POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES DO IBGE
POSIC 2016

IBGE
Instituto Brasileiro de Geografia e Estatística

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

Política de Segurança da Informação e Comunicações do IBGE
POSIC 2016

Rio de Janeiro
2015

Presidenta da República
Dilma Rousseff

Ministro do Planejamento, Orçamento e Gestão
Valdir Moysés Simão

Instituto Brasileiro de Geografia e Estatística - IBGE

Presidenta
Wasmália Bivar

Diretor-Executivo
Fernando J. Abrantes

ÓRGÃOS ESPECÍFICOS SINGULARES

Diretoria de Pesquisas
Roberto Luís Olinto Ramos

Diretoria de Geociências
Wadih João Scandar Neto

Diretoria de Informática
Paulo Cesar Moraes Simões

Centro de Documentação e Disseminação de Informações
David Wu Tai

Escola Nacional de Ciências Estatísticas
Maysa Sacramento de Magalhães

Sumário

1. Introdução 5
   1.1 Contextualização 5
   1.2 Escopo 6
   1.3 Conceitos e definições 8
   1.4 Princípios 11
2. Diretrizes gerais 12
   2.1 Ativos de informação 13
   2.2 Ativos de tecnologia da informação 14
   2.3 Controle de acesso lógico 16
   2.4 Controle de acesso físico a equipamentos 17
   2.5 Conformidade 18
   2.6 Auditoria 19
   2.7 Desenvolvimento e aquisição de sistemas 20
   2.8 Gestão de riscos 21
   2.9 Gestão de incidentes de segurança da informação e rede 22
   2.10 Acesso à Internet 23
   2.11 Sistema de mensageria 24
3. Competências e responsabilidades 25
4. Penalidades 29

Referências 30

Apresentação

A Política de Segurança da Informação e Comunicações – POSIC do IBGE publicada em dezembro de 2014 definiu princípios, diretrizes, responsabilidades e competências para garantir a confidencialidade, integridade, autenticidade e disponibilidade das informações, princípios da Segurança da Informação e Comunicações. Além dos citados, os princípios fundamentais da estatística são utilizados para nortear as boas práticas do tema a serem difundidas entre os colaboradores do IBGE.

Para o cumprimento da missão do IBGE é indispensável assegurar que todas as informações e estudos de natureza estatística, geográfica, cartográfica e demográfica sejam mantidos em segurança, inclusive àquelas fornecidas de forma obrigatória por pessoas e empresas. É obrigação da Instituição manter a privacidade do informante e o sigilo das informações prestadas, conforme previsto na Lei n. 5534, de 14.11.68.

A POSIC atende às exigências legais e normativas da Secretaria de Logística e Tecnologia da Informação do Ministério do Planejamento, Orçamento e Gestão; do Tribunal de Contas da União - TCU; da Controladoria-Geral da União – CGU; e do Gabinete de Segurança Institucional da Presidência da República, assim como as metas estratégicas estabelecidas no Planejamento Estratégico 2012-2015 do IBGE.

De acordo com o que foi previamente definido na POSIC, apresentamos a primeira revisão da Política de Segurança do IBGE referendada pelo Comitê de Segurança da Informação. A estrutura original do documento foi mantida, descrevendo os princípios e as diretrizes que devem nortear a Segurança da Informação e Comunicações na Instituição e relata o andamento na elaboração dos planos, políticas, normas e ordens de serviço que a complementam.

A efetividade da implantação da política depende da implementação dos controles de segurança, que requerem mudanças nos processos de trabalho, nos procedimentos operacionais e no comportamento das pessoas dentro da Instituição. A conscientização dos colaboradores com relação ao tema de segurança da informação e comunicações é fundamental para que as diretrizes estabelecidas na POSIC se tornem uma realidade e o IBGE possa cumprir a sua missão de prover as informações necessárias ao conhecimento da realidade física, econômica e social do País, mantendo a relação de confiança e cooperação entre o Instituição e a sociedade.

Paulo Cesar Moraes Simões
Presidente do Comitê de Segurança da Informação e
Diretor de Informática 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 um grande número de ameaças e vulnerabilidades, em virtude da grande conectividade, e disponibilidade das informações na rede. Por isso, torna-se imprescindível que as organizações se preocupem com o estabelecimento de controles, como as políticas, que protejam as informações da Instituição e em casos mais graves que garantam a continuidade dos negócios.

