos computacionais configuráveis, sendo que tais recursos podem ser provisionados e liberados com mínimo gerenciamento ou interação com o provedor do serviço de nuvem (PSN);

LXIII - COMPROMETIMENTO - perda de segurança resultante do acesso não autorizado;

LXIV - COMUNICAÇÃO DE DADOS: transmissão, emissão ou recepção de dados ou informações de qualquer natureza, por meios confinados, por radiofrequência ou por qualquer outro processo eletrônico ou eletromagnético ou ótico;

LXV - COMUNICAÇÃO DO RISCO: troca ou compartilhamento de informação sobre risco entre o tomador de decisão e outras partes interessadas;

LXVI - COMUNIDADE OU PÚBLICO ALVO: conjunto de pessoas, setores, órgãos ou entidades atendidas por uma Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos;

LXVII - CONFIANÇA ZERO: modelo de segurança criado em 2010, por John Kindervag, cujo principal conceito é não confiar em qualquer entidade interna ou externa à rede de infraestrutura de tecnologia da informação da organização. Atuando

sempre com a suposição de que existem violações de segurança, esse modelo implica em alteração na postura, na política e no processo da organização, visando eliminar os problemas de estratégias, com foco apenas no perímetro, por meio da adoção de três princípios básicos: a) exigência de acesso seguro a todos os recursos, independentemente da origem da solicitação (interna ou externa) ou de quais recursos ela acesse; b) adoção de um modelo de privilégio mínimo, com a utilização de políticas adaptativas baseadas em risco e proteção de dados, em especial, pelo controle de permissões desnecessárias e usuários inativos; c) inspeção e registro de todos os eventos, com a aplicação de análises avançadas, para detectar e responder às anomalias em tempo real;

LXVIII -CONFIDENCIALIDADE: propriedade pela qual se assegura que a informação não esteja disponível ou não seja revelada à pessoa, ao sistema, ao órgão ou à entidade não autorizados nem credenciados;

LXIX - CONFORMIDADE EM SEGURANÇA DA INFORMAÇÃO: cumprimento das legislações, normas e procedimentos relacionados à segurança da informação da organização;

LXX - CONSCIENTIZAÇÃO - atividade que tem por finalidade orientar sobre o que é segurança da informação, levando os participantes a obterem um nível adequado de conhecimento sobre segurança, além de um senso apropriado de responsabilidade. O objetivo dessa atividade é proteger o ativo de informações do órgão ou entidade, para garantir a continuidade dos negócios, minimizar os danos e reduzir eventuais prejuízos financeiros;

LXXI - CONSENTIMENTO: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

LXXII - CONTA DE SERVIÇO: conta de acesso à rede corporativa de computadores, necessária a um procedimento automático (aplicação, script, entre outros) sem qualquer intervenção humana no seu uso;

LXXIII -CONTATO TÉCNICO DE SEGURANÇA: pessoa ou equipe a ser acionada em caso de incidente de segurança envolvendo a administração pública federal, com atribuições eminentemente técnicas sobre a questão;

LXXIV

- **CONTÊINER DOS ATIVOS DE INFORMAÇÃO:** local onde se encontra o ativo de informação. Geralmente, um contêiner descreve algum tipo de ativo tecnológico hardware, software ou sistema de informação (mas também pode se referir a pessoas ou mídias como papel, CD-ROM ou DVD-ROM). Um contêiner, portanto, é qualquer tipo de ativo dentro do qual um ativo de informação é armazenado, transportado ou processado. Ele pode ser um único ativo tecnológico (como um servidor), uma coleção de ativos tecnológicos (como uma rede) ou uma coletânea de mídias digitais, entre outros;

LXXV -CONTINUIDADE DE NEGÓCIOS: capacidade estratégica e tática de um órgão ou entidade de se planejar e responder a incidentes e interrupções de negócios, minimizando seus impactos e recuperando perdas de ativos da informação das atividades críticas, a fim de manter suas operações em um nível aceitável, previamente definido;

LXXVI

- **CONTRATO SIGILOSO:** ajuste, convênio ou termo de cooperação, cujo objeto ou execução implique tratamento de informação classificada;

LXXVII

- **CONTROLADOR:** pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

LXXVIII

- **CONTROLE:** forma de gerenciar o risco, incluindo políticas, procedimentos, diretrizes, práticas ou estruturas organizacionais que podem ser de natureza administrativa, técnica, de gestão ou legal. Trata-se de sinônimo para proteção ou contramedida;

LXXIX

- **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. Via de regra, requer procedimentos de autenticação;

LXXX -CONTROLE DE ACESSO À INFORMAÇÃO CLASSIFICADA: realizado por meio de credencial de segurança e da demonstração da necessidade de conhecer;

LXXXI

- **CONTROLES DE SEGURANÇA:** certificado que autoriza uma pessoa natural para o tratamento de informação classificada;

LXXXII

- **CÓPIA DE SEGURANÇA** - vide backup.

LXXXIII

- **CRENCIAL DE ACESSO:** permissão concedida por autoridade competente, após o processo de credenciamento, que habilita determinada pessoa, sistema ou organização ao acesso de recursos. A credencial pode ser física (como por exemplo um crachá), ou lógica (como por exemplo a identificação de usuário e senha);

LXXXIV

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

LXXXV

- **DADO PESSOAL:** informação relacionada à pessoa natural identificada ou identificável;

LXXXVI

- **DADO PESSOAL SENSÍVEL:** dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

LXXXVII

- **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;

LXXXVIII

- **DATAGRAMA (PACOTE DE DADOS):** trata-se de dados encapsulados, ou seja, dados aos quais são acrescentados cabeçalhos com informações sobre o seu transporte (como o endereço IP de destino). Os dados contidos nos datagramas são analisados e eventualmente alterados pelos switches (roteadores) que permitem o seu trânsito. Os dados circulam na Internet na forma de datagramas;

LXXXIX

- **DDoS:** sigla de negação de serviço distribuída (distributed denial of service);

XC - DECIFRAÇÃO: ato de decifrar, mediante uso de algoritmo simétrico ou assimétrico, com recurso criptográfico, para reverter processo de cifração original;

XCI - DEEPFAKE: forma de vídeo manipulado, utilizando técnicas de síntese de imagem humana, que criam renderizações

artificiais hiper-realistas de um ser humano. Esses vídeos geralmente são criados pela mistura de um vídeo já existente com novas imagens, áudio e vídeo, para criar a ilusão da fala. Esse processo é realizado por meio de redes contraditórias generativas (GAN). A consequência mais perigosa da popularidade dos deepfakes é que eles podem facilmente convencer as pessoas a acreditarem em uma determinada história ou teoria, o que pode resultar em comportamentos com grande impacto na vida política, social ou financeira;

XCII - DESASTRE: evento, ação ou omissão, repentino e não planejado, que tenha permitido 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, causando perda para toda ou parte da organização e gerando sérios impactos em sua capacidade de entregar serviços essenciais ou críticos por um período de tempo superior ao tempo objetivo de recuperação;

XCIII - DESCARTE: eliminação correta de informações, documentos, mídias e acervos digitais;

XCIV - DESCRENCIAMENTO DE SEGURANÇA: processo utilizado para desabilitar órgão ou entidade, pública ou privada, ou para revogar a credencial de pessoal natural, para o tratamento da informação classificada;

XCv - DIREITO DE ACESSO: privilégio associado a um cargo, pessoa ou processo, para ter acesso a um ativo;

XCvI - DISPONIBILIDADE: propriedade pela qual se assegura que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade devidamente autorizados;

XCvII -DISPOSITIVOS MÓVEIS: equipamentos portáteis, dotados de capacidade de processamento, ou dispositivos removíveis de memória para armazenamento, entre os quais se incluem, não limitando a estes: e-books, notebooks, netbooks, smartphones, tablets, pendrives, USB drives, HD externo, e cartões de memória;

XCvIII

- **DLP - sigla de prevenção de perda de dados (data loss prevention);**

XCIX - DOCUMENTO: unidade de registro de informações, qualquer que seja o suporte ou o formato;

C - DOCUMENTOS CLASSIFICADOS: documentos que contenham informação classificada em qualquer grau de sigilo;

CI - DOCUMENTO CONTROLADO: documento que contenha informação classificada em qualquer grau de sigilo ou previsto na legislação como sigiloso, que requeira medidas adicionais de controle;

CII - DOCUMENTO PREPARATÓRIO: documento formal utilizado como fundamento da tomada de decisão ou de ato administrativo, a exemplo de pareceres e notas técnicas;

CIII - DOMÍNIO CIBERNÉTICO: domínio de processamento de informações (dados) eletrônicas, composto de uma ou mais infraestruturas de tecnologia da informação;

CIV - DoS: sigla de negação de serviço (denial of service);

CV - E-MAIL: sigla de correio eletrônico (electronic mail);

CVI - ECOSISTEMA CIBERNÉTICO: infraestrutura de informação interconectada de interações entre pessoas, processos, dados e tecnologias da informação, juntamente com o ambiente e as condições que influenciam essas interações. Engloba diversos participantes - governo, firmas privadas, organizações não-governamentais, indivíduos, processos e dispositivos cibernéticos - que interagem com propósitos diversos;

CVII - ELIMINAÇÃO: exclusão de dado ou conjunto de dados, armazenados em banco de dados, independentemente do procedimento empregado;

CVIII - ENCARREGADO DE TRATAMENTO DE DADOS: pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados;

CIX - ENDEREÇO IP: conjunto de elementos numéricos ou alfanuméricos, que identifica um dispositivo eletrônico em uma rede de computadores. Sequência de números associada a cada computador conectado à Internet. No caso de IPv4, o endereço IP é dividido em quatro grupos, separados por "." e compostos por números entre 0 e 255. No caso de IPv6, o endereço IP é dividido em até oito grupos, separados por ":" e compostos por números hexadecimais (números e letras de "A" a "F") entre 0 e FFFF;

CX - ENGENHARIA SOCIAL: técnica por meio da qual uma pessoa procura persuadir outra a executar determinadas ações. No contexto da segurança da informação, é considerada uma prática de má-fé para tentar explorar a boa-fé ou abusar da ingenuidade e da confiança de indivíduos, a fim de aplicar golpes, ludibriar ou obter informações sigilosas e importantes;

CXI - EQUIPE DE COORDENAÇÃO SETORIAL: equipe de prevenção, tratamento e resposta a incidentes cibernéticos das agências reguladoras, do Banco Central do Brasil ou da Comissão Nacional de Energia Nuclear ou das suas entidades reguladas responsáveis por coordenar as atividades de segurança cibernética e de centralizar as notificações de incidentes das demais equipes do setor regulado;

CXII - EQUIPE DE PREVENÇÃO, TRATAMENTO E RESPOSTA A INCIDENTES CIBERNÉTICOS (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;

CXIII - EQUIPE DE TRATAMENTO E RESPOSTA A INCIDENTES CIBERNÉTICOS (ETIR) - termo alterado pelo Decreto nº 10.641, de 2 de março de 2021, para denominação Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos;

CXIV - EQUIPES PRINCIPAIS: equipes de prevenção, tratamento e resposta a incidentes cibernéticos de entidades, públicas ou privadas, responsáveis por ativos de informação, em especial aqueles relativos a serviços essenciais, cuja interrupção ou destruição, total ou parcial, provoque sério impacto social, ambiental, econômico, político, internacional ou à segurança do Estado e da sociedade, nos termos do disposto no parágrafo único, inciso I, do art. 1º do Anexo ao Decreto nº 9.573, de 22 de novembro de 2018;

CXV - ESFERA DE INFORMAÇÃO: ambiente em que a informação existe e flui de forma estruturada ou randômica, e em que fatos ou conhecimentos residem e são representados ou transmitidos por uma sequência particular de símbolos, impulsos ou caracterizações;

CXVI - ESPAÇO CIBERNÉTICO: espaço virtual composto por um conjunto de canais de comunicação da Internet e outras redes de comunicação, que garantem a interconexão de dispositivos de tecnologia da informação. Engloba todas as formas de atividades digitais em rede, incluindo o armazenamento, processamento e compartilhamento de conteúdo, além de todas as ações, humanas ou automatizadas, conduzidas por meio desse ambiente;

CXVII -ESPAÇO DE INFORMAÇÃO: qualquer meio em que a informação possa ser criada, transmitida, recebida, armazenada, processada ou descartada;

CXVIII

- **ESPIONAGEM CIBERNÉTICA:** atividade que consiste em ataques cibernéticos dirigidos contra a confidencialidade de sistemas de tecnologia da informação, com o objetivo de obter dados e informações sensíveis a respeito de planos e atividades de um governo, instituição, empresa ou pessoa física, sendo geralmente lançados e gerenciados por serviços de inteligência estrangeiros ou por empresas concorrentes;

CXIX - ESTIMATIVA DE RISCOS: processo utilizado para atribuir valores à probabilidade e às consequências de um risco;

CXX - ESTRATÉGIA DE CONTINUIDADE DE NEGÓCIOS: abordagem de um órgão ou entidade que garante a recuperação dos ativos da informação e a continuidade das atividades críticas ao se confrontar com um desastre, uma interrupção ou com outro incidente maior;

CXXI - EVENTO: qualquer mudança de estado que tem importância para a gestão de um item de configuração ou serviço de tecnologia da informação. Em outras palavras, qualquer ocorrência dentro do escopo de tecnologia da informação que tenha relevância para a gestão dos serviços entregues ao cliente;

CXXII - EVENTO DE SEGURANÇA: 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;

CXXIII

- EVIDÊNCIA DIGITAL: informação ou dado, armazenado ou transmitido eletronicamente, em modo binário, que pode ser reconhecida como parte de um evento;

CXXIV

- EVITAR O RISCO: forma de tratamento de risco, na qual a alta administração decide não realizar a atividade, não se envolver ou não agir, a fim de se retirar de uma situação de risco;

CXXV -EXCLUSÃO DE ACESSO: processo que tem por finalidade suspender definitivamente o acesso, incluindo o cancelamento do código de identificação e de perfil de acesso;

CXXVI

- EXPLOIT: técnicas, programas ou parte de programas maliciosos, projetados para explorar uma vulnerabilidade existente em um programa de computador. Entre os tipos mais comuns de exploits estão o SQLinjection, o cross-site scripting, o abuso de configuração de autenticação fraca e o abuso de falhas de configuração de segurança;

CXXVII

- FIDC: sigla de formulário individual de dados para credenciamento;

CXXVIII

- FIREWALL- ferramenta para evitar acesso não autorizado, tanto na origem quanto no destino, a uma ou mais redes. Podem ser implementados por meio de hardware ou software, ou por meio de ambos. Cada mensagem que entra ou sai da rede passa pelo firewall, que a examina a fim de determinar se atende ou não os critérios de segurança especificados;

CXXIX

- FORENSE DIGITAL: aplicação de procedimentos digitais investigativos para a identificação, exame e análise de dados, com a devida preservação da integridade da informação e mantendo uma estrita cadeia de custódia para os dados;

CXXX -GESTÃO DE CONTINUIDADE DE NEGÓCIOS EM SEGURANÇA DA INFORMAÇÃO: processo que identifica ameaças potenciais para uma organização e os possíveis impactos nas operações de negócio, caso estas ameaças se concretizem. Esse processo fornece uma estrutura para que se desenvolva uma resiliência organizacional que seja capaz de responder efetivamente e salvaguardar os interesses das partes interessadas, a reputação, a marca da organização e suas atividades de valor agregado;

CXXXI

- GESTÃO DE INCIDENTES CIBERNÉTICOS: processo que realiza ações sobre qualquer evento adverso relacionado à segurança cibernética dos sistemas ou da infraestrutura de computação;

CXXXII

- GESTÃO DE CONTINUIDADE: processo abrangente de gestão que identifica ameaças potenciais para uma organização e os possíveis impactos nas operações de negócio, caso estas ameaças se concretizem. Esse processo fornece uma estrutura para que se desenvolva uma resiliência organizacional que seja capaz de responder efetivamente e salvaguardar os interesses das partes interessadas, a reputação, a marca da organização e suas atividades de valor agregado;

CXXXIII

- GESTÃO DE RISCOS: 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;

CXXXIV

- GESTÃO DE SEGURANÇA DA INFORMAÇÃO: ações e métodos que visam à integração das atividades de gestão de riscos, à gestão de continuidade do negócio, ao tratamento de incidentes, ao tratamento da informação, à conformidade, ao credenciamento, à segurança cibernética, à segurança física, à segurança lógica, à segurança orgânica e à segurança organizacional aos processos institucionais estratégicos, operacionais e táticos, não se limitando, portanto, à tecnologia da informação e comunicações;

CXXXV

- GESTOR DE SEGURANÇA DA INFORMAÇÃO: responsável pelas ações de segurança da informação no ICMBio;

CXXXVI

- GESTOR DE MUDANÇAS: responsável pelo planejamento e implementação do processo de gestão de mudanças no âmbito do órgão ou entidade da administração pública federal;

CXXXVII

- GESTOR DE SEGURANÇA E CREDENCIAMENTO (GSC): responsável pela segurança da informação classificada, em qualquer grau de sigilo, nos órgãos de registro e postos de controle;

CXXXVIII

- GSC: sigla de gestor de segurança e credenciamento;

CXXXIX

- HABILITAÇÃO DE SEGURANÇA: condição atribuída a um órgão ou a uma entidade, pública ou privada, que lhe confere a aptidão para o tratamento da informação classificada em determinado grau de sigilo;

CXL - HASH- resultado único e de tamanho fixo, gerado por uma função de resumo. O hash pode ser utilizado, entre outras possibilidades, para verificar a integridade de arquivos e gerar assinaturas digitais. Ele é gerado de forma que não é possível realizar o processamento inverso para recuperação da informação original. Além disso, qualquer alteração na informação original produzirá um hash distinto. Apesar de ser teoricamente possível que informações diferentes gerem hashes iguais, a probabilidade de isso ocorrer é bastante baixa;

CXLI - HIPÓTESE LEGAL DE SIGILO: quando uma informação sigilosa é definida por lei específica, diversa da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação);

CXLII -HONEYNET: ferramenta de pesquisa, que consiste em uma rede projetada especificamente para ser comprometida, e que contém mecanismos de controle para prevenir que seja utilizada como base de ataques contra outras redes. Trata-se

de um tipo de honeypot de alta interatividade, projetado para pesquisa e obtenção de informações dos invasores, também conhecido como honeypot de pesquisa;

CXLIII -HONEYPOT: recurso computacional de segurança dedicado a ser sondado, atacado ou comprometido. Existem dois tipos de honeypots: os de baixa interatividade e os de alta interatividade. Em um honeypot de baixa interatividade são instaladas ferramentas para emular sistemas operacionais e serviços com os quais os atacantes irão interagir; desta forma, o sistema operacional real deste tipo de honeypot deve ser instalado e configurado de modo seguro, para minimizar o risco de comprometimento. Nos honeypots de alta interatividade, os atacantes interagem com sistemas operacionais, aplicações e serviços reais;

CXLIV

- HSM: sigla de módulo de segurança em hardware (hardware security module);

CXLV -HSTS: sigla de HTTP strict transport security;

CXLVI

- HTTP: sigla de hypertext transfer protocol;

CXLVII

- HTTPS: sigla de hypertext transfer protocol secure;

CXLVIII

- HTTP STRICT TRANSPORT SECURITY(HSTS): mecanismo de política de segurança web que ajuda a proteger websites contra os ataques do tipo degradação de protocolo e sequestro de cookies. Ele permite que os servidores web determinem que os browsers (ou outros mecanismos de acesso) devem interagir com eles, utilizando apenas conexões seguras HTTPS. O HSTS é um padrão IETF e está especificado na RFC 6797;

CXLIX

- HYPERTEXT TRANSFER PROTOCOL(HTTP): protocolo de comunicação entre sistemas de informação, o qual permite a transferência de dados entre redes de computadores, principalmente na World Wide Web (Internet). Para que esta transferência de dados ocorra, o protocolo HTTP necessita estar agregado a outros dois protocolos de rede, TCP e IP, os quais possibilitam a comunicação entre a URL e o servidor web que armazenará os dados, a fim de que a página HTML solicitada pelo usuário seja enviada;

CL - HYPERTEXT TRANSFER PROTOCOL SECURE(HTTPS): extensão do HTTP, utilizado para comunicação segura pela rede de computadores. No HTTPS o protocolo de comunicação é criptografado usando o TLS ou o seu predecessor, o SSL. A principal motivação para o uso do HTTPS é a autenticação dos sites e a proteção da privacidade e integridade dos dados trocados durante o tráfego de informações;

CLI - HYPERVISOR: também conhecido como monitor de máquina virtual, é um software, firmware ou hardware que cria e roda máquinas virtuais;

CLII - IaaS: sigla de infraestrutura como código (infrastructure as a code);

CLIII - IaaS: sigla de infraestrutura como serviço (infrastructure as a service);

CLIV - IaC: sigla de infraestrutura como código (infrastructure as code);

CLV - IBE: sigla de criptografia baseada em identidade (identity-based encryption);

CLVI - ICP-Brasil: sigla de infraestrutura de chaves públicas brasileira;

CLVII -IDENTIDADE DIGITAL: representação unívoca de um indivíduo dentro do espaço cibernético;

CLVIII -IDENTIFICAÇÃO DE RISCOS: processo de localizar, listar e caracterizar elementos de risco;

CLIX - IDS: sigla de sistema de detecção de intrusão (intrusion detection system);

CLX - IMAGEM DE MÁQUINA VIRTUAL: abrange a definição completa do armazenamento de uma máquina virtual, contendo o disco do sistema operacional e todos os discos de dados, capturando as propriedades do disco (como cache de host) necessárias para implantar uma Virtual Machine em uma unidade reutilizável;

CLXI - 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 crítica ou de alguma atividade crítica por um período de tempo inferior ao tempo objetivo de recuperação;

CLXII -INCIDENTE DE SEGURANÇA: qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;

CLXIII -INCIDENTE CIBERNÉTICO: ocorrência que pode comprometer, real ou potencialmente, a disponibilidade, a integridade, a confidencialidade ou a autenticidade de sistema de informação ou das informações processadas, armazenadas ou transmitidas por esse sistema. Poderá também ser caracterizada pela tentativa de exploração de vulnerabilidade de sistema de informação que caracterize violação de norma, política de segurança, procedimento de segurança ou política de uso. De maneira geral, os tipos de atividade comumente reconhecidas como incidentes cibernéticos são: a) tentativas de obter acesso não-autorizado a um sistema ou a dados armazenados; b) tentativa de utilização não-autorizada de sistemas para a realização de atividades de processamento ou armazenamento de dados; c) mudanças não-autorizadas de *firmware*, *hardware* ou *software* em um ambiente computacional; d) ataques de negação de serviço (DoS); e e) demais ações que visem afetar a disponibilidade ou integridade dos dados. Um incidente de segurança cibernética não significa necessariamente que as informações já estão comprometidas; significa apenas que a informação está ameaçada;

CLXIV

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

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

CLXVI

- INFORMAÇÃO PESSOAL: informação relacionada à pessoa natural identificada ou identificável, relativa à intimidade, vida privada, honra e imagem;

CLXVII

- INFORMAÇÃO SIGILOSA: informação submetida temporariamente à restrição de acesso público, em razão de sua imprescindibilidade para a segurança da sociedade e do Estado; e aquela abrangida pelas demais hipóteses legais de sigilo;

CLXVIII

- INFORMAÇÃO SIGILOSA CLASSIFICADA: vide informação classificada;

CLXIX

- INFORMAÇÃO SIGILOSA PROTEGIDA POR LEGISLAÇÃO ESPECÍFICA: informação amparada pelo sigilo bancário, fiscal,

comercial, profissional ou segredo de justiça (lista com exemplos encontra-se no ANEXO A do Glossário);

CLXX -INFRAESTRUTURA CIBERNÉTICA: sistemas e serviços de informação compostos por todo hardware e software necessários para processar, armazenar e transmitir a informação, ou qualquer combinação desses elementos. O processamento inclui criação, acesso, modificação e destruição da informação. O armazenamento engloba qualquer tipo de mídia na qual a informação esteja armazenada. A transmissão é composta tanto pela distribuição como pelo compartilhamento da informação, por qualquer meio;

CLXXI

- INFRAESTRUTURA COMO CÓDIGO (IaC): processo de gerenciamento e provisionamento de data centers de computador, por meio de arquivos de definição legíveis por máquina, em vez de configuração física de hardware ou ferramentas de configuração interativas;

CLXXII

- INFRAESTRUTURA COMO SERVIÇO (IaaS): tipo de serviço de computação em nuvem onde o provedor de serviço de nuvem oferece ao cliente a capacidade de criar redes virtuais em seu ambiente de computação. Uma solução IaaS permite que o cliente selecione quais sistemas operacionais instalar em máquinas virtuais, bem como a estrutura da rede, incluindo o uso de switches virtuais, roteadores e firewalls. O IaaS também fornece total liberdade quanto ao software ou código personalizado executado nas máquinas virtuais. Uma solução IaaS é a mais flexível de todos os serviços de computação em nuvem; permite uma redução significativa do hardware pelo cliente em sua própria instalação local. Geralmente, é a forma mais cara de serviço de computação em nuvem;

CLXXIII

- INFRAESTRUTURA CRÍTICA: instalações, serviços, bens e sistemas, virtuais ou físicos, que se forem incapacitados, destruídos ou tiverem desempenho extremamente degradado, provocarão sério impacto social, econômico, político, internacional ou à segurança;

CLXXIV

- INFRAESTRUTURA CRÍTICA DE INFORMAÇÃO: sistemas de tecnologia da informação que suportam ativos e serviços chaves da infraestrutura nacional crítica;

CLXXV

- INFRAESTRUTURA DE CHAVE PÚBLICA (PKI): sistema de recursos, políticas e serviços que suportam a utilização de criptografia de tecla pública para autenticar as partes envolvidas na transação. Não há um único padrão que define os componentes de uma infraestrutura de chave pública, mas uma infraestrutura de chave pública geralmente inclui autoridades certificadoras e autoridades de registro. O padrão ITU-T X.509 fornece a base para a infraestrutura de chave pública padrão de mercado;

CLXXVI

- INTERFACE DE PROGRAMAÇÃO DE APLICAÇÕES (API): tem por objetivo disponibilizar recursos de uma aplicação para serem usados por outra aplicação, abstraindo os detalhes da implementação e, muitas vezes, restringindo o acesso a esses recursos com regras específicas para tal;

CLXXVII

- INTERNET: rede global, composta pela interligação de inúmeras redes. Conecta mais de 500 milhões de usuários, provendo comunicação e informações das mais variadas áreas de conhecimento;

CLXXVIII

- INTERNET DAS COISAS (IoT): infraestrutura que integra a prestação de serviços de valor adicionado com capacidades de conexão física ou virtual de coisas, com dispositivos baseados em tecnologias da informação existentes e nas suas evoluções, com interoperabilidade, conforme disposto no Decreto nº 9.854, de 25 de junho de 2019, que institui o Plano Nacional de Internet das Coisas;

CLXXIX

- PROTOCOL (IP): protocolo que permite o endereçamento e o transporte de pacotes de dados (datagramas) na Internet, sem, contudo, assegurar que estes pacotes sejam entregues;

CLXXX

- INTEROPERABILIDADE: característica que se refere à capacidade de diversos sistemas e organizações trabalharem em conjunto (interoperar), de modo a garantir que pessoas, organizações e sistemas computacionais interajam para trocar informações de maneira eficaz e eficiente;

CLXXXI

- INTRANET: rede privada, acessível apenas aos membros da organização a que atende. Utiliza os mesmos recursos e protocolos da Internet, mas é comumente separada desta, por meio de firewalls;

CLXXXII

- INVASÃO: incidente de segurança no qual o ataque foi bem-sucedido, resultando no acesso, na manipulação ou na destruição de informações em um computador ou em um sistema da organização;

CLXXXIII

- INVESTIGAÇÃO PARA CREDENCIAMENTO DE SEGURANÇA: verificação da existência dos requisitos indispensáveis para a concessão da credencial de segurança a uma pessoa natural, a fim de realizar o tratamento de informação classificada;

CLXXXIV

- IoT: - sigla de Internet das coisas (Internet of things);

CLXXXV

- IP: sigla de Internet protocol;

CLXXXVI

- JAILBREAK: processo que modifica o sistema operacional original de um dispositivo, permitindo que ele execute aplicativos não-autorizados pelo fabricante. Um aparelho com um software do tipo jailbreak é capaz de instalar aplicativos anteriormente indisponíveis nos sites oficiais do fabricante, por meio de instaladores não-oficiais, assim como aplicações adquiridas de forma ilegal. O uso de técnicas jailbreak não é recomendado pelos fabricantes, já que permitem a execução de aplicativos não certificados, que podem inclusive conter malware embutidos;

CLXXXVII

- KEYLOGGER- tipo específico de spyware, com a capacidade de capturar e de armazenar as teclas digitadas pelo usuário no teclado do computador. Normalmente, a ativação do keylogger é condicionada a uma ação prévia do usuário, como o acesso a um site específico de comércio eletrônico ou de Internet banking;

CLXXXVIII

- KIT DE DESENVOLVIMENTO DE SOFTWARE (SDK): conjunto de ferramentas de desenvolvimento e de códigos pré-gravados, que podem ser usados pelos desenvolvedores para criar aplicativos. Geralmente, ajudam a reduzir a quantidade de esforço e de tempo que seria necessário para os profissionais escreverem seus próprios códigos;

CLXXXIX

- LAI: sigla de Lei de Acesso a Informação;

CXC - LGPD: sigla de Lei Geral de Proteção de Dados Pessoais;

CXCI - LISTA DE CONTROLE DE ACESSO (ACL): mecanismo que implementa o controle de acesso para um recurso, enumerando as entidades do sistema que possuem permissão para acessar o recurso e definindo, explicita ou implicitamente, os modos de acesso concedidos à cada entidade;

CXCII - LIVRO RAZÃO DISTRIBUÍDO (DLT): banco de dados distribuído por vários nós ou dispositivos de computação. Cada nó replica e salva uma cópia idêntica do livro-razão. Cada nó participante da rede atualiza-se de forma independente. O recurso inovador da tecnologia de contabilidade distribuída é que a planilha não é mantida por nenhuma autoridade central. Atualizações para o livro-razão são independentemente construídas e registradas por cada nó. Os nós então votam nessas atualizações, para garantir que a maioria concorde com a conclusão alcançada. Um sistema blockchain é uma forma de tecnologia de contabilidade distribuída. No entanto, a estrutura do sistema blockchain é distinta de outros tipos de livro-razão distribuídos, pois os dados em um sistema blockchain são agrupados e organizados em blocos, que são então ligados entre si e protegidos usando criptografia;

CXCIII

- LISTA DE BLOQUEIO: vide blacklist;

CXCIV

- LOG (REGISTRO DE AUDITORIA): registro de eventos relevantes em um dispositivo ou sistema computacional;

CXCV - MALWARE: software malicioso, projetado para infiltrar um sistema computacional, com a intenção de roubar dados ou danificar aplicativos ou o sistema operacional. Esse tipo de software costuma entrar em uma rede por meio de diversas atividades aprovadas pela empresa, como e-mail ou sites. Entre os exemplos de malware estão os vírus, worms, trojans (ou cavalos de Troia), spyware, adware e rootkits;

