

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES DO IBGE

Ministério do Planejamento e Orçamento
Instituto Brasileiro de Geografia e Estatística – IBGE
Comitê de Segurança da Informação e Comunicações - CSI

Política de Segurança da Informação e Comunicações do IBGE

Rio de Janeiro
2023

Presidente da República
Luiz Inácio Lula da Silva

Ministra do Planejamento e Orçamento
Simone Nassar Tebet

Instituto Brasileiro de Geografia e Estatística - IBGE

Presidente
Marcio Pochmann

Diretora-Executiva
Flavia Vinhaes Santos

ÓRGÃOS ESPECÍFICOS SINGULARES

Diretoria de Pesquisas
Cimar Azeredo Pereira

Diretoria de Geociências
Claudio Stenner

Diretoria de Tecnologia da Informação
Marcos Vinicius Ferreira Mazoni

Centro de Documentação e Disseminação de Informações
Jose Daniel Castro da Silva

Escola Nacional de Ciências Estatísticas
Paulo de Martino Jannuzzi

Comitê de Segurança da Informação e Comunicações - CSI

Marcos Vinicius Ferreira Mazoni (Gestor de Segurança da Informação e Comunicações)

Adriana Gonçalves Saraiva (GPR)

Adriane Almeida do Sacramento (SES/SE)

Alexandre José Almeida Teixeira (DGC)

André Eduardo Oliveira de Paula Lico (DE)

Andrea Borges Paim (DPE)

Arnaldo Lyrio Barreto (DTI)

Bruno Cesar Barbosa Alves (DTI)

Carlos José Lessa de Vasconcellos (CDDI)

Gliner Dias Alencar (SES/PE)

Helder José Pacheco Freire (CGOC)

Irene Cavaliere Gomes (GPR)

José Luiz Thomaselli Nogueira (DTI)

Juarez Silva Filho (Comitê Sigilo)

Leandro Albertini Leite (CDDI)

Marcio Imamura (CGOC)

Marcus Vinicius Moraes Fernandes (DPE)

Maria do Carmo Dias Bueno (Comitê Sigilo)

Massashige Takiguchi (DE)

Mauro dos Santos Mendonça (ENCE)

Paulo David de Jesus Tostes dos Santos (ENCE)

Rogério Luis Ribeiro Borba (DGC)

Sandra Martins Lino (Secretária Executivo do CSI)

Sumário

Sumário

1	<i>Introdução</i>	4
1.1	Contextualização	4
1.2	Histórico	6
1.3	Escopo	7
1.4	Conceitos e definições	8
1.5	Princípios	11
2	<i>Diretrizes gerais</i>	13
2.1	Tratamento da Informação	14
2.2	Gestão de Ativos	15
2.2.1	Ativos de informação	15
2.2.2	Ativos de tecnologia da informação	16
2.3	Controle de acesso lógico	18
2.4	Segurança Física e do Ambiente	19
2.5	Conformidade	19
2.6	Auditoria	19
2.7	Desenvolvimento e aquisição de sistemas	20
2.8	Gestão de riscos	21
2.9	Gestão de Continuidade de Negócios	22
2.10	Gestão de incidentes em Segurança da Informação	22
2.11	Acesso à Internet	23
2.12	Serviços de Comunicação	24
2.13	Mídias Sociais	24
2.14	Nuvem	25
2.15	Trabalho Remoto	25
3	<i>Competências e responsabilidades</i>	26

4	<i>Penalidades</i>	30
5	<i>Política de Atualização</i>	30
Anexo I		31
	Relação de Normativos	31
	Referências	32

Apresentação

O compromisso legal do IBGE em manter a privacidade do informante e o sigilo das informações prestadas, conforme previsto na Lei n. 5534, de 14.11.68, aliada nos últimos anos à Lei Geral de Proteção de Dados - LGPD, torna indispensável a implementação de controles rígidos de segurança da informação e comunicações e proteção de dados, garantindo que as atividades desempenhadas na Instituição tratem as informações e estudos de natureza estatística, geográfica, cartográfica, demográfica e administrativa com a devida segurança para garantir a legalidade de suas ações.

As atividades do IBGE sempre foram desenvolvidas tendo como guia os princípios fundamentais da estatística, norteando as práticas, e cabe destacar entre esses a prevenção do mau uso dos dados e a confidencialidade, totalmente alinhados com o objetivo pretendido com a LGPD e com os princípios da segurança da informação, conhecido como DICA (Disponibilidade, Integridade, Confidencialidade e Autenticidade). Percebemos que muitos dos conceitos difundidos nos últimos anos já são utilizados e implementados há tempos pelos órgãos de estatística e o IBGE, como o órgão oficial de produção de estatísticas do Brasil, vem cumprindo esse papel no tratamento dos dados de todos os brasileiros, inclusive as informações sensíveis que também são coletadas.

A implementação dos controles de segurança da POSIC vem se apoiando em três pilares principais: processos, pessoas e tecnologia. O Comitê de Segurança da Informação, em conjunto com a Diretoria de Tecnologia da Informação, promove ações direcionadas a esses três pilares através da normatização de diversos procedimentos e processos, do investimento em novas tecnologias de segurança da informação e em ações voltadas para a capacitação e conscientização dos colaboradores da Instituição.

Marcos Vinicius Ferreira Mazoni

Presidente do Comitê de Segurança da Informação e Comunicações e
Diretor de Tecnologia da Informação do IBGE

1 Introdução

1.1 Contextualização

A Missão do IBGE de “Retratar o Brasil com informações necessárias ao conhecimento de sua realidade e ao exercício da cidadania.” ressalta como é importante o tratamento e o cuidado com as informações que são o objeto principal das atividades realizadas pela Instituição, tanto como insumo quanto como resultado de análises e pesquisas.

Essas informações são um bem público utilizado por todos os setores da sociedade, governos, empresas e cidadãos, para o planejamento e tomada de decisões e precisam estar completas e precisas, e como ativos essenciais para a Instituição e para a sociedade precisam ser devidamente protegidas, garantindo-se a sua integridade, relevância, consistência e excelência, não só daquela que é produzida, mas também daquela utilizada no decorrer dos processos produtivos.

Atualmente toda informação está exposta a muitas ameaças e vulnerabilidades, em virtude da grande conectividade e disponibilidade das informações na rede. Por outro lado, é crescente a necessidade de compartilhamento de dados entre os órgãos e entidades da administração pública federal e com outras esferas, bem como com dados de empresas privadas, que organizados e associados aos dados do IBGE, auxiliam à realização das pesquisas do IBGE e a obtenção de resultados de forma mais ágil, podendo, inclusive, desonerar o cidadão e/ou sua empresa de prestar informações coincidentes a dois ou mais órgãos de governo, como já fazem muitos países desenvolvidos.

O compartilhamento de dados na administração pública federal já está regulado pelo Decreto nº 11.266, de 25 de novembro de 2022, onde se dispensa inclusive a necessidade de estabelecimento de convênios para o compartilhamento. Esse decreto impulsiona ainda mais o uso de registros administrativos pelo IBGE, seguindo-se a tendência mundial. Com a obtenção desses registros, e após o pareamento dos dados obtidos com os dados do IBGE, é possível a sua utilização nas pesquisas realizadas pelo Instituto.

Somando-se a isso, temos também a LGPD - Lei Geral de Proteção de Dados, regulada pelas leis nº 13.709/2018, de 14 de agosto de 2018, e sua alteração a Lei nº. 13.853, de 08 de julho de 2019, que nos obriga a implementar novos controles de segurança voltados à privacidade dos dados com a proteção dos dados pessoais e sensíveis. Essa lei determina a nomeação de um Encarregado de Dados, como o canal de comunicação entre os atores envolvidos no tratamento de dados pessoais. Apesar do IBGE já possuir controles de segurança neste sentido, em virtude do sigilo estatístico, novas demandas surgiram com a entrada em vigor da LGPD, e estão sendo endereçadas pela Instituição.

A difusão do trabalho remoto após o ano de 2019, e consequente aumento do uso de armazenamento e serviços em nuvem pública, trouxe novos desafios à área de segurança da informação e comunicação, e a necessidade de rever e adequar normas, políticas, processos e procedimentos operacionais. A nova realidade de trabalho que se impôs gerou um grande volume de acessos externos à rede do IBGE, e o uso intenso de ferramentas de trabalho colaborativo em nuvem (SaS – Software as a Service), aumentando ainda mais a necessidade de controles rígidos de segurança para manutenção de um ambiente tecnológico seguro para uso do IBGE.

Esses fatores tornaram ainda mais relevante a preocupação da Instituição com o estabelecimento e amadurecimento de controles, como as políticas, que protejam as informações da instituição, resguarde os direitos dos titulares-informantes, a privacidade dos dados pessoais e, em casos mais graves, que garantam a continuidade dos serviços prestados pela Instituição.

A visão do IBGE para 2025, estabelecida no Planejamento Estratégico 2022-2025, é de “Consolidar a posição do IBGE como referência nacional e internacional na produção e disseminação de informações estatísticas e geoespaciais públicas, relevantes, tempestivas e de fácil acesso.” (IBGE, 2022). Essa visão está apoiada nos valores institucionais do IBGE, alguns interrelacionados à segurança da informação e comunicações e proteção dos dados pessoais como: o **Respeito à Confidencialidade**, “O IBGE mantém as informações individuais que coleta sob estrito sigilo e as informações ainda não divulgadas oficialmente para a sociedade sob confidencialidade.”; **Foco nas demandas da sociedade**, “O IBGE produz informações oficiais de relevância e suas práticas são orientadas pelos interesses e necessidades da sociedade brasileira mantendo canais permanentes de diálogo com os seus diferentes grupos de usuários (instituições de ensino e pesquisa, setor público e privado, mídia).”; e o **Respeito ao informante**, “O IBGE respeita os informantes e entende que as informações recebidas são essenciais para o cumprimento de sua missão institucional.”.

O alcance da visão do IBGE requer que as informações estatísticas e geocientíficas produzidas e disseminadas sejam íntegras, relevantes, consistentes e disponíveis quando de suas divulgações. Essas características e a manutenção dos valores institucionais só poderão ser garantidas com controles de segurança e proteção de dados efetivamente implementados, de forma eficiente e eficaz, de acordo com princípios e diretrizes desta Política de Segurança da Informação e Comunicações – POSIC.

