02070.000752/2013-03
Número Sei:11777232

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 e a imagem 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, 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;

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 direta, autárquica e 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 Republica, que disciplina a criação de Equipes de Tratamento e Respostas a Incidentes em Redes Computacionais – ETIR nos órgãos e entidades da Administração Publica Federal, direta e indireta – APF;

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 Presidência da Republica, que estabelece as Diretrizes para Gerenciamento de Incidentes em Redes Computacionais 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;

XX - 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

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;

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;

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

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;

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;

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;

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

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

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

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;

ATOS INTERNACIONAIS: vide tratados internacionais;

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

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;

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;

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;

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;

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

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;

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;

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;

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

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

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

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;

BACKUP: conjunto de procedimentos que permitem salvaguardar 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;

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;

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

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

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;

BIOMETRIA: verificação da identidade de um indivíduo por meio de uma característica física o8 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;

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;

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;

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

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

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;

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;

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;

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;

CERT DIVISION: vide computer emergency response team division;

CERTIFICAÇÃO: atesta a validade de um documento ou entidade;

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

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;

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;

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

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;

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

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;

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

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

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;

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;

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

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;

Colaborador: pessoa que atua nos processos laborais do Instituto, independentemente de qual seja o vínculo institucional, exemplo: bolsista, voluntário, terceirizado;

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;

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

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;

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;

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;

COMMON VULNERABITIES 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;

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;

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);

COMPROMETIMENTO - perda de segurança resultante do acesso não autorizado;

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;

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

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

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;

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;

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

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;

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

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;

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;

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;

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;

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

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

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;

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;

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

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

CÓPIA DE SEGURANÇA - vide backup.

CREDENCIAL 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);

CRENDENCIAMENTO: 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;

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

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;

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;

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;

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

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

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;

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;

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

DESCREDENCIAMENTO 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;

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

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;

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;

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

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

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

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

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

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

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

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

ECOSSISTEMA 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;

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

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;

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;

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;

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;

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;

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;

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;

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;

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;

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

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;

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

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;

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;

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;

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

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;

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

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, ocross-site scripting, o abuso de configuração de autenticação fraca e o abuso de falhas de configuração de segurança;

FIDC: sigla de formulário individual de dados para credenciamento;

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;

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;

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;

GESTÃO DE INCIDENTES CIBERNÉTICOS: processo que realiza ações sobre qualquer evento adverso relacionado à

segurança cibernética dos sistemas ou da infraestrutura de computação;

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;

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;

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;

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

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

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;

GSC: sigla de gestor de segurança e credenciamento;

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;

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;

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);

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;

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;

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

HSTS: sigla de HTTP strict transport security;

HTTP: sigla de hypertext transfer protocol;

HTTPS: sigla de hypertext transfer protocol secure;

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;

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;

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 do*site* a cessado e a proteção da privacidade e integridade dos dados trocados durante o tráfego de informações;

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

IaaC: sigla de infraestrutura como código (infrastructure as a code);

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

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

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

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

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

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

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

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;

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;

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

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;

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

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

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

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;

INFORMAÇÃO SIGILOSA CLASSIFICADA: vide informação classificada;

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);

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;

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;

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;

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;

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

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;

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;

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;

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;

INTERNET 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;

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;

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;

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;

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;

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

IP: sigla de Internet protocol;

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;

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;

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;

LAI: sigla de Lei de Acesso a Informação;

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

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;

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;

LISTA DE BLOQUEIO: vide blacklist;

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

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;

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 softwared entro dela não pode adulterar o computador *host*. As máquinas virtuais também podem ser usadas para outras finalidades, como a virtualização de servidores;

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;

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);

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

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;

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

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;

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

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;

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;

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;

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

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;

NSC: sigla de Núcleo de Segurança e Credenciamento;

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;

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;

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;

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;

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

ONE-TIME PASSWORD- vide senha descartável;

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

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;

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

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;

OWASP: sigla de open web application security project;

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

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

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

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;

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

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

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);

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;

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

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

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

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);

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;

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

PROVA DE PARTICIPAÇÃO: vide proof of stake;

PROVA DE TRABALHO: vide proof of work;

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;

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;

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;

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;

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;

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;

PSN: sigla de provedor de serviço de nuvem;

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;

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

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;

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;

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

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;

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;

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;

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

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;

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;

REMETENTES CONFIÁVEIS: vide whitelist;

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;

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;

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);

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

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;

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;

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

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;

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;

RoT - sigla de root of trust;

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

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

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 o*mouse*é clicado, ou a região que circunda a posição onde o*mouse*é clicado. É bastante utilizado por atacantes para capturar as teclas digitadas pelos usuários em teclados virtuais, disponíveis principalmente em sites de Internet banking;

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

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;

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;

SEGURANÇA CORPORATIVA - vide segurança orgânica;

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

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;

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;

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;

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;

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;

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

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;

SI: sigla de segurança da informação;

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;

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

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;

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;

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;

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;

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;

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;

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;

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

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

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;

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;

SSL: sigla de secure sockets layer;

SSO: sigla de single sign-on;

STAR: sigla de security trust and assurance registry;

TCG: sigla de trusted computing group;

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

TCP: sigla de transmission control protocol;

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;

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;

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;

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

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;

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;

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;

TESTE DE INTRUSÃO: vide teste de penetração;

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;

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

TIC: sigla de tecnologia da informação e comunicação;

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

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;

TLS: sigla de transport layer security;

TPM: sigla de trusted platform module;

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;

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;

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

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;

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;

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;

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;

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;

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;

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

TRATAMENTO DE RISCOS: processo de implementação de ações de Segurança da Informação para evitar, reduzir, reter ou transferir um risco;

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;

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;

TROJAN- vide cavalo de Tróia;

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;

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

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 iuentifier). Ressalta-se que, no sistema UNIX, UID significa identificador do usuário (user identifier);

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;

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;

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;

URL - sigla de uniform resource locator;

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;

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;

VENDOR LOCK-IN- também conhecido como lock-in proprietário ou lock-indo 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;

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;

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;

VIRTUAL MACHINE(VM): vide máquina virtual;

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

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);

VM: sigla de máquina virtual (virtual machine);

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

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

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.

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;

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;

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 acidental;

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

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

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

VI - 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 da sociedade e do Estado e a inviolabilidade da intimidade da vida privada, da honra e da imagem das pessoas;

XV - respeito e promoção dos direito 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 acesso às informações.

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 resida 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 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 l (um) membro suplente da Diretoria de Ações Socioambientais e Consolidação Ţerritorial em Unidades de Conservação — DISAT;

V - 01 (um) membro titular e 01 (um) membro suplente da Diretoria de Pesquisa, Avaliação e Monitoramento da Biodiversidade — DIBIO

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 competência 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.

LUIS GUSTAVO BIAGIONI

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**.

ICMBio INSTITUTO CHICO MENDES MMA

MINISTÉRIO DO MEIO AMBIENTE

Criado por 05448953123, versão 6 por 05448953123 em 10/08/2022 18:58:40.