CXCVI

- MÁQUINA VIRTUAL (VM): as máquinas virtuais são computadores de software, com a mesma funcionalidade que os computadores físicos. Assim como os computadores físicos, elas executam aplicativos e um sistema operacional. No entanto, as máquinas virtuais são arquivos de computador, executados em um computador físico, e se comportam como um computador físico. Geralmente, são criadas para tarefas específicas, cujas execuções são arriscadas em um ambiente host, como por exemplo, o acesso a dados infectados por vírus e a testes de sistemas operacionais. Como a máquina virtual é separada por sandbox do restante do sistema, o software dentro dela não pode adulterar o computador *host*. As máquinas virtuais também podem ser usadas para outras finalidades, como a virtualização de servidores;

CXCVII

- MATERIAL DE ACESSO RESTRITO: qualquer matéria, produto, substância ou sistema que contenha, utilize ou veicule conhecimento ou informação classificada, em qualquer grau de sigilo, informação econômica ou informação científico-tecnológica, cuja divulgação implique risco ou dano aos interesses da sociedade e do Estado, tendo seu acesso restrito às pessoas autorizadas pelo órgão ou entidade;

CXCVIII

- MATRIZ RACI: também conhecida como tabela RACI, trata-se de uma ferramenta visual, que define com clareza as atribuições, papéis e responsabilidades de cada colaborador nas atividades de um processo. A sigla RACI representa responsible (responsável), accountable (aprovador), consulted (consultado) e informed (informado);

CXCIX

- MEDIDAS DE SEGURANÇA: medidas destinadas a garantir sigilo, inviolabilidade, integridade, autenticidade e disponibilidade da informação classificada em qualquer grau de sigilo;

CC - METADADOS: representam "dados sobre dados", fornecendo os recursos necessários para entender os dados no decorrer do tempo, ou seja, são dados estruturados que fornecem uma descrição concisa a respeito dos dados armazenados e que permitem encontrar, gerenciar, compreender ou preservar informações a respeito dos dados ao longo do tempo. Possuem um papel importante na gestão de dados, pois, a partir deles, as informações são processadas, atualizadas e consultadas. As informações de como os dados foram criados ou derivados, do ambiente em que residem ou residiram, das alterações realizadas, dentre outras, são obtidas de metadados;

CCI - MFA: sigla de autenticação de multifatores (multifactor authentication);

CCII - MÍDIA: mecanismos em que dados podem ser armazenados. Além da forma e da tecnologia utilizada para a comunicação, inclui discos ópticos, magnéticos, compact disk (CD), fitas, papel, entre outros. Um recurso multimídia combina sons, imagens e vídeos;

CCIII - MODELO DE IMPLEMENTAÇÃO DE NUVEM PRÓPRIA: solução compartilhada de recursos computacionais configuráveis, cuja infraestrutura de nuvem pertence apenas a uma organização e suas subsidiárias;

CCIV - NECESSIDADE DE CONHECER: condição segundo a qual o conhecimento da informação classificada é indispensável para o adequado exercício de cargo, função, emprego ou atividade reservada. O termo "necessidade de conhecer" descreve a restrição de dados que sejam considerados extremamente sigilosos. Sob restrições do tipo necessidade de conhecer, mesmo que um indivíduo tenha as credenciais necessárias para acessar uma determinada informação, ele só terá acesso a essa informação caso ela seja estritamente necessária para a condução de suas atividades oficiais;

CCV - NEGAÇÃO DE SERVIÇO (DoS): bloqueio de acesso devidamente autorizado a um recurso ou a geração de atraso nas operações e funções normais de um sistema, com a resultante perda da disponibilidade aos usuários autorizados. O objetivo do ataque DoS é interromper atividades legítimas de um computador ou de um sistema. Uma forma de provocar o ataque é aproveitando-se de falhas ou de vulnerabilidades presentes na máquina vítima, ou enviar um grande número de mensagens que esgotem algum dos recursos da vítima, como CPU, memória, banda, entre outros. Para isto, é necessária uma única máquina poderosa, com bom processamento e bastante banda disponível, capaz de gerar o número de mensagens suficiente para causar a interrupção do serviço;

CCVI - NEGAÇÃO DE SERVIÇO DISTRIBUÍDA (DDoS): atividade maliciosa, coordenada e distribuída, em que um conjunto de computadores ou de dispositivos móveis é utilizado para tirar de operação um serviço, um computador ou uma rede conectada à Internet. Embora os ataques do tipo DoS sejam, em geral, perigosos para os serviços de Internet, a forma distribuída é ainda mais perigosa, justamente por se tratar de um ataque feito por várias máquinas, que podem estar espalhadas geograficamente e não terem nenhuma relação entre si, exceto o fato de estarem parcial ou totalmente sob controle do atacante. Além disso, mensagens DDoS podem ser difíceis de identificar por conseguirem facilmente se passar por mensagens de tráfego legítimo, pois enquanto é pouco natural que uma mesma máquina envie várias mensagens semelhantes a um servidor em períodos muito curtos de tempo, como no caso do ataque DoS, é perfeitamente natural que várias máquinas enviem mensagens semelhantes de requisição de serviço regularmente a um mesmo servidor, o que disfarça o ataque DDoS;

CCVII - NÍVEIS DE ACESSO: especificam quanto de cada recurso ou sistema o usuário pode utilizar;

CCVIII

- NOTIFICAÇÃO DE INCIDENTE: ato de informar eventos ou incidentes para uma Equipe de Prevenção, Tratamento e

Resposta a Incidentes Cibernéticos (ETIR) ou grupo de segurança;

CCIX - NSC: sigla de Núcleo de Segurança e Credenciamento;

CCX - NÚMERO DE IDENTIFICAÇÃO PESSOAL (PIN): número exclusivo, conhecido somente pelo usuário e pelo sistema, para a autenticação do usuário no sistema. PINs comuns são usados em caixas automáticos para realização de transações bancárias e em chips telefônicos;

CCXI - NUVEM HÍBRIDA: infraestrutura de nuvem composta por duas ou mais infraestruturas distintas (privadas, comunitárias ou públicas), que permanecem com suas próprias características, mas agrupadas por tecnologia padrão que permite interoperabilidade e portabilidade de dados, serviços e aplicações;

CCXII -NUVEM PRIVADA (OU INTERNA): infraestrutura de nuvem dedicada para uso exclusivo do órgão e de suas unidades vinculadas, ou de entidade composta por múltiplos usuários, e sua propriedade e seu gerenciamento podem ser da própria organização, de terceiros ou de ambos;

CCXIII

- NUVEM PÚBLICA (OU EXTERNA): infraestrutura de nuvem dedicada para uso aberto de qualquer organização, e sua propriedade e seu gerenciamento podem ser de organizações públicas, privadas ou de ambas;

CCXIV

- OBSOLESCÊNCIA TECNOLÓGICA: ciclo de vida do software ou de equipamento, definido pelo fabricante ou causado pelo desenvolvimento de novas tecnologias;

CCXV -ONE-TIME PASSWORD- vide senha descartável;

CCXVI

- OPERADOR: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

CCXVII

- OPT-IN- processo em que o usuário autoriza uma determinada ação por parte de uma empresa. Geralmente, a coleta de dados e o seu compartilhamento com empresas parceiras ou o recebimento de mensagens enviadas por empresas;

CCXVIII

- OPT-OUT- processo em que o usuário desautoriza uma empresa a continuar com uma determinada ação previamente permitida;

CCXIX

- ÓRGÃO DE PESQUISA: órgão ou entidade da administração pública, direta ou indireta, ou pessoa jurídica de direito privado sem fins lucrativos, legalmente constituída sob as leis brasileiras, com sede e foro no país, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico;

CCXX -OWASP: sigla de open web application security project;

CCXXI

- PaaS: sigla de plataforma como serviço (platform as a service);

CCXXII

- PADRÕES CORPORATIVOS DE SISTEMAS E DE CONTROLE: conjunto de regras e de procedimentos que compõem os normativos internos das corporações;

CCXXIII

- PERFIL DE ACESSO: conjunto de atributos de cada usuário, definidos previamente como necessários para credencial de acesso;

CCXXIV

- PERFIL INSTITUCIONAL: cadastro do órgão ou entidade da administração pública federal como usuário em redes sociais, alinhado ao planejamento estratégico e à Política de Segurança da Informação da instituição, com observância de sua correlata atribuição e competência;

CCXXV

- PIN: sigla de número de identificação pessoal (personal identification number);

CCXXVI

- PKI: sigla de infraestrutura de chave pública (public key infrastructure);

CCXXVII

- PLATAFORMA COMO SERVIÇO (PaaS): tipo de serviço de computação em nuvem, em que o provedor de serviço de nuvem oferece ao cliente a capacidade de operar códigos ou aplicativos personalizados. Um provedor PaaS determina quais sistemas operacionais ou ambientes de execução são oferecidos, não sendo permitido ao cliente modificar os sistemas operacionais (mesmo patches de segurança) ou alterar o espaço da rede virtual. A principal vantagem do PaaS é permitir ao cliente reduzir a implantação de hardware em sua própria instalação local e aproveitar um modelo de computação sob demanda (no qual o cliente pagará apenas pelos recursos utilizados);

CCXXVIII

- POLÍTICA DE SEGURANÇA DA INFORMAÇÃO (POSIN): documento aprovado pela autoridade responsável do órgão ou entidade da Administração Pública Federal, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação;

CCXXIX

- POSIN: sigla de Política de Segurança da Informação. Substituiu a sigla POSIC;

CCXXX

- PoS: sigla de Prova de Participação (proof of stake);

CCXXXI

- PoW: sigla de Prova de Trabalho (proof of work);

CCXXXII

- PREVENÇÃO DE PERDA DE DADOS (DLP): prática de detectar e prevenir vazamentos de dados, exfiltração de dados ou a destruição de dados sensíveis de uma organização. O termo DLP refere-se tanto a ações contra a perda de dados (evento no qual os dados são definitivamente perdidos pela organização), quanto a ações contra vazamentos de dados (transferência indevida de dados para fora da fronteira da organização);

CCXXXIII

- PROPRIETÁRIO DA INFORMAÇÃO: parte interessada do órgão ou entidade da administração pública federal, direta e indireta, ou indivíduo legalmente instituído por sua posição ou cargo, que é responsável primário pela viabilidade e sobrevivência da informação;

CCXXXIV

- PROTOCOLO: conjunto de parâmetros que definem a forma e como a transferência de informação deve ser efetuada;

CCXXXV

- PROVA DE PARTICIPAÇÃO: vide proof of stake;

CCXXXVI

- PROVA DE TRABALHO: vide proof of work;

CCXXXVII

- PROVEDOR DE SERVIÇOS DE NUVEM: ente, público ou privado, que fornece uma plataforma, infraestrutura, aplicativo, serviços de armazenamento ou ambientes de tecnologia da informação baseados em nuvem;

CCXXXVIII

- PROVISIONAMENTO: processo de definição da infraestrutura de tecnologia da informação. Também se refere às etapas necessárias para gerenciar o acesso aos dados e recursos, e para disponibilizá-los aos usuários e sistemas. O provisionamento e a configuração são diferentes, mas ambos são etapas do processo de implantação. A configuração é feita após o provisionamento;

CCXXXIX

- PROVISIONAMENTO DE REDES: processo de definição de uma rede, para que usuários, servidores, containers, dispositivos de Internet of things (IoT), entre outros, possam acessá-la;

CCXL -PROVISIONAMENTO DE SERVIÇOS: processo de definição de um serviço e do gerenciamento dos dados relacionados, sendo comum em prestação de serviços de computação em nuvem;

CCXLI

- PROVISIONAMENTO DE SERVIDORES: processo de definição de todas as operações necessárias para criar uma nova máquina e colocá-la em funcionamento, incluindo a definição do estado desejado do sistema;

CCXLII

- PROVISIONAMENTO DE USUÁRIOS: processo de gestão das identidades o qual monitora privilégios de autorização e direitos de acesso. Costuma ser realizado pela área de tecnologia da informação e de recursos humanos;

CCXLIII

- PSN: sigla de provedor de serviço de nuvem;

CCXLIV

- PÚBLICO ALVO DA ETIR: conjunto de pessoas, setores, órgãos ou entidades atendidas por uma Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR). Também chamado de comunidade da ETIR;

CCXLV

- QUEBRA DE SEGURANÇA: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação;

CCXLVI

- RANSOMWARE: tipo de malware, que, por meio de criptografia, impede o acesso a dados computacionais. Para recuperar o acesso, exige-se pagamento de um valor de resgate. Caso o pagamento do resgate não seja realizado, pode-se perder definitivamente o acesso aos dados sequestrados;

CCXLVII

- RECOMENDAÇÃO DE ETIR: informação, com ações de curto prazo, enviadas aos usuários, com orientações sobre como lidar com os impactos resultantes de um incidente cibernético e as atividades que devem ser realizadas para proteger ou recuperar os sistemas que foram afetados;

CCXLVIII

- RECURSO CRIPTOGRÁFICO: sistema, programa, processo, equipamento isolado ou em rede, que utiliza algoritmo simétrico ou assimétrico para realizar cifração ou decifração;

CCXLIX

- REDE DE COMPUTADORES: conjunto de computadores, interligados por ativos de rede, capazes de trocar informações e de compartilhar recursos, por meio de um sistema de comunicação;

CCL - REDE DE TELECOMUNICAÇÕES: conjunto operacional contínuo de enlaces e equipamentos, incluindo funções de transmissão, comutação ou quaisquer outras indispensáveis à operação de serviço de telecomunicações;

CCLI - REDE PRIVADA VIRTUAL (VPN): refere-se à 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;

CCLII -REDES SOCIAIS: estruturas sociais digitais, compostas por pessoas ou organizações, conectadas por um ou vários tipos de relações, que partilham valores e objetivos comuns;

CCLIII

- REDUZIR RISCO: 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;

CCLIV

- RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS: documentação do controlador, no qual são descritos os processos de tratamento de dados pessoais, que identificam os riscos às liberdades civis e aos direitos fundamentais, as medidas de salvaguarda, bem como mecanismos de mitigação dos riscos;

CCLV -REMETENTES CONFIÁVEIS: vide whitelist;

CCLVI

- REQUISITOS DE SEGURANÇA DE SOFTWARE: conjunto de necessidades de segurança que um software deve atender. Essas necessidades são determinadas pela política de segurança da informação da organização, compreendendo aspectos funcionais e não funcionais. Os aspectos funcionais descrevem comportamentos que viabilizam a criação ou a manutenção da segurança e, geralmente, podem ser testados diretamente. São exemplos de requisitos funcionais o controle de acesso, baseado em papéis de usuários (administradores, usuários comuns, entre outros) e a autenticação com o uso de credenciais (usuário e senha, certificados digitais, entre outros). Os aspectos não funcionais descrevem procedimentos necessários para que o software permaneça executando suas funções adequadamente, mesmo quando sob uso indevido. São exemplos de requisitos não funcionais a validação das entradas de dados e o registro de logs de auditoria com informações suficientes para análise forense;

CCLVII

- Resiliência: capacidade de uma organização ou de uma infraestrutura de resistir aos efeitos de um incidente, ataque ou desastre e retornar à normalidade das operações;

CCLVIII

- RESUMO CRIPTOGRÁFICO: resultado da ação de algoritmos que fazem o mapeamento de bits de tamanho arbitrário para uma sequência de bits de tamanho fixo menor, conhecido como resultado hash. Dessa forma, torna-se difícil encontrar duas mensagens que produzam o mesmo resultado hash (resistência à colisão), e também realizar o processo reverso (utilizando-se apenas o hash não é possível recuperar a mensagem que o gerou);

CCLIX

- RETER RISCO: tipo de tratamento de risco, em que a alta administração decide realizar a atividade, assumindo as responsabilidades, caso ocorra o risco identificado;

CCLX -RISCO: no sentido amplo, trata-se da possibilidade de ocorrência de um evento que pode impactar o cumprimento dos objetivos. Pode ser mensurado em termos de impacto e de probabilidade;

CCLXI

- RISCOS DE SEGURANÇA DA INFORMAÇÃO: 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;

CCLXII

- SEGURANÇA DA INFORMAÇÃO: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;

CCLXIII

- ROAMING: capacidade de enviar e de receber dados em telefonia móvel, por intermédio de redes móveis, em uma zona onde o serviço é provido por outra operadora;

CCLXIV

- ROOTKIT- conjunto de programas e de técnicas que permitem esconder e assegurar a presença de um invasor ou de outro código malicioso em um computador comprometido. É importante ressaltar que o nome rootkit não indica que as ferramentas que o compõem são usadas para obter acesso privilegiado em um computador (root ou administrator), mas, sim, para manter o acesso privilegiado em um computador previamente comprometido;

CCLXV

- RoT - sigla de root of trust;

CCLXVI

- SaaS - sigla de software como Serviço (software-as-a-service);

CCLXVII

- SANITIZAÇÃO DE DADOS: eliminação efetiva de informação armazenada em qualquer meio eletrônico, garantindo que os dados não possam ser reconstruídos ou recuperados;

CCLXVIII

- SCREENLOGGER- tipo específico de spyware. Programa similar ao keylogger, capaz de armazenar a posição do cursor e a tela apresentada no monitor, nos momentos em que *omouse* é clicado, ou a região que circunda a posição onde *omouse* é clicado. É bastante utilizado por atacantes para capturar as teclas digitadas pelos usuários em teclados virtuais, disponíveis principalmente em sites de Internet banking;

CCLXIX

- SDK: sigla de kit de desenvolvimento de software (software development kit);

CCLXX

- SECURITY BY DESIGN- significa pensar em segurança desde o escopo de desenvolvimento de um novo software, prevendo toda possibilidade de riscos aos quais aquela aplicação pode estar sujeita. É um conceito de grande importância para a indústria de segurança da informação;

CCLXXI

- SEGURANÇA CIBERNÉTICA: ações voltadas para a segurança de operações, visando garantir que os sistemas de informação sejam capazes de resistir a eventos no espaço cibernético, capazes de comprometer a disponibilidade, a integridade, a confidencialidade e a autenticidade dos dados armazenados, processados ou transmitidos e dos serviços que esses sistemas ofereçam ou tornem acessíveis;

CCLXXII

- SEGURANÇA CORPORATIVA - vide segurança orgânica;

CCLXXIII

- SEGURANÇA DA INFORMAÇÃO: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;

CCLXXIV

- SEGURANÇA ORGÂNICA: conjunto de medidas passivas, com o objetivo de prevenir e, até mesmo, obstruir as ações que visem o comprometimento ou a quebra de segurança de uma organização. Inclui os processos relacionados às áreas: de pessoal, de documentação, das comunicações, da tecnologia da informação, dos materiais e das instalações de uma organização, dentre outros;

CCLXXV

- SENHA DESCARTÁVEL (one-time password): senha que é válida somente para uma sessão de login ou transação, em um sistema de computadores ou outros dispositivos digitais;

CCLXXVI

- SENSIBILIZAÇÃO: atividade que tem por objetivo atingir uma predisposição dos participantes para uma mudança de atitude sobre a SI, de tal forma que eles possam perceber em sua rotina, pessoal e profissional, ações que devem ser corrigidas. É uma etapa inicial da educação em segurança da informação;

CCLXXVII

- SERVIÇOS (CONCEITO GERAL): um meio de fornecer valor a clientes, facilitando a obtenção de resultados que eles desejam, sem que tenham que arcar com a propriedade de determinados custos e riscos;

CCLXXVIII

- SERVIÇO DA ETIR: conjunto de procedimentos, estruturados em um processo bem definido, oferecido à comunidade da Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos;

CCLXXIX

- SERVIÇOS DE REDE DE TELECOMUNICAÇÕES: provimento de serviços de telecomunicações, de tecnologia da informação e de infraestrutura para redes de comunicação de dados;

CCLXXX

- SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO: provimento de serviços de desenvolvimento, de implantação, de manutenção, de armazenamento e de recuperação de dados e de operação de sistemas de informação, projeto de infraestrutura de redes de comunicação de dados, modelagem de processos e assessoramento técnico necessários à gestão

da informação;

CCLXXXI

- SI: sigla de segurança da informação;

CCLXXXII

- SINGLE SIGN-ON(SSO): é uma solução tecnológica que permite que diversos aplicativos com senhas de acesso diferentes possam ser acessados de forma transparente e segura pela utilização de uma única senha principal ou meio de identificação pessoal (como a biometria ou um personal identification number- PIN, por exemplo). Ou seja, com o SSO, o usuário digita apenas uma senha quando faz o primeiro acesso e depois vai abrindo os demais aplicativos sem necessidade de digitar a senha específica do aplicativo;

CCLXXXIII

- SISTEMA DE ACESSO: conjunto de ferramentas que se destina a controlar e a dar a uma pessoa permissão de acesso a um recurso;

CCLXXXIV

- SISTEMA BIOMÉTRICO: conjunto de ferramentas que se utiliza das características de uma pessoa, levando em consideração fatores comportamentais e fisiológicos, a fim de identificá-la de forma unívoca;

CCLXXXV

- SISTEMA DE DETECÇÃO DE INTRUSÃO (IDS) - refere-se a um mecanismo que, sigilosamente, ouve o tráfego na rede para detectar atividades anormais ou suspeitas e, deste modo, reduz os riscos de intrusão. Existem duas famílias distintas de IDS: os N-IDS (network based intrusion detection system ou sistema de detecção de intrusões de rede), que garantem a segurança dentro da rede e os H-IDS (host based intrusion detection system ou sistema de detecção de intrusões no host), que asseguram a segurança no host;

CCLXXXVI

- SISTEMA DE INFORMAÇÃO: conjunto de elementos materiais ou intelectuais, colocados à disposição dos usuários, em forma de serviços ou bens, que possibilitam a agregação dos recursos de tecnologia, informação e comunicações de forma integrada;

CCLXXXVII

- SISTEMA DE PROTEÇÃO FÍSICA: sistema composto por pessoas, equipamentos e procedimentos, para a proteção de ativos contra danos, roubo, sabotagem e outros prejuízos causados por ação humana não autorizada, conforme gestão da segurança física e ambiental;

CCLXXXVIII

- SISTEMA ESTRUTURANTE: sistema com suporte de tecnologia da informação, fundamental e imprescindível para o planejamento, coordenação, execução, descentralização, delegação de competência, controle ou auditoria das ações de Estado, além de outras atividades auxiliares, desde que comum a dois ou mais órgãos ou entidades da administração pública federal, direta ou indireta, e que necessitem de coordenação central;

CCLXXXIX

- SOC 2: desenvolvido pelo American Institute of CPAs (AICPA), define critérios para gerenciamento de dados dos usuários, baseados nos cinco princípios de confiança do serviço - disponibilidade, integridade, confidencialidade, segurança e privacidade - sendo considerado um requisito mínimo a ser atendido pelo provedor de serviço de nuvem. O relatório tipo I informa se o projeto dos sistemas do provedor de serviço de nuvem é adequado para atender os princípios de confiança relevantes. O relatório tipo II detalha a efetividade operacional dos sistemas do provedor de serviço de nuvem;

CCXC -SOFTWARE COMO SERVIÇO (SaaS): tipo de serviço de computação em nuvem em que o provedor de serviço de nuvem oferece ao cliente a capacidade de usar um aplicativo fornecido. São exemplos de SaaS serviços de e-mail on-line e sistemas de edição de documentos on-line. Um usuário de uma solução SaaS só é capaz de usar o aplicativo oferecido e de fazer pequenos ajustes de configuração. O provedor SaaS é responsável pela manutenção da aplicação;

CCXCI

- SOLUÇÃO DE IoT (Internet of things): conjunto de dispositivos, softwares ou serviços desenvolvidos para operar no ambiente de Internet das coisas;

CCXCII

- SOLUÇÃO END-TO-END: solução que busca controlar um processo do seu início até o seu término;

CCXCIII

- SPOOFING ato de falsificar a identidade da fonte de uma comunicação ou interação. É possível falsificar endereço IP, ARP, DNS (conhecido com envenenamento do cache de DNS), endereço MAC, site da web, endereço de e-mail, id de chamador, entre outros;

CCXCIV

- SPYWARE- tipo de malware. Programa projetado para monitorar as atividades de um sistema e enviar as informações coletadas para terceiros. Keylogger ,screenlogger e adware são alguns tipos específicos de spyware;

CCXCV

- SSL: sigla de secure sockets layer;

CCXCVI

- SSO: sigla de single sign-on;

CCXCVII

- STAR: sigla de security trust and assurance registry;

CCXCVIII

- TCG: sigla de trusted computing group;

CCXCIX

- TCMS: sigla de termo de compromisso de manutenção de sigilo;

CCC - TCP: sigla de transmission control protocol;

CCCI - TCP/IP: trata-se de um conjunto de protocolos. Esse grupo é dividido em quatro camadas: aplicação, transporte, rede e interface. Cada uma delas é responsável pela execução de tarefas distintas. Essa divisão em camadas é uma forma de garantir a integridade dos dados que trafegam pela rede;

CCCI -TECNOLOGIA DA INFORMAÇÃO: ativo estratégico que apoia processos de negócios institucionais, mediante a conjugação de recursos, processos e técnicas, utilizados para obter, processar, armazenar, disseminar e fazer uso de informações;

CCCI

- TELECOMUNICAÇÕES: transmissão, emissão ou recepção, por fio, radioeletricidade, meios ópticos ou qualquer outro processo eletromagnético, de símbolos, caracteres, sinais, escritos, imagens, sons ou informações de qualquer natureza;

CCCIV

- TEMPO OBJETIVO DE RECUPERAÇÃO: tempo pré-definido no qual uma atividade deverá estar disponível após uma interrupção ou incidente;

CCCV -TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO: termo utilizado para garantir o sigilo de uma informação classificada em grau de sigilo em caráter excepcional, mediante assinatura de pessoa natural não credenciada ou não autorizada por legislação;

CCCVI

- TERMO DE RESPONSABILIDADE: termo assinado pelo usuário, concordando em contribuir com a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações a que tiver acesso, bem como assumir responsabilidades decorrentes de tal acesso;

CCCVII

- TERRORISMO CIBERNÉTICO: crime cibernético perpetrado por razões políticas, religiosas ou ideológicas, contra qualquer elemento da infraestrutura cibernética com os objetivos de: provocar perturbação severa ou de longa duração na vida pública; causar danos severos à atividade econômica, com a intenção de intimidar a população; forçar as autoridades públicas ou uma organização a executar, tolerar, revogar ou a omitir um ato; ou abalar ou destruir as bases políticas, constitucionais, econômicas ou sociais de um Estado, organização ou empresa. É principalmente realizado por atos de sabotagem cibernética, organizados e gerenciados por indivíduos, grupos político-fundamentalistas, ou serviços de inteligência estrangeiros;

CCCVIII

- TESTE DE INTRUSÃO: vide teste de penetração;

CCCIX

- TESTE DE PENETRAÇÃO (PENTEST) - também chamado de teste de intrusão, é fundamental para a análise de vulnerabilidades e consiste em testar todos os sistemas em busca de, além das já verificadas na fase anterior, vulnerabilidades conhecidas e disponibilizadas por especialistas ou pelas instituições detentoras dos softwares que estão sendo utilizados pela instituição;

CCCX -TEMPO OBJETIVO DE RECUPERAÇÃO: tempo pré-definido no qual uma atividade deverá estar disponível após uma interrupção ou incidente;

CCCXI

- TIC: sigla de tecnologia da informação e comunicação;

CCCXII

- TITULAR DO DADO: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

CCCXIII

- TOKEN: algo que o usuário possui e controla (tipicamente uma chave, senha e/ou módulo criptográfico) e que é utilizado para autenticar a identidade do requerente e/ou a requisição em si;

CCCXIV

- TLS: sigla de transport layer security;

CCCXV

- TPM: sigla de trusted platform module;

CCCXVI

- 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;

CCCXVII

- TRANSMISSION CONTROL PROTOCOL(TCP) - protocolo da camada de transporte do modelo TCP/IP, que permite gerenciar os dados originados ou destinados ao protocolo IP. Trata-se de um protocolo orientado à conexão, o qual permite a comunicação entre duas máquinas e o controle do estado da transmissão;

CCCXVIII

- TRANFERÊNCIA INTERNACIONAL DE DADOS: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro;

CCCXIX

- TRATAMENTO: toda operação realizada com dados pessoais, como as que se referem à coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

CCCXX

- 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;

CCCXXI

- TRATAMENTO DE INCIDENTES DE SEGURANÇA EM REDES COMPUTACIONAIS: serviço que consiste em receber, filtrar, classificar e responder às solicitações e aos alertas e realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências;

CCCXXII

- TRATAMENTO DA INFORMAÇÃO CLASSIFICADA: conjunto de ações referentes à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle de informação classificada, independente do meio, suporte ou formato;

CCCXXIII

- TRATAMENTO DE ARTEFATOS MALICIOSOS: serviço que prevê o recebimento de informações ou cópia do artefato malicioso que foi utilizado no ataque, ou de qualquer outra atividade desautorizada ou maliciosa. Uma vez recebido o artefato, este deve ser analisado, ou seja, deve-se buscar a natureza do artefato, seu mecanismo, versão e objetivo, para que seja desenvolvida, ou sugerida, uma estratégia de detecção, remoção e defesa contra esses artefatos;

CCCXXIV

- TRATAMENTO DE INCIDENTES CIBERNÉTICOS: consiste nas ações e procedimentos tomados imediatamente após a identificação do incidente, visando garantir a continuidade de operações, preservar evidências e emitir as notificações necessárias;

CCCXXV

- TRATAMENTO DE INCIDENTES DE SEGURANÇA EM REDES COMPUTACIONAIS: vide tratamento de incidentes cibernéticos;

CCCXXVI

- TRATAMENTO DE RISCOS: processo de implementação de ações de Segurança da Informação para evitar, reduzir,

reter ou transferir um risco;

CCCXXVII

- **TRATAMENTO DE VULNERABILIDADES:** serviço que prevê o recebimento de informações sobre vulnerabilidades, em hardware ou software, objetivando analisar sua natureza, mecanismo e suas consequências, e desenvolver estratégias para detecção e correção dessas vulnerabilidades;

CCCXXVIII

- **TRILHA DE AUDITORIA:** registro ou conjunto de registros gravados em arquivos de *log* ou outro tipo de documento ou mídia, que possam indicar, de forma cronológica e inequívoca, o autor e a ação realizada em determinada operação, procedimento ou evento;

CCCXXIX

- **TROJAN-** vide cavalo de Tróia;

CCCXXX

- **TRUSTED COMPUTING GROUP(TCG)** - organização sem fins lucrativos, formada para desenvolver, definir e promover padrões abertos e neutros do setor global, apoiando uma raiz de confiança baseada em hardware, para plataformas de computação confiáveis interoperáveis;

CCCXXXI

- **TVM:** sigla de máquina virtual confiável (trusted virtual machine);

CCCXXXII

- **UID** - sigla de identificador único (unique identifier) em sistemas de computadores. Baseados nessa definição, também temos o GUID (identificador global único ou globalunique identifier) e UUID (identificador universal único ou universal unique identifier). Ressalta-se que, no sistema UNIX, UID significa identificador do usuário (user identifier);

CCCXXXIII

- **USO COMPARTILHADO DE DADOS:** comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais, por órgãos e entidades públicos, no cumprimento de suas competências legais, ou entre esses entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados;

CCCXXXIV

- **USUÁRIO DE INFORMAÇÃO:** 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 administração pública federal, formalizada por meio da assinatura de Termo de Responsabilidade;

CCCXXXV

- **USUÁRIO VISITANTE COM DISPOSITIVO MÓVEL:** agentes públicos ou não, que utilizem dispositivos móveis, de sua propriedade ou do órgão ou entidade a que pertencem, dentro dos ambientes físicos de órgãos ou entidades da administração pública federal dos quais não fazem parte;

CCCXXXVI

- **URL** - sigla de uniform resource locator;

CCCXXXVII

- **USUÁRIO:** pessoa física, seja servidor ou equiparado, empregado ou prestador de serviços, habilitada pela administração para acessar os ativos de informação do ICMBio, formalizada por meio da assinatura do Termo de Responsabilidade;

CCCXXXVIII

- **VAZAMENTO DE DADOS:** transmissão não autorizada de dados de dentro de uma organização para um destino ou recipiente externo. O termo pode ser usado para descrever dados que são transferidos eletronicamente ou fisicamente. Pode ocorrer de forma acidental ou intencional (pela ação de agentes internos, pela ação de agentes externos ou pelo uso de software malicioso). É conhecido também como roubo de dados low-and-slow (rasteiro-e-lento), pois a exfiltração de dados para fora da organização é feita usando técnicas do tipo low-and-slow, a fim de evitar detecção;

CCCXXXIX

- **VENDOR LOCK-IN-** também conhecido como lock-in proprietário ou lock-into cliente, usado para designar a situação em que há um alto custo de troca para o consumidor em um ou mais serviços. Isso faz com que um cliente fique dependente de um fornecedor de produtos e serviços, pois a mudança de fornecedor implica em substanciais custos de mudança;

CCCXL

- **VERIFICAÇÃO DE CONFORMIDADE EM SEGURANÇA DA INFORMAÇÃO:** procedimentos que fazem parte da avaliação de conformidade, que visam identificar o cumprimento das legislações, normas e procedimentos relacionados à segurança da informação da organização;

CCCXLI

- **VÍRUS:** seção oculta e autorreplicante de um software de computador, geralmente utilizando lógica maliciosa, que se propaga pela infecção (inserindo uma cópia sua e tornando-se parte) de outro programa. Não é auto executável, ou seja, necessita que o seu programa hospedeiro seja executado para se tornar ativo;

CCCXLII

- **VIRTUAL MACHINE(VM):** vide máquina virtual;

CCCXLIII

- **VIRTUAL MACHINE IMAGE(VMI):** vide imagem de máquina virtual;

CCCXLIV

- **VISHING:** uma forma de ataque de phishing que ocorre em VoIP, sendo que as vítimas não precisam estar utilizando VoIP. O atacante usa sistemas VoIP para efetuar ligações para qualquer número de telefone, sem cobrança de taxas, e, geralmente, falsifica (spoofing) sua identificação de chamada, a fim de levar a vítima a acreditar que está recebendo um telefonema de uma fonte legítima ou confiável (como um banco, uma loja de varejo, entre outros);

CCCXLV

- **VM:** sigla de máquina virtual (virtual machine);

CCCXLVI

- **VMI:-** sigla de imagem de máquina virtual (virtual machine image);

CCCXLVII

- **VPN:** sigla de rede privada virtual (virtual private network);

CCCXLVIII

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

CCCXLIX

- lista de itens aos quais é garantido o acesso a certos recursos, sistemas ou protocolos. Utilizar uma whitelist para controle de acesso significa negar o acesso a todas as entidades, exceto àquelas incluídas na whitelist;

CCCL -WORM: programa capaz de se propagar automaticamente pelas redes, enviando cópias de si mesmo de computador para computador. Diferente do vírus, o worm não embute cópias de si mesmo em outros programas ou arquivos, e não necessita ser explicitamente executado para se propagar. Sua propagação se dá por meio da exploração de vulnerabilidades existentes ou de falhas na configuração de programas instalados em computadores;

CCCLI

- XSS: sigla decross-site scripting.