A POSIC é uma das práticas listada da norma da International Organization for Standardization - ISO e a International Electrotechnical Commission - IEC (ISO/IEC 27002, 2022) para auxiliar a gestão da segurança da informação, que também estabelece como fator crítico de sucesso dentro de uma organização. A POSIC do IBGE deverá ser seguida por todos que exercem atividades no âmbito do IBGE e que tenham acesso às informações de propriedade ou sob custódia da Instituição.

O valor dos ativos de informação produzidos pelo IBGE é medido de acordo com sua relevância social e econômica para a sociedade. A disponibilidade dos ativos de informação deve ocorrer no momento certo e para o público certo.

A disseminação interna e externa das informações do IBGE, realizada de modo formal ou informal, deve ser cuidadosamente avaliada pelo gestor quanto à importância e aos possíveis impactos, positivos ou negativos, nas atividades do IBGE.

1.2 Histórico

A Política de Segurança da Informação e Comunicações do IBGE foi publicada em 02.08.2017 através de Resolução do Conselho Diretor nº. 24/2017, e o Comitê de Segurança da Informação foi inicialmente instaurado em 21.10.2015 através da Resolução do Conselho Diretor nº. 26/2015. Após a publicação da POSIC, várias políticas, planos, normas e procedimentos foram publicados detalhando as diretrizes definidas na Política. Podemos afirmar que a Segurança da Informação e Comunicações do IBGE está apoiada em diversos documentos estratégicos, táticos e operacionais emitidos pelo Comitê e pela DTI - Diretoria de Tecnologia da Informação.

Destaca-se a elaboração e execução do Plano de Conscientização e Capacitação em Segurança da Informação e Comunicações, desenvolvido pela DTI em conjunto com a ENCE – Escola Nacional de Ciências Estatísticas e implementado com o apoio do CDDI – Centro de Documentação e Disseminação de Informações. Após a finalização deste plano, manteve-se a realização de palestras e a divulgação de matérias informativas para que o corpo técnico do IBGE estivesse sempre em alerta sobre o tema de segurança da informação. O Plano de Gestão de Continuidade de Negócios, voltado para a área de TIC, também foi elaborado inicialmente em julho de 2016, e precisa ser atualizado, pois o parque tecnológico do IBGE já está bastante modificado. Cabe destacar também que após a publicação da POSIC, vários normativos como de controle de acesso, uso de software, uso de recursos de comunicação, dentre outros, foram elaborados e revistos durante este período entre publicações da POSIC.

A entrada em vigor da Lei Geral de Proteção de Dados e a difusão do trabalho remoto tornaram necessária a atualização desta Política para sua adequação às questões de privacidade de dados, bem como as questões que surgiram com o teletrabalho, como a crescente utilização do ambiente de nuvem e o grande número de acessos externos à rede interna do IBGE. O uso de soluções em nuvem permitiu a continuidade dos trabalhos, pois garantiram a colaboração remota entre os servidores na realização de suas tarefas através dos serviços de videoconferências, troca de mensagens instantâneas e o armazenamento de arquivos.

1.3 Escopo

A POSIC do IBGE é o documento corporativo que define os princípios e as diretrizes que norteiam a segurança de informação e proteção de dados no IBGE, estabelecendo quais controles de segurança serão aplicados e, ainda, as responsabilidades e competências na aplicação, gerenciamento e monitoramento dos controles definidos.

A POSIC e os documentos que a complementam em seus princípios e diretrizes permeiam vários objetivos estratégicos, distribuídos nas perspectivas de **Aprendizagem e Crescimento, Processos e Sociedade**. O alinhamento dos controles de segurança e proteção de dados estabelecidos nesta Política impactam significativamente no alcance dos objetivos estratégicos, com destaque para os seguintes:

- **Objetivo Estratégico nº. 2 – Coordenar e promover o Sistema Estatístico Nacional e o Sistema Geocientífico Nacional**

Fortalecer e consolidar o papel do IBGE como coordenador do Sistema Estatístico e do Sistema Geocientífico Nacional, por meio da articulação com órgãos e entidades produtores, provedores e/ou usuários de dados, a fim de assegurar informações de natureza estatística, geográfica, cartográfica e demográfica necessárias ao conhecimento da realidade física, econômica e social do País.

- **Objetivo Estratégico nº. 5 - Aprimorar procedimentos para o uso de registros administrativos, bases de dados e dados não estruturados**

Implementar e desenvolver novas estratégias de aquisição de dados, de forma institucional, contemplando procedimentos para a captação / prospecção, recepção, armazenamento, processamento e o uso de registros administrativos, imagens de sensores remotos, bases de dados e dados não estruturados, incluindo também *crowdsourcing* e *Big Data*. Envolve também a negociação e parceria com outras instituições e provedores de dados para acesso regular a novas fontes.

Por outro lado, o desenvolvimento e fortalecimento da segurança da informação e proteção de dados e de sua absorção pelos colaboradores do IBGE depende também do pleno desenvolvimento dos seguintes objetivos estratégicos:

- **Objetivo Estratégico nº. 9 - Fortalecer a governança de TIC**

Fortalecer o Comitê de Tecnologia da Informação e Comunicação (CTIC) para prover a discussão das iniciativas / projetos / soluções de Tecnologia da Informação e Comunicações do IBGE, alinhando e estimulando a integração.

- **Objetivo Estratégico nº. 11 - Ampliar a governança de dados**

Desenvolver a governança de dados para o avanço da ciência de dados no IBGE.

- **Objetivo Estratégico nº. 18 - Prover ambiente tecnológico adequado e seguro**

Implantar soluções de TIC, infraestrutura e sistemas, que atendam as demandas do IBGE e utilizem as melhores práticas de segurança da informação e comunicações e proteção de dados, garantindo a conformidade com as legislações vigentes

A POSIC deve ser amplamente divulgada no âmbito do IBGE e ter seu conteúdo integralmente disponibilizado para consulta interna, permitindo o acesso de todos os colaboradores do IBGE, para promover a cultura de segurança da informação e comunicações e alcançar a conscientização de todos, fator considerado crítico para o sucesso de uma POSIC, conforme a norma ISO/IEC 27001.

O IBGE desenvolveu e executou um Plano de Capacitação e Conscientização, que define ações para capacitar o corpo funcional do IBGE, bem como manter permanentemente ações de conscientização. O IBGE deve continuar desenvolvendo de forma constante e periódicas ações nesse sentido, como matérias, seminários, cartilhas entre outras que gerem nos colaboradores um alto nível de atenção e consciência ao lidar com as tecnologias de nosso dia a dia, entendendo a importância de cada um de nós no processo de segurança da informação e proteção de dados, como um importante pilar de sustentação.

A implementação da POSIC é norteada por planos e políticas (nível estratégico), instruções normativas (nível tático) e procedimentos (nível operacional), alinhados às diretrizes estabelecidas na mesma. Esses documentos complementares da política estão listados no Anexo I, e poderão ser consultados no site do Comitê de Segurança da Informação e Comunicações do IBGE, <https://w3.csi.ibge.gov.br>.

Seguindo a recomendação da Instrução Normativa nº. 01, de 27 de maio de 2020 (BRASIL, 2020) este documento possui os seguintes tópicos: Escopo; Conceitos e definições; Princípios; Diretrizes Gerais; Competências; Penalidades; além da Política de Atualização

1.4 Conceitos e definições

Ação de evitar o risco – decisão de não se envolver ou agir de forma a se retirar de uma situação de risco. (NBR ISO/IEC 27005, 2008)

Aceitar/Reter o risco - aceitação do ônus da perda ou do benefício do ganho associado a um determinado risco. (NBR ISO/IEC 27005, 2008)

Agente Público - todo aquele que exerce, ainda que sem remuneração ou apenas transitoriamente, mandato, cargo, emprego ou função nos órgãos e entidades públicas. (Exemplos: Servidores, Nomeados em Cargo em Comissão, Contratados Temporários, Estagiários e demais Situações Funcionais)

Ameaça – causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização. (ISO/IEC 27000, 2018)

Ativo - qualquer coisa que tenha valor para a organização. (NBR ISO/IEC 27002, 2005)

Ativos Críticos de Tecnologia da Informação – são os Ativos de Tecnologia da Informação indispensáveis aos processos diretamente relacionados aos objetivos estratégicos da Instituição.

Ativo de Informação – dados, informações e conhecimentos obtidos, gerados, tratados e/ou armazenados no IBGE. Exemplos desses ativos: base de dados, arquivos, contratos, acordos, documentação de sistema, informações sobre pesquisa, manuais de usuário, material de treinamento, procedimentos e planos institucionais, processos de trabalho entre outros.

Ativo de Tecnologia da Informação – composto por ativos de software e ativos físicos, permitindo o armazenamento, a transmissão e processamento das informações. Entre os ativos de software podemos citar os aplicativos, sistemas, ferramentas de desenvolvimento e utilitários. Nos ativos físicos estão incluídos os equipamentos computacionais fixos e móveis, equipamentos utilizados para comunicação de dados e mídias removíveis.

Autoridade Competente – diretor/coordenador-geral responsável pela informação que indica o gestor da informação e/ou do sistema.

Conformidade - ser conforme, análogo ou similar; estar de acordo com determinadas normas, regras ou preceitos.

Contas de Serviço - contas de acesso à rede corporativa de computadores necessários a um procedimento automático (aplicação, *script* etc.), sem qualquer intervenção humana no seu uso.

Controle de Acesso - conjunto de procedimentos, recursos e meios utilizados com a finalidade de garantir que os acessos aos ativos só ocorrerão após autorização e serão restritos, baseados nos requisitos de segurança e nas atividades do usuário. (ISO/IEC 27000, 2018)

Credenciais ou Contas de Acesso - identificação única, concedida de forma pessoal e intransferível a uma pessoa, em conjunto com um método de autenticação. Esse par de informações habilita o seu dono a acessar equipamentos, sistemas e aplicações específicas, de acordo com o perfil definido.