A visão do IBGE para 2020, estabelecida no Planejamento Estratégico do IBGE 2012-2015, de "Ser reconhecido e valorizado, no país e internacionalmente, pela integridade, relevância, consistência e excelência de todas as informações estatísticas e geocientíficas que produz e dissemina em tempo útil" (IBGE, 2013, p. 21) define características importantes da informação prestada pela Instituição que só poderão ser garantidas se uma Política de Segurança da Informação e Comunicações - POSIC estiver efetivamente implementada, e sendo conduzida com eficiência e eficácia.

A POSIC é uma das práticas listada na terceira edição da norma da International Organization for Standardization - ISO e a International Electrotechnical Commission - IEC (ISO/IEC 27000, 2014) para auxiliar a gestão da segurança da informação, que também a estabelece como fator crítico de sucesso dentro de uma organização. A POSIC do IBGE (POSIC) 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 levar em consideração a classificação das informações e ser cuidadosamente avaliada pelo gestor quanto

à importância e aos possíveis impactos, positivos ou negativos, nas atividades do IBGE.

1.2 Escopo

A Política de Segurança da Informação e Comunicações – POSIC do IBGE é o documento corporativo que define os princípios e as diretrizes que norteiam a segurança de informação 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 está alinhada ao Planejamento Estratégico 2012-2015 do IBGE, mas tão logo o Planejamento Estratégico 2016-2020 do IBGE seja publicado, este documento será revisto à luz do novo planejamento.

Assim, os objetivos estratégicos que norteiam este documento são:

- **Objetivo Estratégico 01.10.** Desenvolver a cultura da gestão de risco no IBGE, iniciando com o aprimoramento da segurança nos processos de produção, armazenamento e disseminação de informações estatísticas e geocientíficas.
- **Objetivo Estratégico 10.02.** Implantar as diretrizes de TIC institucional, de forma a garantir a integridade, a segurança das informações e o atendimento à legislação pertinente.

Nesses objetivos existem as metas estratégicas 01.10.02 e 10.02.01 a serem executadas, a saber: Elaborar e disseminar em todo IBGE a primeira versão da Política Institucional de Segurança da Informação, no segundo semestre de 2013.

A POSIC deve ser amplamente divulgada no âmbito do IBGE e ter seu conteúdo integralmente disponibilizado para consulta interna, permitindo o acesso de todos 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 27000, de 15.01.2014.

A implementação da POSIC é sustentada por planos e políticas (nível estratégico), normas (nível tático) e ordens de serviço (nível operacional), alinhados às diretrizes estabelecidas na mesma. Esses documentos complementares da política serão referidos ao longo deste documento.

Durante o ano de 2015, foi iniciado o desenvolvimento dos documentos complementares. O Plano de Recuperação de Desastre dos Centros de Processamento de Dados do IBGE foi desenvolvido como estabelecido na Meta Estratégica 10.02.07 do Planejamento Estratégico 2012-2015 (IBGE, 2013). Este plano é composto por um levantamento de riscos e pelo Plano de Gerenciamento e Tratamento de Incidentes em Tecnologia da Informação e Comunicações, dos principais serviços de Tecnologia da Informação e Comunicações hospedados nos Centros de Processamento de Dados do IBGE.

No ano de 2016, será desenvolvido o Plano de Capacitação Contínua em Segurança da Informação a ser aplicado em toda a Instituição, tornando o tema mais próximo à realidade de todos os colaboradores. Os demais planos previstos na POSIC 2015, a saber Plano de Continuidade do Negócio e o Plano de Gerenciamento de Riscos em Tecnologia da Informação e Comunicações serão elaborados em 2017.

Além dos planos, conforme definido na POSIC 2015, diversos documentos no nível estratégico, tático e operacional complementam a política. A relação abaixo lista quais desses documentos foram elaborados em 2015, sendo alguns já publicados, em virtude da urgência de regulamentação, a saber as Políticas e Ordens de Serviço sobre o Acesso à Internet e Uso do Correio Eletrônico. Os documentos abaixo relacionados serão referendados pelo Comitê de Segurança da Informação - CSI, durante o ano de 2016.