CAPÍTULO III DOS PRINCÍPIOS

Art. 6º. Para efeitos de aplicação desta política, são considerados princípios da segurança da informação:

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

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

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

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

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

VI - simplicidade: a complexidade aumenta a chance de erros, portanto todos os controles de segurança deverão ser simples e objetivos;

VII - 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;

VIII - privilégio mínimo: usuários devem ter acesso apenas aos recursos de tecnologia da informação necessários para realizar as tarefas que lhe foram designadas;

IX - educação como alicerce fundamental para o fomento da cultura em segurança da informação;

XI - auditabilidade: todos os eventos significantes de usuários e processos devem ser rastreáveis até o evento inicial por meio de registro consistente e detalhado, orientando à gestão de riscos e à gestão da segurança da informação;

XII - resiliência: os controles de segurança deverão ser projetados para que possam resistir e se recuperarem dos efeitos de um desastre;

XIII - defesa em profundidade: os controles de segurança devem ser concebidos em múltiplas camadas de modo a prover redundância para que, no caso de falha, outro controle possa ser aplicado, prevenindo e tratando incidentes de segurança da informação;

XIV - dever dos órgãos, das entidades e dos agentes públicos de garantir o sigilo das informações imprescindíveis à segurança das pessoas;

XV - respeito e promoção dos direitos humanos e das garantias fundamentais, em especial a liberdade de expressão, a proteção de dados pessoais, a proteção da privacidade e acesso à informação;

XV - articulação entre as ações de segurança cibernética, e de proteção de dados e ativos da informação;

XVI - necessidade de conhecer : para o acesso à informação sigilosa, nos termos da legislação.

CAPÍTULO IV DAS DIRETRIZES GERAIS

Art. 7º. As diretrizes de segurança da informação estabelecidas nesta POSIN aplicam-se aos dados armazenados , acessados , produzidos e transmitidos no âmbito do ICMBio, e que devem ser seguidas pelos agentes públicos, incumbindo a todos a responsabilidade e o comprometimento com sua aplicação.

Parágrafo único. Seja qual for a forma ou o meio pelo qual o dado seja apresentado ou compartilhado, será sempre protegido adequadamente, de acordo com esta política.

Art. 8º. Os recursos de tecnologia da informação e comunicação disponibilizados pelo ICMBio serão utilizados estritamente para apoiar as atividades laborais dos servidores e colaboradores deste instituto, com alinhamento ao Planejamento Estratégico Integrado do Ministério do Meio Ambiente e suas vinculadas.

I - os recursos de tecnologia da informação disponíveis para o usuário deverão ser utilizados em atividades relacionadas às suas funções institucionais;

II - é vedado a qualquer agente público do ICMBio o uso dos recursos de tecnologia da informação 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, a autenticidade ou a disponibilidade das informações.

SEÇÃO I DA GESTÃO DA SEGURANÇA DA INFORMAÇÃO

Art. 9º. A Gestão da Segurança da Informação não se limita à tecnologia da informação, compreendendo as ações e métodos que visam à integração das atividades de gestão de riscos, de gestão de continuidade do negócio, de tratamento de incidentes, de tratamento da informação, da conformidade, do credenciamento, da segurança cibernética, da segurança orgânica e aos processos

institucionais estratégicos, táticos e operacionais do Instituto.

Art. 10. As informações geradas pelos usuários, no exercício de suas atividades no ICMBio, é considerada um bem de propriedade do Instituto. As informações custodiadas, em decorrência das competências do Instituto, devem ser protegidas de acordo com a sua classificação e conforme as diretrizes descritas nesta Política e demais regulamentações em vigor.

Art. 11. A utilização dos recursos de tecnologia da informação será monitorada, com a finalidade de detectar e corrigir divergências entre as normas que integram a Política de Segurança da Informação as práticas e os procedimentos adotados, fornecendo evidências nos casos de incidentes de segurança ou registros de incompatibilidades para ajustes das práticas e orientações das equipes.

Parágrafo único. Poderão ser realizadas auditorias, a serem programadas a pedido da seção de Auditoria Interna do ICMBio, com o intuito de apurar eventos que deponham contra a segurança e as boas práticas no uso dos recursos de tecnologia da informação, cujos relatórios serão encaminhados ao Comitê de Segurança da Informação.

SEÇÃO II DA PROPRIEDADE DA INFORMAÇÃO

Art. 12. A propriedade da informação será regida pelas seguintes diretrizes:

I - toda informação criada ou custodiada que for manuseada, armazenada, transportada ou descartada por usuários que tenham acesso às informações do ICMBio, no exercício de suas atividades, é de propriedade desta entidade e será protegida segundo estas diretrizes e regulamentações em vigor, conforme a classificação das informações, sem prejuízo da autoria, conforme definido em lei;

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

III - as normas e procedimentos que complementam esta Política deverão abordar, mas não limitados a estes, os seguintes aspectos: segurança física; gestão de mudanças; privacidade; criptografia; acesso à rede; gestão de senhas e contas de usuário; dispositivos móveis; gestão de incidentes; plano de continuidade de negócios; proteção à propriedade intelectual; treinamento e sensibilização para segurança;

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

SEÇÃO III DA CLASSIFICAÇÃO E TRATAMENTO DA INFORMAÇÃO

Art. 13. A classificação e o tratamento da informação observarão os seguintes requisitos e critérios:

I - o valor, os requisitos legais, a sensibilidade e a criticidade da informação para o ICMBio, por conter informações sensíveis, deverão ser classificados na forma da lei e divulgados aqueles cujas atribuições requerem conhecimento das mesmas;

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

Art. 14. As informações criadas, manuseadas, armazenadas, transportadas ou descartadas no ICMBio que se enquadrem nas hipóteses previstas na Lei nº 12.527, de 18 de novembro de 2011, serão classificadas com o grau de sigilo correspondente.

Art. 15. O ICMBio utilizará 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.

Art. 16. As informações sob gestão do ICMBio terão segurança de maneira a serem adequadamente protegidas quanto ao acesso e ao uso, sendo que para as consideradas de alta criticidade, serão necessárias medidas especiais de tratamento com o objetivo de limitar a exploração às informações exclusivas do Instituto.

Parágrafo único. Os dispositivos de proteção deverão ser implementados de forma proporcional ao grau de confidencialidade e de criticidade da informação capazes de assegurar a sua autenticidade, integridade e disponibilidade, independentemente do suporte em que reside ou da forma pela qual seja veiculada.

SEÇÃO IV DA PROTEÇÃO DE DADOS PESSOAIS

Art. 17. O uso compartilhado de dados pessoais e/ou sensíveis do titular, de crianças e adolescentes deverão atender a finalidades específicas de execução do ICMBio e ser processado de forma legal, justa e transparente em relação aos seus titulares, respeitados os princípios e requisitos de proteção e tratamento de dados pessoais elencados na Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709, de 14 de agosto de 2018.

I - As operações de tratamento de dados pessoais deverão ser comunicadas ao Encarregado de Tratamento de Dados Pessoais, nos termos do art. 39 da Lei 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais);

II - A política de tratamento de dados pessoais deverá ser divulgada no site do ICMBio para a divulgação das hipóteses em que, no exercício de suas competências, o Instituto efetua o tratamento de dados pessoais, além de apresentar a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades.

SEÇÃO V DO TRATAMENTO DE INCIDENTES DE REDE

Art. 18. A área de Tecnologia da Informação manterá Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos - ETIR, com a responsabilidade de receber, analisar e responder notificações e atividades relacionadas a incidentes de segurança em rede de computadores.

SEÇÃO VI DA GESTÃO DE RISCOS

Art. 19. O Processo de Gestão de Riscos em Segurança da Informação será implementado considerando, prioritariamente, os objetivos estratégicos, os processos, os requisitos legais e a estrutura do ICMBio e estará alinhado a Política de Gestão de Riscos e Integridade do ICMBio e observando diretrizes e normas específicas no âmbito da Administração Pública Federal, de modo a fomentar sua melhoria contínua.

SEÇÃO VII DA GESTÃO DE CONTINUIDADE DO NEGÓCIO

Art. 20. As unidades descentralizadas do ICMBio, com apoio das áreas técnicas da DIPLAN, devem manter processo de gestão de continuidade das atividades e dos serviços, visando não permitir que estes sejam interrompidos e assegurar a sua retomada em tempo hábil, quando for o caso.

Art. 21. Aprovado pelo Comitê de Segurança da Informação, a área de Tecnologia da Informação do ICMBio deverá manter o Plano de Contingências, formalizado de acordo com o grau de probabilidade de ocorrência do evento ou sinistro, estabelecendo o conjunto de estratégias e procedimentos que devem ser adotados em situações que comprometam o andamento normal dos processos e a consequente prestação dos serviços.

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

SEÇÃO VIII DO MONITORAMENTO, AUDITORIA E CONFORMIDADE

Art. 22. O monitoramento, a auditoria e a conformidade observarão o seguinte:

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

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

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

SEÇÃO IX DOS CONTROLES DE ACESSOS E USO DE SENHAS

Art. 23. O controle de acesso a dados inclui o credenciamento de usuário e a criação de senha segura, com fator de múltipla autenticação, ou outro método de acesso seguro a ativos de informação usados pela Administração.

Parágrafo único. O controle de acesso e o uso de senhas observará:

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

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

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

IV - os usuários serão orientados, de forma regular e periódica, a seguir as boas práticas de segurança da informação na seleção e no uso de senhas;

V - é responsabilidade do Gestor ou do Chefe da área requisitante que autorizou o cadastro do usuário, a comunicação à área de Tecnologia da Informação quando do desligamento do usuário para que seja retirado o seu acesso aos recursos disponibilizados;

VI - constitui falta gravíssima, sujeita às sanções administrativas cabíveis, o usuário que realize, de forma intencional, o compartilhamento de senha ou meio de acesso a perfil com privilégio de administrador, mantenedor ou desenvolvedor, bem como a serviço digital essencial, a sistema estruturante, a informação classificada ou a dado pessoal.

Art. 24. O acesso físico às instalações da rede de computadores do ICMBio, compostas pelo Datacenter, pelas salas do edifício Sede que possuem os switches de rede e pelos ambientes onde estão localizados os equipamentos de rede (switches, roteadores e servidores de redes) em todas as Unidades Descentralizadas, possui as seguintes diretrizes:

I - a área de tecnologia da informação deverá garantir, por meio dos contratos de serviços de TI, a atuação presencial ou remota de profissionais especializados na área de segurança da informação, devendo garantir a atuação presencial de profissional especializado em TI durante o horário comercial, com capacidade de identificar os equipamentos em operação, alertas de falhas mecânicas dos equipamentos e dos dispositivos de energia elétrica e de climatização, além de ser o responsável pelo acompanhamento e registro de todos os acessos físicos de pessoal ao datacenter;

II - sempre que houver acesso de terceiros às dependências do Datacenter do ICMBio, este acesso deverá ser realizado com acompanhamento de um servidor da área de tecnologia da informação da ou da empresa contratada para a sustentação do Datacenter;

III - o acesso às salas do edifício Sede que possuem os switches de rede deverá ser realizado com acompanhamento de um servidor da área de tecnologia da informação ou da empresa contratada para a sustentação da infraestrutura do Instituto. Já para os ambientes onde estão localizados os equipamentos de rede (switches, roteadores e servidores de redes) em todas as Unidades Descentralizadas, deverá ser realizado com acompanhamento do chefe da Unidade de Conservação ou colaborador por ele indicado;

IV - o acesso físico de terceiros ao Datacenter do ICMBio deverá ocorrer com agendamento prévio e acompanhado por servidores da área de tecnologia da informação do ICMBio;

V - o acesso físico ao Datacenter do ICMBio durante feriados e finais de semana somente será permitido aos servidores da área de Tecnologia da Informação e da empresa contratada para sustentação do Datacenter para suporte emergencial ou manutenções programadas com autorização da autoridade responsável pela área de Tecnologia da Informação do ICMBio;

VI - todo o acesso remoto ao Datacenter será mediante esquema de autenticação e deverá ser identificado (usuário, data e hora) com registros de logs de acesso;

VII - todo o acesso físico ao Datacenter deverá ser registrado (usuário, data e hora) em software de autenticação ou na falta deste, através de formulário próprio;

VIII - a entrada ou retirada de qualquer equipamento do Datacenter se dará com o preenchimento da solicitação de liberação e autorização formal deste instrumento pela autoridade competente da área de Tecnologia da Informação, de acordo com os termos do procedimento e controle de transferência patrimonial vigentes;

IX - quando possível, as portas de acesso ao Datacenter devem permanecer fechadas, com mecanismos de autenticação individual;

X - o acesso às dependências do Datacenter com quaisquer equipamentos de gravação, fotografia, vídeo, som ou outro tipo de equipamento similar, poderá ser feito somente com autorização formal, do responsável pela área de tecnologia da informação ou do Gestor de Segurança da Informação do ICMBio;

XI - o acesso ao Datacenter sem identificação prévia só poderá ocorrer em situações de emergência, quando a segurança física do Datacenter estiver comprometida, como por incêndio, inundação, abalo da estrutura predial.

SEÇÃO X DO USO DE E-MAIL

Art. 25. O correio eletrônico é um meio de comunicação corporativa, volátil, do ICMBio.

I - as regras de acesso e utilização de e-mail institucional devem atender às orientações desta POSIN e seus anexos, norma interna e demais diretrizes do Governo;

II - o serviço de correio tem como finalidade o envio e o recebimento eletrônico de mensagens e documentos relacionados com as funções institucionais do ICMBIO;

III - a área de Tecnologia da Informação deverá manter os controles do uso e cancelamento de acesso ao correio eletrônico.

SEÇÃO XI DO ACESSO À INTERNET

Art. 26. O acesso à rede mundial de computadores (Internet), no ambiente de trabalho, deverá ser regido por norma interna, atendendo a esta POSIN, seus anexos e as demais orientações governamentais e legislação em vigor.

SEÇÃO XII DA COMPUTAÇÃO EM NUVEM

Art. 27. O uso de tecnologias de Computação em Nuvem deverá estar em conformidade com as diretrizes e normas específicas relacionadas à Segurança da Informação, no âmbito da Administração Pública Federal.

Parágrafo único. Ao Gestor de Segurança da Informação (GSIN), no âmbito de suas atribuições, cabe propor ações de segurança da informação e a implementação para a contratação de tecnologias de Computação em Nuvem.

SEÇÃO XIII DO USO, AQUISIÇÃO, DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMA DE INFORMAÇÃO

Art. 28. O uso, a aquisição, o desenvolvimento e a manutenção de sistema de informação observarão as seguintes regras:

I - os sistemas desenvolvidos no âmbito do ICMBio devem ser padronizados e direcionados para a plataforma GOV.BR;

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

III - a área de Tecnologia da Informação do ICMBio fica autorizada a desinstalar todo e qualquer *software* ilegal ou que comprometa a segurança dos ativos de informação do ICMBio;

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

V - o gerenciamento de mudanças deve incluir a garantia de que suas implementações, preferencialmente, sejam realizadas em horários apropriados, sendo transparente ao usuário, com planejamento de análise de risco e rollback, sem a perturbação dos processos de negócios.

Art. 29. Cabe à área de Tecnologia da Informação do ICMBio, por meio de servidores designados, a supervisão e o monitoramento do desenvolvimento terceirizado de *software*, de forma a garantir que critérios de segurança, qualidade, conformidade e desempenho sejam devidamente implementados.

Art. 30. É responsabilidade dos gerentes, gestores de projetos e demais servidores a comunicar formalmente à área de Tecnologia da Informação quando da elaboração de projetos ou iniciativas que envolvam o desenvolvimento de sistemas, portais ou aplicativos, mesmo que estes venham a ser desenvolvidos com o uso de recursos externos.

SEÇÃO XIV DA SENSIBILIZAÇÃO, CONSCIENTIZAÇÃO E CAPACITAÇÃO

Art. 31. Cabe ao gestor de segurança da informação apoiar a DIPLAN e a área de comunicação institucional, quanto ao desenvolvimento de plano permanente de divulgação, sensibilização, conscientização e capacitação dos seus servidores sobre os cuidados e deveres relacionados à segurança da informação e comunicações.

Art. 32. Os investimentos para capacitação em segurança da informação deverão ser estabelecidos de forma planejada e contemplados no Plano Anual de Capacitação do ICMBio, com base na priorização dos riscos a serem tratados, considerando a probabilidade, severidade e relevância destes.

CAPÍTULO V

DAS COMPETÊNCIAS E RESPONSABILIDADES

Art. 33. A estrutura de Gestão de Segurança da Informação no ICMBio será composta pelo Gestor de Segurança da Informação (GSIN), pelo Comitê de Segurança da Informação (CSIN) e pela Equipe de Tratamento e Resposta a Incidentes Cibernéticos.

Art. 34. Compete ao Comitê de Governança Digital (CGD) aprovar a POSIN e demais normas de segurança da informação propostas pelo CSIN.

Art. 35. Compete à Presidência do ICMBio, no âmbito da POSIN:

- I - promover a cultura de segurança da informação;
- II - instituir o Comitê de Segurança da Informação (CSIN);
- III - nomear o Gestor de Segurança da Informação (GSIN);
- IV - instituir a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR);
- V - reservar recursos orçamentários para as ações de segurança da informação, alinhadas a esta política;
- VI - aplicar ações corretivas e disciplinares cabíveis nos casos de quebra de segurança.

Art. 36. Compete à Alta Administração:

- I - promover a simplificação administrativa, a modernização da gestão pública e a integração dos serviços públicos, especialmente aqueles prestados por meio eletrônico, com vistas à segurança da informação;
- II - monitorar o desempenho e avaliar a concepção, a implementação e os resultados da sua política de segurança da informação e das normas internas de segurança da informação;
- III - incorporar padrões elevados de conduta para a garantia da segurança da informação e orientar o comportamento dos agentes públicos, em consonância com as funções e as atribuições de seus órgãos e de suas entidades;
- IV - planejar a execução de programas, de projetos e de processos relativos à segurança da informação;
- V - estabelecer diretrizes para o processo de gestão de riscos de segurança da informação;
- VI - observar as normas que estabelecem requisitos e procedimentos para a segurança da informação publicadas pelo Gabinete de Segurança Institucional da Presidência da República
- VII - implementar controles internos fundamentados na gestão de riscos da segurança da informação;
- VIII - instituir um sistema de gestão de segurança da informação;
- IX - implantar mecanismo de comunicação imediata sobre a existência de vulnerabilidades ou incidentes de segurança que impactem ou possam impactar os serviços prestados ou contratados pelos órgãos da administração pública federal;
- X - observar as normas e os procedimentos específicos aplicáveis, implementar e manter mecanismos, instâncias e práticas de governança da segurança da informação em consonância com os princípios e as diretrizes estabelecidos neste Decreto e na legislação;
- XI - compete à alta administração apoiar e exigir o cumprimento da Política, Normas e Procedimentos de Segurança da Informação e Comunicação; e
- XII - zelar para que contratos, convênios e outros instrumentos similares elaborados pelo ICMBio estejam alinhados a presente política e suas normas adjacentes.

Art. 37. Compete ao Gestor de Segurança da Informação (GSIN) do ICMBio:

- I - acompanhar a aplicação de ações corretivas e administrativas cabíveis nos casos de violação da segurança da informação;
- II - acompanhar os trabalhos da Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR);
- III - assessorar a alta administração na implementação da Política de Segurança da Informação (POSIN);
- IV - propor recursos necessários às ações de segurança da informação;
- V - estimular ações de capacitação e de profissionalização de recursos humanos em temas relacionados à segurança da informação;
- VI - coordenar o Comitê de Segurança da Informação (CSIN);
- VII - incentivar estudos de novas tecnologias, bem como seus eventuais impactos relacionados à segurança da informação;
- VIII - manter contato direto com o Departamento de Segurança da Informação (DSI) do Gabinete de Segurança Institucional da Presidência da República (GSI/PR) em assuntos relativos à segurança da informação;
- IX - verificar os resultados dos trabalhos de auditoria sobre a gestão da segurança da informação;
- X - coordenar a elaboração da Política de Segurança da Informação (POSIN) e das normas internas de segurança da informação do órgão, observadas as normas afins exaradas pelo Gabinete de Segurança Institucional da Presidência da República (GSI/PR);
- XI - 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;
- XII - participar da elaboração da Política de Segurança da Informação (POSIN) e das normas internas de segurança da informação;
- XIII - deliberar sobre normas internas de segurança da informação.

Art 38. O CSIN é composto por 09, (nove) membros, 01 (um) Gestor de Segurança da Informação é responsável pela sua coordenação; e os demais distribuídos entre as 04 (quatro) Diretorias do ICMBio, cada qual com seu membro titular e respectivo suplente. Assim, são membros do CSIN:

- I - 01 (um) Gestor de Segurança da Informação;
- II - 01 (um) membro titular e 01 (um) membro suplente da Diretoria de Planejamento, Administração e Logística — DIPLAN;
- III - 01 (um) membro titular e 01 (um) membro suplente da Diretoria, de Criação e Manejo de Unidades de Conservação — DIMAN;
- IV - 01 (um) membro titular e 1 (um) membro suplente da Diretoria de Ações Socioambientais e Consolidação Territorial em Unidades de Conservação — DISAT;
- V - 01 (um) membro titular e 01 (um) membro suplente da Diretoria de Pesquisa, Avaliação e Monitoramento da

Art 39. Os representantes indicados desempenharão suas atribuições sem prejuízos decorrentes de seus respectivos cargos e funções sendo que a participação no CSIN será considerada prestação de serviço relevante e não remunerada.

Art. 40. Compete ao Comitê de Segurança da Informação (CSIN):

- I - assessorar na implementação das ações de segurança da informação no ICMBio;
- II - constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação;
- III - propor alterações na Política de Segurança da Informação interna e às normas internas de segurança da informação;
- IV - participar da elaboração da Política de Segurança da Informação e das normas internas de segurança da informação;
- V - deliberar sobre normas internas de segurança da informação.

Art. 41. O Comitê de Governança Digital poderá editar atos para definir a forma de funcionamento do CSIN, observado o disposto no Decreto nº 9.637, de 26 de dezembro de 2018.

Art. 42 São competências das Gerências Regionais:

- I - observar rigorosamente esta Política de Segurança de Informação e implementar no prazo de 90 dias, a contar da publicação desta política, o Plano Regional de Segurança da Informação-PRSI baseado nesta POSIN;
- II - difundir para as suas unidades de conservação a POSIN, através dos PRSI;
- III - propor alterações na Política de Segurança da Informação;
- IV - fiscalizar o uso das políticas de segurança de suas unidades de conservação subordinadas;
- V - fazer cumprir as normas em vigor previstas nesta POSIN.

Art. 43. São obrigações do usuário:

- I - observar rigorosamente esta Política de Segurança de Informação, bem como as Normas e Procedimentos a ela vinculados;
- II - assegurar o uso racional dos recursos de tecnologia da informação colocados à sua disposição, priorizando o interesse público e institucional;
- III - comunicar à Equipe de Tratamento e Resposta a Incidentes Cibernéticos (ETIR) quaisquer riscos ou incidentes de segurança que venham a tomar conhecimento;
- IV - assegurar-se que as senhas e credenciais para acesso estejam de acordo com os procedimentos estabelecidos e que as mesmas sejam protegidas não devendo ser compartilhada;
- V - manter, obrigatoriamente, os dados críticos das Diretorias nos compartilhamentos de rede disponibilizados pelo ICMBio.

Art. 44. São obrigações da Área de Tecnologia da Informação:

- I - realizar, com a periodicidade necessária, cópias de segurança dos dados armazenados nos compartilhamentos de rede, precavendo-se quanto a catástrofes;
- II - assegurar o pleno e efetivo funcionamento dos recursos de tecnologia da informação disponibilizados pelo ICMBio;
- III - assegurar a integridade e disponibilidade dos ativos que se encontram no ambiente computacional do ICMBio;
- IV - dar assistência ao CSIN na elaboração de Normas e Procedimentos de Segurança da Informação no tocante às informações e processos relativos presentes no ambiente computacional do ICMBio;
- V - realizar trabalhos de análise de vulnerabilidade, com o intuito de aferir o nível de segurança dos sistemas de informação que se encontram no ambiente ICMBio;
- VI - requisitar informações às demais áreas do ICMBio, realizar testes e averiguações em sistemas e equipamentos, com o intuito de verificar o cumprimento da Política e das Normas de Segurança da Informação no tocante aos ativos informatizados;
- VII - elaborar o Plano de Resposta a Incidentes;
- VIII - empregar servidores públicos do órgão na gestão de processos de Tecnologia da Informação;

Art. 45. São obrigações do proprietário:

- I - identificar e definir as informações críticas e os requisitos de confidencialidade, integridade, disponibilidade e autenticidade dos seus ativos;
- II - classificar e rever periodicamente a classificação dos ativos sob sua propriedade que requerem algum grau de sigilo, observando a legislação em vigor;
- III - participar do processo de avaliação e aceitação de risco;
- IV - participar nas decisões relacionadas a qualquer violação de segurança dos ativos sob sua propriedade;
- V - autorizar a liberação de acesso à informação sob sua responsabilidade;
- VI - participar da investigação de incidentes de segurança relacionados à informação sob sua responsabilidade;
- VII - participar, sempre que convocado, das reuniões do Comitê de Gestão de Segurança da Informação, prestando os esclarecimentos solicitados;

Art. 46. São obrigações do custodiante:

- I - prestar assistência ao Proprietário na definição dos procedimentos operacionais e de controle, referentes a manuseio, armazenamento e disposição final dos ativos;
- II - controlar e proteger os ativos sob sua custódia;
- III - realizar, verificar e manter cópias de segurança (backups) dos ativos de informação sob sua custódia;
- IV - comunicar a ETIR e ao proprietário qualquer incidente de segurança que afete os ativos sob sua custódia;
- V - implementar os controles de segurança contratando, se necessário, bens e serviços em Segurança da Informação.

CAPÍTULO VI DAS PENALIDADES

Art. 47. Os incidentes, as quebras de segurança e o descumprimento das normas estabelecidas nesta POSIN serão devidamente apurados e implicará a responsabilidade civil, penal e administrativa dos que estiverem envolvidos na violação, podendo ensejar, do ponto de vista administrativo, apuração de responsabilidade, conforme os art. 124 e art. 143 da Lei nº 8.112, de 1990.

§1º O não cumprimento das determinações da POSIN sujeita o infrator às penalidades previstas na legislação e nos regulamentos internos do ICMBio.

§2º O descumprimento das disposições constantes nessa Política e nas Normas Complementares sobre segurança da informação caracteriza infração funcional, a ser apurada em processo administrativo disciplinar, sem prejuízo das responsabilidades penal e civil.

§3º Os casos omissos e as dúvidas surgidas na aplicação dessa política serão submetidos ao CSIN.

CAPÍTULO VII DA ATUALIZAÇÃO

Art. 48. Esta portaria deverá ser revisada e atualizada a cada 03 (três) anos, a contar da data de sua publicação ou a qualquer tempo por solicitação o Comitê de Governança Digital.

Art. 49. As unidades organizacionais do ICMBio terão o prazo de 90 (noventa) dias da data da publicação desta, para submeterem ao Comitê de Segurança da Informação, as propostas de atualização ou criação das normas e procedimentos internos complementares sobre segurança da informação e segurança orgânica, no âmbito de suas atividades finalísticas ou administrativas, de modo a garantir a segurança das informações tratadas no exercício das atividades laborais de suas equipes, independentemente do ambiente em que tais informações sejam tratadas (ex.: reuniões de planejamento de operações, reuniões estratégicas instruções de campo, manuais físicos e digitais, painéis informativos e etc).