Classificação da Informação – identificação do nível de proteção requerido pela informação, atribuído por autoridade competente.

Colaboradores – agentes públicos do IBGE e consultores.

Comitê de Segurança da Informação e Comunicações CSI – especialistas das áreas setoriais do IBGE, nomeados pela presidente do IBGE, para tratamento dos assuntos relativos à temática de segurança da informação e comunicações.

Confidencialidade – nenhuma informação estará disponível ou será divulgada a entidades (pessoas, sistemas ou órgãos) não autorizadas.

Criticidade – medida de risco obtida da combinação entre o possível impacto na Instituição ou em um projeto e a probabilidade de ocorrência de um evento que afete o mesmo.

Custodiante do Ativo - unidade administrativa responsável pelo armazenamento, operação, administração e preservação de ativos.

Custodiante da Informação - colaborador responsável pela guarda adequada do dado.

Divulgação - ato de tornar público o resultado de uma pesquisa.

Equipe de Tratamento de Incidentes - Grupo de pessoas com a responsabilidade de analisar, tratar e documentar os incidentes de segurança nas redes de computadores e o tratamento aplicado.

Gestor - unidade administrativa responsável por gerenciar determinado segmento de dados e todos os ativos relacionados.

Incidente - um ou mais eventos indesejados ou inesperados que podem causar algum dano, colocando em risco o(s) ativo(s) de informação do IBGE, com probabilidade de interromper ou afetar a qualidade dos serviços e/ou atividades da Instituição.

Infraestrutura de TIC - instalações prediais, equipamentos, computadores, software, redes, telecomunicações, sistemas de armazenamento e recuperação de dados, aplicações computacionais, cabeamento e rede telefônica.

Mitigar/Reduzir o risco – efetuar ações que reduzam a probabilidade, consequências negativas, ou ambas, associadas a um risco. (NBR ISO/IEC 27005, 2008)

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.

Política – intenções e diretrizes da organização, formalmente expressas pela direção da Instituição. (ISO/IEC 27000, 2018)

Risco – efeito da incerteza sobre os objetivos de segurança da informação e é associado com o potencial que as ameaças explorarão vulnerabilidades de um ativo de informação ou grupo de ativos de informação e, assim, causar danos a uma organização. (ISO/IEC 27000, 2018)

Segurança da Informação - preservação da confidencialidade, da integridade e da disponibilidade das informações. (ISO/IEC 27000, 2018)

Sigilo – confidencialidade, segredo.

Sigilo Estatístico – sigilo que deve ser mantido sobre dado coletado no âmbito de operação estatística protegida por lei.

Transferir o risco – compartilhamento com uma outra entidade do ônus da perda ou do benefício do ganho associado a um risco. (NBR ISO/IEC 27005, 2008)

Vulnerabilidade – fragilidade de um ativo ou controle que pode ser explorada por uma ou mais ameaças. (ISO/IEC 27000, 2018)

1.5 Princípios

A POSIC deve obedecer aos princípios constitucionais, administrativos e do arcabouço legislativo vigente que regem a Administração Pública Federal.

Esta POSIC considerou alguns conceitos de Segurança da Informação definidos na Norma ISO/IEC 27000 (Fev;2018), e também nos Princípios Fundamentais das Estatísticas Oficiais estabelecidos pelas Nações Unidas.

São, portanto, os princípios desta POSIC no IBGE:

- **Atualidade** – tanto a POSIC quanto as normas e procedimentos que a compõem devem ser revisados sempre que se fizer necessário, de modo a refletir as mudanças legais, sociais e tecnológicas que interferem na sua aplicabilidade;
- **Aplicabilidade** – os processos de segurança devem ser coordenados e integrados entre si e incorporados nos processos de trabalho e práticas de todas as unidades do IBGE;
- **Autenticidade** – toda informação terá sua origem certificada;
- **Clareza** – normas e procedimentos de segurança produzidos a partir da POSIC devem ser claros o suficiente para que todos os envolvidos com a informação entendam suas responsabilidades, seus direitos e limites;
- **Conhecimento** – colaboradores devem ser continuamente capacitados para o desenvolvimento da cultura de segurança da informação;
- **Confidencialidade** – nenhuma informação estará disponível ou será divulgada a entidades (pessoas, sistemas ou órgãos) não autorizadas;
- **Disponibilidade** – toda informação estará disponível e poderá ser utilizada sob demanda por entidade autorizada (pessoa, sistema ou órgão); e
- **Integridade** – proteção à precisão e à completude dos ativos de informação, garantindo que os mesmos só serão alterados de forma autorizada e não acidental.
- **Privacidade** – proteção dos dados pessoais de acessos não autorizados ou de tratamento inadequado, garantindo seu uso somente para a finalidade definida.

2 Diretrizes gerais

As diretrizes de segurança da informação estabelecidas na POSIC do IBGE aplicam-se aos ativos de informação produzidos, obtidos de terceiros e/ou mantidos no âmbito do IBGE e a todos os ativos de tecnologia da informação e comunicações que compõem o patrimônio do IBGE. Essas diretrizes devem ser seguidas por todos os colaboradores, que se tornam responsáveis pela sua aplicação.

Os ativos devem ser utilizados para a finalidade prevista e para cumprir os objetivos corporativos. Os ativos de informação (dados) devem ter um gestor indicado pela unidade curadora, que, entre outras funções, é responsável por indicar os dados pessoais e sensíveis, para a implementação do tratamento de proteção de dados adequado, como por exemplo a sua possível anonimização, conforme determina a Lei Geral de Proteção de Dados Pessoais (BRASIL, 2018). Os tratamentos realizados nos dados devem ser registrados e informados ao gestor.

A conscientização de todos os colaboradores sobre a importância da segurança da informação e comunicações deve ser realizada continuamente. Através do Plano de Conscientização e Capacitação em Segurança da Informação e Comunicações foram desenvolvidas ações de capacitação e conscientização fundamentais, que contribuíram para que o IBGE preserve seu compromisso legal de sigilo dos dados coletados de pessoas físicas e jurídicas, evitando a identificação do informante ou o vazamento de informações de forma antecipada, provocando também uma mudança comportamental dentro da Instituição. Os produtos deste plano devem ser constantemente revisitados, buscando-se sua atualização quando necessário.

Todos os colaboradores devem estar cientes das penalidades inerentes ao não cumprimento das responsabilidades e obrigações descritas na POSIC e suas normas complementares.

A Gestão de Segurança da Informação e Comunicações do IBGE será realizada com estrutura composta: pelo Gestor de Segurança da Informação e Comunicações, posição exercida pelo Diretor de Tecnologia da Informação, pelo Comitê de Segurança da Informação e Comunicações – CSI e pela Equipe de Tratamento de Incidentes – ETIR.

O Comitê de Adequação à Lei Geral de Proteção de Dados Pessoais (CLGPD), criado em 30.03.2023 através de Resolução do Conselho Diretor nº. 5, desenvolve ações direcionadas à privacidade e proteção de dados pessoais, principalmente aquelas relacionadas ao inventário de dados pessoais, confecção de relatórios de impacto e políticas e programas relacionadas ao tema da LGPD. Os dois comitês devem trabalhar em conjunto, alinhando demandas e ações para alcance dos objetivos de conformidade à LGPD, com a adequada proteção de dados pessoais e sensíveis.

O CSI foi instituído pela Resolução do Conselho Diretor nº 26/2015, de 21.10.2015, e recriado em 20.12.2019 através da Resolução do Conselho Diretor nº. 47/2019, mantendo-se a competência, mas com sua

composição alterada, pois houve a inclusão de representante do Comitê de Sigilo e de representante de Superintendência Estadual. Os especialistas das áreas setoriais do IBGE que constituem o CSI são designados através de Portaria específica da Presidência do IBGE.

O CSI poderá convidar para assessorá-lo, quando necessário, qualquer colaborador do IBGE, bem como, consultar especialistas e representantes de outras instituições.

O CSI deve orientar a priorização de ações e investimentos com vistas a implantar os mecanismos de proteção definidos na POSIC e seus documentos complementares, tendo como base a importância dos ativos para o IBGE.

A ETIR do IBGE foi instituída pela Resolução do Conselho Diretor nº. 120/2022, de 12.12.2022 que cria a ETIR e estabelece sua missão, público-alvo, modelo de implementação, estrutura organizacional, autonomia e serviços a serem realizados pela Equipe, ressaltando-se que esta equipe será responsável por planejar, coordenar, executar e registrar as atividades de tratamento e resposta a incidentes cibernéticos, e é formada por servidores alocados em outras unidades do IBGE, que trabalharam conjuntamente no caso do tratamento de um incidente de segurança da informação.

2.1 Tratamento da Informação

Os ativos de informação armazenados, coletados ou produzidos no IBGE bem como aqueles compartilhados com o IBGE devem possuir um gestor de dados na unidade responsável. As atividades de manutenção e administração dos recursos físicos e lógicos utilizados para recepcionar, armazenar e disponibilizar os dados, em bases de dados ou não, e as soluções de visualização, análise e exploração de dados, armazenados nos *data center* do IBGE são de responsabilidade da Diretoria de Tecnologia da Informação. As ferramentas e soluções de TIC, a serem incluídas no parque tecnológico do IBGE, devem constar no Plano Diretor de Tecnologia da Informação - PDTI definido pelo CTIC.

Os ativos de informação da Instituição que estão em meio digital devem ser armazenados em um *data center* do IBGE ou em uma nuvem (privada ou pública), com os controles de segurança adequados ao dado armazenado. A contratação de serviços em nuvem deve estar alinhada e em conformidade com a Política de Governança de Dados do IBGE.

As informações armazenadas em meio não digital devem ser mantidas por suas áreas gestoras em ambiente e condições que estejam em conformidade com a LGPD.

Os ativos de informação classificados como dados pessoais devem ser inventariados e ter um tratamento diferenciado, aplicando-se sempre que possível a sua anonimização. Esses dados devem ser

mantidos somente pelo tempo necessário para cumprir os propósitos declarados. O compartilhamento de dados pessoais somente deve ocorrer mediante necessidade para o cumprimento de obrigação legal ou da função pública.