Nível Estratégico

- Política de Acesso à Internet – Resolução do Conselho Diretor - RCD n. 30, de 29.12.2014; e
- Política sobre o Uso do Correio Eletrônico no IBGE – Resolução do Conselho Diretor - RCD n. 22, de 05.11.2014.

Nível Tático

- Norma de Mensageria Instantânea e Videoconferência.

Nível Operacional

- Ordem de Serviço de Acesso à Internet - OS.DI/COINF n. 2/2015, de 14.04.2015 e Boletim de Serviço n. 2.761, de 17.04.2015;
- Ordem de Serviço de *Backup*;
- Ordem de Serviço de Controle de Acesso Físico;
- Ordem de Serviço de Controle de Acesso Lógico;
- Ordem de Serviço de Implantação de Sistemas;
- Ordem de Serviço de Nomenclatura de Ativos de Tecnologia da Informação;
- Ordem de Serviço de Senhas;
- Ordem de Serviço para Armazenamento de Dados;
- Ordem de Serviço sobre o Uso de Ativos de Tecnologia da Informação;
- Ordem de Serviço sobre o Uso de Mensageria Instantânea e Videoconferência;
- Ordem de Serviço sobre o Uso de Rede Sem Fio;
- Ordem de Serviço sobre o Uso de Software no IBGE;
- Ordem de Serviço sobre o Uso do Correio Eletrônico – OS.DI/COINF/COINF n. 3/2015, de 20.05.2015 e Boletim de Serviço n. 2.766, de 22.05.2015;
- Termo de Confidencialidade; e
- Termo de Responsabilidade sobre Ativo de Tecnologia.

Para o ano de 2016, serão elaborados os seguintes documentos:

Nível Estratégico

- Política de Classificação de Ativos de Informação.

Nível Tático

- Norma para Desenvolvimento de Sistemas.

Nível Operacional

- Ordem de Serviço para Aquisição de Sistemas.

A Ordem de Serviço para Uso de Dispositivos Móveis, prevista na POSIC 2015, foi considerada desnecessária, pois durante a sua discussão verificou-se que os assuntos planejados para a mesma já haviam sido normatizados nas Ordens de Serviço sobre o Uso de Ativos de Tecnologia da Informação; para Armazenamento de Dados; e sobre o Uso de Rede Sem Fio.

Seguindo a recomendação da Norma Complementar n. 03, de 30 de junho de 2009 (BRASIL, 2009) este documento possui os seguintes tópicos: Escopo; Conceitos e definições; Princípios; Diretrizes gerais; Competências e responsabilidades; Penalidades; além das Referências legais e normativas e Equipe técnica responsável.

1.3 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)

Ameaça – causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização. (ISO/IEC 27000, 2014)

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, 2014)

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 – servidores do quadro do IBGE, estagiários e terceirizados contratados.

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.

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

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 os ativo(s) de informação do IBGE, com probabilidade de interromper ou afetar a qualidade dos serviços e/ou atividades da Instituição.

Infraestrutura de TI - 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)

Política – intenções e diretrizes da organização, formalmente expressas pela direção da Instituição. (ISO/IEC 27000, 2014)

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, 2014)

Segurança da Informação - preservação da confidencialidade, da integridade e da disponibilidade das informações. (ISO/IEC 27000, 2014)

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, 2014)

1.4 Princípios

A Política de Segurança da Informação e Comunicações - 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, de 15.01.2014 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 derivados devem ser constantemente atualizados, 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.

2. Diretrizes gerais

As diretrizes de segurança da informação estabelecidas na Política de Segurança da Informação e Comunicações do IBGE - 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 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 os fins previstos e para cumprir os objetivos corporativos.

A conscientização de todos os colaboradores sobre a importância da POSIC deve ser realizada continuamente.

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

Um Plano de Capacitação Contínua em Segurança da Informação deve ser elaborado, considerando não só programas de treinamento, como também ações de disseminação tais como confecção e distribuição de material (panfletos, *folders*, cartilhas e outros), além da publicação na Intranet.

A Gestão de Segurança da Informação e Comunicações do IBGE será realizada por estrutura composta: pelo Gestor de Segurança da Informação e Comunicações, posição exercida pelo Diretor da Diretoria de Informática e pelo Comitê de Segurança da Informação e Comunicações – CSI.