CAPÍTULO VIII DAS DISPOSIÇÕES FINAIS

Art. 50. Integram esta Política de Segurança da Informação as Normas de Segurança da Informação - NSIs - elencadas nos anexos a seguir:

Anexo I NSI 001/2022 - Gestão de Incidentes de Segurança da Informação - que estabelece as diretrizes e defini o processo de Gestão de Incidentes de Segurança da Informação relacionada ao ambiente tecnológico no âmbito do ICMBio;;

Anexo II NSI 002/2022 - Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos - ETIR - que estabelece as diretrizes para o funcionamento da Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR) do ICMBio;

Anexo III NSI 003/2022 - Gestão de Riscos de Tecnologia da Informação - que estabelece as diretrizes da gestão de riscos relacionada ao ambiente tecnológico, aos projetos e processos de Tecnologia da Informação e Comunicações (TI), e defini o processo de Gerenciamento de Riscos de Segurança da Informação e Comunicações do ICMBio;

Anexo IV NSI 004/2022 - Uso de Recursos de Tecnologia da Informação e Controle de Acesso - que estabelece diretrizes e padrões para a utilização dos recursos de tecnologia da informação e para o controle de acesso físico e lógico;

Anexo V NSI 005/2022 - Controle de Acesso à Internet e à Intranet - que estabelece diretrizes e padrões para o acesso à internet e à intranet;

Anexo VI NSI 006/2022 - Serviço de Correio Eletrônico Institucional - que estabelece regras e padrões para a utilização do serviço de correio eletrônico;

Anexo VII NSI 007/2022 - Sistemas - que estabelece as diretrizes e defini o processo de utilização dos sistemas no âmbito do ICMBio;

Anexo VIII NSI 008/2022 - Política de backup e recuperação de dados - que estabelece diretrizes e padrões para os procedimentos de backup, testes e recuperação de dados;

Anexo IX NSI 009/2022 - Gestão de Continuidade de TI - que estabelece as diretrizes e defini o processo de Gestão de Continuidade de Tecnologia da Informação e Comunicações, aplicáveis ao ambiente tecnológico do ICMBio.

Art. 51. Os servidores e colaboradores do ICMBio devem observar as diretrizes e responsabilidades estabelecidas nesta POSIN, nas normas e procedimentos complementares e nas melhores práticas de segurança da informação recomendados por órgãos e entidades públicas e privadas responsáveis pelo estabelecimento de padrões e normas de segurança.

Art. 52. Os servidores e colaboradores do ICMBio devem comunicar aos gestores responsáveis pelos ativos da informação quaisquer ocorrências de incidentes de segurança da informação.

Art. 53. Os servidores e colaboradores do ICMBio são responsáveis pela segurança dos ativos de informação, que estejam sob sua custódia, e por todos os atos executados com suas credenciais, tais como: crachá, identidade funcional, login, senha eletrônica, certificado digital e endereço de correio eletrônico, devendo comunicar imediatamente a *Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos - ETIR*, a perda ou extravio de documentos ou equipamentos que contenham informações institucionais ou senhas e credenciais de acesso.

Art. 54. Os contratos, convênios, acordos e instrumentos congêneres devem observar, no que couber, as seguintes diretrizes:

I - conter cláusulas que estabeleçam a obrigatoriedade de observância desta POSIN;

II - prever a obrigação da outra parte de divulgar esta POSIN e suas normas complementares aos seus empregados e prepostos envolvidos em atividades no ICMBio;

III - nos casos de obtenção de informações de terceiros, o gestor da área na qual a informação será utilizada deve, se necessário, providenciar junto ao cedente a documentação formal relativa à cessão de direitos sobre informações de terceiros antes de seu uso.

Art. 55. Após a publicação oficial, esta portaria será disponibilizada no Painel de Legislação Ambiental.

Art. 56. Este ato entra em vigor no primeiro dia útil do mês subsequente de sua publicação.



Documento assinado eletronicamente por **Luis Gustavo Biagioni, Presidente Substituto**, em 10/08/2022, às 19:00, conforme art. 1º, III, "b", da Lei 11.419/2006.



A autenticidade do documento pode ser conferida no site <https://sei.icmbio.gov.br/autenticidade> informando o código verificador **11777232** e o código CRC **328E8CA0**.



MINISTÉRIO DO
MEIO AMBIENTE



MINISTÉRIO DO MEIO AMBIENTE
INSTITUTO CHICO MENDES DE CONSERVAÇÃO DA BIODIVERSIDADE
GABINETE DA PRESIDÊNCIA

EQSW 103/104, Bloco "C", Complexo Administrativo - Bloco C - Bairro Setor Sudoeste - Brasília - CEP 70670-350

Telefone: (61) 2028-9011/9013

ANEXOS I- NORMA DE SEGURANÇA DA INFORMAÇÃO (NSI)
NSI 001/2022 - GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

1. OBJETIVOS

1.1 Estabelecer diretrizes e padrões para: Gestão de Incidentes de Segurança da Informação, no âmbito do Instituto Chico Mendes de Conservação da Biodiversidade - ICMBio.

2. MOTIVAÇÕES

2.1. Alinhamento as normas, regulamentações e melhores práticas, relacionadas a matéria.

2.2. Necessidade de tratar os incidentes de segurança da informação com resposta rápida e eficiente.

2.3. Correto direcionamento e dimensionamento de recursos tecnológicos e humanos para prover uma Gestão de Incidentes de Segurança da Informação com menor custo e maior qualidade.

2.4. Formalização de um processo sistemático para gerenciamento dos incidentes de segurança da informação provendo insumos para minimizar e/ou evitar eventos futuros.

3. REFERÊNCIAS NORMATIVAS

3.1. Instrução Normativa nº 1, de 27 de maio de 2020, do Gabinete de Segurança Institucional da Presidência da República, que dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal;

3.2. Norma Complementar nº 05/IN01/DSIC/GSIPR, de 14 de agosto de 2009, do Departamento de Segurança da Informação e Comunicações da Presidência da República, que disciplina a criação de Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais - ETIR nos órgãos e entidades da Administração Pública Federal, direta e indireta - APF.

3.3. Norma Complementar nº 08/IN01/DSIC/GSIPR, de 14 de agosto de 2010, do Departamento de Segurança da Informação e Comunicações da Presidência da República, que estabelece as Diretrizes para Gerenciamento de Incidentes em Redes Computacionais nos órgãos e entidades da Administração Pública Federal.

3.4. Norma Complementar nº 21/ON01/DSIC/GSIPR, de 08 de outubro de 2014, que estabelece as diretrizes para o Registro de Eventos, Coleta e Preservação de Evidências de Incidentes de Segurança em Redes nos órgãos e entidades da Administração Pública Federal, direta e indireta.

3.5. Norma Técnica ABNT NBR ISO/IEC 27001:2013, que especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação dentro do contexto da organização.

3.6. Norma Técnica ISO/IEC 27000:2018, que especifica conceitos e definições relacionados às normas de Segurança da Informação.

3.7. Instrução Normativa nº 1, de 04 de abril de 2019, que dispõe sobre o processo de contratação de soluções das áreas de tecnologia da informação pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISF do Poder Executivo Federal.

4. CONCEITOS E DEFINIÇÕES

4.1. Artefato malicioso: é qualquer programa de computador, ou parte de um programa, construído com a intenção de provocar danos, obter informações não autorizadas ou interromper o funcionamento de sistemas e/ou redes de computadores.

4.2. Ativos da Informação: os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas e as pessoas que a eles tem acesso.

4.3. CTIR GOV: Centro de Tratamento e Resposta a Incidentes de Segurança em Redes de Computadores da Administração Pública Federal, subordinado ao departamento de Segurança da Informação e Comunicações - DISC do Gabinete de Segurança Institucional da Presidência da República - gsi.

4.4. Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos - ETIR: grupo de pessoas com a responsabilidade de receber, analisar e responder as notificações e atividades relacionadas a incidentes de segurança da informação.

4.5. 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 uma situação previamente desconhecida, que possa ser relevante para a segurança da informação.

4.6. Gestor da Unidade: Coordenador Geral, Coordenador, Chefe de Divisão, Chefe de Serviço ou servidor designado para responder por uma unidade ou serviço constante de Regimento Interno do ICMBio.

4.7. Incidente de Segurança da Informação: é indicado por um simples ou por uma série de eventos de segurança da informação indesejados ou inesperados, que tenham uma grande probabilidade e comprometer as operações do negócio e ameaçar a segurança da informação.

4.8. Medida de contenção: controle e/ou ação tomada para evitar que danos causados por um determinado incidente continuem aumentando com o passar do tempo. Além disso, tais medidas visam o restabelecimento do sistema/serviço afetado, mesmo que não seja em sua capacidade total.

4.9. Medida de solução: controle e/ou ação tomada para sanar vulnerabilidades e problemas que sejam a causa-raiz de um ou mais incidentes de segurança da informação.

4.10. Rede Nacional de Computadores do ICMBio: Infraestrutura de Rede de computadores conectados via MPLS ou VPN *Site-to-Site*.

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

4.12. Usuários: colaboradores e servidores ocupantes de cargo efetivo ou em comissão, requisitados e cedidos, desde que previamente autorizados, empregados de empresas prestadoras de serviços terceirizados, consultores, estagiários e outras pessoas que se encontram a serviço do ICMBio utilizando em caráter temporário os recursos tecnológicos do Instituto.

4.13. Vulnerabilidade: fragilidade de um ativo ou controle que pode ser explorado por uma ameaça.

5. DIRETRIZES

5.1. A Gestão de Incidentes de Segurança da Informação tem como principal objetivo assegurar que incidentes de segurança da informação sejam identificados, registrados e avaliados em tempo hábil para a tomada de medidas de contenção e/ou solução adequadas.

5.2. Estão abrangidos por esta norma os eventos, confirmados ou suspeitos, relacionados a segurança de sistemas ou redes computacionais, que comprometam o ambiente tecnológico do ICMBio, seus ativos, informações e processos de negócio, bem como aqueles que contrariem a Política de Segurança da Informação deste Instituto, e dos quais decorram interrupção, parcial ou total, de serviço essencial ao desempenho das atividades, vulnerabilidades de segurança, divulgação, alteração ou destruição de informações e/ou prática de ato definido como crime ou infração administrativa.

5.3. A infraestrutura de tecnologia da informação do ICMBio deverá ser provida de dispositivos de monitoramento, ferramentas de segurança e detecção de intrusão, a fim de subsidiar a Gestão de Incidentes de Segurança da Informação.

6. PROCESSO DE GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

6.1. O processo de Gestão de Incidentes de Segurança da Informação é contínuo e aplicado na implementação e operação do Sistema de Gestão de Segurança da Informação (SGSI).

6.2. O processo de Gestão de Incidentes de Segurança da Informação é composto pelas seguintes etapas:

6.2.1. Detecção e registro: compreende o recebimento, registro e autorizações necessárias para o encaminhamento da investigação;

6.2.2. Investigação e contenção: compreende a investigação e tratamento do incidente, coleta de dados, comunicação às áreas afetadas, proposição e aplicação de ações de contenção, quando necessárias;

6.2.3. Encerramento: compreende a análise do incidente, com verificação da necessidade de outras ações, providências ou comunicações, e após seu cumprimento, o encerramento do incidente;

6.2.4. Avaliação de incidentes: compreende a avaliação do histórico de incidentes, com consolidação das informações e indicadores e verificação das oportunidades de melhoria e lições aprendidas.

6.3. Os incidentes, notificados ou detectados, devem ser objeto de registro, com a finalidade de assegurar a manutenção do histórico e auxiliar na geração de indicadores.

6.4. A notificação de incidente poderá ser feita por qualquer usuário, sem necessidade de prévia autorização do gestor, através do formulário de solicitação de atendimento da Central de Serviços, pelo telefone ou pelo e-mail cotec@icmbio.gov.br, que será reportado a Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação.

6.5. Os usuários devem notificar, o mais breve possível, os incidentes de segurança da informação e vulnerabilidades de que te

6.6. Vulnerabilidades ou fragilidades suspeitas não deverão ser objeto de teste ou prova pelos usuários, sob o risco de violar a política de segurança da informação e/ou provocar danos aos serviços ou recursos tecnológicos.

6.7. A equipe da área de tecnologia da informação responsável pelo monitoramento dos ativos, serviços e sistemas devem notificar os incidentes a eles relacionados a Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação, para o devido registro e encaminhamento.

6.8. O ICMBio poderá receber notificações externas (CTIR.BR, CSIRT ou outras empresas) sobre incidentes (ocorridos ou suspeitos) por meio de sistemas gerenciadores de demandas, e-mail, telefone e etc, que deverão ser remetidas ao setor responsável pela Segurança da Informação.

6.9. O tratamento da Informação deve ser realizado de forma a viabilizar e assegurar a disponibilidade, integridade, confidencialidade e autenticidade da informação, com retorno das operações a normalidade no menor prazo possível, bem como evitar as futuras ocorrências, com a proposição de ações de solução, quando existente.

6.10. A Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação deve conduzir, apoiada pelas outras áreas do Instituto, investigação do incidente e artefatos maliciosos, propondo e implementando as ações de contenção, comunicando as áreas afetadas e coletando os dados necessários.

6.11. A coleta de evidência dos incidentes de segurança da informação deve ser realizada pela equipe de Tratamento e Resposta a Incidentes de Segurança da Informação ou por pessoal competente e por ela autorizado.

6.12. Quando o incidente de segurança da informação decorrer de suspeita de descumprimento da Política de Segurança da Informação, será observado o sigilo durante todo o processo, ficando as evidências, informações e demais registros restritos, aos envolvidos na investigação;

6.13. Quando houver indícios de ilícitos criminais durante o gerenciamento dos incidentes de segurança, o Comitê Gestor de Tecnologia da Informação do ICMBio deverá ser comunicado, para avaliação das providências cabíveis.

6.14. O encerramento do incidente de segurança da informação será realizado pelo setor responsável pela Segurança da Informação, com comunicação a todas as áreas interessadas e ao Centro de Tratamento de Incidentes de Segurança de Redes de Computadores da Administração Pública Federal (CTIR.BR), na forma e nos casos definidos pelo referido órgão.

6.15. A avaliação do processo de gestão de incidentes de segurança da informação ocorrerá através do histórico de incidentes, com verificação das oportunidades de melhoria.

6.16. O desenho do processo de Gestão de Incidentes de Segurança da Informação, a descrição das atividades, os

respectivos papéis e responsabilidades dos envolvidos no processo, bem como os modelos de documentos a serem utilizados nas etapas do processo, serão publicados no Portal de Governança de TI, após aprovação pela Presidência.

6.17.O processo será revisto bianualmente ou em menor prazo, quando necessário, e eventuais alterações propostas nos documentos acima indicados serão, após aprovação pela Presidência deste Instituto, objeto de imediata divulgação na forma do item anterior.

7. MONITORAMENTO E AUDITORIAS

7.1.As auditorias ordinárias ou extraordinárias serão coordenadas pelo Gestor de Segurança da Informação e Comitê de Governança Digital.

7.2.As auditorias extraordinárias deverão ser precedidas de autorização do Comitê de Segurança da Informação.

7.3.Os procedimento constantes desta norma deverão ter monitoramento contínuo da área de tecnologia da informação visando a melhoria contínua.

8. ATUALIZAÇÃO DA NORMA

8.1.O disposto na presente norma será atualizado sempre que alterados os procedimentos da Gestão de Incidentes de Segurança da Informação, observada, ainda, a periodicidade prevista para a revisão da política de Segurança da Informação.

LUIS GUSTAVO BIAGIONI

Presidente Substituto



Documento assinado eletronicamente por **Luis Gustavo Biagioni, Presidente Substituto**, em 10/08/2022, às 18:57, conforme art. 1º, III, "b", da Lei 11.419/2006.



A autenticidade do documento pode ser conferida no site <https://sei.icmbio.gov.br/autenticidade> informando o código verificador **11777496** e o código CRC **12953543**.



MINISTÉRIO DO
MEIO AMBIENTE



MINISTÉRIO DO MEIO AMBIENTE
INSTITUTO CHICO MENDES DE CONSERVAÇÃO DA BIODIVERSIDADE
GABINETE DA PRESIDÊNCIA

EQSW 103/104, Bloco "C", Complexo Administrativo - Bloco C - Bairro Setor Sudoeste - Brasília - CEP 70670-350

Telefone: (61) 2028-9011/9013

ANEXOS II - NORMA DE SEGURANÇA DA INFORMAÇÃO (NSI)

NSI 002/2022 - EQUIPE DE PREVENÇÃO, TRATAMENTO E RESPOSTA A INCIDENTES CIBERNÉTICOS - ETIR

1. OBEJETIVOS

1.1. Estabelecer diretrizes e padrões para: Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos - ETIR, no âmbito do Instituto Chico Mendes de Conservação da Biodiversidade - ICMBio.

2. MOTIVAÇÕES

- 2.1. Alinhamento as normas, regulamentações e melhores práticas, relacionadas a matéria.
- 2.2. Necessidade de formalização da Equipe de Prevenção, Tratamento e Resposta a incidentes Cibernéticos (ETIR) e seu funcionamento.
- 2.3. Proteção do ambiente tecnológico do Instituto.
- 2.4. Facilitar e coordenar as atividades de prevenção, tratamento e resposta a incidentes em redes computacionais do Instituto.
- 2.5. Receber e notificar qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores, a fim de contribuir para a adequada prestação dos serviços do Instituto.
- 2.6. Analisar e escalar, quando necessário, ataques e intrusões nos sistemas e redes de computadores.

3. REFERÊNCIAS NORMATIVAS

- 3.1. Decreto da PR nº 9637/2018, de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação;
- 3.2. Decreto da PR nº 10.222/2020, de 05 de fevereiro de 2020, que aprova a Estratégia Nacional de Segurança Cibernética;
- 3.3. Decreto da PR nº 10.748, de 16 de julho de 2021, que institui a Rede Federal de Gestão de Incidentes Cibernéticos;
- 3.4. Instrução Normativa nº 1, de 27 de maio de 2020, do Gabinete de Segurança Institucional da Presidência da República, que dispõe sobre a estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da Administração Pública Federal;
- 3.5. Norma Complementar nº 05/IN01/DISC/GSIPR, de 14 de agosto de 2009, do Departamento de Segurança da Informação e Comunicação da República, que disciplina a criação de Equipes de Tratamento e Respostas a incidentes em Redes Computacionais - ETIR nos órgãos e entidades da Administração Pública Federal, direta e indireta - APF;
- 3.6. Norma Complementar nº 08/IN01/DSIC/GSIPR/, de 14 de agosto de 2010, do Departamento de Segurança da Informação e Comunicações da Presidência da República, que estabelece as Diretrizes para Gerenciamento de Incidentes em Redes Computacionais nos órgãos e entidades da Administração Pública Federal;
- 3.7. Norma Técnica ISO/IEC 27000:2018, que especifica conceitos e definições relacionados as normas de segurança da informação;
- 3.8. Portaria GSI/PR nº 93/2019, de 18 de outubro de 2021, que aprova o Glossário de Segurança da Informação;
- 3.9. Instrução Normativa nº 1, de 04 de abril de 2019, que dispõe sobre o processo de contratação de soluções de Tecnologia da Informação - TI pelos órgão e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal.

4. CONCEITOS E DEFINIÇÕES

- 4.1. Agente responsável da ETIR: servidor público ocupante de cargo efetivo ou militar de carreira de órgão ou entidade da Administração Pública Federal, direta ou indireta incumbido de chefiar e gerenciar a ETIR.
- 4.2. Artefato Malicioso: é qualquer programa de computador, ou parte de um programa, construído com a intenção de provocar danos, obter informações não autorizadas ou interromper o funcionamento de sistemas e/ou redes de computadores.
- 4.3. Comunidade ou Público Alvo: e o conjunto de pessoas, setores, órgãos ou entidades atendidas pela Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos.
- 4.4. CTIR GOV: Centro de Tratamento e Resposta a Incidentes de Segurança em Redes de Computadores da Administração Pública Federal, subordinado ao departamento de Segurança da Informação e Comunicações - DISC do Gabinete de Segurança Institucional da Presidência da República - GSI.
- 4.5. Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos - ETIR: grupo de pessoas com a responsabilidade de receber, analisar e responder as notificações e atividades relacionadas a incidentes de segurança da informação.

4.6.Gestor da unidade: Coordenador Geral, Coordenador, Chefe de Divisão, Chefe de Serviço ou servidor designado para responder por uma unidade ou serviço constante do Regimento interno do ICMBio.

4.7.Incidente de Segurança da Informação: um único ou uma série de eventos indesejados ou inesperados de segurança da informação que tem uma probabilidade significativa de colocar em perigo as operações da instituição e ameaça a segurança da Informação.

4.8.SISP - Sistema de Administração dos Recursos de Tecnologia da Informação do Poder Executivo Federal.

4.9.Tratamento de Incidentes: conjunto de processos para detectar, relatar, avaliar, responder, lidar e aprender com incidentes de segurança da informação;

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

5. **MODELO DE IMPLEMENTAÇÃO**

5.1.A ETIR será composta por servidores da área de tecnologia da informação que , além de suas funções regulares , desempenharão as atividades relacionadas ao tratamento e a resposta a incidentes de segurança da informação.

6. **ESTRUTURA ORGANIZACIONAL E COMPOSIÇÃO**

6.1.A ETIR/ICMBIO fará parte, automaticamente, da Rede Federal de Gestão de Incidentes Cibernéticos, instituída pelo Decreto nº 10.748, de 16 de julho de 2021;

6.2.A ETIR é subordinada a Diretoria de Planejamento, Administração e Logística - DIPLAN e coordenada pelo setor responsável de Segurança da Informação;

6.3.A ETIR será composta, preferencialmente, por servidores públicos civis ocupantes de cargo efetivo, com capacidade técnica compatível com as atividades dessa equipe;

6.4.Os membros da ETIR deverão ser selecionados, sempre que possível, dentre o pessoal existente, com perfil técnico adequado às funções de tratamento de incidentes de rede;

6.5.Seus integrantes serão indicados pelo Comitê de Governança Digital do ICMBio - CGD/ICMBio e designados por meio de portaria do Presidente do Instituto;

6.6.Para cada membro titular da ETIR, deverá ser designado um substituto que deverá ser treinado e orientado para a realização das tarefas e atividades da equipe;

6.7.As atividades da ETIR/ICMBio deverão ser desempenhadas de forma proativa e reativa, sendo o Agente Responsável da ETIR quem irá atribuir as responsabilidades;

6.8.Caso necessário, deverão ser convocados outros servidores da área de tecnologia e/ou servidores de outras áreas do Instituto (jurídica, gestão de pessoas, comunicação social, etc.) para auxiliar a equipe no desenvolvimento de suas atividades.

7. **ATRIBUIÇÕES**

7.1.Investigar e propor ações de contenção para os incidentes de segurança da informação relacionados aos ativos de tecnologia da informação;

7.2.Receber e analisar as informações sobre vulnerabilidades, artefatos maliciosos e tentativas de intrusão, com definição de estratégias e ações para sua detenção ou correção;

7.3.Fornecer informações aos envolvidos, sobre a ocorrência e, ao público interno, orientações de prevenção de incidentes de segurança da informação;

7.4.Manter os registros dos incidentes de segurança da informação relacionados aos ativos de tecnologia da informação;

7.5.Divulgar alertas ou advertências diante da ocorrência de um incidente de segurança da informação ou, de forma proativa, em face de vulnerabilidades e incidentes conhecidos e que possam gerar impactos nas atividades dos usuários;

7.6.Interagir com outras equipes e órgãos relacionados ao tratamento de incidentes de segurança, participação em fóruns e redes nacionais e internacionais;

7.7.O Agente Responsável da ETIR/ICMBio possui as seguintes competências:

7.7.1.coordena e orienta os membros da ETIR na gestão de incidentes em redes de computadores;

7.7.2.ser a interface com o CTIR GOV;

7.7.3.gerenciar as atividades, os procedimentos internos e distribuir tarefas para os integrantes da ETIR;

7.7.4.enviar notificações de incidentes de segurança da informação;

7.7.5.ser interface com o Gestor de Segurança da Informação no processo de capacitação e treinamento dos membros da ETIR; e

7.7.6.representar a ETIR junto ao CGD/ICMBio quanto às medidas no tratamento de incidentes de segurança da informação.

8. **COMUNICAÇÃO**

8.1.A comunicação de incidentes cibernéticos suspeitos ou confirmados para a equipe deve ser realizada por e-mail, para o endereço etir@icmbio.gov.br.

8.2.A ETIR deverá comunicar de imediato a ocorrência de todos os incidentes ao CTIR GOV, sobre a existência de vulnerabilidades ou incidentes de segurança cibernética que impactem ou que possam impactar os serviços prestados ou contratados;

8.3.As notificações enviadas ao CTIR GOV, bem como a troca de informações entre as equipes existentes, devem seguir os formatos e os procedimentos estabelecidos pelo próprio CTIR GOV, a fim de permitir a geração de estatísticas e soluções integradas para a Administração Pública Federal.

9. **MONITORAMENTO E AUDITORIAS**

9.1. As auditorias ordinárias ou extraordinárias serão coordenadas pelo Gestor de Segurança da Informação e Comitê de Governança Digital.

9.2. As auditorias extraordinárias deverão ser precedidas de autorização do Comitê de Segurança da Informação.

9.3. Os procedimentos constantes desta norma deverão ter monitoramento contínuo da área de tecnologia da Informação visando a melhoria contínua.

10. ATUALIZAÇÃO DA NORMA

10.1. O disposto na presente norma será atualizado sempre que alterados os procedimentos de tratamento e resposta a incidentes de segurança da informação, observada, ainda, a periodicidade prevista para a revisão da Política de Segurança da Informação.

LUIS GUSTAVO BIAGIONI

Presidente Substituto



Documento assinado eletronicamente por **Luis Gustavo Biagioni, Presidente Substituto**, em 10/08/2022, às 18:58, conforme art. 1º, III, "b", da Lei 11.419/2006.



A autenticidade do documento pode ser conferida no site <https://sei.icmbio.gov.br/autenticidade> informando o código verificador **11778060** e o código CRC **7F544730**.



MINISTÉRIO DO
MEIO AMBIENTE



MINISTÉRIO DO MEIO AMBIENTE
INSTITUTO CHICO MENDES DE CONSERVAÇÃO DA BIODIVERSIDADE
GABINETE DA PRESIDÊNCIA

EQSW 103/104, Bloco "C", Complexo Administrativo - Bloco C - Bairro Setor Sudoeste - Brasília - CEP 70670-350

Telefone: (61) 2028-9011/9013

ANEXOS III - NORMA DE SEGURANÇA DA INFORMAÇÃO (NSI)
NSI 003/2022 - GESTÃO DE RISCOS DE TECNOLOGIA DA INFORMAÇÃO

1. OBJETIVOS

1.1. Estabelecer diretrizes e padrões para: Gestão de Riscos de Tecnologia da Informação, no âmbito do Instituto Chico Mendes de Conservação da Biodiversidade - ICMBio.

2. MOTIVAÇÕES

2.1. Necessidade de um processo sistemático para gerenciar riscos referentes a segurança da informação, projetos e processos de TI, provendo insumos para aumentar a proteção contra eventos indesejados;

2.2. Correto direcionamento de esforços e investimentos financeiros, tecnológicos e humanos;

2.3. Conformidade com normatizações e regulamentações relacionados ao assunto.

3. REFERÊNCIAS NORMATIVAS

3.1. Instrução Normativa nº 1, de 27 de maio de 2020, do Gabinete de Segurança Institucional da Presidência da República, que dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal;

3.2. Instrução Normativa GSI/PR nº 3, de 28 de maio de 2021 que dispõe sobre os processos relacionados à gestão de segurança da informação nos órgãos e nas entidades da administração pública federal;

3.3. Norma técnica ABNT NBR ISO/IEC 27005:2019, que fornece diretrizes para o processo de gestão de riscos de segurança da informação;

3.4. Norma Técnica ABNT NBR ISO 31000:2018, que fornece princípios e diretrizes para a gestão de riscos;

3.5. Norma ABNT NBR ISO/IEC 27002: 2013, que trata de Código de Prática para a Gestão da Segurança da Informação;

3.6. Norma Técnica ABNT ISO/IEC 27001:2013, que especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão de segurança da informação dentro do contexto da organização;

3.7. Norma Técnica ABNT ISO GUIA 73:2009, que fornece as definições de termos genéricos relativos a gestão de riscos;

3.8. Norma Técnica ABNT ISO/IEC 27000:2018, que especifica conceitos e definições relacionados as normas de segurança da informação;

3.9. Instrução Normativa nº 01, de 04 de abril de 2019, que dispõe sobre o processo de contratação de soluções de Tecnologia da Informação - TI pelo órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal;

3.10. Portaria nº 255, de 01 de abril de 2020, que Institui a Política de Gestão de Riscos e Integridade no âmbito do ICMBio;

3.11. Portaria nº 975, de 10 de dezembro de 2021, que aprova a Metodologia de Gestão de Riscos do Instituto Chico Mendes de Conservação da Biodiversidade-ICMBio.

4. CONCEITOS E DEFINIÇÕES

4.1. 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;

4.2. Gerenciamento de Risco: processo para identificar, avaliar, administrar e controlar potenciais eventos ou situações e fornecer segurança razoável no alcance dos objetivos organizacionais;

4.3. Gestão de Riscos: conjunto de princípios, diretrizes, processos e atividades, destinados a enfrentar os riscos e fornecer segurança razoável na execução ordenada, ética, econômica, eficiente e eficaz das operações, no cumprimento das obrigações de transparência e responsabilização, no cumprimento das leis e regulamentos aplicáveis e na salvaguarda dos bens e recursos para evitar perdas, mau uso e danos às suas atividades e aos bens sob sua responsabilidade;

4.4. Gestão de Riscos em Projetos de TI: conjunto de atividades que envolve a identificação, a análise, o planejamento de respostas, o monitoramento e o controle de riscos de um projeto;

4.5. Gestão de Riscos em Processos de TI: 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;

4.6. Gestão de Riscos de Segurança da Informação: 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 equilibra-los com os custos operacionais e financeiros envolvidos;

4.7. Gestor da Unidade: Coordenador Geral, Coordenador, Chefe de Divisão, Chefe de Serviço ou servidor designado para responder por uma unidade ou serviço constante do Regimento interno do ICMBio;

4.8. Governança: combinação de processos e estruturas implantadas pela alta administração da organização, para informar,

dirigir, administrar, avaliar e monitorar atividades organizacionais, com o intuito de alcançar os objetivos e prestar contas para a sociedade;

4.9.Integridade: princípio da governança pública que se traduz na adesão a valores, princípios e normas éticas comuns para sustentar e priorizar o interesse público sobre os interesses privados;

4.10.Identificação de Riscos: processo para localizar, listar e caracterizar elementos do risco;

4.11.Risco: possibilidade de ocorrência de um evento que tenha impacto no atingimento dos objetivos da organização;

4.12.Riscos de Segurança da Informação: potencial associado a 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.;

4.13.Nível de Risco: magnitude de um risco, expressa em termos da probabilidade de ocorrência do evento e seu impacto para o cumprimento dos objetivos do ICMBio;

4.14.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;

4.15.Tratamento dos riscos: processo e implementação de ações de segurança da informação para evitar, reduzir, reter ou transferir um risco;

4.16.Processo: conjunto de ações e atividades inter-relacionadas, que são executadas para alcançar produto, resultado ou serviço predefinido; e

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

5. ESCOPO

5.1.A Gestão de Riscos, definida por esta Norma, tem seu escopo limitado as medidas protetivas dos ativos de informação, bem como dos projetos e processos relacionados a área de TI, que suportam os principais processos de negócio do ICMBio.

6. DIRETRIZES

6.1.A Gestão de Riscos leva em consideração as definições do Planejamento Estratégico Institucional e do Planejamento Diretor de TI e a esta alinhada a Política de Segurança da Informação deste Instituto;

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

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

6.4.As orientações e procedimentos previstos na Política de Gestão de Riscos e Integridade do ICMBio serão observadas na prática de gestão de risco de tecnologia da informação e comunicação no que couber.