O tratamento de dados realizado deve ser documentado e registrado no relatório de impacto, e qualquer incidente ou violação que envolva dados pessoais e que possa acarretar riscos aos direitos e liberdades das pessoas deve ser notificado à Autoridade Nacional de Proteção de Dados - ANPD, através do Encarregado de Dados do IBGE.

O IBGE, através de sua Política de Privacidade, declara como serão utilizados os dados pessoais coletados, inclusive pelos *cookies* utilizados no site e nos sistemas *web*. Podemos afirmar que a maioria dos dados pessoais armazenados no IBGE se enquadram nos incisos II, III, IV e V do Art. 7º. da Lei Geral de Proteção de Dados, ou seja, são para o cumprimento de obrigação legal ou regulatória pelo controlador (inciso II), ou para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres (inciso III) ou para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais (inciso IV) ou ainda para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados (inciso V).

Os dados coletados dos colaboradores do IBGE, em virtude de sua contratação e/ou utilização em sistemas e aplicações para realização de suas atividades institucionais atendem aos incisos acima relacionados, não cabendo, também nesses casos, a necessidade de consentimento.

Independente da hipótese de coleta, serão aplicados controles de segurança para garantir a disponibilidade, integridade, confidencialidade, autenticidade e privacidade dos dados coletados.

2.2 Gestão de Ativos

2.2.1 Ativos de informação

No momento de sua geração ou aquisição, os gestores de ativos de informação devem informar se o dado é pessoal, se é sensível, o grau de confidencialidade, a temporalidade e o ciclo de vida do dado. De acordo com essas informações e a classificação feita de acordo com Política de Classificação de Ativos, quando esta for publicada, serão aplicados sobre os dados controles de segurança específicos, de acordo com a disponibilidade e proteção definidas, a fim de garantir durante o ciclo de vida do dado, desde a criação até a eliminação, a segurança necessária.

O acesso e a utilização dos ativos de informação devem ser precedidos do aceite ao Termo de Confidencialidade, para todos os colaboradores.

Nos contratos estabelecidos com as empresas devem constar cláusulas de confidencialidade, bem como cláusulas que determinem a aderência à POSIC e as sanções cabíveis em caso de descumprimento.

A fim de resguardar informações sensíveis, bem como limitar seu acesso e controlar quaisquer cópias de documentos, dados e reproduções que porventura sejam extraídas da mesma, todos os colaboradores devem se certificar de que documentos sensíveis impressos ou em mídia digital não devem estar expostos e seu descarte deve ser realizado de forma adequada impedindo que a informação possa ser recuperada futuramente.

2.2.2 Ativos de tecnologia da informação

O acesso à rede corporativa do IBGE deve ser realizado exclusivamente através da infraestrutura disponibilizada e autorizada pela unidade gestora de tecnologia da informação do IBGE, cumprindo as recomendações constantes em instrução normativa específica para uso de ativos de tecnologia da informação. Em situações específicas e períodos curtos de tempo pode ser relaxada essa obrigação, por uma situação de trabalho específica, mas todos os profissionais com acessos administrativos à algum serviço, sistema ou infraestrutura do IBGE não podem utilizar equipamentos que não sejam da Instituição. Situações específicas poderão ser avaliadas pela Diretoria de Tecnologia da Informação.

A utilização de ativos de tecnologia da informação do IBGE, do tipo equipamento, requer recebimento, ciência e aceite formal pelos servidores concursados e estagiários do Termo de Responsabilidade sobre o Ativo de Tecnologia que será enviado pela Instituição de forma automática. Os colaboradores contratados pelas empresas prestadores de serviços de TIC ao IBGE, que receberem um equipamento do IBGE, em função do tipo de atividade desempenhada para a Instituição, deverão assinar o Termo de Responsabilidade para Terceiros sobre o Ativo de Tecnologia, e a empresa será informada através de uma carta de todos os equipamentos que se encontram cedidos aos seus funcionários.

Não é permitido adicionar, remover ou manipular os componentes físicos (*hardware*) de ativos de tecnologia da informação sem o consentimento da unidade gestora de infraestrutura de tecnologia da informação.

São considerados ativos críticos de tecnologia da informação todos aqueles necessários para suportar os processos que são diretamente relacionados aos objetivos estratégicos da Instituição e que, de alguma forma, quando não executados de acordo com seus requisitos possam causar prejuízo material ou danos significativos à imagem do IBGE ou à Administração Pública.

Os ativos de tecnologia da informação, assim como suas credenciais de acesso, devem ser inventariados periodicamente e ter seus gestores e custodiantes identificados. A identificação dos ativos de tecnologia deve

seguir as orientações descritas em instrução normativa específica sobre a nomenclatura de ativos de tecnologia da informação.

Não é permitida a instalação de programas (*software*) em ativos de tecnologia da informação do IBGE, independente do regime de licenciamento, sem o consentimento da unidade gestora de infraestrutura de tecnologia da informação do IBGE, conforme instrução normativa específica sobre uso de software no IBGE. O suporte da Diretoria de Tecnologia da Informação só será realizado em equipamentos da própria Instituição, de maneira remota ou presencial na Unidade do IBGE ao qual o colaborador está alocado.

A Diretoria de Tecnologia da Informação deverá dispor de processos de manutenção contínua que assegurem a disponibilidade e a integridade dos ativos de tecnologia da informação, tanto física quanto lógica. Estes processos visam acompanhar os contratos de garantia dos equipamentos e a realização de manutenções preventivas e a aplicação constante das atualizações de *software*.

Os ativos de tecnologia da informação devem, sempre que possível, ser protegidos contra falhas no fornecimento de energia elétrica e de problemas ambientais, como temperatura e umidade, bem como contra perdas, danos, furtos, roubos, acessos indevidos ou qualquer interrupção não programada. Maior atenção deve ser dada aos ativos críticos.

As condições de temperatura e umidade dos ambientes onde há ativos críticos de tecnologia da informação devem, sempre que possível, ser monitoradas com vistas a detectar situações que possam causar problemas de funcionamento ou redução de sua vida útil.

Outra proteção que deve existir nos ativos tecnológicos é a cópia de segurança de todo ativo de interesse da organização, garantindo a recuperação de dados, configurações e sistemas, em caso de falhas ou perdas nos ativos, tanto físicas quanto lógicas. As regras sobre a realização de cópias de segurança (*backup*) estão definidas na Política de Backup e Recuperação de Dados Digitais.

O uso eventual de ativos de tecnologia da informação para fins pessoais é tolerado, desde que não conflite com determinações e normas internas do IBGE e o Código de Ética dos Funcionários Públicos. Veta-se seu uso para fins de entretenimento, veiculação de opiniões político-partidárias, sindicais, religiosas, discriminatórias ou afins. O IBGE não se responsabiliza por informações de caráter pessoal armazenadas nestes recursos.

A movimentação dos ativos de tecnologia da informação deverá ser precedida de registro e autorização, formalmente concedida. Nesses casos, e também em casos de alienação e descartes, deverão ser seguidos procedimentos adequados para que não haja risco de vazamento ou perda de informações.

2.3 Controle de acesso lógico

As credenciais de acesso dos colaboradores do IBGE devem ser individuais e o seu compartilhamento não é permitido. O responsável pela credencial responde por toda e qualquer ação realizada mediante utilização de sua credencial de acesso. A autenticação em dois fatores deve ser implementada no acesso à rede do IBGE.

A concessão de privilégios de acesso deve ser realizada em conformidade com o princípio do privilégio mínimo, ou seja, cada credencial de acesso deve possuir apenas o conjunto de privilégios estritamente necessário ao desempenho das suas atribuições profissionais.

A utilização de privilégios administrativos deve ser realizada com a observância de rigorosos preceitos éticos e somente quando indispensável para a execução de atividade necessária à sustentação de ativos de tecnologia da informação ou para o cumprimento de tarefa específica formalmente atribuída.

A concessão de acesso remoto a ativos de tecnologia da informação, realizada obrigatoriamente a partir de equipamentos do IBGE, deve ser precedida de autorização do custodiante do ativo, após análise da justificativa fornecida pelo gestor explicitando a necessidade do acesso. Este acesso deve contemplar somente os ativos necessários à realização do serviço, utilizar canal seguro, concedido em caráter provisório ou definitivo.

As credenciais de acesso, chamadas contas de serviço, são destinadas à execução de programas, rotinas e procedimentos, que demandem acesso automatizado a ativos de tecnologia da informação, devem ser utilizadas exclusivamente para tal fim e seu uso ordinário por colaboradores do IBGE não é permitido.

O acesso ao ambiente de execução de sistemas, em regime de produção, por colaboradores que atuam nas atividades de desenvolvimento de sistemas deve ser rigorosamente limitado, sendo permitido somente em caso de exceção, transitoriamente, com o objetivo de viabilizar operação específica e com o acompanhamento do colaborador responsável pela gestão desse ambiente.

Todos os sistemas de informação do IBGE devem possuir um gestor, formalmente designado pela autoridade competente, que será responsável por solicitar e definir os privilégios de acesso às informações relacionadas ao sistema em questão. As alterações de atribuições dos colaboradores devem ser informadas pelo gestor imediatamente para adequação dos privilégios de acesso.

Baseada nessas diretrizes, a instrução normativa específica sobre controle de acesso determina os diferentes tipos de credenciais, as formas de administração (concessão, revogação e revisão de privilégios de acesso) e as regras para uso das credenciais para acesso aos ativos de tecnologia da informação, bem como os critérios de formação das senhas para as credenciais.

2.4 Segurança Física e do Ambiente

Os equipamentos considerados críticos ao desempenho das atividades do IBGE devem ser armazenados em áreas apropriadas, com acesso restrito e, sempre que possível, controlado por dispositivos de identificação física, característica física ou comportamental do indivíduo que tenta acessar a área e outra lógica, relacionada a uma informação que o indivíduo precisa saber. Esses acessos devem ser registrados.

A instrução normativa de controle de acesso também estabelece regras e critérios de segurança para o acesso físico aos *Data Centers* do IBGE e para infraestrutura necessária para o seu funcionamento.