O CSI foi instituído pela Resolução do Conselho Diretor n. 26, de 21.10.2015 onde se estabelece a sua competência e composição. A Portaria da Presidência n. 552, publicada em 22.10.2015, designa os especialistas das áreas setoriais que irão constituir o Comitê.

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

A efetividade desta POSIC e de suas normas complementares deve ser verificada periodicamente, pelo CSI ou sob demanda do Conselho Diretor.

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 a IBGE.

2.1 Ativos de informação

Os ativos de informação devem ter um gestor que, em conjunto com o custodiante da informação, aplicarão o tratamento de segurança adequado a este ativo. Cabe ao gestor analisar e aprovar o conjunto de controles aplicados para garantir a segurança dos ativos sob sua responsabilidade. Devem ser realizadas também auditorias para verificar se os requisitos de segurança da informação e comunicações estão sendo aplicados corretamente.

No momento de sua geração ou aquisição, os ativos de informação devem ser classificados pelo gestor quanto à sua importância e grau de confidencialidade, e submetidos a procedimentos regulares de avaliação quanto a esta classificação, conforme Política de Classificação de Ativos de Informação.

A classificação da informação determinará sua disponibilidade e proteção, a fim de garantir a sua segurança durante o ciclo de vida, desde a criação até a eliminação. Informações sem classificação não podem ser tacitamente consideradas sem restrição de acesso.

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 a POSIC e as sanções cabíveis em caso de descumprimento.

O transporte de informações deve utilizar procedimento para proteção e ser precedido de registro e autorização do gestor da informação, conforme definido na Ordem de Serviço para Armazenamento de Dados, que também irá regular a utilização e a concessão de permissões nos dispositivos de armazenamento.

2.2 Ativos de tecnologia da informação

A utilização de ativos de tecnologia da informação, do tipo equipamento, deve ser precedida de recebimento, ciência e aceite formal do Termo de Responsabilidade sobre o Ativo de Tecnologia. Além disso, deve ser realizada exclusivamente através da infraestrutura disponibilizada e autorizada pela unidade gestora de tecnologia da informação do IBGE, cumprindo as recomendações constantes na Ordem de Serviço para Uso de Ativos 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 deverá seguir a Ordem de Serviço de 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 Ordem de Serviço para Uso de *Software* no IBGE.

A Diretoria de Informática 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. Para tal, a Ordem de Serviço de *Backup* torna-se necessária para definição das regras sobre a realização de cópias de segurança.

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.

Não é permitida a utilização de ativos de equipamentos de terceiros na rede corporativa do IBGE, salvo em casos de exceção, devidamente justificados junto à unidade gestora de infraestrutura de tecnologia da informação do IBGE. Também 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.

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 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 necessários 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, seja a partir de equipamentos do IBGE ou não, 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 e ser concedido em caráter provisório.

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 de funcionário ou 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.

Baseado nessas diretrizes, a Ordem de Serviço de Controle de Acesso Lógico determinará 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. Os critérios de formação das senhas para as credenciais serão definidos na Ordem de Serviço de Senhas.

2.4 Controle de acesso físico a equipamentos

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.

O acesso de colaboradores/visitantes às áreas que hospedam equipamentos críticos deverá ser autorizado pelo custodiante e acompanhado de um servidor público. A restrição de acesso deve estar alinhada aos riscos identificados.

A Ordem de Serviço de Controle de Acesso Físico definirá os controles de acesso aos Centros de Processamento de Dados - CPD que poderão ser utilizados, bem como, as condições físicas a serem observadas. As orientações serão diferenciadas de acordo com a avaliação da proporcionalidade entre o custo da alteração e o risco envolvido.

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. Este último já vem sendo solucionado no IBGE com a proibição de instalação de produtos diretamente pelo colaborador que utiliza a máquina, 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 Política de Segurança da Informação e Comunicações - 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 Política de Segurança da Informação e Comunicações - 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 Política de Segurança da Informação e Comunicações - POSIC.

As manutenções de sistemas já implantados que impliquem em mudanças significativas nos mesmos e/ou no ambiente, devem incluir no seu planejamento o gerenciamento dos riscos envolvidos.

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 Norma para Desenvolvimento de Sistemas definirá os critérios de segurança necessários aos sistemas, bem como os processos a serem incluídos na metodologia de desenvolvimento de sistemas, para garantir a segurança da informação dos novos sistemas e daqueles em manutenção, durante todo o ciclo de vida dos sistemas. Quanto mais cedo os critérios de segurança forem definidos, menores são os custos e os riscos envolvidos na sua entrega.