7. GESTÃO DE RISCOS EM PROJETOS DE TI

7.1.As atividades inerentes ao gerenciamento de riscos em projetos relacionados a TI, devem observar o disposto na metodologia de Gestão de Riscos do Instituto Chico Mendes de Conservação da Biodiversidade.

8. GESTÃO DE RISCOS EM PROCESSOS DE TI

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

8.2.A gestão de riscos em processos de TI é monitorada pela área de tecnologia da informação.

9. GESTÃO DE RISCOS EM SEGURANÇA DA INFORMAÇÃO

9.1.O processo de Gestão de Riscos em Segurança da Informação é contínuo, fornecendo subsídios e integrando-se a implantação e operação do Sistema de Gestão de Segurança da Informação.

9.2.O processo de Gestão de Riscos em Segurança da Informação esta baseado nas definições constantes nas normas técnicas ABNT NBR ISO/IEC 27005:2019 e ABNT NBR ISO/IEC 31000:2018, na Instrução Normativa nº 1, de 27 de maio de 2020, do Gabinete de Segurança Institucional da Presidência da República e na portaria nº 975 de 10 de dezembro de 2021, do Instituto Chico Mendes de Conservação da Biodiversidade.

9.3.A Metodologia de Gestão de Riscos da informação objetiva estabelecer e estruturar as etapas necessárias para a operacionalização da gestão de riscos, por meio da definição de um processo de gerenciamento de riscos. Para tanto, são necessárias, no mínimo, as seguintes etapas:

I - Entendimento do Contexto: etapa em que são identificados os objetivos relacionados ao processo organizacional e definidos os contextos externo e interno a serem levados em consideração ao gerenciar riscos.

a)O mapeamento do Processo deve ser realizado, preferencialmente, por meio da ferramenta SIPOC (suppliers, inputs, process, outputs e customers) com a finalidade de esclarecer melhor a cadeia do negócio, definindo e formalizando diversos fatores que impactam diretamente na execução do trabalho;

Mapeamento do Processo

(5) Fornecedores	(4) Insumos	(1) Processos	(2) Produtos/Serviços	(3) Clientes
São essas origens dos insumos. Podem ser pessoas, departamentos, instituições ou outros processos	Elementos necessários para que o processo aconteça. Podem ser dados, materiais, recursos,colaboradores, entre outros	Conjunto de ações e atividades interrelacionadas, que são executadas para alcançar produto,resultado ou serviço predefinido	São os resultados de um processo, aquilo que os clientes esperam receber	São pessoas, departamentos, instituições ou outros processos que recebem os produtos/serviços entregues pelos processos

b)A análise do ambiente tem a finalidade de colher informações para apoiar a identificação de riscos, bem como contribuir para a escolha de ações mais adequadas para assegurar o alcance dos objetivos do macroprocesso/processo. Deve ser realizada, preferencialmente, por meio da matriz SWOT, que identificará as forças e fraquezas, as oportunidades e ameaças inerentes ao objeto ou processo avaliado.

Matriz SWOT- fatores do Contexto Geral

Internos	Pontos (Indicativos)	Pontos Fortes (S)	Pontos Fracos (W)
	<ul style="list-style-type: none"> - Governança, estrutura organizacional, funções e responsabilidades; - Políticas, objetivos e estratégias implementadas para atingi-los; - Capacidades, entendidas em termos de recursos e conhecimento (por exemplo, capital, tempo, pessoas, processos, sistemas e tecnologias); - Sistemas de informação, fluxos de informação e processos de tomada de decisão (formais e informais); - Relações com as partes interessadas internas, e suas percepções e valores; - Cultura organizacional; - Normas, diretrizes e modelos adotados pelo Instituto, e forma e extensão das relações contratuais 		
Externos	Pontos (Indicativos)	Oportunidades (O)	Ameaças (T)
	<ul style="list-style-type: none"> - Ambientes cultural, social, político, legal, regulatório, orçamentário, tecnológico, econômico e natural, quer seja internacional, nacional, regional ou local; - Fatores-chave e tendências que tenham impacto sobre os objetivos do Instituto; - Relações com as partes interessadas externas e suas percepções e valores. 		

II - Identificação de Riscos: Etapa em que são identificados possíveis riscos para objetivos associados aos processos organizacionais. Deverá ser realizada nas fases iniciais do processo de trabalho, visto que sua identificação em fases posteriores implicaria retrabalho e assunção de maiores custos. A partir dos resultados da etapa anterior, deve-se construir uma lista abrangente dos riscos que podem evitar, atrasar, prejudicar ou impedir o cumprimento dos objetivos do processo organizacional ou das suas etapas críticas. Recomenda-se que a identificação inclua todos os riscos, inclusive os provenientes de fontes não controladas pela área do respectivo gestor de riscos, bem como os efeitos cumulativos, as causas, as consequências e as reações em cadeia.

a) A descrição dos riscos deve ser realizada com a participação de servidores e colaboradores com conhecimento do processo e visão geral dos negócios/serviços da unidade nos seus diferentes níveis. Deve-se utilizar diversas técnicas para uma melhor compreensão dos riscos, como por exemplo, brainstorming, questionários, entrevistas, check-list, matriz SWOT, análise de dados históricos, análises de premissas, opiniões especializadas, necessidades das partes interessadas e diagramas de causa e efeito.

b) A descrição do risco deverá ser efetuada conforme a sintaxe: "**Devido o(a) < CAUSA> , poderá ocorrer o(a) < EVENTO DE RISCO>, ocasionando o(a) < CONSEQUÊNCIA> e impactando o alcance do < OBJETIVO ESTRATÉGICO> .**

c) Os riscos devem ser classificados e categorizados conforme as definições estabelecidas no anexo da política de gestão de riscos do ICMBio.

Categorias do Risco

Categoria	Descrição da Categoria
Operacional	Eventos que podem comprometer as atividades da ICMBio, normalmente associados a falhas, deficiência ou inadequação de processos internos, pessoas, infraestrutura e sistemas
Legal	Eventos derivados de alterações legislativas ou normativas que podem comprometer as atividades da ICMBio
Financeiro/Orçamentário	Eventos que podem comprometer a capacidade da ICMBio de contar com os recursos orçamentários e financeiros necessários à realização de suas atividades, ou eventos que possam comprometer a própria execução orçamentária, como atrasos no cronograma de licitações
Reputação	Eventos que podem comprometer a confiança da sociedade em relação à capacidade do ICMBio em cumprir sua missão institucional, interferem diretamente na imagem da autarquia
Integridade	Eventos que podem favorecer ou facilitar a ocorrência de práticas de corrupção, fraudes, irregularidades e/ou desvios éticos e de conduta, podendo comprometer os objetivos da instituição

d) Os riscos da categoria integridade são trabalhados no âmbito do Programa de Integridade - Integra+ do Instituto Chico Mendes, instituído pela Portaria ICMBio nº. 923, de 08 de setembro de 2020. Para facilitar a gestão dos riscos para a integridade a metodologia os divide em 06 (seis) subcategorias, conforme listado na " Subcategorias do Risco para a Integridade".

Subcategorias do Risco para a Integridade

Subcategoria	Descrição da Subcategoria
Abuso de posição ou poder em favor de interesses privados	Conduta contrária ao interesse público, valendo-se da sua condição para atender interesse privado, em benefício próprio ou de terceiros.
Nepotismo	Uma das formas de abuso de posição ou poder em favor de interesses privados, em que se favorecem familiares. Ele pode ser presumido ou requerer apuração específica
Conflito de interesses	Situação gerada pelo confronto entre interesses públicos e privados, que possa comprometer o interesse coletivo ou influenciar, de maneira imprópria, o desempenho da função pública
Pressão interna ou externa ilegal para influenciar agente público	Pressões explícitas ou implícitas de natureza hierárquica (interna), de colegas de trabalho (organizacional), política ou social (externa), que podem influenciar indevidamente atuação do agente público
Solicitação ou recebimento de vantagem indevida	Caracteriza-se por qualquer tipo de enriquecimento ilícito, seja dinheiro ou outra utilidade, dado que ao agente público não se permite colher vantagens em virtude do exercício de suas atividades
Utilização de recursos públicos em favor de interesses privados	Apropriação indevida, irregularidades em contratações públicas e outras formas de utilização de recursos públicos para uso privado (exemplos: veículos oficiais, utilização imprópria de tempo de trabalho, de equipamentos do escritório, entre outros).

III - A análise de riscos tem por finalidade estabelecer as probabilidades e os impactos dos riscos levantados na etapa anterior. Os impactos são os efeitos da ocorrência de um risco. Eles são medidos analisando-se o efeito do risco, que terá um nível de impacto sobre o objetivo que deseja ser alcançado. A probabilidade é a chance de o risco ocorrer. Ela é medida analisando-se as causas do risco. A etapa deverá ser executada a partir dos seguintes instrumentos:

a) Escala de probabilidade: define como a probabilidade será medida. A probabilidade está associada às chances de um evento ocorrer. A Tabela "Escala de Probabilidade" define a escala de probabilidade a ser utilizada no processo de gestão de riscos. O gestor de riscos pode, quando necessário, adequar somente os quantitativos da coluna "Ocorrências".

Escala de Probabilidade

Descritor	Descrição	Ocorrências	Nível
Muito baixa	Evento extraordinário, sem histórico disponível de ocorrência.	Até 5	1
Baixa	Evento casual, com histórico conhecido de ocorrência.	> 5 até 10	2
Média	Evento esperado, de frequência reduzida, com histórico conhecido pela maioria dos gestores e operadores do processo	> 10 até 15	3
Alta	Evento usual, de ocorrência habitual, com histórico conhecido amplamente por parte dos gestores e operadores do processo	> 15 até 20	4
Muito alta	Evento repetitivo e constante, de ocorrência numerosa, com histórico disponível ou não, mas evidente para os que conhecem o processo.	> 20	5

b) Escala de impacto: define a natureza e os tipos de consequências, e como elas serão medidas nas diversas áreas. Para que o nível de impacto seja definido, é necessário considerar quais são as dimensões (custo, prazo, escopo e qualidade) do objetivo do processo de trabalho avaliado que serão influenciadas direta ou indiretamente, conforme Tabela "Impacto nas Dimensões do Objeto". O impacto está associado às consequências do evento ocorrido.

Impacto nas Dimensões do Objeto

Custo (aumento %)	Prazo (atraso %)	Escopo (afetação)	Qualidade (degradação)	Nível
Até 5	Até 5	Insignificante	Irrisória	1
> 5 até 10	> 5 até 10	Pouco	Pouco	2
> 10 até 15	> 10 até 15	Significativa	Relevante	3
> 15 até 20	> 15 até 20	Muito significativa	Muito relevante	4

> 20	> 20	Ampla	Grave	5
------	------	-------	-------	---

c) Após considerar o impacto nas dimensões do objetivo, chega-se aos níveis de impacto, conforme apresentados na "Escala de Impacto".

Escala de Impacto

Descritor	Descrição	Nível
Muito baixo	Impacto insignificante nos objetivos, com dispensa de medida de reparação/recuperação	1
Baixo	Impacto mínimo nos objetivos, com possibilidade de fácil reparação/recuperação.	2
Médio	Impacto mediano nos objetivos, com possibilidade de reparação/recuperação.	3
Alta	Impacto significativo nos objetivos, com possibilidade remota de reparação/recuperação.	4
Muito alto	Impacto máximo nos objetivos, sem possibilidade de reparação/recuperação.	5

IV - A avaliação de riscos é o momento em que são estimados os níveis dos riscos identificados. Utiliza os resultados da análise de riscos como subsídio para a tomada de decisões sobre quais riscos necessitam ser tratados e com qual prioridade. A avaliação deve considerar a probabilidade de ocorrência, bem como o impacto sobre os objetivos. Quanto maior a probabilidade e o impacto, maior será o nível do risco. A combinação da probabilidade com o impacto serve para determinar o nível do risco inerente, ou seja, o nível do risco sem considerar quaisquer controles que reduzem ou possam reduzir a probabilidade da sua ocorrência ou do seu impacto.

a) A etapa deverá ser executada a partir dos seguintes instrumentos:

b) Matriz 'Impacto x Probabilidade': define como o nível de risco deve ser determinado. A "Matriz Impacto x Probabilidade" tem por finalidade apurar a magnitude de um risco expresso, considerando a combinação entre a probabilidade e o impacto.

Matriz Impacto x Probabilidade

Legenda		Probabilidade				
Extremo	Alto	1 Muito baixa	2 Baixa	3 Média	4 Alta	5 Muito alta
	Médio					
	Baixo					
Impacto	5 Muito alta	5	10	15	20	25
	4 Alta	4	8	12	16	20
	3 Média	3	6	9	12	15
	2 Baixa	2	4	6	8	10
	1 Muito baixa	1	2	3	4	5

c) Matriz de Classificação de Riscos: define como os riscos serão classificados quanto à significância. A matriz de Classificação de Riscos é, na prática, uma máscara para a "Matriz Impacto x Probabilidade" e serve para categorizar os riscos identificados em "Extremo", "Alto", "Médio" ou "Baixo". Tal matriz se encontra representada na Tabela "Matriz de Classificação de Riscos", sendo passível de adequações pelos gestores de risco na elaboração do contexto específico. A análise de riscos só se completa quando se avança na análise sobre os controles adotados aos riscos inerentes. Nesse caso, avaliam-se os efeitos dos controles existentes na mitigação dos riscos.

Matriz de Classificação de Riscos

Legenda		Probabilidade				
Extremo	Alto	1 Muito baixa	2 Baixa	3 Média	4 Alta	5 Muito alta
	Médio					
	Baixo					

Impacto	5 Muito alta	Médio	Alto	Extremo	Extremo	Extremo
	4 Alta	Médio	Alto	Alto	Extremo	Extremo
	3 Média	Médio	Médio	Alto	Alto	Extremo
	2 Baixa	Baixo	Médio	Médio	Alto	Alto
	1 Muito baixa	Baixo	Baixo	Médio	Médio	Médio

d) Definição da eficácia dos controles: estabelece critérios objetivos para análise dos controles implementados e para cálculo do risco residual. A Tabela "Definição da Eficácia dos Controles" estabelece os níveis de eficácia do controle e seu respectivo multiplicador. O gestor de riscos não pode fazer adequações nessa definição.

Definição da Eficácia dos Controles

Eficácia do Controle	Situação do Controle Existente	Multiplicador do Risco Inerente
Inexistente	Ausência completa de controle.	1,00
Fraco	Controle depositado na esfera de conhecimento pessoal dos operadores do processo, em geral, realizado de maneira manual.	0,80
Mediano	Controle pode falhar por não contemplar todos os aspectos relevantes do risco ou porque seu desenho ou as ferramentas que o suportam não são adequados.	0,60
Satisfatório	Controle formalizado e sustentado por ferramentas adequadas que, embora não contemple todos os aspectos relevantes, mitiga o risco razoavelmente.	0,40
Forte	Controle formalizado que mitiga o risco associado em todos os aspectos relevantes, podendo ser enquadrado num nível de "melhor prática".	0,20

e) O valor final da multiplicação entre o valor do risco inerente e o fator de avaliação dos controles corresponde ao nível de risco residual, que é o risco a que uma organização está exposta após a implementação de ações gerenciais para o tratamento do risco.

V - A priorização de Riscos é etapa em que são definidos quais riscos terão suas respostas priorizadas, levando em consideração os níveis calculados na etapa anterior.

a) A Tabela "Diretrizes para Priorização do Tratamento de Riscos" contém as diretrizes definidas pelo Comitê Gestor para o estabelecimento do contexto geral. O gestor de riscos não pode fazer adequações nas diretrizes.

Diretrizes para Priorização do Tratamento de Riscos

Nível de Risco	Descrição	Diretriz para Resposta
Extremo	Indica um nível de risco absolutamente Inaceitável	Qualquer risco nesse nível deve ser comunicado ao Comitê Gestor e ter uma resposta imediata. Admite-se postergação de medidas somente mediante deliberação do Comitê Gestor.
Alto	Indica um nível de risco inaceitável	Qualquer risco nesse nível deve ser comunicado ao Comitê Gestor e ter uma ação tomada em período determinado. Admite-se postergação de medidas somente mediante manifestação escrita do dirigente máximo da unidade (Diretor nas Diretorias e Chefe de Gabinete no GABIN) dando ciência ao Presidente do ICMBio, que poderá avocar a decisão caso entenda oportuno ou conveniente.
Médio	Indica um nível de risco aceitável	Geralmente nenhuma medida especial é necessária, porém requer atividades de monitoramento específicas e atenção da unidade na manutenção de respostas e controles para manter o risco nesse nível, ou reduzi-lo sem custos adicionais.
Baixo	Indica um nível de risco muito baixo	É possível que existam oportunidades de maior retorno que podem ser exploradas assumindo-se mais riscos e avaliando a relação custo x benefício, como diminuir o nível de controles

VI - A etapa Definição de Respostas aos Riscos objetiva definir as estratégias e as medidas de tratamento para os riscos priorizados na etapa anterior. Cada risco priorizado deve ser relacionado a uma estratégia de tratamento.

a) A escolha da estratégia de tratamento de riscos depende do nível do risco, contexto do ICMBio ou custo do controle.

Estratégias para Tratamento do Risco

Estratégia de Tratamento	Descrição

Mitigar	Um risco normalmente é mitigado quando é classificado como “Alto” ou “Extremo”. A implementação de controles, neste caso, apresenta um custo/benefício adequado. No ICMBio, mitigar o risco significa implementar controles que possam diminuir os efeitos dos riscos.
Compartilhar	Um risco normalmente é compartilhado quando é classificado como “Alto” ou “Extremo”, mas a implementação de controles não apresenta um custo/benefício adequado. No ICMBio, pode-se compartilhar o risco por meio de terceirização ou apólice de seguro, por exemplo.
Evitar	Um risco normalmente é evitado quando é classificado como “Alto” ou “Extremo”, e a implementação de controles apresenta um custo muito elevado, inviabilizando sua mitigação, ou não há entidades dispostas a compartilhar o risco. No ICMBio, evitar o risco significa encerrar o processo organizacional. Nesse caso, essa estratégia deve ser aprovada pelo Comitê Gestor.
Aceitar	Um risco normalmente é aceito quando é classificado como “Médio” ou “Baixo”. Nessa situação, nenhum novo controle precisa ser implementado para mitigar o risco.

b) O Plano de Tratamento de riscos é especificar como as estratégias de tratamento escolhidas serão implementadas de maneira que os arranjos sejam compreendidos pelos envolvidos, e o progresso em relação ao Plano possa ser monitorado. Esta etapa deverá ser executada a partir da criação de um Plano de Tratamento construído tendo por base a ferramenta 5W2H, conforme a Tabela "Plano de Tratamento do Risco".

Plano de Tratamento do Risco

Estratégia de Tratamento	Medidas de Tratamento	Ações	Unidade Responsável	Pessoa Responsável	Data de Início	Data de Conclusão	Situação(a ser iniciada, em andamento)

VII - A Comunicação e Monitoramento é etapa que ocorre durante todo o processo de gerenciamento de riscos e é responsável pela integração de todas as instâncias envolvidas, bem como pelo monitoramento contínuo da própria gestão de riscos, com vistas à sua melhoria.

a) A comunicação consiste em um processo contínuo e iterativo que a organização realiza para fornecer, compartilhar ou obter informações necessárias para dialogar com as partes interessadas, relacionadas com a gestão de riscos. O monitoramento compreende o acompanhamento e a verificação do desempenho ou da situação de elementos da gestão de riscos e deve ser realizado principalmente pela unidade responsável pelo processo organizacional, de forma a:

- b) garantir que os controles sejam eficazes e eficientes;
- c) analisar as ocorrências dos riscos;
- d) detectar mudanças que possam requerer revisão dos controles e/ou do Plano de Tratamento; e
- e) identificar os riscos emergentes.

10. MONITORAMENTO E AUDITORIAS

10.1. As auditorias ordinárias ou extraordinárias serão coordenadas pelo Gestor de Segurança da Informação e os relatórios serão encaminhados ao Comitê de Segurança da Informação e Comitê de Governança Digital.

10.2. As auditorias extraordinárias deverão ser precedidas de autorização do Comitê de Segurança da Informação.

10.3. Os procedimentos constantes desta norma deverão ter monitoramento contínuo da área de tecnologia da informação visando a melhoria contínua.

11. ATUALIZAÇÃO DA NORMA

11.1. O disposto na presente norma será atualizado sempre que alterados os procedimentos de Gestão de Riscos de TI, observada, ainda, a periodicidade prevista para a revisão da Política de Segurança da Informação.

LUIS GUSTAVO BIAGIONI

Presidente Substituto



Documento assinado eletronicamente por **Luis Gustavo Biagioni, Presidente Substituto**, em 10/08/2022, às 18:58, conforme art. 1º, III, "b", da Lei 11.419/2006.



A autenticidade do documento pode ser conferida no site <https://sei.icmbio.gov.br/autenticidade> informando o código verificador **11778168** e o código CRC **95D1D792**.



MINISTÉRIO DO
MEIO AMBIENTE



MINISTÉRIO DO MEIO AMBIENTE
INSTITUTO CHICO MENDES DE CONSERVAÇÃO DA BIODIVERSIDADE
GABINETE DA PRESIDÊNCIA

EQSW 103/104, Bloco "C", Complexo Administrativo - Bloco C - Bairro Setor Sudoeste - Brasília - CEP 70670-350

Telefone: (61) 2028-9011/9013

ANEXOS IV - NORMA DE SEGURANÇA DA INFORMAÇÃO (NSI)

NSI 004/2022 - USO DE RECURSOS DE TECNOLOGIA DA INFORMAÇÃO E CONTROLE DE ACESSO

1. OBJETIVOS

1.1. Estabelecer diretrizes e padrões para: Uso de Recursos de Tecnologia da Informação e Controle de Acesso, no âmbito do Instituto Chico Mendes de Conservação da Biodiversidade - ICMBio.

2. MOTIVAÇÕES

- 2.1. Alinhamento as normas, regulamentações e melhores práticas, relacionadas a matéria.
- 2.2. Proteção da Rede Nacional de Computadores do ICMBio.
- 2.3. Garantia de que os acessos aos recursos tecnológicos sejam feitos de forma segura e controlada.
- 2.4. Correto direcionamento e dimensionamento de recursos tecnológicos para apoiar as atividades laborais dos servidores e colaboradores.
- 2.5. Necessidade de um processo sistemático para gerenciar o uso de recursos de Tecnologia da Informação, visando garantir a segurança e a integridade dos dados.
- 2.6. Orientações gerais para gestores e usuários de serviços de Tecnologia da Informação, lotados em todas as outras Unidades do ICMBio.

3. REFERÊNCIAS NORMATIVAS

- 3.1. Instrução Normativa nº 1, de 27 maio de 2020, do Gabinete de Segurança Institucional da Presidência da República, que dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal;
- 3.2. Instrução Normativa GSI/PR nº 3, de 28 de maio de 2021, que dispõe sobre os processos relacionados à gestão de segurança da informação nos órgãos e nas entidades da administração pública federal.
- 3.3. Instrução Normativa GSI/PR nº 5, de 30 de agosto de 2021, que dispõe sobre os requisitos mínimos de segurança da informação para utilização de soluções de computação em nuvem pelos órgãos e pelas entidades da administração pública federal.
- 3.4. Instrução Normativa GSI/PR nº 6, de 23 de dezembro de 2021, que estabelece diretrizes de segurança da informação para o uso seguro de mídias sociais nos órgãos e nas entidades da administração pública federal.
- 3.5. Norma Complementar nº 07/IN01/DSIC/GSIPR, de 15 de julho de 2014, do Departamento de Segurança da Informação e Comunicações da Presidência da República, que estabelece diretrizes para a implementação de controles de acesso à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta.
- 3.6. Norma Complementar nº 12/IN01/DSIC/GSIPR, de 30 de janeiro de 2012, que estabelece diretrizes para o Uso de Dispositivos Móveis nos Aspectos relativos à Segurança da Informação e Comunicações nos órgãos e entidades da Administração Pública Federal.
- 3.7. Norma Complementar nº 21/IN01/DSIC/GSIPR, de 08 de outubro de 2014, que estabelece as Diretrizes para o Registro de Eventos, Coleta e Preservação de Evidências de Incidentes de Segurança em Redes no direta e indireta.
- 3.8. Norma Técnica ABNT NBR ISO/IEC 27001:2013, que especifica os requisitos para estabelecer, implementar, manter e melhorar um Sistema de Gestão de Segurança da Informação.
- 3.9. Norma Técnica ABNT NBR ISO/IEC 27002:2013, que fornece diretrizes para práticas de gestão de segurança da informação.
- 3.10. Norma Técnica ISO/IEC 27000:2018, que especifica conceitos e definições relacionados às normas de segurança da informação.
- 3.11. Instrução Normativa nº 1, de 04 de abril de 2019, que dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação - TIC pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal.

4. CONCEITOS E DEFINIÇÕES

- 4.1. Acesso privilegiado: nível de acesso restrito onde uma pessoa tem permissão para gerenciar um sistema e/ou serviço.
- 4.2. Arquivo de registro de mensagens (logs): registro de eventos relevantes, utilizados para restaurar um sistema, diagnosticar problemas ou realizar auditorias.
- 4.3. Código malicioso: termo comumente utilizado para genericamente se referir a programas desenvolvidos para executar ações danosas e atividades maliciosas em um computador ou dispositivo móvel. Tipos específicos de códigos maliciosos são: vírus, worm, bot, spyware, backdoor, cavalo de troia e rootkit.
- 4.4. Computador servidor: Computador com alta capacidade de armazenamento e processamento, destinado ao provimento de serviços e sistemas de TI.

- 4.5. Controle de acesso: métodos para garantir que o acesso aos ativos seja autorizado e restrito com base nas necessidades de negócio e em segurança.
- 4.6. Domínio: Parte final do endereço eletrônico, localizada após o símbolo de arroba (@).
- 4.7. Dispositivo móvel: Equipamento portátil dotado de capacidade computacional que permite conexão à rede cabeada ou à rede sem-fio, podendo acessar recursos de rede e internet. São exemplos: smartphones, notebooks e tablets, dentre outros.
- 4.8. Endereço Eletrônico: Conjunto de caracteres que individualiza e identifica o remetente e o destinatário da mensagem eletrônica. É formado por um identificador e por um domínio, separados pelo símbolo de arroba (@).
- 4.9. Firewall: Dispositivo de segurança da rede que monitora o tráfego de rede de entrada e saída e decide permitir ou bloquear tráfegos específicos de acordo com um conjunto definido de regras de segurança.
- 4.10. Gestor da Unidade: Coordenador Geral, Coordenador, Chefe de divisão, Chefe de serviço ou servidor designado para res
- 4.11. Identificadora: Parte inicial do endereço eletrônico, localizada antes do símbolo de arroba (@), que o diferencia das demais caixas postais e identifica seu usuário, setor
- 4.12. Hoax: Mensagem eletrônica encaminhada a muitos destinatários, de conteúdo geralmente alarmante e com pouca ou nenhuma veracidade, cujo objetivo é a propagação de boatos e informações distorcidas.
- 4.13. Lista de distribuição: Agrupamento de diversos endereços eletrônicos, representado por um endereço eletrônico específico, que permite a distribuição conjunta de uma mensagem eletrônica a todos os seus integrantes.
- 4.14. Malware: Programas indesejados, desenvolvidos com a finalidade de executar ações danosas e atividades maliciosas em um computador ou sistema (ex.: worm, bot, spyware, backdoor, cavalo de troia, ransomware e rootkit).
- 4.15. Material criptografado: Dados e/ou informações codificadas por meio de técnicas que impossibilitam o seu entendimento/leitura, cuja reversão ocorre somente com a utilização de uma senha previamente conhecida e/ou dispositivo criptográfico (ex.: token, smart card).
- 4.16. Phishing: Fraude eletrônica, caracterizada pela tentativa de obtenção de dados e informações pessoais com o uso de meios técnicos e de engenharia social.
- 4.17. Proprietário do ativo de informação: Pessoa ou outra entidade que tem a responsabilidade (aprovação pela administração) para qualificar o ciclo de vida de um ativo.
- 4.18. Proxy: Também conhecido por filtro de conteúdo, é o servidor responsável por intermediar o acesso à internet, aplicand
- 4.19. Proxy externo: São servidores não administrados pelo ICMBio, responsáveis por intermediar o acesso à internet, que não acesso e mecanismos de proteção da mesma forma que o proxy administrado pelo ICMBio.
- 4.20. Rede Nacional de Computadores do ICMBio: Infraestrutura de Rede de computadores conectados via MPLS ou VPN *Site-to-Site*.
- 4.21. Rede cabeada: Corresponde ao acesso dos recursos tecnológicos e à transmissão de dados através da utilização de meios físicos (ativos de distribuição de dados, cabos e pontos de rede).
- 4.22. Rede lógica: É a rede de dados utilizada pelo ICMBio, abrangendo serviços e sistemas de tecnologia da informação, rede cabeada, rede sem-fio, ativos de distribuição de dados e equipamentos conectados nessa rede.
- 4.23. Rede sem fio: Também conhecida como rede wireless ou wi-fi, corresponde ao acesso aos recursos tecnológicos e à transmissão de dados sem a utilização de meios físicos (cabamento), através da u
- 4.24. Remoção de acesso: Processo que tem por finalidade remover/excluir definitivamente ou parcialmente determinado(s) acesso(s).
- 4.25. Serviço de correio eletrônico institucional: Serviço de envio e recebimento de mensagens eletrônicas (e-mail) no âmbito do ICMBio.
- 4.26. SISP: Sistema de Administração dos Recursos de Tecnologia da Informação do Poder Executivo Federal.
- 4.27. Sistema Eletrônico de Informações (SEI): ferramenta de gestão de documentos e processos eletrônicos com o objetivo de O SEI integra o Processo Eletrônico Nacional (PEN), uma iniciativa conjunta de órgãos e entidades de diversas esferas da administração pública, com o intuito de construir uma infraestrutura pública de processos e documentos administrativos eletrônico.
- 4.28. Sítio: É um conjunto de páginas web organizadas a partir de um URL básico, onde fica a página principal, e geralmente são armazenadas numa única pasta ou subpastas relacionadas no mesmo diretório de um servidor.
- 4.29. Situação de contingência: Estado ou condição na qual exista a ocorrência de falha/problema, em um ou mais recursos tecnológicos, que reduzam a capacidade dos sistemas e serviços que suportam a atividade da organização.
- 4.30. Solução baseada em nuvem: Modelo computacional que permite acesso por demanda e independente da localização a recursos configuráveis de computação (rede de computadores, servidores, armazenamento, aplicativos e serviços), provisionados com esfor
- 4.31. Spam: Mensagem enviada a um grande número de endereços eletrônicos, que não possua caráter institucional e/ou cujo objeto não seja inerente à atividade funcional do usuário ou da unidade.
- 4.32. Usuários: Colaborador ou estagiário, servidores ocupantes de cargo efetivo ou em comissão, requisitados e cedidos, e, autorizados, empregados de empresas prestadoras de serviços terceirizados, consultores, estagiários e outras pessoas que se encontrem a
- 4.33. VPN Client to Site: Conexão remota segura entre o Usuário/Cliente e o Datacenter.
- 4.34. VPN Site to Site: Conexão remota segura entre redes internas.