2.5 Conformidade

A garantia da conformidade do ponto de vista dos requisitos legais exige um conhecimento prévio desses requisitos relacionados aos sistemas de informação existentes no IBGE, bem como das características de guarda associadas a esses requisitos legais, como o período de retenção e o tipo de mídia existente, evitando-se com isso a violação de qualquer lei criminal ou civil, estatutos, regulamentações ou obrigações contratuais.

Destaca-se o requisito legal relacionado à propriedade intelectual no uso de materiais e produtos de *software* proprietários. Esse último já vem sendo solucionado no IBGE com a proibição de instalação de produtos diretamente pelo colaborador que utiliza o equipamento, sendo somente realizadas com o consentimento da unidade gestora de infraestrutura de tecnologia da informação.

Já a garantia da conformidade com a segurança da informação e suas normas visa à efetividade da POSIC dentro da Instituição. Análises rotineiras devem ser realizadas, tanto no ambiente quanto nos ativos de tecnologia da informação, se necessário baseada na priorização dos riscos levantados para cada ativo. Essa avaliação utilizará diversas técnicas, como análise de documentos, análise de registros (log), análise de código-fonte, entrevistas e teste de invasão.

2.6 Auditoria

As tentativas de autenticação, concessão e revogação de privilégios de acesso, em qualquer ativo de tecnologia da informação, devem ser registradas de modo que seja possível determinar a data e hora na qual ocorreram, os identificadores de acesso utilizados e o ativo de informação alvo, bem como os privilégios concedidos e revogados. A auditoria deve permitir a rastreabilidade do acesso.

O IBGE tem o direito de monitorar e registrar todo acesso e utilização dos dados armazenados ou em trânsito, principalmente as informações sigilosas do IBGE ou sob sua custódia, bem como o uso dos equipamentos, com o objetivo de zelar pelo fiel cumprimento da POSIC, de acordo com as leis e

procedimentos legais vigentes. Deve ser possível registrar a data e hora na qual a manipulação ocorreu e as informações alteradas.

2.7 Desenvolvimento e aquisição de sistemas

Os sistemas utilizados no IBGE devem dispor de três ambientes segregados, voltados ao seu desenvolvimento (quando interno), à sua homologação e à sua execução em regime de produção.

O processo de desenvolvimento e aquisição de sistemas deve ser realizado em conformidade com as diretrizes, normas e padrões definidos internamente para este fim, bem como estar de acordo com a POSIC.

Todos os produtos gerados durante o ciclo de vida de desenvolvimento de sistemas devem estar hospedados em repositórios sujeitos a mecanismos de controle de acesso, garantindo que somente colaboradores autorizados tenham acesso a estes produtos. Os códigos-fonte de programas devem ser armazenados utilizando sistemas de controle de fontes institucional.

Os contratos de desenvolvimento de software devem conter cláusula contratual que garanta a entrega do código-fonte e da documentação no padrão exigido pelo IBGE, de acordo com os marcos do projeto, garantindo-se a completa documentação ao término ou no momento da interrupção do contrato.

A metodologia de desenvolvimento de sistemas do IBGE foi atualizada em 2023, definindo o método ágil como padrão para os novos projetos e as manutenções evolutivas. No desenvolvimento de novos sistemas, o dono do produto (*Product Owner*) em conjunto com o Facilitador (membro da área de demandante) define os requisitos do sistema/aplicação, incluindo nesses requisitos os controles de segurança e privacidade de dados.

Os conceitos de *Privacy by Design* e *Security by Default* devem ser aplicados no desenvolvimento de sistemas. O primeiro conceito busca atendimento à LGPD, com a proteção dos dados pessoais durante todo o ciclo de vida do sistema com transparência e respeito à privacidade do usuário. O segundo conceito, de *Security by Default*, instrui sobre mecanismos para o desenvolvimento seguro das aplicações, com o uso, por exemplo, dos conceitos de privilégio mínimo e de nunca confiar nas entradas do usuário, validando-se cada operação que o usuário faz. Esses conceitos de privacidade e segurança devem ser implantados no desenvolvimento de novos projetos e sistemas, bem como nas manutenções realizadas.

Sistemas e aplicações que apresentarem vulnerabilidades críticas, altas ou médias deverão ser corrigidas. Caso seja imperativa a entrada do sistema em produção com tais tipos de vulnerabilidades, o coordenador responsável pelo desenvolvimento da aplicação deverá registrar a necessidade da entrada em produção, indicando o motivo, as vulnerabilidades que foram aceitas, prazo para correção dessas vulnerabilidades e a formalização da concordância do Diretor de Tecnologia da Informação. Para as implantações desenvolvidas

fora da Diretoria de Tecnologia da Informação, o registro deverá conter também o de acordo do diretor/coordenador geral da unidade de origem da aplicação.

Todo o ciclo de vida de uso dos sistemas e aplicações deve ser monitorado com relação à segurança da informação. As orientações de segurança da informação relacionadas à atualização das soluções (sistemas operacionais, framework, serviços de aplicações, sistemas de banco de dados entre outros) utilizados em sistemas e aplicações devem ser incluídas no plano de atualização dos sistemas.

2.8 Gestão de riscos

O Plano de Gestão de Riscos em Tecnologia da Informação e Comunicações deve ser desenvolvido e atualizado periodicamente para evitar que ameaças, de origem natural ou humana, de forma acidental ou proposital, explorem as vulnerabilidades dos ativos provocando perdas e prejuízos para a Instituição, através da destruição não autorizada, revelação ou exposição indevida, adulteração, dano, indisponibilidade ou perda de informações da organização.

Este plano se inicia com inventário dos processos de negócio do IBGE e dos ativos de tecnologia de informação e a seleção e priorização dos ativos de informação (baseada nos processos críticos) onde deverá ser realizado o mapeamento das ameaças e vulnerabilidades *versus* a probabilidade de ocorrência e seu impacto nos ativos selecionados, estabelecendo a criticidade do risco. A partir deste levantamento, no Plano de Gestão de Riscos em Tecnologia da Informação e Comunicações será indicado para cada risco qual a ação a ser tomada, tanto para pequenos incidentes quanto para aqueles que podem interromper um processo de negócio do IBGE ou até a continuidade da Instituição.

O IBGE possui uma Política de Gestão de Riscos e uma Metodologia Gestão de Riscos que deve ser aplicada na elaboração do Plano de Gestão de Riscos em Tecnologia da Informação e Comunicações, utilizando-se para tal a mesma Matriz de Risco e escalas de classificação.

De acordo com a Política de Gestão de Riscos do IBGE, as ações possíveis para tratamento dos riscos são: evitar o risco, remover a fonte do risco, alterar a probabilidade de ocorrência e/ou consequência do impacto(mitigar) ou transferir/compartilhar o risco e aceitar o risco. Essas opções de tratamento não são mutuamente exclusivas e podem ser combinadas. A escolha das opções de tratamento depende da relação custo/benefício, entre custo e o esforço para a implementação desta solução *versus* o benefício que será obtido com a mesma. Em alguns casos, mesmo após o tratamento pode restar um risco, chamado risco residual, que deve ser analisado e avaliado como os que foram inicialmente identificados. A detecção e o conhecimento prévio das alterações nos ambientes e nos sistemas de informação aumentam as possibilidades de ações impeditivas e corretivas, reduzindo os riscos.

2.9 Gestão de Continuidade de Negócios

O Plano de Gestão de Continuidade de Negócios foca nos riscos que podem causar a descontinuidade de um ou mais processos de negócio críticos e descreve como manter ou recuperar as operações e assegurar a disponibilidade do ativo no nível e escala de tempo requerida, com o mínimo de recursos. Esse plano deve identificar os procedimentos, responsabilidades, dependências externas, contratos existentes, as perdas de informações e serviços aceitáveis e deve estar armazenado em um ambiente remoto, junto com os outros materiais necessários para sua execução. O local de armazenamento do plano deve possuir nível de controle de segurança lógica e física equivalente ao ambiente principal.

O grande desafio neste caso é manter um ambiente preparado e disponível para a continuidade dos sistemas críticos do IBGE no caso de um desastre no *data center* principal.

2.10 Gestão de incidentes em Segurança da Informação

É responsabilidade de todos os colaboradores do IBGE notificar, o mais rápido, qualquer incidente ou fragilidade de segurança que seja percebida, e nunca tentar verificar ou testar por conta própria.

O procedimento de notificação formal se dá através do envio de e-mail para o endereço <abuse@ibge.gov.br>, que é o canal institucional para recebimento de qualquer observação de falhas de segurança da informação ou suspeita de fragilidade na segurança de informação do IBGE, seja de circulação de pessoas em áreas não autorizadas, na utilização dos equipamentos, dos sistemas ou dos serviços disponibilizados pela Instituição.

Além da notificação de eventos e fragilidades por parte dos colaboradores do IBGE, o monitoramento de sistemas, alertas e vulnerabilidades são realizados para a detecção de incidentes de segurança da informação e comunicações. O IBGE implantou um Centro de Operações de Segurança, mais conhecido por sua sigla em inglês – SOC, para monitorar o seu ambiente e avisar aos gestores a ocorrência de qualquer incidente ou situação indesejada que possa levar a um incidente. Em conjunto com a equipe da DTI do IBGE, situações conhecidas na literatura foram mapeadas e seus procedimentos de tratamento estão sendo descritos, os chamados *playbooks*.

Os incidentes detectados serão direcionados para a Gerência de Segurança da Informação e Comunicação. Essa gerência é responsável por coletar todas as informações relacionadas à ocorrência do incidente, documentando o passo a passo da ocorrência do incidente e suas evidências (trilhas de auditoria, capturas de tela, entre outros). A partir dos dados coletados, deverá avaliar e tomar as devidas providências para encaminhamento do incidente para tratamento, bem como iniciar o tratamento dos reflexos do incidente para evitar a sua repetição.

O encaminhamento dos incidentes, após a avaliação preliminar, varia de acordo com o tipo de incidente identificado, e podem ser:

1. Incidentes de rede, direcionar o incidente para a gerência de segurança de redes;
2. Incidentes mapeados, iniciar o tratamento de acordo com o *playbook*, encaminhando quando necessário para as equipes responsáveis pelos ativos afetados as ações a serem realizadas; e
3. Incidentes não mapeados e/ou de alta severidade, acionar a ETIR para tratamento.