A Ordem de Serviço para Aquisição de Sistemas definirá os critérios de segurança, conformidade e desempenho necessários aos sistemas e pacotes, quando aplicável, adquiridos pela Instituição, bem como as verificações que serão realizadas para validar a segurança deste sistema.

Com relação à aceitação do sistema e sua implantação em ambiente de produção é necessário que o mesmo possua um gestor responsável, e que tenha sido avaliado com sucesso em testes de vulnerabilidade e de carga. Além disso, deve existir um conjunto de documentos que descreva o sistema e/ou produto a ser implantado, que permita o seu gerenciamento e suporte. Os critérios de sucesso dos testes e o conjunto de informações necessárias à implantação dos sistemas serão especificadas na Ordem de Serviço de Implantação de Sistemas.

2.8 Gestão de riscos

Os ativos de informação devem possuir um Plano de Gerenciamento de Riscos em Tecnologia da Informação e Comunicações, 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, um Plano de Gerenciamento de Riscos em Tecnologia da Informação e Comunicações será elaborado, indicando 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.

As quatro ações possíveis para tratamento dos riscos são: mitigar, aceitar, evitar ou transferir/compartilhar 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.

A introdução de ativos de tecnologia da informação no ambiente de produção, bem como a implementação de mudanças nesses ativos, deve ser precedida de homologação, que inclua avaliação do impacto à segurança e verificação de conformidade com as diretrizes, normas e padrões internos. Em caso de vulnerabilidades, as mesmas devem ser tratadas de forma adequada ao seu grau de risco antes da implantação em ambiente de produção.

Para os riscos que podem causar a descontinuidade de um ou mais processos de negócio críticos, deve-se elaborar um Plano de Continuidade do Negócio que descreva como manter ou recuperar as operações e assegurar a disponibilidade do ativo no nível e escala de tempo requerida, com o mínimo de recursos.

Este plano deve identificar os procedimentos, responsabilidades, dependências externas, contratos existentes, as perdas de informações e serviços aceitáveis. Deve ser armazenado em um ambiente remoto, junto com os outros materiais necessários para sua execução e que este local possua nível de controle de segurança lógica e física equivalente ao ambiente principal.

2.9 Gestão de incidentes de segurança da informação e rede

Os incidentes de segurança da informação devem ser sempre informados o mais rápido possível. É responsabilidade de todos os colaboradores do IBGE notificar 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 também devem ser realizados para a detecção de incidentes de segurança da informação.

Os incidentes detectados serão direcionados para a Equipe de Tratamento de Incidentes, formada por profissionais de diversas áreas, selecionados de acordo com as características do incidente. Esta equipe irá coletar todas as informações relacionadas à ocorrência do incidente, como trilhas de auditoria, e avaliá-las para tomar as devidas providências e tratar os reflexos do incidente, evitando sua repetição.

As providências podem incluir revisão de normas e procedimentos existentes, aquisição de novos equipamentos e/ou ferramentas, reconfiguração de permissões, encaminhar informações para possível 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 já foi iniciado, abordando os principais serviços que proveem a infraestrutura de tecnologia da informação e alguns canais institucionais disponíveis na Internet. O plano determinará os procedimentos para tratamento e resposta aos diferentes tipos de incidentes, a fim de assegurar respostas rápidas, efetivas e ordenadas, as estratégias de monitoramento, os planos de contingência e a normatização do registro dos incidentes.

2.10 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. Este acesso pode ser revogado nos casos de ameaça iminente a qualquer ativo, por desrespeito Política de Segurança da Informação e Comunicações - POSIC e/ou por necessidade de serviço.

A operacionalização da política será realizada pela Ordem de Serviço de Acesso à Internet.

2.11 Sistema de mensageria

A utilização de qualquer sistema de mensageria 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.

Os serviços de mensageria, correio eletrônico, mensageria instantânea e videoconferência são ferramentas de trabalho fornecidas aos colaboradores do IBGE para a comunicação, intercâmbio de dados, ideias e informações e para o apoio às atividades da Instituição.