5. DIRETRIZES

5.1. RECURSOS DE TECNOLOGIA DA INFORMAÇÃO:

- 5.1.1. O uso adequado dos recursos de tecnologia da informação visa a garantir a continuidade das atividades desenvolvidas no âmbito de todas as unidades do ICMBio.
- 5.1.2. Os recursos de tecnologia da informação disponibilizados pelo ICMBio aos usuários serão utilizados em atividades relacio
- 5.1.2.1. os computadores servidores, os computadores para uso individual ou coletivo, de qualquer porte, os equipamentos de armazenamento e distribuição de dados, os dispositivos móveis, as impressoras, as copiadoras e os equipamentos multifuncionais, assim como os respectivos suprimentos periféricos e acessórios;
- 5.1.2.2. a rede lógica do ICMBio e os respectivos canais e pontos de distribuição;

5.1.2.3.as contas de acesso dos usuários, assim como os certificados digitais;

5.1.2.4.os sistemas computacionais desenvolvidos com base nos recursos providos pelo ICMBio ou de parceiros em prol do Instituto;

5.1.2.5.os sistemas computacionais contratados de terceiros, sob licença ou na forma de software livre ou aberto, incluídas as soluções baseadas em nuvem;

5.2.A utilização dos recursos de tecnologia, com finalidade pessoal, é permitida, desde que seja em um nível mínimo e que não viole a Política, as Normas Complementares e o Código de Ética dos Servidores Públicos Federais.

5.3.O usuário de equipamento de propriedade do ICMBio deve assinar termo de guarda e uso.

5.4.Os servidores e demais colaboradores, ao solicitar o empréstimo de equipamentos portáteis do ICMBio localizados na sede em Brasília, deve assinar o Termo de Responsabilidade.

5.5.As transferências de equipamentos portáteis da Sede do ICMBio para as demais unidades do Instituto devem ser acompanhadas da assinatura de Termo de Responsabilidade pelo receptor e a respectiva transferência de patrimônio para a cidade unidade;

5.6.O usuário deve evitar armazenar informações confidenciais em equipamentos portáteis do ICMBIO.

6. RESPONSABILIDADES DOS USUÁRIOS

6.1. O usuário é responsável por:

6.1.1.zelar pelos recursos que lhe sejam destinados para o exercício de suas atribuições, especialmente os de utilização

6.1.2.preservar o sigilo de sua senha ou outro mecanismo de autenticação que venha a ser utilizado para acesso aos recursos tecnológicos disponibilizados;

6.1.3.não compartilhar sua senha para utilização de terceiros;

6.1.4.preservar o sigilo das informações a que tiver acesso, sendo vedada sua revelação a usuários ou terceiros

6.1.5.responder por atos praticados e acessos realizados aos recursos de tecnologia por meio de sua credencial de acesso.

7. SUPORTE TÉCNICO

7.1.Os procedimentos de instalação, configuração e manutenção de equipamentos e softwares serão realizados pela área de TI do Instituto ou por terceiros por ela autorizados, sob a supervisão do gestor da unidade, que verificará a adequação do serviço realizado ao atendimento das atividades desenvolvidas pela unidade.

7.2.Não será fornecido suporte técnico a equipamentos particulares (computadores, notebooks, e tablets).

7.3.Quanto aos softwares e recursos disponibilizados pelo ICMBIO que sejam autorizados para uso em equipamentos particulares, o suporte técnico se limitará a disponibilização de manuais e orientações aos usuários para que os mesmos efetuem os procedimentos em seus equipamentos (procedimentos de instalação de aplicativos de governo para smartphone e certificados digitais, por exemplo).

7.4.Os equipamentos institucionais, servidores e os computadores para uso individual ou coletivo, de qualquer porte, serão dotados de mecanismos de proteção contra malwares.

8. REDE LÓGICA

8.1.Todas as unidades do ICMBio devem, preferencialmente, dispor de rede lógica cabeada estruturada com capacidade para oferecer conexão individual para cada estação de trabalho a um concentrador.

8.2.Todos os equipamentos e dispositivos conectados à rede lógica de dados do ICMBio terão seus acessos registrados e monitorados por questões de segurança e para fins de auditoria.

8.3.É proibida a conexão de qualquer dispositivo não fornecido pelo ICMBio na rede cabeada do Instituto, sem a prévia anuência da Área de TI.

8.4.As intervenções no ambiente de rede somente serão permitidas mediante supervisão pelos técnicos autorizados pela Área de Tecnologia da Informação.

8.5.Os ativos de rede somente devem ser liberados para uso após a efetiva homologação, realizada em ambiente apropriado, distinto do ambiente de produção, e devidamente documentado.

9. SERVIDORES

9.1.Todo equipamento servidor de rede deve estar, preferencialmente, instalado em salas adequadas para este fim.

9.2.Somente os técnicos autorizados deverão ter acesso aos servidores.

9.3.O usuário somente terá acesso ao servidor de rede se atender aos seguintes requisitos:

9.3.1.Solicitação formal à área de tecnologia da informação com a justificativa e finalidade do acesso pretendido;

9.3.2.Avaliação e aprovação pela Área de Tecnologia;

9.4.Todos os servidores de rede devem utilizar os sistemas operacionais atualizados.

9.5.A atualização dos servidores de rede deverá ser realizada pelos técnicos autorizados.

10. REDE SEM FIO

10.1.A área de tecnologia da informação do ICMBio disponibilizará acesso à rede sem fio para usuários internos e externos.

10.2.A conexão para os usuários internos será feita por meio da credencial (nome de usuário e senha) utilizada para o acesso à rede, e para os usuários externos será feita mediante cadastramento prévio

10.2.1.é permitida a conexão de dispositivos móveis particulares nas redes sem fio administradas pelo ICMBio;

10.2.2.O acesso à internet por meio das redes sem fio observará as regras dispostas no controle de acesso à internet, da Política de Segurança da Informação;

10.2.3. Por questões de segurança tecnológica, regras específicas poderão ser implementadas no acesso à internet via rede sem fio;

10.2.4. Poderão ser bloqueados os acessos à rede sem fio, temporariamente ou por tempo indeterminado, de dispositivos intencionais ou não, ou em que detectadas vulnerabilidades ou problemas de segurança tecnológica;

10.2.5. A rede destinada a uso de visitantes deverá ser isolada da rede de usuários comuns.

11. ARMAZENAMENTO DE DADOS

11.1. A área de tecnologia da informação do ICMBio deverá disponibilizar espaço de armazenamento em rede para salvaguardar os arquivos relacionados ao trabalho desenvolvido, com garantia de integridade, disponibilidade, controle de acesso e cópia de segurança.

11.2. Os dados armazenados nas estações de trabalho dos usuários não estão contemplados pelas garantias mencionadas cabendo aos usuários providenciar eventual cópia de segurança e a eliminação periódica dos arquivos armazenados nos discos rígidos locais

11.3. É proibido o armazenamento, em qualquer diretório na rede do ICMBio ou nas soluções baseadas em nuvem, de arquivos não relacionados ao trabalho, tais como:

11.3.1. fotos, músicas e filmes de qualquer formato;

11.3.2. programas não homologados ou não licenciados;

11.3.3. programas de conteúdo prejudicial à segurança do parque computacional do ICMBio.

12. NUVEM CORPORATIVA

12.1. É vedado o armazenamento, na nuvem corporativa ou em diretórios da rede ICMBio, de arquivos cuja criação e edição sejam efetuados em sistemas próprios, tais como: despachos, ofícios, processos, e demais documentos que são elaborados e armazenados no Sistema Eletrônico de Informações - SEI/ICMBio ou sistema que o substitua.

12.2. Os arquivos institucionais das unidades administrativas e finalísticas deverão ser armazenados, preferencialmente em espaço disponibilizados na nuvem corporativa do Instituto.

12.3. Os arquivos armazenados na nuvem corporativa deverão ser vinculados (ter como proprietário) à caixa postal institucional.

13. EQUIPAMENTOS FORNECIDOS PELO ICMBIO

13.1. O fornecimento de equipamentos a servidores e colaboradores, quando autorizado, está condicionado às necessidades de

13.2. Estação de Trabalho portátil (notebook, tablets).

13.2.1. Os computadores portáteis serão fornecidos com instalação padrão desenvolvida pelo ICMBio, composta por software e suporte ao desempenho das funções de trabalho, além de softwares para proteção, monitoramento e auditoria do equipamento;

13.2.2. Os problemas de software serão solucionados pela reinstalação padrão desenvolvida pelo ICMBio, que fica desobrigado de reinstalar e configurar programas que o usuário tenha instalado por iniciativa própria e isento da responsabilidade sobre eventual perda de dados;

13.2.3. Para a instalação de aplicativos e recursos, sempre que possível, o usuário deverá solicitar apoio da equipe de suporte técnico do ICMBio;

13.2.4. A instalação, manutenção e suporte de qualquer software/sistema não fornecido pelo ICMBio, bem como o backup

13.2.5. Em caso de falecimento, aposentadoria, exoneração, demissão, cedência, remoção, redistribuição, dispensa de serviço ao ICMBio, com todos os acessórios que o acompanharam, no prazo de 20 dias, se outro prazo não houver sido estipulado em norma específica;

13.2.6. Nos casos de perda, furto ou roubo do equipamento, bem como nas hipóteses de ausência de devolução ou verificação de existência de avarias no equipamento devolvido, a área de tecnologia da informação informará à CGATI a situação ocorrida, com a documentação respectiva, para as providências cabíveis;

14. ESTAÇÃO DE TRABALHO DESKTOP

14.1. Os desktops serão fornecidos com instalação padrão desenvolvida pelo ICMBio, composta por softwares e aplicativos necessários ao desempenho das funções de trabalho, além de softwares para proteção, monitoramento e auditoria do equipamento.

14.2. Sempre que disponíveis pontos lógicos fisicamente, os desktops deverão ser conectados a rede cabeada e separados por VLAN criada especificamente para esta finalidade;

14.3. Toda aquisição de estações de trabalho com recursos do ICMBio deve ser realizada pela Área de Tecnologia da Informação.

14.4. Toda aquisição de estações de trabalho com recursos extra orçamentários deve ser submetida para análise prévia da Área de Tecnologia da Informação.

14.5. A troca de peças e componentes das estações de trabalho e demais equipamentos de Tecnologia da Informação, somente será efetuada pela Área de Tecnologia da Informação ou por profissional indicado por ela.

14.6. A área de Tecnologia da Informação deverá disponibilizar equipamentos adequados às necessidades das áreas requisitantes, para tanto, caberá à coordenação:

14.6.1. Elaborar especificações técnicas padronizadas para atender as necessidades das atividades laborais dos servidores e colaboradores do ICMBio;

14.6.2. Disponibilizar modelos de estações de trabalho padronizadas classificando-as em pelo menos três modelos (exemplo: Desktop Básico, Desktop Intermediário e Desktop de Alto Desempenho);

14.6.3. Quando viável tecnicamente, efetuar o aproveitamento de peças e componentes disponíveis para a realização de upgrade de equipamentos para atender as necessidades das áreas requisitantes.

15. LICENÇAS E SOFTWARES

15.1.As licenças de softwares, de qualquer natureza, contratadas ou adquiridas pelo ICMBio são de uso institucional.

15.2.É proibida a instalação de softwares não licenciados ou não homologados pela área de tecnologia da informação nos equipamentos conectados à rede do Instituto.

15.2.1.A instalação de softwares não homologados poderá ser autorizada excepcionalmente pela área de tecnologia da informação, desde que demonstrada a necessidade de sua utilização para o desempenho das atribuições funcionais do usuário, observadas computacionais disponibilizados pelo ICMBio;

15.2.2.As unidades organizacionais do ICMBio poderão encaminhar à Área de Tecnologia da Informação pedido de homologação de softwares, para o uso em suas atividades;

15.2.3.Homologado o uso, o software poderá integrar a formatação padrão utilizada na configuração dos novos equipamentos;

15.2.4.Toda aquisição de licença de software deve ser informada pelo gestor da unidade à Área de Tecnologia da Informação para documentação e atualização do inventário de softwares do ICMBio.

16. CONTROLE DE ACESSO

16.1.Para ter acesso aos recursos de tecnologia da informação disponibilizados pelo ICMBio, é necessário que o usuário possua uma conta de rede.

16.2.A identificação do usuário será composta pelo CPF do servidor, estagiário ou colaborador.

16.3.A cada conta de acesso será associada uma senha, de uso pessoal e intransferível.

16.4.Os acessos à rede, serviços e aos sistemas computacionais disponibilizados pelo ICMBio serão solicitados à Área de Tecnologia da Informação, por meio de formulário específico no SEI/ICMBio ou por meio do sistema de atendimento, em que devem ser registrados os níveis de acesso adequados às atividades desenvolvidas.

16.5.Incumbem à chefia imediata e aos gestores de equipes, solicitar à Área de Tecnologia da Informação:

16.5.1.os acessos necessários ao desenvolvimento das atividades dos servidores, estagiários e demais colaboradores vinculados a sua unidade;

16.5.2.a alteração dos níveis de acesso ou a remoção do acesso a sistemas concedidos a servidores, estagiários e demais colaboradores da unidade, sempre que necessária sua adequação às atividades desenvolvidas;

16.5.3.a remoção dos acessos concedidos a servidores, estagiários e demais colaboradores da unidade, imediatamente após o afastamento ou desligamento da unidade.

16.6.Não solicitada a alteração ou exclusão no momento oportuno, a chefia poderá ser responsabilizada pelo acesso indevido dos servidores, estagiários e demais colaboradores a informações da unidade.

16.7. Coordenação Geral de Gestão de Pessoas - CGGP deverá informar a Área de Tecnologia da Informação quando da ocorrência de atos que encerrem o vínculo de servidores e estagiários com o ICMBio, para que sejam efetuados os procedimentos de descredenciamento destes usuários da rede ICMBio.

16.8.Os gestores de contratos de terceirização deverão informar, no prazo máximo de 5 (cinco) dias úteis, quando da ocorrência de atos que encerrem o vínculo do colaborador terceirizado com o ICMBio, para que sejam efetuados os procedimentos de descredenciamento destes usuários da rede ICMBio.

16.9.A Área de Tecnologia da Informação comunicará à unidade respectiva sobre a efetivação do cadastro, fornecendo as informações necessárias ao acesso, e encaminhará a Política de Segurança da Informação, em formato eletrônico, para a caixa postal institucional pessoal do usuário para ciência.

16.10.As solicitações de acessos de prestadores de serviço aos recursos tecnológicos do ICMBio terão caráter temporário e deverão ser acompanhadas da respectiva justificativa, bem como do prazo previsto.

17. SENHAS DE USUÁRIOS

17.1.As novas senhas (PROVISÓRIAS) solicitadas serão fornecidas por meio de comunicação eletrônica para a caixa postal usuário ou para caixa postal institucional pessoal do usuário, proibido o fornecimento de senhas por qualquer outro meio, inclusive telefone.

17.2.É responsabilidade do usuário a alteração da senha inicial fornecida pela Área de Tecnologia da Informação no primeiro acesso realizado.

17.3.O privilégio de administrador na estação de trabalho é restrito aos membros da equipe técnica da Área de Tecnologia que necessitem de acesso privilegiado para o desempenho das atividades funcionais.

17.4.Nos computadores portáteis disponibilizados pelo ICMBio aos servidores, estes terão privilégio de administrador local.

17.5.Os acessos privilegiados aos sistemas e serviços de TI serão concedidos aos membros da equipe técnica da Área de Tecnologia, sempre que necessários ao desempenho das atividades funcionais, de modo a permitir a gestão e configuração do ambiente tecnológico.

17.6.Na utilização das credenciais de acesso, compete ao usuário observar os procedimentos a seguir indicados, bem como adotar outras medidas de segurança de caráter pessoal, com vista a impedir o uso não autorizado dos recursos de tecnologia da informação a partir de sua conta de acesso:

17.6.1.não compartilhar a senha com outras pessoas;

17.6.2.não armazenar senhas em local acessível por terceiros;

17.6.3.não utilizar senhas de fácil dedução como as que contém nomes próprios e de familiares, datas festivas e sequências numéricas;

17.6.4.ao ausentar-se de sua estação de trabalho, ainda que temporariamente, o usuário deverá encerrar ou bloquear a sessão;

17.7.A senha de rede deverá contemplar os seguintes requisitos:

17.7.1.ter, no mínimo, 8 (oito) caracteres;

17.7.2.não conter o nome de usuário (login) de rede;

17.7.3.conter letras maiúsculas e minúsculas;

17.7.4. conter ao menos um caractere especial: (ex. @#!&%).

17.8. Não poderão ser utilizadas as 10 (dez) últimas senhas de rede definidas pelo(a) usuário(a).

17.9. A conta do usuário será bloqueada após 10 (dez) tentativas consecutivas de acesso não reconhecidas, considerando também as tentativas inválidas de acesso à rede sem fio.

17.10. A senha de rede definida pelo usuário expirará em 120 (cento e vinte) dias.

17.11. Em caso de suspeita de comprometimento da senha ou de outro recurso de autenticação, o usuário comunicará imediatamente a área de tecnologia da informação, que poderá, como medida preventiva, suspender temporariamente o acesso.

18. SENHAS DE USO PRIVILEGIADO:

18.1. Todas as contas privilegiadas (ex: administrador, asgv, root, etc.) devem ter as senhas trocadas, renomeadas e desabilitadas.

18.2. Os acessos privilegiados, por questões de segurança, devem ser realizados por uma quantidade mínima de usuários, que

18.3. Caso as contas privilegiadas não possam ter as senhas trocadas ou renomeadas, serão desabilitadas e consideradas "contas de serviço" não sendo utilizadas para qualquer tipo de acesso;

18.4. As senhas não devem ser introduzidas em linhas de comando (códigos fontes) e ou em scripts abertas, mas, caso seja necessário, devem ser criptografadas e consideradas "contas de serviço";

18.5. Todas as senhas em trânsito, ou seja, que sejam trafegadas pela rede obrigatoriamente deverão estar encriptadas;

18.6. Usuários de contas privilegiadas deverão utilizar senhas fortes e duplo fator de autenticação.

19. REGISTRO DE EVENTOS

19.1. Serão mantidos, por um período mínimo de 3 (três) meses, os registros dos acessos dos usuários e dos acessos privilegiados no ICMBio, inclusive para fins de apuração e comprovação de incidentes de segurança.

19.2. Serão registrados os seguintes dados:

19.2.1. identificação de usuário de quem efetuou o acesso;

19.2.2. data e hora de entrada e saída do sistema;

19.2.3. origem do acesso;

19.2.4. erros ou falhas de conexão e acesso;

19.2.5. troca de senhas de Serviços de Infraestrutura de TI;

19.2.6. outras informações que venham a ser necessárias para os controles de segurança.

20. MONITORAMENTO E AUDITORIAS

20.1. As auditorias ordinárias ou extraordinárias serão coordenadas pelo Gestor de Segurança da Informação e os relatórios serão encaminhados ao Comitê de Segurança da Informação e Comitê de Governança Digital.

20.2. As auditorias extraordinárias deverão ser precedidas de autorização do Comitê de Segurança da Informação.

20.3. Os procedimentos constantes desta norma deverão ter monitoramento contínuo da área de tecnologia da informação visando

21. ATUALIZAÇÃO DA NORMA

21.1. O disposto na presente norma será atualizado sempre que alterados os procedimentos da Gestão de Incidentes de Segurança da Informação, observada, ainda, a periodicidade prevista para a revisão da Política;

LUIS GUSTAVO BIAGIONI

Presidente Substituto



Documento assinado eletronicamente por **Luis Gustavo Biagioni, Presidente Substituto**, em 10/08/2022, às 18:59, conforme art. 1º, III, "b", da Lei 11.419/2006.



A autenticidade do documento pode ser conferida no site <https://sei.icmbio.gov.br/autenticidade> informando o código verificador **11778344** e o código CRC **1FA435C3**.



MINISTÉRIO DO
MEIO AMBIENTE



MINISTÉRIO DO MEIO AMBIENTE
INSTITUTO CHICO MENDES DE CONSERVAÇÃO DA BIODIVERSIDADE
GABINETE DA PRESIDÊNCIA

EQSW 103/104, Bloco "C", Complexo Administrativo - Bloco C - Bairro Setor Sudoeste - Brasília - CEP 70670-350

Telefone: (61) 2028-9011/9013

ANEXOS V - NORMA DE SEGURANÇA DA INFORMAÇÃO (NSI)
NSI 005/2022 - CONTROLE DE ACESSO À INTERNET E À INTRANET

1. OBJETIVOS

1.1. Estabelecer diretrizes e padrões para o acesso à internet e à intranet no âmbito do Instituto Chico Mendes de Conservação da Biodiversidade - ICMBio.

2. MOTIVAÇÕES

2.1. Alinhamento às normas, regulamentações e melhores práticas relacionadas à matéria.

2.2. Proteção da Rede Nacional de Computadores do ICMBio.

2.3. Correto direcionamento e dimensionamento de recursos tecnológicos para prover o serviço de acesso à internet.

2.4. Orientações gerais para gestores e usuários de serviços de Tecnologia da informação, lotados em todas as outras Unidades do ICMBio.

3. REFERÊNCIAS NORMATIVAS

3.1. Instrução Normativa nº 1, de 27 de maio de 2020, do Gabinete de Segurança Institucional da Presidência da República, que dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal.

3.2. Instrução Normativa GSI/PR nº 6, de 23 de dezembro de 2021 que estabelece diretrizes de segurança da informação para o uso seguro de mídias sociais nos órgãos e nas entidades da administração pública federal.

3.3. Norma Complementar nº 07/IN01/DSIC/GSIPR, de 15 de julho de 2014, do Departamento de Segurança da Informação e Comunicações da Presidência da República, que estabelece diretrizes para a implementação de

controles de acesso à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta.

3.4.Norma Técnica ABNT NBR ISO/IEC 27001:2013, que especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação dentro do contexto da organização.

3.5.Norma Técnica ABNT NBR ISO/IEC 27002:2013, que fornece diretrizes para práticas de gestão de segurança da informação.

3.6.Instrução Normativa nº 1, de 04 de abril de 2019, que dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação - TIC pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISF do Poder Executivo Federal.

4. CONCEITOS E DEFINIÇÕES

4.1.Arquivo de registro de mensagens (logs): registro de eventos relevantes, utilizados para restaurar um sistema, diagnosticar problemas ou realizar auditorias;

4.2.Código malicioso: termo comumente utilizado para genericamente se referir a programas desenvolvidos para executar ações danosas e atividades maliciosas em um computador ou dispositivo móvel. Tipos específicos de códigos maliciosos são: vírus, worm, phishing, spyware, backdoor, cavalo de troia e rootkit;

4.3.DATA LOST PREVENTION (DLP): prevenção de perda de dados;

4.4.Firewall: Dispositivo de segurança da rede que monitora o tráfego de rede de entrada e saída e decide permitir ou bloquear tráfegos específicos de acordo com um conjunto definido de regras de segurança;

4.5.Proxy: também conhecido por filtro de acesso, é o servidor responsável por intermediar o acesso à internet, aplicando regras de controle de acesso e mecanismos de proteção contra códigos maliciosos, previamente configurados, e por controlar a alocação de recursos de rede;

4.6.Redes Nacionais de Computadores do ICMBio: Infraestrutura de Rede de computadores conectados;

4.7.SISF: Sistema de Administração dos Recursos de Tecnologia da Informação do Poder Executivo Federal;

4.8.Portal: É um conjunto de páginas web organizadas a partir de uma URL básico, onde fica a página principal;

4.9.Situação de contingência: estado ou condição na qual exista a ocorrência de falha/problema, suportados pela situação de redundância;

4.10.Situação de redundância: estado ou condição em que exista duplicação de um ou mais recursos tecnológicos;

4.11.VPN Client to Site: Conexão remota segura entre o Usuário/Cliente e o Datacenter;

4.12.VPN Site to Site: Conexão remota segura entre redes internas;

5. DIRETRIZES

5.1.O acesso à internet e à intranet dar-se-á, exclusivamente, pelos meios autorizados, configurados pela área de tecnologia;

5.2.O acesso à internet é disponibilizado pelo ICMBio para uso nas atividades relacionadas ao trabalho, observado o disposto na Política de Segurança da Informação do ICMBio e anexos.

5.3.É expressamente proibido:

5.3.1.Utilização intencional de aplicações ou serviços para burlar as ferramentas de controle e segurança do ICMBio;

5.3.2.Utilização de proxies externos ou similares, sem a autorização da Área de tecnologia;

5.3.3.Utilizar programas de troca de mensagens em tempo real (bate-papo) ou programas para troca de conteúdo via rede ponto-a-ponto (peer-to-peer), exceto programas homologados pela área de tecnologia ou autorizados pelo Comitê de Segurança da Informação;

5.3.4.Utilizar programas e/ou acessar páginas de áudio e vídeo em tempo real, ou sob demanda que não estejam relacionados às atividades laborais, exceto programas homologados pela área de tecnologia ou autorizados pelo Comitê de Segurança da Informação;

5.3.5.Acessar sítios que representem ameaça de segurança ou que possam comprometer de alguma forma a integridade da rede de computadores do ICMBio;

5.3.6.As contas de usuários deverão ter níveis de acesso distintos, conforme a necessidade dos serviços, de acordo com os perfis definidos pela setor solicitante;

5.3.7.Acessar ou fazer download de arquivos não relacionados ao trabalho, em especial músicas, imagens, vídeos, jogos e programas de qualquer tipo;

5.3.8.A liberação de acesso a sítios e serviços bloqueados, quando necessários ao desempenho das atribuições funcionais do usuário, dependerá de solicitação, devidamente justificada, à área de tecnologia da informação, que a submeterá, quando for o caso, ao Comitê de Segurança da Informação para deliberação;

5.3.9.Acessar páginas de conteúdo considerado ofensivo, ilegal, impróprio ou incompatível com as atividades funcionais tais como: pornografia, pedofilia, racismo, jogos e páginas de distribuição e de compartilhamento de software

5.3.10.Cada usuário é responsável pelas ações e acessos realizados por meio da sua Conta de Acesso;

5.3.11.As aplicações a serem disponibilizadas na Intranet devem ser previamente analisadas, homologadas e aprovadas pela DCOM;

5.3.12.As contas com privilégio de administração de rede devem ser utilizadas somente para execução das atividades correspondentes à administração do ambiente conforme as responsabilidades atribuídas, em equipamentos previamente definidos. As variáveis necessárias para acesso e administração devem ser de conhecimento restrito aos administradores dos equipamentos de rede e chefia respectiva;

5.3.13.Divulgação de informações confidenciais da instituição por meio de correio eletrônico, grupos ou listas de discussão, sistemas de mensageria ou bate-papo, blogs, microblogs, ou ferramentas semelhantes;

5.3.14. Desvio na finalidade de qualquer software licenciado à área de tecnologia da informação ou dados de propriedade deste instituto ou de seus usuários, salvo expressa e fundamentada autorização do responsável pela sua guarda;

5.3.14.1. A restrição de que trata o item 5.3 pode ser flexibilizada: por razão de trabalho, desde que, previamente, autorizada pelo Comitê de Segurança da Informação ou pela área de tecnologia em atendimento a processo de solicitação devidamente documentado pela área requisitante;

5.4. Todo tráfego de internet será controlado, de forma automática, e poderá ser inspecionado por soluções de segurança implementadas pela área de tecnologia (filtros de conteúdo, proxy, DLP, etc.), configuradas de acordo com os limites estabelecidos na Política de Segurança da Informação do ICMBio, normas e legislação pertinentes ao tema.

5.5. Os navegadores de Internet e Intranet utilizados no âmbito do ICMBio deverão ser homologados pela Área de Tecnologia.

5.6. As paralisações dos serviços de Internet/intranet, para manutenção preventiva, devem ser previamente divulgadas pela área de tecnologia.

5.7. Os problemas técnicos verificados pelos usuários, ocorridos durante o acesso aos serviços de Internet e Intranet, devem ser imediatamente comunicados à área de tecnologia, para serem analisados e solucionados.

5.7.1. Cabe aos gestores das Gerências Regionais, em complementação às ações de divulgação do ICMBio relacionadas ao tema, orientar os usuários sob suas responsabilidades a respeito do uso adequado do recurso de internet, conforme as regras estabelecidas nos seus Planos Regionais de Segurança da Informação (PRSI), informando à área de tecnologia da informação do ICMBio ou ao Comitê de Segurança da Informação o seu descumprimento;

5.7.2. Comprovada a utilização irregular, o usuário envolvido terá o seu acesso à Internet bloqueado pela área de tecnologia, sendo comunicado o fato à chefia imediata, podendo incorrer em processo administrativo disciplinar e nas sanções legalmente previstas, assegurados o contraditório e a ampla defesa;

5.8. A critério da DIPLAN, poderão ser adotadas medidas visando a manutenção da disponibilidade e da qualidade do acesso à internet, seja em situações normais de funcionamento, seja em situações de contingência, tais como:

5.8.1. Bloqueios totais ou parciais e/ou priorização de acessos a determinados sítios e serviços; e

5.8.2. Limitação de banda de tráfego de dados;

5.9. As medidas identificadas no item anterior, quando implementadas, serão comunicadas às equipes de suporte técnico, a fim de possibilitar o repasse de informações aos usuários interessados.

5.10. Os processos de contratações de serviço de acesso à internet devem ser gerenciados pela área de tecnologia de modo a garantir a implementação dos recursos de segurança da informação.

5.10.1. Sempre que identificada a necessidade, desde que verificadas a viabilidade técnica e econômica, poderão ser contratados os serviços de links redundantes para garantir a alta disponibilidade do serviço

de acesso à internet.

5.10.1.1.O link redundante é um link alternativo ou auxiliar, que serve como suporte ou opção ao link principal de uma rede em caso de uma queda;

5.10.1.2.O link redundante poderá ser configurado para atuar de forma agregada ao link principal, ampliando a capacidade do serviço de acesso à internet ofertado pelo link principal.

6. MONITORAMENTO E AUDITORIAS

6.1.Por motivos de segurança, todo acesso à internet fornecido pelo ICMBio será monitorado e os registros serão mantidos pela área de Tecnologia.

6.2.Em caso de indícios de descumprimento das diretrizes previstas nesta norma, desde que devidamente apresentados os registros dos indícios, poderá ser solicitado por qualquer servidor ao Comitê de Segurança da Informação a realização de auditoria extraordinária;

6.3.Os relatórios decorrentes das auditorias ordinárias e extraordinárias serão encaminhados ao Comitê de Segurança da Informação, para os devidos fins;

6.4.Os registros de acessos dos usuários poderão ser analisados pela área de tecnologia para investigação de incidentes que comprometam a segurança das informações institucionais;

6.5.Os registros de acesso dos usuários poderão ser fornecidos aos órgãos de segurança para investigações quanto a incidentes de segurança;

6.6.Os registros de acesso poderão ser disponibilizados a outras instituições, desde que para atender a determinações judiciais.

7. ATUALIZAÇÃO DA NORMA

7.1.O disposto na presente norma será atualizado sempre que alterados os procedimentos de controle de acesso à internet e intranet, observada, a periodicidade prevista para a revisão da Política de Segurança da Informação.

LUIS GUSTAVO BIAGIONI

Presidente Substituto



Documento assinado eletronicamente por **Luis Gustavo Biagioni, Presidente Substituto**, em 10/08/2022, às 19:01, conforme art. 1º, III, "b", da Lei 11.419/2006.



A autenticidade do documento pode ser conferida no site <https://sei.icmbio.gov.br/autenticidade> informando o código verificador **11778570** e o código CRC **E8675775**.