Após o tratamento do incidente, deve-se avaliar a necessidade de revisão de normas e procedimentos existentes, aquisição de novos equipamentos e/ou ferramentas, reconfiguração de permissões, abertura de processo disciplinar entre outros. Caso a solução definitiva, para evitar uma nova ocorrência do incidente, não possa ser efetivada imediatamente, deve-se registrar esta demanda e os riscos associados, e uma solução de contorno deve ser imediatamente adotada.

As informações do incidente devem ser armazenadas, para servir como lições aprendidas e para serem disponibilizadas em caso de realização de processo disciplinar de averiguação de responsabilização pela ocorrência do incidente como evidências do ocorrido.

O tratamento dos incidentes será regulado por um Plano de Gerenciamento e Tratamento de Incidentes em Tecnologia da Informação e Comunicações que determina os procedimentos para tratamento e resposta aos diferentes tipos de incidentes, a fim de assegurar respostas rápidas, efetivas e ordenadas.

2.11 Acesso à Internet

A Política de Acesso à Internet do IBGE estabelece princípios, direitos, deveres, regras e procedimentos para o uso dos recursos corporativos de Internet, disponibilizados como ferramenta de trabalho para a produção dos serviços institucionais, para a realização de consultas, pesquisas, intercâmbio de dados, ideias e informações em apoio aos projetos, atividades e eventos de interesse da Instituição. Além disso, disciplina a utilização dos recursos de acesso à Internet e lista os casos em que o acesso pode ser bloqueado e/ou revogado.

Tendo como princípio assegurar que os recursos corporativos de Internet sejam prioritariamente utilizados na produção de serviços operacionais ou administrativos e na execução dos projetos, atividades e eventos institucionais do IBGE, que seu uso não viole os aspectos éticos e legais e que seja efetuado de forma segura para assegurar a devida proteção contra riscos à segurança das informações institucionais.

Todos os acessos à Internet devem ser registrados e, a critério do IBGE, pode ser monitorado todo e qualquer dado transmitido ou recebido através de seus ativos de tecnologia da informação. Esse acesso pode

ser revogado nos casos de ameaça iminente a qualquer ativo, por desrespeito à POSIC e/ou por necessidade de serviço.

A instrução normativa específica sobre o uso de Internet detalha as regras, orientações e responsabilidades relativas à utilização dos serviços de acesso à Internet do IBGE.

2.12 Serviços de Comunicação

O IBGE disponibiliza diversas ferramentas que permitem a comunicação, intercâmbio de dados, ideias e informações e para o apoio às atividades da Instituição, como serviços de mensageria, correio eletrônico, mensageria instantânea e videoconferência, webcast, TV IBGE, entre outros.

A utilização desses serviços deve estar em consonância com as atividades desempenhadas pelo colaborador no IBGE, que deve adotar linguagem e postura de acordo com o estabelecido no Código de Ética do Funcionário Público Federal.

A Política para Utilização do Correio Eletrônico no IBGE estabelece critérios, procedimentos e regras para o acesso e uso do serviço de Correio Eletrônico. Os demais serviços de comunicação são normatizados através de instrução normativa específica.

2.13 Mídias Sociais

Os administradores de mídias sociais do IBGE são os profissionais responsáveis por criar, alterar, excluir e controlar os perfis institucionais em mídias sociais e remover, tão logo tomem conhecimento, postagens que atentem contra a segurança da informação e informar imediatamente à Gerência de Segurança da Informação e Comunicação para que a mesma possa atuar na resolução do incidente. Será realizada em conjunto com os administradores a restauração da mídia social junto aos fornecedores, se necessário, acionando todas as esferas necessárias para resolução do problema. Além disso, poderão ser indicadas ações na configuração de contas e comportamentos na administração dos perfis que deverão ser seguidos pelos administradores.

Os administradores de mídias sociais devem utilizar tão somente equipamento do IBGE para realização dessa atividade, evitando o compartilhamento desse equipamento com outras atividades.

A função de administração de mídias sociais no IBGE é realizada por unidades organizacionais relacionada às atividades de comunicação e/ou disseminação.

2.14 Nuvem

O ato normativo que rege a utilização de Nuvem está descrito na Política de Governança de Dados, R.CD 31/2021 e na Instrução Normativa nº 5, de 30.08.2021.

A nuvem privada do IBGE está disponível para todos os usuários e pode ser utilizada para armazenamento e compartilhamento de informações relacionadas às atividades do colaborador no IBGE. Cabe ressaltar que para assegurar o cumprimento dos normativos institucionais, o conteúdo armazenado nesse serviço é monitorado pelo IBGE. A nuvem pública poderá ser utilizada para armazenamento de informações e disponibilização de dados públicos à população, sempre seguindo as determinações da LGPD.

O uso de serviço de nuvem pública para hospedar dados do IBGE só poderá ser realizado após verificação da aderência do provedor do serviço à Lei Geral de Proteção de Dados Pessoais, garantindo-se o direito à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações.

2.15 Trabalho Remoto

A implantação do Programa de Gestão, permitindo aos colaboradores a realização de suas atividades Institucionais em diferentes modalidades de trabalho, incluindo o teletrabalho, tornou necessária a criação de diretrizes para utilização dos recursos de tecnologia da informação e comunicação. O acesso aos ativos de tecnologia da informação da rede IBGE para realização dessas atividades, sejam esses ativos físicos (através de conexão remota, usando a rede privada virtual – VPN), ou virtuais (uso da solução de *desktop* virtual – VDI), devem ser efetuados com os equipamentos do IBGE. Esses equipamentos devem estar configurados para realizar criptografia automática, aumentando-se a segurança no transporte dos equipamentos.

Os casos de inviabilidade de utilização do equipamento do IBGE devem ser informados à Diretoria de Tecnologia da Informação para que outras medidas de proteção sejam implantadas para esses usuários. Como regra geral, a partir de Abril de 2024, somente os equipamentos do IBGE serão permitidos nesses acessos aos ativos de tecnologia da informação.

Para as outras atividades, onde o uso do equipamento institucional não é obrigatório, sugere-se evitar o compartilhamento do seu equipamento com outros usuários e utilizar os softwares atualizados, inclusive antivírus, para acesso ao ambiente do IBGE.

Para os equipamentos do IBGE utilizados nas moradias particulares dos colaboradores, a equipe do suporte da Diretoria de Tecnologia da Informação estará autorizada, quando necessário, a realizar acessos remotos para identificação e resolução de problemas físicos e lógicos. Caso não seja possível solucionar o problema de forma remota, o equipamento deverá ser levado às dependências do IBGE pelo colaborador, sendo sua responsabilidade o deslocamento seguro do mesmo.

O suporte será realizado somente nos serviços e software institucionais.

3 Competências e responsabilidades

A todos os colaboradores compete:

- conhecer e cumprir a POSIC e seus documentos complementares;
- informar imediatamente qualquer evento ou incidente que possa comprometer a segurança da informação e da comunicação, no âmbito do IBGE, através dos canais formais;
- zelar pelo sigilo de suas credenciais de acesso aos ativos; e
- responder por toda e qualquer ação realizada sobre os ativos utilizando as suas credenciais de acesso.

Ao Conselho Diretor compete:

- aprovar a POSIC e suas atualizações de acordo com o Art. 12, do Estatuto do IBGE, aprovado pelo Decreto nº 11.177, de 18 de agosto de 2022; e
- prover a alocação de recursos humanos, financeiros e materiais necessários para a POSIC.

Aos Gestores de Diretorias, Coordenações-Gerais e Superintendentes Estaduais do IBGE compete:

- promover o acesso do conjunto de documentos atualizados que compõem a POSIC aos colaboradores sob sua gestão;
- incorporar as diretrizes da POSIC nos processos de trabalho de suas unidades de gestão; e
- exigir o cumprimento da POSIC pelos colaboradores sob sua gestão.

Ao Gestor de Segurança da Informação e Comunicações compete:

- presidir o Comitê de Segurança da Informação e Comunicações - CSI;
- analisar o Relatório de Tratamento de Incidentes;

- enviar o Relatório de Tratamento de Incidentes ao CSI;
- encaminhar ao Conselho Diretor as novas versões da POSIC para aprovação;
- representar a Instituição e manter contatos com grupos e comitês externos ao IBGE sobre esta temática; e
- deliberar sobre os casos omissos da POSIC.

Ao Comitê de Segurança da Informação e Comunicações - CSI compete:

- manter a atualização da POSIC de acordo com as normas e legislações vigentes;
- buscar o alinhamento da POSIC com os objetivos do Planejamento Estratégico do IBGE;
- manter o alinhamento da POSIC com as determinações do Grupo de Sigilo do IBGE;
- coordenar ações de conscientização e capacitação em segurança da Informação e Comunicações com vistas à disseminação e conscientização da importância da segurança da informação e comunicações entre todos os colaboradores;
- publicar a versão vigente da POSIC e seus documentos complementares; e
- indicar os recursos necessários à aderência da POSIC no IBGE e encaminhá-los às áreas competentes.

À área de Recursos Humanos compete:

- promover o conhecimento todos os servidores públicos e estagiários, o do conjunto de documentos que compõem a POSIC;
- garantir a assinatura e a guarda do Termo de Confidencialidade dos servidores públicos e estagiários; e
- atualizar o Banco de Dados de Recursos Humanos com qualquer movimentação de servidores públicos, contratados temporários ou estagiários, com vistas a regularizar o acesso aos ativos de tecnologia.

Aos Gestores de Contratos de Prestação de Serviços compete:

- dar conhecimento do conjunto de documentos que compõem a POSIC aos prestadores de serviço;
- garantir a assinatura e a guarda do Termo de Confidencialidade dos representantes de empresas no momento da assinatura do contrato;
- garantir a assinatura e a guarda do Termo de Responsabilidade de Terceiros sobre Ativo de Tecnologia no momento de seu ingresso nas dependências do IBGE;
- enviar às empresas prestadoras de serviço a Carta de Responsabilidade sobre Ativo de Tecnologia, quando houver cessão de equipamentos aos consultores contratados;
- exigir o cumprimento da POSIC pelos prestadores de serviço; e
- notificar a Diretoria de Tecnologia da Informação qualquer movimentação referente a prestadores de serviço com vistas a regularizar o acesso aos ativos de tecnologia.

À Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do IBGE –compete:

- receber e analisar as notificações relacionadas aos incidentes de segurança cibernéticos;
- registrar e documentar os incidentes cibernéticos;
- definir e manter um plano de tratamento de incidentes;
- coordenar as atividades de tratamento e resposta a incidentes cibernéticos com objetivo de reparar os danos causados;
- investigar e analisar causas, impactos e responsáveis pelos incidentes; e
- apoiar a disseminação de boas práticas de segurança digital, baseada no aprendizado sobre os incidentes tratados.

A todos os Gestores de Ativos de Informação compete:

- classificar os ativos de informação sob sua custódia, de acordo com a Política de Classificação de Ativos de Informação, quando esta for publicada;

- garantir que a classificação dos ativos de informação sob sua custódia esteja registrada em seus devidos controles de acesso;
- avaliar, regularmente, a classificação dos ativos de informação e promover as alterações pertinentes;
- informar se um ativo de informação é um dado pessoal ou pessoal sensível;
- definir as regras de acesso e concessão de acesso, conforme o critério de segurança do privilégio mínimo;
- avaliar, regularmente, se os requisitos de segurança da informação e comunicações estão sendo aplicados corretamente; e
- repassar a curadoria dos ativos a outros servidores públicos da Instituição em caso de afastamentos, aposentadorias e mudanças de responsabilidade.

À área de Auditoria Interna compete:

- avaliar o controle interno decorrente da POSIC e dos planos por ela produzidos.

À Diretoria de Tecnologia da Informação compete:

- prospectar novas tecnologias que permitam a melhoria nos processos de segurança de informação e comunicação previstos na POSIC;
- monitorar e acompanhar os ativos de tecnologia de informação e comunicações com vistas a atuar preventivamente na ocorrência de incidentes;
- realizar vistoria periódica em áreas e instalações físicas onde estão localizados os ativos e gerar relatórios de visita indicando não conformidades identificadas em relação à POSIC;
- manter atualizado o Plano de Gerenciamento e Tratamento de Incidentes com vistas a garantir a continuidade dos processos de negócio do IBGE;
- elaborar informativos sobre os incidentes de segurança da informação e comunicações no IBGE e apresentar ao CSI;
- implantar e acompanhar os processos de segurança da informação e comunicações;

- avaliar tecnicamente as novas tecnologias propostas pelo Comitê de Tecnologia da Informação e Comunicação - CTIC, quanto à aderência à POSIC, antes de sua inclusão no Plano Diretor de Tecnologia da Informação e Comunicação – PDTI do IBGE;
- promover a melhoria contínua dos processos de gestão de segurança da informação e comunicações do IBGE; e
- verificar a conformidade da aplicação da POSIC.

4 Penalidades

O descumprimento da POSIC do IBGE e/ou de suas normas e procedimentos é passível de sanções administrativas, cíveis e penais previstas no Estatuto do Servidor Público Federal (BRASIL, 1990), e pela avaliação da Comissão de Ética do IBGE, no Código Penal (BRASIL, 2000b) e no Código Civil (BRASIL, 2002b), e/ou na legislação que regule ou venha a regular a matéria. Devem-se considerar também os termos contratuais para os profissionais terceirizados e os estagiários.

5 Política de Atualização

A Política de Segurança da Informação e Comunicações do IBGE deverá ser atualizada a cada quatro anos, ou intervalo menor caso existam alterações que precisem ser incorporadas.

Anexo I

Relação de Normativos

Compõem a Política de Segurança da Informação e Comunicações do IBGE um conjunto de normativos, políticas, instruções normativas e termos, que definem e detalham diretrizes aqui mencionadas e que devem ser de conhecimento de todo o corpo funcional da Instituição.

Políticas

- Política de Acesso à Internet
- Política de Uso do Correio Eletrônico
- Política de Backup e Recuperação de Dados Digitais (em desenvolvimento para substituição da atual Instrução Normativa de Backup)
- Política de Governança de Dados

Planos

- Plano de Gestão de Vulnerabilidades (a ser desenvolvido)
- Plano de Gerenciamento e Tratamento de Incidentes em Tecnologia da Informação e Comunicações (em desenvolvimento)
- Plano de Gestão de Riscos em Tecnologia da Informação e Comunicações (em desenvolvimento)
- Plano de Continuidade de Negócios (a ser desenvolvido)

Instruções Normativas

- Instrução Normativa de Uso de Ativos de TIC
- Instrução Normativa de Uso de Software
- Instrução Normativa de Nomenclatura de Ativos
- Instrução Normativa de Correio Eletrônico
- Instrução Normativa de Telecomunicações
- Instrução Normativa de Acesso à Internet
- Instrução Normativa de Ativos de Telecomunicações
- Instrução Normativa de Controle de Acesso Físico e Lógico
- Instrução de Gestão de Mudanças (em desenvolvimento)
- Instrução de Gestão de Incidentes (em desenvolvimento)

Termos

- Termo de Responsabilidade sobre Ativo de Tecnologia
- Termo de Responsabilidade de Terceiros sobre Ativo de Tecnologia
- Carta de Responsabilidade sobre Ativo de Tecnologia
- Termo de Confidencialidade

Referências

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 27001: tecnologia da informação: técnicas de segurança: sistema de gestão da segurança da informação: requisitos. Rio de Janeiro: ABNT, 2013.

_____. NBR ISO/IEC 27002: tecnologia da informação: técnicas de segurança: código de prática para controles de segurança da informação. Rio de Janeiro: ABNT, 2013.

_____. NBR ISO/IEC 27005: tecnologia da informação: técnicas de segurança: gestão de riscos de segurança da informação. Rio de Janeiro: ABNT, 2008.

_____. NBR ISO/IEC 27005: tecnologia da informação: técnicas de segurança: gestão de riscos de segurança da informação. Rio de Janeiro: ABNT, 2011.

BRASIL. Decreto n. 1.171, de 22 de junho de 1994. Aprova o Código de Ética Profissional do Servidor Público Civil do Poder Executivo Federal. Diário Oficial [da] República Federativa do Brasil, Brasília, DF, ano 132, n. 118, 23 jun. de 1994. Seção 1, p. 9295-9297.

Disponível em: < https://www.planalto.gov.br/ccivil_03/decreto/d1171.htm>. Acesso em: julho. 2023.

_____. Decreto n. 9.637, de 26 de dezembro de 2018. 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, Brasília, DF, ano 155, n. 248, 27 dez. de 2018. Seção 1, p. 23.

Disponível em: < https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/d9637.htm>. Acesso em: julho. 2023.

_____. Decreto n. 4.073, de 3 de janeiro de 2002. Regulamenta a Lei n. 8.159, de 8 de janeiro de 1991, que dispõe sobre a política nacional de arquivos públicos e privados. Diário Oficial da União, Brasília, DF, ano 139, n. 3, 04 jan. de 2002a. Seção 1, p. 1-3.

Disponível em: < https://www.planalto.gov.br/ccivil_03/decreto/2002/d4073.htm>. Acesso em: julho. 2023.

_____. Decreto n. 7.724, de 16 de maio de 2012. Regulamenta a Lei n. 12.527, de 18 de novembro de 2011, que dispõe sobre o acesso a informações previsto no inciso XXXIII do caput do art. 5º, no inciso II do § 3º do art. n. 37 e no § 2º do art. n. 216 da Constituição. Diário Oficial da União, Brasília, DF, ano 149, n. 94-A, 16 maio de 2012a. Seção 1, p. 1-6.

Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/decreto/d7724.htm>. Acesso em: julho. 2023.

_____. Decreto n. 7.845, de 14 de novembro de 2012. Regulamenta procedimentos para o credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento. Diário Oficial da União, Brasília, DF, ano 149, n. 221, 16 nov. de 2012b. Seção 1, p. 1-4.

Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/decreto/d7845.htm>.
Acesso em: julho. 2023.

_____. Decreto n. 10.046, de 09 de outubro de 2019. Dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados. Diário Oficial da União, Brasília, DF, ano 157, n. 197, Seção 1, p. 2, 2019.

Disponível em: < https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D10046.htm>
Acesso em: julho 2023.

_____. Decreto n. 11.266, de 25 de novembro de 2022. Altera o Decreto nº 10.046, de 9 de outubro de 2019, que dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados. Diário Oficial da União, Brasília, DF, ano 160, n. 222-A, Seção 1-Extra A, p. 1, 2022.

Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/decreto/D11266.htm> Acesso em: julho 2023.

_____. Decreto n. 73.177, de 20 de novembro de 1973. Regulamenta a Lei n. 5.534, de 14 de novembro de 1968, modificada pela Lei n. 5.878, de 11 de maio de 1973, de que dispõe sobre a obrigatoriedade da prestação de informações necessárias ao Plano Nacional de Estatísticas Básicas e ao Plano Geral de Informações Estatísticas e Geográficas. Diário Oficial da República Federativa do Brasil, Brasília, DF, ano 111, n. 223, 22 nov. de 1973a. Seção 1, p. 11.964.

Disponível em: < https://www.planalto.gov.br/ccivil_03/decreto/antigos/d73177.htm>. Acesso em: julho. 2023.

_____. Decreto-lei n. 161, de 13 de fevereiro de 1967. Autoriza o Poder Executivo a instituir a "Fundação Instituto Brasileiro de Geografia e Estatística" e dá outras providências. Diário Oficial [dos] Estados Unidos do Brasil, Brasília, DF, ano 105, n. 30, 14 fev. de 1967. Seção 1, p. 1785-1787. Disponível em: < https://www.planalto.gov.br/ccivil_03/decreto-lei/1965-1988/del0161.htm>. Acesso em: julho. 2023.

_____. Gabinete de Segurança Institucional da Presidência da República. Instrução Normativa n. 01, de 27 de maio de 2020. Atividade de normatização.

Disponível em: <https://www.in.gov.br/en/web/dou/-/instrucao-normativa-n-1-de-27-de-maio-de-2020-258915215>. Acesso em: julho 2023.