A Política para Utilização do Correio Eletrônico no IBGE e a Norma de Mensageria Instantânea e Videoconferência estabelecem os critérios, procedimentos e regras para o acesso e uso desses serviços, sendo operacionalizadas pelas Ordens de Serviço para Uso do Correio Eletrônico e para Uso de Mensageria Instantânea e Videoconferência, respectivamente.

3. Competências e responsabilidades

Ao Conselho Diretor compete:

- aprovar a Política de Segurança da Informação e Comunicações - POSIC e suas atualizações; e
- prover a alocação de recursos humanos, financeiros e materiais necessários para a POSIC.

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

- garantir 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 e à Auditoria do IBGE;
- 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:

- garantir que a POSIC atenda as normas e legislações vigentes;
- garantir que a POSIC esteja alinhada com os objetivos e metas do Planejamento Estratégico do IBGE;
- garantir que a POSIC esteja em consonância com as determinações do Grupo de Sigilo do IBGE;
- coordenar o Plano de Capacitação Contínua em Segurança da Informação 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;
- indicar os recursos necessários à aderência da POSIC no IBGE e encaminhá-los as áreas competentes;
- analisar os relatórios de violação de confidencialidade, integridade e autenticidade a serem encaminhados às áreas competentes; e
- encaminhar às áreas competentes as informações de violação da segurança da informação e comunicações.

À área de Recursos Humanos compete:

- garantir a todos os servidores públicos e estagiários, o conhecimento do conjunto de documentos que compõem a POSIC;
- garantir a assinatura e a guarda do Termo de Confidencialidade dos servidores públicos e estagiários; e
- notificar a Diretoria de Informática qualquer movimentação referente a servidores públicos e estagiários, com vistas a regularizar o acesso aos ativos de tecnologia.

Aos Gestores de Contratos de Prestação de Serviços compete:

- garantir o acesso 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 sobre Ativo de Tecnologia no momento de seu ingresso nas dependências do IBGE;
- exigir o cumprimento da POSIC pelos prestadores de serviço; e
- notificar a Diretoria de Informática qualquer movimentação referente a prestadores de serviço com vistas a regularizar o acesso aos ativos de tecnologia.

À Equipe de Tratamentos de Incidentes compete:

- realizar ações reativas de tratamento dos incidentes após serem notificados;
- reduzir/eliminar os efeitos dos incidentes o mais rápido possível.
- buscar as causas, danos e responsáveis pelos incidentes ocorridos; e
- analisar e documentar as evidências do incidente e o tratamento adotado em resposta aos

incidentes, enviando o Relatório de Tratamento de Incidentes ao Gestor de Segurança da Informação e Comunicações.

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;
- 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;
- avaliar, regularmente, se os requisitos de segurança da informação e comunicações estão sendo aplicados corretamente; e
- repassar a custódia 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.

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

A Diretoria de Informática 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 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 a POSIC;

- elaborar 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; e
- promover a melhoria contínua dos processos de gestão de segurança da informação e comunicações do IBGE.

4. Penalidades

O descumprimento da Política de Segurança da Informação e Comunicações 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), 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.

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. Disponível em: <http://www.abnt.org.br/normalizacao/lista-de-publicacoes/abnt>. Acesso em: jan. 2016.

_____. NBR ISO/IEC 27002: tecnologia da informação: técnicas de segurança: código de prática para a gestão de segurança da informação. Rio de Janeiro: ABNT, 2005.

_____. NBR ISO/IEC 27002: tecnologia da informação: técnicas de segurança: código de prática para controles de segurança da informação. Rio de Janeiro: ABNT, 2013. Disponível em: <http://www.abnt.org.br/normalizacao/lista-de-publicacoes/abnt>. Acesso em: jan. 2016.

_____. 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. Disponível em: <http://www.abnt.org.br/normalizacao/lista-de-publicacoes/abnt>. Acesso em: jan. 2016.

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: <http://www.presidencia.gov.br/legislacao>. Acesso em: jan. 2016.

_____. Decreto n. 3.505, de 13 de junho de 2000. Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal. Diário Oficial [da] República Federativa do Brasil, Brasília, DF, ano 138, n. 114, 14 jun. de 2000a. Seção 1, p. 2-3. Disponível em: <http://www.presidencia.gov.br/legislacao>. Acesso em: jan. 2016.

_____. 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: <http://www.presidencia.gov.br/legislacao>. Acesso em: jan. 2016.