MINISTÉRIO DO
MEIO AMBIENTE



MINISTÉRIO DO MEIO AMBIENTE
INSTITUTO CHICO MENDES DE CONSERVAÇÃO DA BIODIVERSIDADE
GABINETE DA PRESIDÊNCIA

EQSW 103/104, Bloco "C", Complexo Administrativo - Bloco C - Bairro Setor Sudoeste - Brasília - CEP 70670-350

Telefone: (61) 2028-9011/9013

ANEXOS VI - NORMA DE SEGURANÇA DA INFORMAÇÃO (NSI)

NSI 006/2022 - USO DO CORREIO ELETRÔNICO INSTITUCIONAL

1. OBJETIVOS

1.1. Estabelecer diretrizes e padrões para utilização do serviço de correio eletrônico institucional, no âmbito do Instituto Chico Mendes de Conservação da Biodiversidade - ICMBio

2. MOTIVAÇÕES

2.1. Alinhamento às normas, regulamentações e melhores práticas relacionadas à matéria.

2.2. Proteção da Rede Nacional de Computadores do ICMBio.

2.3. Correto direcionamento e dimensionamento de recursos tecnológicos para prover o uso do correio eletrônico institucional.

2.4. Orientações gerais para gestores e usuários de serviços de Tecnologia da Informação, lotados em todas as outras Unidades.

3. REFERÊNCIAS NORMATIVAS

3.1. Instrução Normativa nº 1, de 27 de maio de 2020, do Gabinete de Segurança Institucional da Presidência da República, que dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal.

3.2. Norma Complementar nº 07/IN01/DSIC/GSIPR, de 15 de julho de 2014, do Departamento de Segurança da Informação e Comunicações da Presidência da República, que estabelece diretrizes para a implementação de controles de acesso à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta.

3.3. Norma Técnica ABNT NBR ISO/IEC 27001:2013, que especifica os requisitos para estabelecer, implementar, manter e melhorar

3.4. Norma Técnica ABNT NBR ISO/IEC 27002:2013, que fornece diretrizes para práticas de gestão de segurança da informação

3.5. Instrução Normativa nº 1, de 04 de abril de 2019, que dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação - TIC pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo

4. CONCEITOS E DEFINIÇÕES

4.1. Aliás: endereço eletrônico alternativo para uma conta de correio eletrônico. Pode ser usado para exibir um endereço genérico

4.2. Arquivo de registro de mensagens (logs): registro de eventos relevantes, utilizados para restaurar um sistema, diagnosticar problemas ou realizar auditorias.

4.3. Caixa postal institucional pessoal: conta de correio eletrônico de um único usuário, servidor ou colaborador.

4.4. Caixa postal institucional da unidade: conta de correio eletrônico de uma unidade administrativa constante da estrutura organizacional do ICMBio, ou em casos justificados, relacionada a atividades específicas ou eventos extraordinários temporários.

4.5. Caixa postal de sistema: conta de correio eletrônico de um sistema informatizado que necessite desse recurso para o seu funcionamento.

4.6. Código malicioso: termo comumente utilizado para genericamente se referir a programas desenvolvidos para executar ações danosas e atividades maliciosas em um computador ou dispositivo móvel. Tipos específicos de códigos maliciosos são: vírus, worm, phishing, spyware, backdoor, cavalo de troia e rootkit.

4.7. Domínio: parte final do endereço eletrônico, localizada após o símbolo arroba (@).

4.8. Endereço Eletrônico: conjunto de caracteres que individualiza e identifica o remetente e o destinatário da mensagem eletrônica. É formado por um identificador e por um domínio, separados pelo símbolo arroba (@).

4.9. Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos - ETIR: grupo de pessoas com a responsabilidade de receber, analisar e responder as notificações e atividades relacionadas a incidentes de segurança da informação.

4.10. Firewall: Dispositivo de segurança da rede que monitora o tráfego de rede de entrada e saída e decide permitir ou bloquear tráfegos específicos de acordo com um conjunto definido de regras de segurança.

4.11. Gestor da Unidade: Coordenador Geral, Coordenador, Chefe de divisão, Chefe de serviço ou servidor designado para responder por uma unidade ou serviço constante do Regimento interno do ICMBio.

4.12. Identificador: Parte inicial do endereço eletrônico, localizada antes do símbolo arroba (@), que o diferencia das demais caixas postais e identifica seu usuário, setor, ou finalidade.

4.13. Hoax: mensagem eletrônica encaminhada a muitos destinatários, de conteúdo geralmente alarmante e com pouca ou nenhuma veracidade, cujo objetivo é a propagação de boatos e informações distorcidas.

4.14. Lista de distribuição: agrupamento de diversos endereços eletrônicos, representado por um endereço eletrônico específico, que permite a distribuição conjunta de uma mensagem eletrônica a todos

4.15. Malware: programas indesejados, desenvolvidos com a finalidade de executar ações danosas e atividades maliciosas em um computador ou sistema (ex.: worm, bot, spyware, backdoor, cavalo de troia, ransomware e rootkit).

4.16. Material criptografado: dados e/ou informações codificadas por meio de técnicas que impossibilitam o seu entendimento/leitura, cuja reversão ocorre somente com a utilização de uma senha previamente conhecida e/ou dispositivo criptográfico (ex.: token, smart card).

4.17. Phishing: fraude eletrônica, caracterizada pela tentativa de obtenção

de dados e informações pessoais com o uso de meios técnicos e de engenharia social.

4.18.Proxy: também conhecido por filtro de conteúdo, é o servidor responsável por intermediar o acesso à internet, aplicando

4.19.Serviço de correio eletrônico institucional: serviço de envio e recebimento de mensagens eletrônicas (e-mail) no âmbito do ICMBio.

4.20.Spam: mensagem enviada a um grande número de endereços eletrônicos, que não possua caráter institucional e/ou cujo objeto não seja inerente à atividade funcional do usuário ou da unidade.

4.21.Usuário de correio eletrônico: servidor, colaborador ou estagiário que utiliza alguma caixa postal eletrônica.

4.22.VPN Client to Site: Conexão remota segura entre o Usuário/Cliente e o Datacenter.

4.23.VPN Site to Site: Conexão remota segura entre redes internas.

5. DIRETRIZES

5.1.CAIXAS POSTAIS DE CORREIO ELETRÔNICO (criação, alteração e exclusão)

5.1.1.As caixas postais são identificadas unicamente por meio de seu endereço eletrônico.

5.1.2.No âmbito deste ICMBio, o domínio do endereço eletrônico é "icmbio.gov.br".

5.1.3.A capacidade máxima de armazenamento padrão das caixas postais será de 100 gigabytes (GB).

5.1.4.Somente será criada caixa postal institucional pessoal, caixa postal institucional da unidade ou caixa postal de tecnologia.

5.1.5.As solicitações de criação, alteração e exclusão de caixas postais devem ser encaminhadas à área de tecnologia.

5.2.CAIXA POSTAL INSTITUCIONAL PESSOAL

5.2.1.A caixa postal institucional pessoal é destinada ao envio e recebimento de correspondências relacionadas às atividades como repositório de documentos, desta forma:

I - Documentos de interesse institucionais, recebidos na caixa postal institucional pessoal, devem ser inseridos no Sistema Eletrônico de Informações - SEI;

II - Todos os e-mails enviados com o uso da caixa postal institucional pessoal deverão ser encaminhados com a identificação modelo de assinatura fornecido pelo ICMBio.

5.2.2.SERVIDORES EFETIVOS

5.2.2.1.Todo servidor lotado no Instituto terá uma caixa postal institucional pessoal.

5.2.2.2.criação de caixa postal institucional pessoal de servidor será feita pela área de tecnologia, após a formalização da demanda que deve ser solicitada pela chefia imediata ou pela Coordenação Geral de Gestão de Pessoas.

5.2.2.3.O identificador do endereço de correio eletrônico será formado pelo primeiro nome e pelo último sobrenome do servidor, separados pelo sinal de ponto.

5.2.2.4.Em situações justificadas, o identificador dos endereços de correio eletrônico poderá ser formado segundo outra ordem ou abreviação do nome do usuário.

5.2.2.5.A adequação dos endereços de correio eletrônico que não correspondam ao padrão estabelecido nesta norma será solicitada à área de tecnologia pelo usuário interessado.

5.2.2.6.A caixa postal institucional pessoal de servidores será excluída definitivamente nos casos de falecimento, exoneração, demissão, redistribuição, aposentadoria, remoção, permuta, vacância por posse em outro cargo inacumulável e cessão a outro órgão ou retorno à origem.

5.2.2.7.Ocorridos os fatos descritos no item anterior incumbe à Coordenação Geral de Gestão de Pessoas - CGGP comunicá-los à área de tecnologia no prazo de até 3 (três) dias da publicação do ato respectivo, exceto nos casos de demissão, quando a comunicação deverá ocorrer de imediato à ciência do afastamento pela Coordenação Geral de Gestão de Pessoas - CGGP.

5.2.2.8.Não ocorrerá a exclusão da caixa postal institucional pessoal nos casos de licenças ou quando solicitada a manutenção da caixa postal pela respectiva Diretoria.

5.2.2.9.A exclusão da caixa postal institucional pessoal será realizada somente após comunicada pela Coordenação Geral de Gestão de Pessoas - CGGP a decisão administrativa definitiva.

5.2.2.10.Nos demais casos de que trata o item 5.2.2.6, incumbe à área de tecnologia, no prazo de 5 (cinco) dias, excluir definitivamente a caixa postal.

5.2.3.SERVIDORES TEMPORÁRIOS

5.2.3.1.Todo servidor temporário poderá ter uma caixa postal institucional pessoal, desde que solicitada pela chefia imediata

5.2.3.2.A criação de caixa postal institucional pessoal de servidor será feita pela área de tecnologia, após a formalização da demanda que deve ser solicitada pela chefia imediata.

5.2.3.3.O identificador do endereço de correio eletrônico será formado pelo primeiro nome e pelo último sobrenome do servidor, separados pelo sinal de ponto.

5.2.3.4.Em situações justificadas, o identificador dos endereços de correio eletrônico poderá ser formado segundo outra ordem ou abreviação do nome do usuário.

5.2.3.5.A adequação dos endereços de correio eletrônico que não corresponda ao padrão estabelecido nesta norma será solicitada à área de tecnologia pelo usuário interessado.

5.2.3.6.A caixa postal institucional pessoal de servidores temporários será excluída definitivamente nos casos de falecimento, exoneração, demissão, redistribuição, aposentadoria, remoção, permuta, vacância por posse em outro cargo inacumulável e cedência permanente a outro órgão ou retorno à origem.

5.2.3.7.Ocorridos os fatos descritos no item anterior, incumbe à Coordenação Geral de Gestão de Pessoas - CGGP comunicá-los à área de tecnologia, no prazo de até 3 (três) dias da publicação do ato respectivo, exceto nos casos de demissão, quando a comunicação deverá ocorrer de imediato à ciência do afastamento pela Coordenação Geral de Gestão de Pessoas - CGGP.

5.2.3.8.Não ocorrerá a exclusão da caixa postal institucional pessoal nos casos de licenças, devidamente solicitada pela respectiva Diretoria;

5.2.3.9.A exclusão da caixa postal institucional pessoal será realizada somente após comunicada pela Coordenação Geral de Gestão de Pessoas - CGGP a decisão administrativa definitiva.

5.2.3.10.Nos demais casos de que trata o item 5.2.3.6, incumbe à área de tecnologia da informação, no prazo de 20 (vinte) dias, excluir definitivamente a caixa postal.

5.2.3.11. Nos casos de demissão haverá suspensão imediata da caixa postal institucional, a partir da comunicação da Coordenação Geral de Gestão de Pessoas - CGGP.

5.2.4. Estagiários

5.2.4.1. O gestor da unidade poderá solicitar, por escrito, à área de tecnologia, a criação de caixa postal institucional pessoal ao estagiário somente quando houver essa necessidade para o serviço a ser desempenhado.

5.2.4.2. O envio de mensagens por estagiários será restrito a endereços eletrônicos mantidos pelo ICMBio. Quando solicitado, com a devida justificativa pelo gestor da unidade a que vinculado, será permitido o envio a endereços externos.

5.2.4.3. O uso do correio eletrônico pelo estagiário será de responsabilidade do gestor da unidade a que estiver vinculado.

5.2.4.4. O identificador padrão do endereço eletrônico do estagiário será formado pelo nome seguido do último sobrenome, acrescido pela palavra "estagiário", separados pelo sinal de ponto.

5.2.4.5. A caixa postal institucional pessoal de estagiários será excluída definitivamente quando da comunicação da Coordenação Geral de Gestão de Pessoas - CGGP sobre o término do estágio.

5.2.5. Bolsistas

5.2.5.1. O gestor da unidade poderá solicitar, por escrito, à área de tecnologia, a criação de caixa postal institucional pessoal para o bolsista somente quando houver essa necessidade para o serviço a ser desempenhado.

5.2.5.2. O envio de mensagens por bolsistas será restrito a endereços eletrônicos mantidos pelo ICMBio. Quando for expressamente solicitado, com a devida justificativa pelo gestor da unidade a que esteja vinculado, será permitido o envio a endereços externos.

5.2.5.3. O uso do correio eletrônico pelo bolsista será de responsabilidade do gestor da unidade a que estiver vinculado.

5.2.5.4. O identificador padrão do endereço eletrônico do Bolsista será formado pelo nome seguido do último sobrenome, acrescido pela palavra "bolsista", separados pelo sinal de ponto.

5.2.5.5. Caberá a área responsável pelo contrato do colaborador bolsista, informar à área de tecnologia, em até 03 (três) dias, sempre que houver o desligamento de qualquer bolsista para que seja efetuada a exclusão da caixa postal institucional pessoal do mesmo.

5.2.6. Terceirizados

5.2.6.1. O gestor da unidade poderá solicitar, por escrito, à área de tecnologia a criação de caixa postal institucional pessoal ao terceirizado somente quando houver essa necessidade para o serviço a ser desempenhado.

5.2.6.2. Avisos, informes e outras necessidades de comunicação institucional do Instituto aos terceirizados podem ser realizados para os e-mails dos colaboradores e/ou por meio de outros canais de comunicação tais como murais físicos e eletrônicos, site do ICMBio e intranet, além do uso de listas de e-mails.

5.2.6.3. O envio de mensagens por terceirizados será restrito a endereços eletrônicos mantidos pelo ICMBio. Quando unidade a que esteja vinculado, será permitido o envio a endereços externos.

5.2.6.4. O uso do correio eletrônico pelo terceirizado autorizado será de responsabilidade do gestor da unidade a que esteja vinculado.

5.2.6.5. O identificador padrão do endereço eletrônico do terceirizado será formado pelo nome seguido do último sob

5.2.6.6. Caberá à área responsável pelo contrato do colaborador terceirizado, informar a área de tecnologia, em até 03 (três) dias, sempre que houver o desligamento de qualquer empregado para que seja efetuada a exclusão da caixa postal institucional pessoal.

5.3. CAIXA POSTAL INSTITUCIONAL DA UNIDADE

5.3.1. As unidades institucionais da estrutura organizacional do ICMBio poderão ter caixa postal institucional da unidade.

5.3.2. O gestor da unidade será também o gestor da respectiva caixa postal, competindo-lhe:

I - solicitar a criação, a alteração e a exclusão da caixa postal institucional da unidade;

II - autorizar o acesso de outros servidores públicos, mediante delegação no sistema de correio eletrônico, bem como excluir esse acesso;

III - compartilhar o acesso a caixas específicas com outros usuários.

5.3.3. A caixa postal institucional da unidade terá um único endereço de correio eletrônico, cujo identificador será formado pela denominação da unidade ou por sigla que permita a sua identificação.

5.3.4. O acesso a caixa compartilhada dar-se-á por meio da conta institucional pessoal. Para aumentar a rastreabilidade da caixa compartilhada a mesma deve ser bloqueada para acesso direto com senha.

5.3.5. Em casos excepcionais, devidamente justificados, poderão ser criadas caixas postais institucionais a fim de atender comi sistemas, demandas de trabalho específicas e eventos temporários.

5.3.5.1. Nessa hipótese, quando da solicitação de criação da caixa postal, deverão ser indicados o servidor ou unidade que será responsável pelo respectivo gerenciamento e o período em que a caixa postal deverá ser mantida.

5.3.5.2. Findada a necessidade para a qual a caixa postal institucional da unidade foi criada, o responsável pelo gerenciamento deverá informar à área de tecnologia da informação para a exclusão da caixa postal.

5.3.5.3. O envio de mensagens em nome da unidade deverá ser assinado pelo usuário que faz uso da caixa compartilhada, devendo inserir sua assinatura de acordo com o padrão fornecido pelo ICMBio.

5.4. LISTA DE DISTRIBUIÇÃO (criação, alteração e exclusão)

5.4.1. É permitida a criação de lista de distribuição, com o objetivo de facilitar e otimizar a troca de informações sobre assuntos de interesse do ICMBio.

5.4.2. A criação de lista de distribuição pode ser solicitada pelo gestor da unidade a qual se destina ou pela Presidência.

5.4.3. A solicitação deve ser encaminhada, por escrito, à área de tecnologia da informação, acompanhada de justificativa e de informações sobre a finalidade da lista, nome do gestor da lista, e, quando destinada à atividade temporária, do período de sua duração.

5.4.4. Cada lista de distribuição terá um gestor, a quem incumbe:

I - manter permanentemente atualizado o rol de integrantes da lista de distribuição;

solicitar exclusão como gestor e indicar, simultaneamente, o novo responsável pela lista de distribuição;

III - solicitar exclusão da lista de distribuição, quando esta não for mais necessária.

5.4.5.O identificador do endereço eletrônico será formado pela denominação ou sigla, que permita, de forma clara, a identificação de sua finalidade, ou do grupo de endereços eletrônicos nela reunidos, seguido da palavra "lista", separados por hífen.

5.5.UTILIZAÇÃO DOS RECURSOS DO SISTEMA DE CORREIO ELETRÔNICO

5.5.1.uso do correio eletrônico institucional restringe-se a mensagem cujo objeto seja, necessariamente, inerente à atividade funcional do usuário ou da unidade, sendo vedado o uso para fins particulares

5.5.2.O acesso ao correio eletrônico a partir de estações de trabalho fornecidas pelo ICMBio será feito a partir do navegador de internet ou utilização de aplicativo.

5.5.3.É vedada a tentativa de acesso a caixas postais às quais o usuário não tenha autorização de acesso.

5.5.4.O tamanho máximo da mensagem eletrônica, incluindo os anexos, não pode exceder 35 megabytes (MB).

5.5.5.O envio de mensagem eletrônica para lista de distribuição que englobe elevado número de endereços eletrônicos - acima de 200 (duzentos) destinos, é permitido em caráter excepcional ou a unidades administrativas, desde que autorizado pelas Diretorias ou Presidência.

5.5.6.É de responsabilidade do usuário de e-mail institucional:

I - eliminar periodicamente as mensagens eletrônicas contidas nas caixas postais;

II - manter exclusivo o acesso à sua caixa postal institucional pessoal, não compartilhando a respectiva senha e/ou delegando o acesso a terceiros.

III - informar à área de tecnologia da informação o recebimento de mensagem que contrarie o disposto na vedação a seguir.

5.5.7.É vedado aos usuários o envio de qualquer mensagem eletrônica contendo:

informações privilegiadas, confidenciais e/ou de propriedade do ICMBio para destinatários não autorizados;

II - materiais obscenos, ilegais ou antiéticos;

III - materiais preconceituosos ou discriminatórios;

IV- materiais caluniosos ou difamatórios;

V - propaganda com objetivo comercial;

VI- listagem com endereços eletrônicos institucionais;

VII - malwares;

VIII - material de natureza político-partidária, associativa ou sindical, que promova a eleição de candidatos para cargos eletivos;

IX - material protegido por lei de propriedade intelectual; X - entretenimentos e "correntes";

X - assuntos ofensivos;

XI - músicas, vídeos ou animações que não sejam de interesse específico do trabalho;

XII - spam, phishing e hoax;

XIII -

materiais criptografados, exceto nos casos em que as informações da mensagem necessitem proteção quanto ao sigilo.

5.5.8.A recuperação de mensagens de caixas postais institucionais de unidade poderá ser solicitada pelo respectivo usuário e justificado por meio de sistema de atendimento de TI ou outros canais disponibilizados para suporte aos usuários do ICMBio.

5.5.9.A área de tecnologia da informação não garante a recuperação de mensagens de e-mails ou de caixas postais excluídos há mais de 20 dias.

5.5.10.Recuperada(s) a(s) mensagem(ns) de e-mail, a área de tecnologia da informação verificará com o solicitante a melhor forma de disponibilizá-la(s) novamente;

5.5.11.Casos omissos nessa norma de segurança serão tratados pela área de tecnologia da informação pontualmente, que poderá submeter para análise do Comitê de Segurança, sempre que necessário.

6. MONITORAMENTO E AUDITORIAS

6.1.O uso do correio eletrônico será monitorado por meio de ferramentas com o intuito de impedir o recebimento de contendo vírus e outros arquivos que coloquem em risco a segurança da infraestrutura tecnológica do ICMBio ou que contenham conteúdo impróprio.

6.2.As auditorias ordinárias ou extraordinárias serão coordenadas pelo Gestor de Segurança da Informação e os relatórios serão encaminhados ao Comitê de Segurança da Informação e Comitê de Governança Digital.

6.3.As auditorias extraordinárias deverão ser precedidas de autorização do Comitê de Segurança da Informação.

6.4.Os arquivos de registro de mensagens eletrônicas (logs) serão mantidos pelo prazo de 30 dias, exceto nos casos de auditoria ou notificação administrativa ou judicial, em que serão devidamente armazenados pela Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos - ETIR, a fim de salvaguardar os dados respectivos.

Tecnologia encaminhará, em dezembro de cada ano, um relatório às unidades e aos respectivos gestores, com o rol das listas de distribuição elas vinculadas, bem como a lista de eventuais caixas postais de estagiários lotados na respectiva unidade.

6.6.Cabe ao gestor conferir os dados do relatório referido no item anterior e, no prazo de 10 (dez) dias úteis, solicitar os ajustes necessários a Área de Tecnologia.

7. ATUALIZAÇÃO DA NORMA

7.1.O disposto na presente norma será atualizado sempre que alterados os procedimentos de uso do correio eletrônico institucional, observada, ainda, a periodicidade prevista para a revisão da Política de Segurança.

LUIS GUSTAVO BIAGIONI

Presidente Substituto



Documento assinado eletronicamente por **Luis Gustavo Biagioni, Presidente Substituto**, em 10/08/2022, às 19:02, conforme art. 1º, III, "b", da Lei 11.419/2006.



A autenticidade do documento pode ser conferida no site <https://sei.icmbio.gov.br/autenticidade> informando o código verificador **11778666** e o código CRC **05495920**.



MINISTÉRIO DO
MEIO AMBIENTE



MINISTÉRIO DO MEIO AMBIENTE
INSTITUTO CHICO MENDES DE CONSERVAÇÃO DA BIODIVERSIDADE
GABINETE DA PRESIDÊNCIA

EQSW 103/104, Bloco "C", Complexo Administrativo - Bloco C - Bairro Setor Sudoeste - Brasília - CEP 70670-350
Telefone: (61) 2028-9011/9013

MINUTA ANEXOS VII - NORMA DE SEGURANÇA DA INFORMAÇÃO (NSI)

NSI 007/2022 - SISTEMAS

1. OBJETIVO

1.1. Estabelecer diretrizes e padrões para o desenvolvimento e evolução de sistemas, no âmbito do Instituto Chico Mendes de Conservação da Biodiversidade - ICMBio.

2. MOTIVAÇÕES

2.1 Alinhamento às normas, regulamentações e melhores práticas relacionadas à matéria.

2.2.

Correto direcionamento e dimensionamento de recursos tecnológicos para prover o uso do correio eletrônico institucional.

2.3. Orientações gerais para gestores e usuários de serviços de Tecnologia da Informação, lotados em todas as outras unidades do ICMBio.

3. REFERÊNCIAS NORMATIVAS

3.1. Acórdão 1137/2012 aperfeiçoe as críticas de entrada de dados do [Sistema], para mitigar os riscos de incorreção, (...) observando as orientações contidas no item 12.2.1 da Norma Técnica ABNT NBR ISO/IEC 27002:2005;

3.2. Acórdão 1722/2008 continue a executar alterações no sistema (...), para validação de dados de entrada, controle do processamento interno de dados e validação de dados de saída, em conformidade com o previsto nos itens 12.2.1, 12.2.2 e 12.2.4 da ABNT NBR ISO/IEC 17799:2005, aperfeiçoe o tratamento de exceções do sistema (...), a validação de dados de entrada e o controle do processamento interno, em conformidade com a especificação de requisitos do sistema e com os itens 12.2.1 e 12.2.2 da ABNT NBR ISO/IEC 17799:2005;

3.3. Decreto nº 9.637, de 26 de dezembro de 2018, que institui a Política de Segurança da Informação, dispõe sobre a governança da segurança da informação, e altera o Decreto nº 2.295, de 4 de agosto de 1997, que regulamenta o disposto no art. 24, caput, inciso IX, da Lei nº 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional;

3.4. Decreto nº 10.332, de 28 de abril de 2020, que Institui a Estratégia de Governo Digital para o período de 2020 a 2022, no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional e dá outras providências;

3.5. Decreto nº 10.996, de 14 de março de 2022, que Altera o Decreto nº 10.332, de 28 de abril de 2020, que institui a Estratégia de Governo Digital para o período de 2020 a 2022, no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional.- Decreto nº 10.222/2020, de 05 de fevereiro de 2020, que aprova a Estratégia Nacional de Segurança Cibernética.

3.6. Portaria SGD/ME nº 5.651, de 28 de junho de 2022, que estabelece modelo para a contratação de serviços de desenvolvimento, manutenção e sustentação de software, no âmbito dos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISF do Poder Executivo Federal.

4. CONCEITOS E DEFINIÇÕES

4.1. Serviço de TI: é o conjunto de pessoas, processos e tecnologias com fim de apoiar os processos de negócio da Instituição. Sistema (produto), então, é a tecnologia necessária a um serviço de TI.

4.2. Processo de Software: é um "conjunto de atividades relacionadas que levam à produção de um software ou o conjunto de atividades métodos, práticas e transformações que guiam pessoas na produção de software";

4.3. Desenvolvimento de Sistema: é o esforço temporário, na forma de Processo de Software, empreendido para atender Demanda de TI.

4.4. Demanda de TI : é a solicitação, pedido ou requisição feita a Área de Tecnologia, cujo atendimento é realizado através de um Projeto de TI ou de Ação de TI.

4.5. Demanda de TI Emergencial: é basicamente a demanda cujo desenvolvimento de sistema busca resolver

um problema com maior celeridade. Não há nenhuma atividade ou artefato específico para esse tipo de demanda.

4.6. O desenvolvimento é caracterizado como:

4.6.1. Formal, por ser controlado por este processo;

4.6.2. Eficiente, por comportar e recomendar práticas ágeis;

4.6.3. Confiável, por ser iniciado segundo um Projeto de TI ou Ação de TI, válido pelas atividades reconhecidas.

4.6.4. Assim, documentos operacionais que já orientam processos específicos de desenvolvimento de softwares (a serem implantados no ambiente de Tecnologia da Informação (TI)) da Área de TI não necessitam ser substituídos, porém passam a ser baseados neste processo.

5. DIRETRIZES

5.1. Essa seção da norma orienta a direção quanto à definição dos requisitos necessários de segurança de sistemas de informação, medidas preventivas contra processamento incorreto das aplicações, uso de controles criptográficos, além de fornecer diretrizes para a segurança dos arquivos de sistema, segurança em processos de desenvolvimento e suporte, e gestão de vulnerabilidades técnicas.

6. PAPÉIS E RESPONSABILIDADES

6.1. Encontram-se definidos os papéis dos usuários presentes em todo processo (Gerente do Processo, Dono do Processo, Analista e Designer do Processo), conforme definições:

6.1.1. Demandante de TI - patrocinador, tomador de decisão quanto a iniciar, continuar, interromper ou encerrar a atividade (dono da atividade). Nesse caso, deve haver apenas um papel envolvido.

6.1.2. Gerente de Projetos - assegurar o planejamento do desenvolvimento do sistema com escopo, cronograma, custos e responsáveis definidos, assegurar a existência de modelos para construção de documentos técnicos específicos ao projeto de software.

6.1.3. Equipe do Projeto - equipe de desenvolvimento.

6.1.4. Analista de Requisitos - elaborar documento de visão do produto, construir documentos de requisitos, planejar desenvolvimento do sistema com escopo, cronograma, custos e responsáveis definidos.

6.1.5. Arquiteto de Software - construir documento de arquitetura do Produto.

6.1.6. Arquiteto de Informação - Construir documento de interface do Produto.

6.1.7. Analista de Testes - construir Plano de Testes.

6.1.8. Analista de Configuração - construir Plano de Implantação e Liberação do Produto.

6.1.9. Testador - validar implementação de requisito conforme plano de teste.

6.1.10. Desenvolvedor - validar implementação de requisito conforme Plano de Testes, implementar requisito de sistema conforme documento de requisitos, documento de arquitetura do produto e documento de interface do produto.

6.1.11. Configurador - preparar e validar pacote de liberação conforme Plano de Implementação e liberação do produto.

6.1.12. Homologador - validar a implementação de requisitos conforme escopo planejado do projeto, documento de visão do produto e/ou documento de requisitos.

6.1.13. Dono do Processo - orientar outros setores a adquirir maior qualidade técnica no desenvolvimento de sistemas (vide indicador qualidade técnica do desenvolvimento), quando solicitado, orientar outros setores a realizar a medição do desempenho (servidor da área de TI, preferencialmente da gerência dedicada ao desenvolvimento de sistemas da Área de TI).

7. ATIVIDADES DO PROCESSO

7.1. Microatividades indispensáveis ao desenvolvimento do sistema:

7.2. Planejar o desenvolvimento/evolução do sistema

7.2.1. Uma vez que a Demanda de TI foi solicitada pelo demandante de TI e analisada pelo Gerente do Projeto, conforme definido pelo Processo de Gerenciamento de Projetos e Ações de TI, o Dono do Produto planeja o desenvolvimento do sistema (Projeto de TI ou Ação de TI) de modo a atender a Demanda de TI.

7.2.2. O resultado do planejamento do desenvolvimento/evolução do sistema, o projeto propriamente dito(o Projeto de TI ou a Ação de TI), é a principal saída desta microatividade. Esse projeto deve ser registrado e conter escopo, cronograma, custos e responsáveis envolvidos, conforme orienta a atividade de "Iniciar e Planejar Projetos e Ações" do Processo de Gerenciamento de Projetos e Ações. Esses elementos podem ser melhor definidos com o apoio do Analista de Requisitos através da construção do Documento de Visão do Produto. A construção desse documento consiste em coletar, analisar e definir as características e necessidades de alto nível do sistema.

7.2.3. Quanto ao projeto de software (Projeto de TI ou Ação de TI), o escopo é composto dos requisitos funcionais e não funcionais do sistema, elucidados pelo Analista de Requisitos, a serem desenvolvidos ou modificados pelo Desenvolvedor durante a construção do sistema (vide atividade Construir). O escopo do projeto de software não são todos os requisitos especificados ou identificados para conter no sistema, mas são aqueles escolhidos para o desenvolvimento de uma ou mais versões do sistema em um determinado projeto. Nesse sentido, o Dono do Produto pode optar por entregar uma versão do sistema no ambiente de TI a cada fase do projeto (vide atividade Entregar). O incremento ou definição da versão deve seguir o Processo de Gerenciamento de Versões.

7.2.4. O requisito de software é uma descrição curta de uma característica-chave contada na perspectiva do usuário, utilizando uma linguagem comum ao negócio e testes;

7.2.5. Desenvolver o requisito, neste processo, é o mesmo que implementar um novo requisito;

7.2.6. Um requisito pode ser modificado para fins de melhoria ou de correção;

7.2.7. O cronograma, os responsáveis (a Equipe do Projeto ou a Equipe de Desenvolvimento) e os custos devem ser definidos e informados pelo Dono do Produto conforme orientação dada pelo Processo de Gerenciamento de Projetos e Ações de TI.