_____. Gabinete de Segurança Institucional da Presidência da República. Instrução Normativa n. 05, de 30 de agosto de 2021. Atividade de normatização.

Disponível em: <https://www.in.gov.br/en/web/dou/-/instrucao-normativa-n-5-de-30-de-agosto-de-2021-341649684>. Acesso em: julho 2023.

_____. Gabinete de Segurança Institucional da Presidência da República. Instrução. Norma Complementar n. 05, de 14 de agosto de 2009. Criação de equipes de tratamento e resposta a incidentes em redes computacionais - ETIR.

Disponível em:

< <https://www.gov.br/gsi/pt-br/composicao/SSIC/dsic/legislacao/NC05.pdf> >. Acesso em: julho. 2023.

_____. Gabinete de Segurança Institucional da Presidência da República. Instrução. Norma Complementar n. 08, de 19 de agosto de 2010. Gestão de ETIR: diretrizes para gerenciamento de incidentes em redes computacionais nos órgãos e entidades da administração pública federal. Disponível em: < <https://www.gov.br/gsi/pt-br/composicao/SSIC/dsic/legislacao/NC08.pdf> >. Acesso em: julho. 2023.

_____. Gabinete de Segurança Institucional da Presidência da República. Instrução. Norma Complementar n. 09, de 15 de julho de 2014. Orientações específicas para o uso de recursos criptográficos em segurança da informação e comunicações.

Disponível em: <

<https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=16/07/2014&jornal=1&pagina=4&totalArquivos=84> >. Acesso em: julho. 2023.

_____. Gabinete de Segurança Institucional da Presidência da República. Instrução. Norma Complementar n. 12, de 30 de janeiro de 2012. Uso de dispositivos móveis nos aspectos relativos à segurança da informação e comunicações nos órgãos e entidades da administração pública federal. Disponível em: < <https://www.gov.br/gsi/pt-br/composicao/SSIC/dsic/legislacao/NC12.pdf> >. Acesso em: julho. 2023.

_____. Lei n. 5.534, de 14 de novembro de 1968. Dispõe sobre a obrigatoriedade de prestação de informações estatísticas e dá outras providências. Diário Oficial [da] República Federativa do Brasil, Brasília, DF, ano 106, n. 222, 18 de nov. 1968. Seção 1, p. 9985. Disponível em: <https://www.planalto.gov.br/ccivil_03/leis/15534.htm>. Acesso em: julho. 2023.

_____. Lei n. 5.878, de 11 de maio de 1973. Dispõe sobre a Fundação Instituto Brasileiro de Geografia e Estatística - IBGE, e dá outras providências. Diário Oficial [da] República Federativa do Brasil, Brasília, DF, ano 15, n. 89, 15 de maio 1973b. Seção 1, p. 4697. Disponível em: < https://www.planalto.gov.br/ccivil_03/leis/15878.htm >. Acesso em: julho. 2023.

_____. Lei n. 8.112, de 11 de dezembro de 1990. Dispõe sobre o regime jurídico dos servidores públicos civis da União, das autarquias e das fundações públicas federais. Diário Oficial [da] República Federativa do Brasil, Brasília, DF, ano 128, n. 237, 12 de dez. 1990. Seção 1, p. 1. Disponível em: < https://www.planalto.gov.br/ccivil_03/leis/18112cons.htm >. Acesso em: julho. 2023.

_____. Lei n. 8.159, de 8 de janeiro de 1991. Dispõe sobre a política nacional de arquivos públicos e privados e dá outras providências. Diário Oficial [da] República Federativa do Brasil, Brasília, DF, ano

129, n. 6, 09 de jan. 1991, Seção 1, p. 455-456. Disponível em:

< http://www.planalto.gov.br/ccivil_03/leis/L8159.htm >. Acesso em: julho. 2023.

_____. Lei n. 9.296, de 24 de julho de 1996. Regulamenta o inciso XII, parte final, do art. 5º da Constituição Federal. O disposto nesta lei aplica-se a interceptação do fluxo de comunicações em sistemas de informática e telemática. Diário Oficial [da] República Federativa do Brasil, Brasília, DF, ano 134, n. 143, 25 de jul. 1996. Seção 1, p. 13.757. Disponível em:

< https://www.planalto.gov.br/ccivil_03/leis/19296.htm >. Acesso em: julho. 2023.

_____. Lei n. 9.609, de 19 de fevereiro de 1998. Dispõe sobre a proteção da propriedade intelectual de programa de computador, sua comercialização no País, e dá outras providências. Diário Oficial [da] República Federativa do Brasil, Brasília, DF, ano 136, n. 36, 20 fev. de 1998a. Seção 1, p. 1-3. Disponível em: < https://www.planalto.gov.br/ccivil_03/leis/19609.htm > Acesso em: julho. 2023.

_____. Lei n. 9.610, de 19 de fevereiro de 1998. Altera, atualiza e consolida a legislação sobre direitos autorais e dá outras providências. Diário Oficial [da] República Federativa do Brasil, Brasília, DF, ano 136, n. 36, 20 de fev. 1998b. Seção 1, p. 3-9. Disponível em:
< https://www.planalto.gov.br/ccivil_03/leis/19610.htm >. Acesso em: julho. 2023.

_____. Lei n. 9.983, de 14 de julho de 2000. Altera o Decreto-lei n. 2.848, de 7 de dezembro de 1940. Código Penal e dá outras providências. Diário Oficial [da] República Federativa do Brasil, Brasília, DF, ano 138, n. 136, 17 jul. de 2000b. Seção 1, p. 4-5. Disponível em: < https://www.planalto.gov.br/ccivil_03/leis/19983.htm >. Acesso em: julho. 2023.

_____. Lei n. 10.406, de 10 de janeiro de 2002. Institui o Código Civil. Diário Oficial da União, Brasília, DF, ano 139, n. 8, 11 jan. 2002b. Seção 1, p. 1-74. Disponível em:
< https://www.planalto.gov.br/ccivil_03/leis/2002/110406.htm >. Acesso em: julho. 2023.

_____. Lei n. 12.527, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei n. 8.112, de 11 de dezembro de 1990; revoga a Lei n. 11.111, de 5 de maio de 2005, e dispositivos da Lei n. 8.159, de 8 de janeiro de 1991; e dá outras providências. Diário Oficial da União, Brasília, DF, ano 148, n. 221-A, 18 nov. de 2011. Seção 1, p. 1-4.
Disponível em: < https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/112527.htm >. Acesso em: julho. 2023.

_____. Lei n. 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Diário Oficial da União, Brasília, DF, ano 151, n. 77, 24 abr. de 2014. Seção 1, p. 1-3.
Disponível em: < https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/112965.htm >. Acesso em: julho. 2023.

_____. Lei n. 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Diário Oficial da União, Brasília, DF, Ano 155, n. 157, 15 ago. de 2018. Seção 1, p. 59-64.
Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm >. Acesso em: julho. 2023.

_____. Lei n. 13.853, de 08 de julho de 2019. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. Diário Oficial da União, Brasília, DF, Ano. 157, n. 246, 20 dez. de 2019. Seção 1, p. 1. Disponível em: < https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/113853.htm >. Acesso em: julho. 2023.

_____. Portaria P.PR n. 320/2021, de 23. setembro 2021. Designa servidores do Comitê de Segurança da Informação (CSI). Boletim de Serviço, Rio de Janeiro, n. 3097, p. 4-5, 24 setembro 2021.

_____. Resolução RCD n. 12/2021, de 23 de julho de 2021. Cria o Comitê de Segurança da Informação e Comunicações do IBGE - CSI. Boletim de Serviço, Rio de Janeiro, n. 3089, p. 4-5, 30 julho de 2021.

_____. Plano Estratégico do IBGE 2022-2025, versão revisada, original 1ª. Edição Junho 2017.

Disponível em: <

https://www.ibge.gov.br/np_download/novoportal/documentos_institucionais/Plano_Estrategico_2022-2025.pdf>. Acesso em: julho. 2023.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. ISO/IEC 27000: Information Technology - Security Techniques - Information Security Management Systems - Overview and vocabulary. 5 ed.

Vernier, Geneva, Switzerland, Fev 2018. Disponível em:

<<http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html>>. Acesso em: julho. 2023.



Instituto Brasileiro de Geografia e Estatística

Conselho Diretor

RESOLUÇÃO CD/IBGE Nº 33, DE 08 DE NOVEMBRO DE 2023

Aprova a nova Política de Segurança da Informação e das Comunicações (POSIC) do IBGE

O CONSELHO DIRETOR da FUNDAÇÃO INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA (IBGE), no uso das competências que lhe foram atribuídas pelo art. 12 do Estatuto aprovado pelo Decreto nº 11.177, de 18 de agosto de 2022, tendo em vista o disposto no Decreto nº 9.637, de 26 de dezembro de 2018, e considerando a necessidade de definir e atualizar diretrizes estratégicas, responsabilidades e competências para garantir a confidencialidade, integridade, autenticidade e disponibilidade das informações, difundindo as boas práticas e a cultura de segurança da informação ao corpo de colaboradores desta Fundação IBGE, RESOLVE:

Art. 1º Aprovar a Política de Segurança da Informação e das Comunicações (POSIC) do IBGE, revisão de 2023, elaborada pelo Comitê de Segurança da Informação (CSI) do Instituto, na forma do ANEXO a esta Resolução.

Art. 2º Fica revogada a Resolução do Conselho Diretor/IBGE nº 24, de 02 de agosto de 2017.

Art. 3º Por conta da urgência da matéria, esta Resolução entra em vigor em 13 de novembro de 2023.

MARCIO POCHMANN
Presidente



Documento assinado eletronicamente por MARCIO POCHMANN, Presidente, em 8 de Novembro de 2023, às 21:42:27, horário de Brasília, com fundamento legal no § 3º do Art. 4º do Decreto Nº 10.543, de 13 de Novembro de 2020.



A autenticidade deste documento pode ser conferida no site <https://transparenciasda.ibge.gov.br/docs/validador.jsf> informando o código verificador 4962810060930399321 e o código CRC 63D198EC.