_____. 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: <http://www.presidencia.gov.br/legislacao>. Acesso em: jan. 2016.

_____. 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.presidencia.gov.br/legislacao>. Acesso em: jan. 2016.

_____. 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: <http://www.presidencia.gov.br/legislacao>. Acesso em: jan. 2016.

_____. 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: <http://www.presidencia.gov.br/legislacao>. Acesso em: jan. 2016.

_____. Departamento de Segurança da Informação e Comunicações da Presidência da República. Norma Complementar n. 01, de 13 de outubro de 2008. Atividade de normatização. Disponível em: <http://dsic.planalto.gov.br/legislacaodsic/23-dsic/legislacao/53-normas-complementares>. Acesso em: jan. 2016.

BRASIL. Departamento de Segurança da Informação e Comunicações da Presidência da República. Norma Complementar n. 02, de 13 de outubro de 2008. Metodologia de gestão de segurança da informação e comunicações. Disponível em: <http://dsic.planalto.gov.br/legislacaodsic/23-dsic/legislacao/53-normas-complementares>. Acesso em: jan. 2016.

_____. Departamento de Segurança da Informação e Comunicações da Presidência da República. Norma Complementar n. 03, de 30 de junho de 2009. Diretrizes para elaboração de política de segurança da informação e comunicações nos órgãos e entidades da administração pública federal. Disponível em: <http://dsic.planalto.gov.br/legislacaodsic/23-dsic/legislacao/53-normas-complementares>. Acesso em: jan. 2016.

_____. Departamento de Segurança da Informação e Comunicações da Presidência da República. Norma Complementar n. 04, de 15 de fevereiro de 2013. Gestão de riscos de segurança da informação e comunicações - GRSIC. Disponível em: <http://dsic.planalto.gov.br/legislacaodsic/23-dsic/legislacao/53-normas-complementares>. Acesso em: jan. 2016.

_____. Departamento de Segurança da Informação e Comunicações da Presidência da República. 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: <http://dsic.planalto.gov.br/legislacaodsic/23-dsic/legislacao/53-normas-complementares>. Acesso em: jan. 2016.

_____. Departamento de Segurança da Informação e Comunicações da Presidência da República. Norma Complementar n. 06, de 11 de novembro de 2009. Gestão de continuidade de negócios em segurança da informação e comunicações. Disponível em: <http://dsic.planalto.gov.br/legislacaodsic/23-dsic/legislacao/53-normas-complementares>. Acesso em: jan. 2016.

_____. Departamento de Segurança da Informação e Comunicações da Presidência da República. Norma Complementar n. 07, de 15 de julho de 2014. Diretrizes para implementação de controles de acesso relativos à segurança da informação e comunicações. Disponível em: <http://dsic.planalto.gov.br/legislacaodsic/23-dsic/legislacao/53-normas-complementares>. Acesso em: jan. 2016.

_____. Departamento de Segurança da Informação e Comunicações da Presidência da República. 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: <http://dsic.planalto.gov.br/legislacaodsic/23-dsic/legislacao/53-normas-complementares>. Acesso em: jan. 2016.

_____. Departamento de Segurança da Informação e Comunicações da Presidência da República. 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: <http://dsic.planalto.gov.br/legislacaodsic/23-dsic/legislacao/53-normas-complementares>. Acesso em: jan. 2016.

_____. Departamento de Segurança da Informação e Comunicações da Presidência da República. Norma Complementar n. 10, de 30 de janeiro de 2012. Inventário e mapeamento de ativos de informação nos aspectos relativos à segurança da informação e comunicações nos órgãos e entidades da administração pública federal. Disponível em: <http://dsic.planalto.gov.br/legislacaodsic/23-dsic/legislacao/53-normas-complementares>. Acesso em: jan. 2016.

_____. Departamento de Segurança da Informação e Comunicações da Presidência da República. Norma Complementar n. 11, de 30 janeiro de 2012. Diretrizes para avaliação de conformidade nos aspectos relativos à segurança da informação e comunicações. Disponível em: <http://dsic.planalto.gov.br/legislacaodsic/23-dsic/legislacao/53-normas-complementares>. Acesso em: jan. 2016.

_____. Departamento de Segurança da Informação e Comunicações da Presidência da República. 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: <http://dsic.planalto.gov.br/legislacaodsic/23-dsic/legislacao/53-normas-complementares>. Acesso em: jan. 2016.