7.2.8. Havendo necessidade de analisar, informar e verificar comportamentos ou restrições mais específicas do sistema, o Dono do Produto pode detalhar o projeto com informações ou documentos técnicos específicos ao projeto de software, com auxílio de técnicos especializados. É o caso de:

7.2.8.1 Regras de negócio, casos de uso, especificações de tela, entre outros afins, que não sejam restrições de arquitetura ou de interface, os quais devem ser especificados e gerenciados pelo Analista de Requisitos em ferramenta ou documento próprio (Documento de Requisitos);

7.2.8.2. Restrições arquiteturais, tais como princípios de arquitetura a serem seguidos, padrões de codificação, entre outros afins, os quais devem ser analisados, modelados e gerenciados pelo Arquiteto de Software em ferramenta ou documento próprio (Documento de Arquitetura do Produto);

7.2.8.3. Restrições de interface, tais como identidade visual, layout, modelos, entre outros afins, os quais devem ser especificados e gerenciados pelo Arquiteto de Informação em ferramenta ou documento próprio (Documento de Interface do Produto);

7.2.8.4. Restrições de testes, tais como ferramentas, estratégias, scripts, cenários e casos específicos, entre outros afins, para a execução dos testes, os quais devem ser planejados e gerenciados pelo Analista de Testes em ferramenta ou documento próprio (Plano de Testes);

7.2.8.5. Restrições de configuração, implantação e liberação para uso, tais como branches de trabalho, política de commit, ambientes de execução (desenvolvimento, testes ou homologação), gitflow, montagem do pacote de liberação, entre outros afins, a serem planejados e gerenciados pelo Analista de Configuração em ferramenta ou documento próprio (Plano de Implantação e Liberação do Produto);

7.2.9. Por meio de uma ação conjunta, especialmente no contexto de práticas ágeis, o Dono do Produto pode planejar o projeto com iterações de construção de uma versão do sistema para um ou mais requisitos, de modo a tornar o desenvolvimento mais eficiente. Nesse caso, os documentos técnicos (Documento de Requisitos, Documento de Arquitetura do Produto, entre outros) também passam a ser construídos "parcialmente" conforme o escopo de cada versão. Modelos ou instruções de trabalho para o preenchimento desses documentos devem ser asseguradas pelo Gerente do Projeto.

7.3. Construir o sistema

7.3.1. Uma vez planejado o sistema pelo Dono do Produto (vide atividade Planejar), o desenvolvedor implementa (desenvolve ou modifica) o requisito e o Testador ou Homologador valida a implementação desse requisito, conforme os documentos técnicos específicos existentes. Logo, a principal saída desta microatividade é o sistema implementado, validado e disponível para entrega, assim, a construção é incompleta se não houver teste (pelo Testador) ou homologação (pelo Homologador).

7.3.2. É recomendável realizar a validação em ambiente de execução distinto (ambiente de testes ou de homologação) do próprio ambiente de desenvolvimento (do Desenvolvedor). Esses ambientes devem ser preparados e disponibilizados pelo Configurador conforme Plano de Implantação e Liberação do Produto definido pelo Analista de Configuração. Além disso, a abordagem ágil de integração contínua (com as interações, se planejadas) aumenta a eficiência da "entrega" para fins de validação.

7.4. Entregar o Sistema

7.4.1. Uma vez validada a versão do sistema em sua construção (vide atividade Construir), o Configurador prepara e valida o Pacote de Liberação da versão do sistema, principal saída desta microatividade (Pacote de Liberação validado). O projeto, contudo, não se encerra com o término desta microatividade, mas continua a sua execução seguindo para a implantação com base no Processo de Gerenciamento de Implantação e Liberação.

7.4.2. O Pacote de Liberação, conforme o Processo de Gerenciamento de Implantação e Liberação, é o conjunto de itens de processo, sistema ou infraestrutura a serem implantados formalmente no ambiente de TI para uso efetivo do usuário. Logo, o pacote neste processo é composto de itens relacionados a sistema: scripts de banco de dados, documento de release notes, Plano de Implantação e Liberação do Produto, entre outros.

7.4.3. A validação do Pacote de Liberação do sistema em sua entrega é posterior e distinto da validação do sistema em sua construção e consiste em analisar e verificar a implantação em ambiente similar ao do ambiente de TI no qual o usuário fará uso efetivo do sistema. Nesse caso, seguir práticas ágeis da cultura DevOps é altamente recomendável para aumentar a eficiência e segurança da implantação.

8. MATRIZ RACI (PAPÉIS E ATIVIDADES)

8.1. Esta seção tem por objetivo auxiliar o entendimento quanto ao nível de envolvimento de cada papel em cada atividade por meio da matriz RACI. Os níveis de envolvimento são:

8.1.1. Realizador (Responsible): quem executa a atividade (operador da atividade). Nesse caso, deve haver pelo menos um papel envolvido;

8.1.2. Autoridade (Accountable): quem pode tomar a decisão de iniciar, continuar, interromper ou encerrar a atividade (dono da atividade). Nesse caso, deve haver apenas um papel envolvido;

8.1.3. Consultado (Consulted): quem deve ser consultado para a Autoridade prosseguir com sua decisão. Pode haver um ou mais papéis envolvidos;

8.1.4. Informado (Informed): quem deve ser informado sobre a atividade executada. Pode haver um ou mais papéis envolvidos;

8.2. Segue matriz RACI dos principais papéis e atividades deste processo.

Atividades \ Papéis	Demandante de TI	Gerente do Projeto	Dono do Produto	Desenvolvedor	Configurador	Testador	Homologador
Planejar	C	A	R	I	I	I	I
Construir		I	A	R	I	R	R
Entregar		I	A	I	R		

9. INDICADORES DE DESEMPENHO DO PROCESSO

9.1. O indicador é definido e medido pelo Analista e Designer do Processo designado pelo Gerente do Processo, auxiliado pelo Dono do Processo e pelo Grupo de Planejamento e Definição do Processo ou pelas pessoas atribuídas aos papéis específicos do processo. Assim, definir metas de desempenho baseadas no indicador não é o objetivo desta seção. A definição de tais metas, por sua vez, deve ser realizada pelo Dono do Processo.

9.2. Em geral, o papel responsável por coletar os dados do indicador é o Dono do Processo. No entanto, havendo um responsável diferente, então o mesmo deve ser informado na tabela descritiva do respectivo indicador.

10. QUALIDADE TÉCNICA DO DESENVOLVIMENTO

10.1. A qualidade técnica do desenvolvimento do sistema (não a qualidade do sistema) é a medida de quais papéis, atividades ou artefatos técnicos, reconhecidos por este processo, foram empreendidos no desenvolvimento do sistema. Assim, quanto menor a qualidade, maior a atenção durante a implantação e liberação para uso efetivo do usuário. Além disso, o valor esperado pode variar conforme o setor de origem do desenvolvimento do sistema.

10.1.1. Finalidade - dar visibilidade da qualidade técnica do desenvolvimento do sistema de modo a auxiliar a tomada de decisões por parte de quem propriamente realiza a implantação e liberação para uso efetivo do usuário;

10.1.2. Periodicidade - mensal;

10.1.3. Cálculo - utiliza a Fórmula: $(SQS / (QTMS * TSE)) * 100$.

SQS = Somatório da qualidade técnica do desenvolvimento de cada sistema entregue.

TSE = Total de sistemas entregues (desenvolvidos).

QTMS = Qualidade técnica máxima do desenvolvimento de sistema.

10.1.4. Fonte - gerente do projeto;

10.1.5. Cálculo do QTMS - é um número natural com valor inicial zero (0) e para cada item confirmado do checklist abaixo soma-se mais um (+1), de modo que o valor máximo a ser alcançado é 13.

10.1.5.1. Checklist referente à versão entregue:

- I - Demanda de TI foi analisada pelo Gerente do Projeto;
- II - Dono do Produto definiu escopo, cronograma, custos e responsáveis (detalhou o projeto de software);
- III - Há Documento de Visão do Produto (desde versão anterior);
- IV - Há Documento de Requisitos;
- V - Há Documento de Arquitetura do Produto;
- VI - Há Documento de Interface do Produto;
- VII - Há Plano de Testes;
- VIII - Há Plano de Implantação e Liberação do Produto;
- IX - Implementação foi validada por Testador;
- X - Implementação foi validada por Homologador;
- XI - Pacote de Liberação foi validado por Configurador em ambiente de desenvolvimento distinto do ambiente do Desenvolvedor;
- XII - Pacote de Liberação foi validado por Configurador em ambiente de testes;
- XIII - Pacote de Liberação foi validado por Configurador em ambiente de homologação.

11. MONITORAMENTO E AUDITORIA

11.1. As auditorias ordinárias ou extraordinárias serão coordenadas pelo Gestor de Segurança da Informação e os relatórios serão encaminhados ao Comitê de Segurança da Informação e Comitê de Governança Digital.

11.2. As auditorias extraordinárias deverão ser precedidas de autorização do Comitê de Segurança da Informação.

12. ATUALIZAÇÃO DA NORMA

12.1. O disposto na presente norma será atualizado sempre que alterados os procedimentos de Sistemas, observada, ainda, a periodicidade prevista para a revisão da Política de Segurança da Informação.

LUIS GUSTAVO BIAGIONI

Presidente Substituto



Documento assinado eletronicamente por **Luis Gustavo Biagioni, Presidente Substituto**, em 10/08/2022, às 19:03, conforme art. 1º, III, "b", da Lei 11.419/2006.



A autenticidade do documento pode ser conferida no site <https://sei.icmbio.gov.br/autenticidade> informando o código verificador **11778758** e o código CRC **DC04B20E**.



MINISTÉRIO DO
MEIO AMBIENTE



MINISTÉRIO DO MEIO AMBIENTE
INSTITUTO CHICO MENDES DE CONSERVAÇÃO DA BIODIVERSIDADE
GABINETE DA PRESIDÊNCIA

EQSW 103/104, Bloco "C", Complexo Administrativo - Bloco C - Bairro Setor Sudoeste - Brasília - CEP 70670-350

Telefone: (61) 2028-9011/9013

ANEXOS VIII - NORMA DE SEGURANÇA DA INFORMAÇÃO (NSI)
NSI 008/2022 - POLÍTICA DE BACKUP E RECUPERAÇÃO DE DADOS

1. OBJETIVO

1.1. Estabelecer diretrizes e padrões para: Procedimentos de *backup* e recuperação de dados, no âmbito do Instituto Chico Mendes de Conservação da Biodiversidade - ICMBio.

1.2. Regulamentar a política de backup das informações eletrônicas no âmbito do ICMBio, com o objetivo de estabelecer diretrizes para o processo de cópia e armazenamento dos dados sob a guarda do Centro de Processamento de Dados.

1.3. Os dados e informações do ICMBIO estão localizados dentro de um sistema de armazenamento conhecido por *Storage*. A proposta da política de backup é gerenciar por meio de um software de controle e em conjunto com as partes interessadas (usuários) toda a massa de dados do ICMBIO que necessite de cópia de segurança em fita, especificando o momento de cópia, retenção, restauração e descarte da informação.

2. MOTIVAÇÕES

2.1. Alinhamento as normas, regulamentações e melhores práticas, relacionadas a matéria.

2.2. Garantia de que a salvaguarda das informações seja realizada de forma otimizada, atendendo as necessidades do ICMBio.

3. REFERÊNCIAS NORMATIVAS

3.1. Instrução Normativa nº 1, de 27 de maio de 2020, do Gabinete de Segurança Institucional da Presidência da República, que dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da Administração

Pública Federal.

3.2.Instrução Normativa Nº 03, de 28 de maio de 2021, do Gabinete de Segurança Institucional da Presidência da República, que dispõe sobre os processos relacionados à gestão de segurança da informação nos órgãos e nas entidades da administração pública federal.

3.3.Norma Técnica ABNT NBR ISO/IEC 27001:2013, que especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação dentro do contexto da organização.

3.4.Norma Técnica ABNT NBR ISO/IEC 27002:2013, que fornece diretrizes para práticas de gestão de segurança da informação.

3.5.Lei nº 13.709/2018 , de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais.

3.6.Instrução Normativa nº 1, de 04 de abril de 2019, que dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação - TIC pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISF do Poder Executivo Federal.

4. CONCEITOS E DEFINIÇÕES

4.1.Backup: Salvaguarda de arquivos com o propósito de prevenir perda de dados em um evento de falha ou destruição de equipamento.

4.2.Backup Full: backup dos arquivos do servidor em sua totalidade (inclui arquivos que não são alterados na rotina de trabalho diária).

4.3.Backup Incremental: backup somente de arquivos que foram modificados desde último backup.

4.4.Backup Diferencial: backup somente de arquivos que foram modificados desde o último "backup full".

4.5.Momento de cópia (janela de backup): O horário para realização do backup. As "melhores práticas" apontam para realização do backup fora do horário de produção, visto que este processo pode consumir recursos de rede e servidores, impactando no trabalho dos usuários. Informamos que não existem backups das máquinas dos usuários e de servidores implantados nas Unidades Descentralizadas.

4.6.Retenção: Tempo o qual os dados copiados permanecem guardados esperando para serem apagados. Os dados expirados (fim do período de retenção) são "deletados" e abrem espaço para novos dados (novas cópias de backup). Caso a retenção seja infinita há um acúmulo constante de dados.

4.7.Restauração: Processo de trazer dados de volta a produção, podendo ser restaurados no local de origem ou alternativo.

4.8.Descarte da informação: Não é necessário esperar o momento de expiração dos dados retidos para reciclar a mídia utilizada no backup (disco, fita magnética, pendrive, etc) o descarte pode ocorrer com a permissão do usuário a fim recuperar espaço para realização de outros backups.

4.9.Administrador de Backup: servidor público ou colaborador do Instituto responsável pelos procedimentos de configuração, execução, monitoramento e testes dos procedimentos de backup e restauração.

4.10.RPO (Recovery-Point Objective): o quanto é necessário voltar no tempo para encontrar um backup dos dados, ou seja, o tempo máximo de perda de

dados.

4.11.RTO (Recovery-Time Objective): tempo estimado para restaurar os dados ou para tornar os sistemas operacionais novamente.

5. DIRETRIZES

5.1.RESPONSABILIDADES E ATRIBUIÇÕES:

5.1.1A área de tecnologia da informação do ICMBio será responsável pela política e procedimentos relativos aos serviços de backup e restauração, bem como de guardar as mídias móveis e assegurar o cumprimento das normas aplicáveis.

5.2.São atribuições do administrador de backup:

5.2.1.propor modificações visando o aperfeiçoamento da política de backup;

5.2.2.criar e manter as tarefas de backup;

5.2.3.configurar a ferramenta de backup e os clientes;

5.2.4.criar e manter mídias;

5.2.5.testar o backup e a restauração;

5.2.6.criar notificações e relatórios;

5.2.7.verificar periodicamente os relatórios gerados pela ferramenta de backup;

5.2.8.restaurar os backups em momentos definidos pela área de tecnologia da informação para teste de funcionalidade e extraordinariamente quando solicitado;

5.2.9.gerenciar mensagens e logs diários dos backups, fazendo o tratamento dos erros de forma que o procedimento de backup tenha sequencia e os erros na sua execução sejam eliminados;

5.2.10.fazer manutenções periódicas dos dispositivos de backup;

5.2.11.fazer o carregamento das mídias necessárias para os backups programados.

6. ESCOPO DO BACKUP

6.1.Todo e qualquer ativo de TI que armazene dados e que esteja sob responsabilidade do CPD deverá ser considerado para avaliação de inclusão no processo de backup.

6.2.Esta política aplica-se a todos os dados em posse da instituição que foram solicitados para salvaguarda pelos usuários. O sistema de backup não possui autonomia para definir qual(is) dado(s) tem valor/importância para instituição nem o seu período de retenção, cabendo apenas à função de consulente.

7. PROCEDIMENTOS DO BACKUP

7.1.O responsável pelo produto, sistema ou serviço deve solicitar formalmente a área de Tecnologia da Informação a inserção de dados ao sistema de backup, previamente a entrada em operação de tais soluções.

7.2.Cabe ao responsável pelo produto, sistema ou serviço, definir, com apoio da área de Tecnologia da Informação, os requisitos para realização do backup, tais como: os dados que devem estar contemplados no backup, tempo de retenção, RTO, RPO, dentre outros.

7.3.Em caso de alteração dos requisitos para realização do backup, o responsável deverá atualizar a Área de Tecnologia da Informação das novas demandas, para correta salvaguarda das informações.

7.4.Os dados armazenados no disco rígido de estações de trabalho ou de notebooks não serão objeto de backup de dados. Nesse sentido, sua recuperação não é garantida em casos de indisponibilidade causados por erros de hardware no disco rígido, apagamentos acidentais ou intencionais, falhas no sistema operacional, ação de códigos maliciosos, dentre outros.

7.5.A periodicidade, o tempo de retenção, o RPO e o RTO dos backups observarão as seguintes regras:

Tipo e Política	Retenção
Incremental: Segunda a Quinta às 18:40 Diferencial: Sexta às 18:40 Full: Mensal - única Sexta por mês às 18:40	Incremental: 62 dias Semanal: 62 dias Mensal: 365 dias
Incremental: Segunda a Quinta às 19:50 Diferencial: Sexta às 19:50 Full: Mensal - única Sexta por mês às 19:50	Incremental: 62 dias Semanal: 62 dias Mensal: 365 dias

7.6.No caso de serviços armazenados na nuvem, a responsabilidade pelo *backup* será da prestadora de serviços, assegurando um prazo de retenção de, no mínimo, 30 dias.

7.7.As mídias de *backup*, quando transportadas, deverão ser protegidas de extravio e de eventos que possam causar dano físico.

7.8.A movimentação de mídias de *backup* deverá ser realizada por servidor designado, com registro, no mínimo, da identificação da mídia e a data e a hora da movimentação

8. RECUPERAÇÃO DE DADOS

8.1.A recuperação de dados e arquivos, sempre que não puder ser realizada pelo próprio usuário, será solicitada a Área de Tecnologia da Informação.

8.2.A recuperação de backups deverá obedecer as seguintes orientações:

8.2.1.A solicitação de recuperação de objetos deverá sempre partir do responsável pelo recurso, através de chamado técnico, utilizando a ferramenta de controle de atendimentos;

8.2.2.O chamado técnico deve conter, ao menos, o nome e setor do usuário, o(s) objeto(s) a ser(em) recuperado(s), localização em que se encontra(m), a data da versão que deseja recuperar, local alternativo para o armazenamento do(s) objeto(s) recuperado(s), se for o caso, e a justificativa para recuperação;

8.2.3. Este chamado será encaminhado ao Administrador de Backup, que após a conclusão da tarefa, realizará o fechamento do chamado indicando a restauração do(s) objeto(s);

8.2.4. A restauração de objetos somente será possível nos casos em que este tenha sido atingido pela estratégia de backup.

9. DESCARTE DAS MÍDIAS

9.1. O descarte das Mídias de backup inservíveis ou inutilizáveis deverá ser feito pela área de tecnologia da informação mediante solicitação do Administrador de Backup.

9.2. As Mídias de backup a serem descartadas deverão ser destruídas de forma a impedir a sua reutilização ou acesso indevido aos dados por pessoas não autorizadas conforme preconiza a Política de Segurança da Informação (POSIN) do ICMBio.

10. MONITORAMENTO E AUDITORIAS

10.1. As auditorias ordinárias ou extraordinárias serão coordenadas pelo Gestor de Segurança da Informação e os relatórios serão encaminhados ao Comitê de Segurança da Informação e Comitê de Governança Digital.

10.2. As auditorias extraordinárias deverão ser precedidas de autorização do Comitê de Segurança da Informação.

11. ATUALIZAÇÃO DA NORMA

11.1. O disposto na presente norma será atualizado sempre que alterados os procedimentos de backup, observada, ainda, a periodicidade prevista para a revisão da Política de Segurança da Informação.

LUIS GUSTAVO BIAGIONI

Presidente Substituto



Documento assinado eletronicamente por **Luis Gustavo Biagioni, Presidente Substituto**, em 10/08/2022, às 19:03, conforme art. 1º, III, "b", da Lei 11.419/2006.



A autenticidade do documento pode ser conferida no site <https://sei.icmbio.gov.br/autenticidade> informando o código verificador **11778864** e o código CRC **0B26D69E**.



MINISTÉRIO DO
MEIO AMBIENTE



**MINISTÉRIO DO MEIO AMBIENTE
INSTITUTO CHICO MENDES DE CONSERVAÇÃO DA BIODIVERSIDADE
GABINETE DA PRESIDÊNCIA**

EQSW 103/104, Bloco "C", Complexo Administrativo - Bloco C - Bairro Setor
Sudoeste - Brasília - CEP 70670-350

Telefone: (61) 2028-9011/9013

ANEXOS IX - NORMA DE SEGURANÇA DA INFORMAÇÃO (NSI)

NSI 009/2022 - GESTÃO DE CONTINUIDADE DE TI

1. OBJETIVOS

1.1. Estabelecer diretrizes e padrões para: Gestão de Continuidade de TI, no âmbito do Instituto Chico Mendes de Conservação da Biodiversidade - ICMBio.

2. MOTIVAÇÕES

2.1. Alinhamento as normas, regulamentações e melhores práticas relacionadas a matéria.

2.2. Correto direcionamento e dimensionamento de recursos tecnológicos para prover a Gestão de Continuidade de TI.

2.3. Manutenção de um nível aceitável de resiliência dos serviços e sistemas de TI frente a eventos que possam causar sua interrupção, contribuindo para contínua melhoria da prestação dos serviços do ICMBio.

2.4. Estabelecer procedimentos de gestão para assegurar a continuidade das operações de TI.

3. REFERÊNCIAS NORMATIVAS

3.1. Instrução Normativa GSI/PR nº 3, de 28 de maio de 2021 que dispõe sobre os processos relacionados à gestão de segurança da informação nos órgãos e nas entidades da administração pública federal.

3.2. Norma Técnica ABNT NBR ISO/IEC 27001:2013, que especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação dentro do contexto da organização.

3.3. Norma Técnica ABNT NBR ISO/IEC 27002:2013, que fornece

diretrizes para práticas de gestão de segurança da informação.

3.4. Norma Técnica ABNT NBR ISO/IEC 22301:2020, que normatiza o sistema de gestão de continuidade de negócios e especifica os requisitos para planejar, estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar continuamente um sistema de gestão documentado para se proteger, reduzir a possibilidade de ocorrência, preparar-se, responder e recuperar-se de incidentes de interrupção quando estes ocorrerem.

3.5. Instrução Normativa nº 1, de 04 de abril de 2019, que dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação - TIC pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal

4. CONCEITOS E DEFINIÇÕES

4.1. Análise de Impacto nos Negócios (AIN): estimativa dos impactos resultantes da interrupção de atividades e de cenários de desastres que possam afetar a prestação dos serviços do ICMBio, bem como técnicas para quantificar e qualificar esses impactos. Define também a criticidade dos processos de negócio, prioridades, interdependências e os requisitos de segurança da informação para que os objetivos de recuperação sejam atendidos nos prazos estabelecidos.

4.2. Atividades Críticas: atividades que devem ser executadas de forma a garantir a consecução dos produtos e serviços fundamentais do órgão ou entidade, de forma que permitam atingir os objetivos mais importantes e sensíveis ao tempo.

4.3. Continuidade de Negócios: capacidade de um órgão ou entidade de, quando ocorrer algum incidente de interrupção, manter suas operações em um nível aceitável, previamente definido, minimizando os impactos e recuperando perdas de ativos da informação das atividades críticas.

4.4. Desastre: incidente que tenha causado algum dano grave, colocado em risco algum ativo de informação crítico ou interrompido a execução de alguma atividade crítica por um período de tempo superior ao aceito pela organização.

4.5. Estratégia de Continuidade: abordagem de um órgão ou entidade que garante a recuperação dos ativos de informação e a continuidade das atividades críticas ao se defrontar com um desastre, uma interrupção ou outro incidente maior.

4.6. Gestão de Continuidade: processo abrangente de gestão que identifica ameaças potenciais para uma organização e os possíveis impactos nas operações de negócio, caso estas ameaças se concretizem. Este processo fornece uma estrutura para que se desenvolva uma resiliência organizacional que seja capaz de responder efetivamente e salvaguardar os interesses das partes interessadas, a reputação, a marca da organização e suas atividades de valor agregado.

4.7. Gestor da Unidade: Coordenador Geral, Coordenador, Chefe de divisão, Chefe de serviço ou servidor designado para responder por uma unidade ou serviço constante do Regimento interno do ICMBio.

4.8. Plano de Continuidade: conjunto de procedimentos documentados que orientam a organização, após a interrupção, em como responder, recuperar, retomar e restaurar para um nível predefinido de operação, composto por Plano de Continuidade Operacional e Plano de Recuperação de Desastres.

4.9.Plano de Continuidade Operacional (PCO): documento que descreve procedimentos operacionais e técnicos a serem realizados frente a determinados cenários de falha, para manutenção dos serviços, ainda que em um nível mínimo de operacionalidade.

4.10.Plano de Recuperação de Desastres (PRD): documento que descreve procedimentos técnicos, focado em ativos e serviços tecnológicos, a serem realizados frente a determinados cenários de falhas dos principais serviços de TI, visando o retorno a normalidade.

4.11.Redes Nacionais de Computadores do ICMBio: Infraestrutura de Rede de computadores conectados via MPLS ou VPN *Site-to-Site*.

4.12.Resiliência: poder de recuperação ou capacidade de uma organização resistir aos efeitos de um desastre.

4.13.RPO (Recovery Point Objective): ponto em que a informação usada por uma atividade deve ser restaurada para permitir a operação da atividade na retomada.

4.14.RTO (Recovery Time Objective): Tempo máximo para retorno operacional de um serviço ou processo de negócio após a ocorrência de um desastre.

4.15.SISP: Sistema de Administração dos Recursos de Tecnologia da Informação do Poder Executivo Federal.

5. DIRETRIZES

5.1.A Gestão de Continuidade de TI visa:

5.1.1.Reduzir o risco e minimizar o impacto de interrupções dos serviços e sistemas de TI que suportam as atividades críticas do ICMBio;

5.1.2.Manter os sistemas e serviços críticos de TI em um nível minimamente operável e aceitável durante a ocorrência de um desastre, de forma a não interromper a prestação dos serviços do ICMBio;

5.1.3.Definir procedimentos para que as atividades críticas operem em nível de contingência quando da ocorrência de um desastre ou interrupção não programada, até que a situação retorne a normalidade.

5.1.4.Nortear as estratégias de continuidade de TI, de modo a observar o resultado das análises de riscos de TI e da análise de impacto de negócio realizadas.

5.1.5.Elaborar Plano de Continuidade de TI, com vistas a documentar os procedimentos necessários a operação em nível de contingência e comunicações necessárias, bem como o retorno a normalidade, quando da ocorrência de interrupções dos serviços e sistemas de TI.

5.1.6.Fornecer recursos humanos, tecnológicos e financeiros para a manutenção e melhoria contínua da gestão de continuidade de TI.

6. PROCESSO DE GESTÃO DE CONTINUIDADE DE TI

6.1.O processo de Gestão de Continuidade de TI é composto

pelas seguintes etapas:

6.1.1.Planejamento: compreende a análise dos processos críticos para o negócio, a fim de estabelecer quais atividades do Instituto são essenciais para a prestação dos serviços, quais deverão ser tratadas na Continuidade de TI e quais estratégias serão utilizadas durante a ocorrência de um incidente. Compreende também a avaliação da necessidade de revisão dos planos já instituídos, seja em virtude do tempo decorrido desde sua aprovação, seja em razão de mudanças na infraestrutura, procedimentos ou testes realizados;

6.1.2.Execução: abrange a elaboração ou revisão dos planos pelas equipes técnicas, com a descrição dos cenários de falhas e os procedimentos técnicos para lidar com os problemas, a aprovação dos planos, seu armazenamento e divulgação;

6.1.3.Verificação: abrange a realização de testes periódicos dos Planos desenvolvidos e a análise dos incidentes críticos ocorridos (desastres) a fim de subsidiar a etapa de melhoria;

6.1.4.Melhoria: compreende a identificação das oportunidades de melhoria e seu encaminhamento a consideração superior, com vistas a dar início a novo ciclo do processo.

6.2.O desenho do processo de Gestão de Continuidade de TI, a descrição das atividades, os respectivos papéis e responsabilidades dos envolvidos no processo, bem como os modelos de documentos e indicadores definidos para o processo serão publicados no Portal de Governança de TI, após aprovação pela Presidência.

6.3.O processo será revisto bianualmente ou em menor prazo, quando necessário, e eventuais alterações propostas nos documentos acima indicados serão, após aprovação pela Presidência deste Instituto, objeto de imediata divulgação na forma do item anterior.

7. PLANO DE CONTINUIDADE

7.1.O Plano de Continuidade de TI é composto pelos Planos de Continuidade Operacional e Planos de Recuperação de Desastres.

7.2.O Plano de Continuidade de TI deve ser periodicamente testado, de forma a garantir sua efetividade.

7.3.O Plano de Continuidade de TI deve ser revisado bianualmente em função dos resultados de testes realizados ou após mudança significativa nos ativos de informação (infraestrutura tecnológica, processo, atividades, etc.).

7.4.O Plano de Continuidade de TI será acionado quando verificadas interrupções parciais ou totais que impactem nas atividades críticas do ICMBio.

7.5.Ocorrido o incidente, considerados os serviços, sistemas ou ativos afetados e a criticidade, as equipes técnicas responsáveis acionarão os Planos de Continuidade Operacional para a manutenção da continuidade das atividades, ainda que de forma contingencial, e os Planos de Recuperação de Desastre para retorno das atividades a normalidade.

7.6.A comunicação as partes interessadas observará as orientações contidas nos Planos de Continuidade Operacional.

7.7.Os ativos e serviços afetados pelo incidente serão monitorados

pelas equipes responsáveis, a fim de subsidiar o fornecimento de informações a autoridade superior.

7.8.A ativação do Plano de Continuidade de TI será encerrado quando da comunicação de retorno a normalidade dos serviços, sistemas ou ativos afetados.

8. MONITORAMENTO E AUDITORIAS

8.1.As auditorias ordinárias ou extraordinárias serão coordenadas pelo Gestor de Segurança da Informação e os relatórios serão encaminhados ao Comitê de Segurança da Informação e Comitê de Governança Digital.

8.2.As auditorias extraordinárias deverão ser precedidas de autorização do Comitê de Segurança da Informação.

8.3.Os procedimentos constantes desta norma deverão ter monitoramento contínuo da área de tecnologia da informação visando a melhoria contínua.

9. ATUALIZAÇÃO DA NORMA

9.1.O disposto na presente norma será atualizado sempre que alterados os procedimentos de gestão de continuidade de TI, observada, ainda a periodicidade prevista para a revisão da política de Segurança da Informação.

LUIS GUSTAVO BIAGIONI

Presidente Substituto



Documento assinado eletronicamente por **Luis Gustavo Biagioni, Presidente Substituto**, em 10/08/2022, às 19:05, conforme art. 1º, III, "b", da Lei 11.419/2006.



A autenticidade do documento pode ser conferida no site <https://sei.icmbio.gov.br/autenticidade> informando o código verificador **11778886** e o código CRC **63796799**.



MINISTÉRIO DO
MEIO AMBIENTE