_____. Departamento de Segurança da Informação e Comunicações da Presidência da República. Norma Complementar n. 13, de 30 de janeiro de 2012. Diretrizes para gestão de mudanças nos aspectos relativos à segurança da informação e comunicações nos órgãos e entidades da administração pública federal. Disponível em: <http://dsic.planalto.gov.br/legislacaodsic/23-dsic/legislacao/53-normas-complementares>. Acesso em: jan. 2016.

_____. Departamento de Segurança da Informação e Comunicações da Presidência da República. Norma Complementar n. 14, de 30 de janeiro de 2012. Diretrizes relacionadas à segurança da informação e comunicações para o uso de computação em nuvem nos órgãos e entidades da administração pública federal. Disponível em: <http://dsic.planalto.gov.br/legislacaodsic/23-dsic/legislacao/53-normas-complementares>. Acesso em: jan. 2016.

_____. Departamento de Segurança da Informação e Comunicações da Presidência da República. Norma Complementar n. 15, de 11 de junho de 2012. Diretrizes para o uso seguro das redes sociais na administração pública federal. Disponível em: <http://dsic.planalto.gov.br/legislacaodsic/23-dsic/legislacao/53-normas-complementares>. Acesso em: jan. 2016.

_____. Departamento de Segurança da Informação e Comunicações da Presidência da República. Norma Complementar n. 16, de 21 de novembro de 2012. Diretrizes para desenvolvimento e obtenção de software seguro nos órgãos e entidades da administração pública federal. Disponível em: <http://dsic.planalto.gov.br/legislacaodsic/23-dsic/legislacao/53-normas-complementares>. Acesso em: jan. 2016.

_____. 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: <http://www.presidencia.gov.br/legislacao>. Acesso em: jan. 2016.

_____. 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: <http://www.presidencia.gov.br/legislacao>. Acesso em: jan. 2016.

_____. 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: <http://www.presidencia.gov.br/legislacao>. Acesso em: jan. 2016.

_____. 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.presidencia.gov.br/legislacao>. Acesso em: jan. 2016.

_____. 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: <http://www.presidencia.gov.br/legislacao>. Acesso em: jan. 2016.

_____. 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: <http://www.presidencia.gov.br/legislacao>. Acesso em: jan. 2016.

_____. 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: <http://www.presidencia.gov.br/legislacao>. Acesso em: jan. 2016.

_____. 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: <http://www.presidencia.gov.br/legislacao>. Acesso em: jan. 2016.

_____. 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: <http://www.presidencia.gov.br/legislacao>. Acesso em: jan. 2016.

_____. 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: <http://www.presidencia.gov.br/legislacao>. Acesso em: jan. 2016.

_____. 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: <http://www.presidencia.gov.br/legislacao>. Acesso em: jan. 2016.

CONSELHO DE DEFESA NACIONAL (Brasil). Instrução Normativa GSI n. 01, de 13 de junho de 2008. Disciplina a gestão de segurança da informação e comunicações na administração pública federal, direta e indireta, e dá outras providências. Diário Oficial da União, Brasília, DF, ano 145, n. 115, 18 jun. 2008. Seção 1, p. 6-7. Disponível em: <http://dsic.planalto.gov.br/legislacaodsic>. Acesso em: jan. 2016.

IBGE. Ordem de Serviço DI/COINF n. 2/2015, de 14 de abril de 2015. Define ordem de serviço para o acesso à internet na Fundação Instituto Brasileiro de Geografia e Estatística (IBGE). Boletim de Serviço, Rio de Janeiro, n. 2761, p. 1-3, 17 abr. 2015.

_____. Ordem de Serviço DI/COINF n. 3/2015, de 20 de maio de 2015. Estabelece critérios e procedimentos sobre o uso do Correio Eletrônico da Fundação Instituto Brasileiro de Geográfica e Estatística (IBGE). Boletim de Serviço, Rio de Janeiro, n. 2766, p. 2-5, 22 maio 2015.

_____. Plano estratégico 2012-2015. Edição revisada. Rio de Janeiro, 2013. 73 p. Disponível em: <http://www.ibge.gov.br/home/disseminacao/eventos/missao/planejamento_estrategico_ibge_2012_2015.pdf>. Acesso em: jan. 2016.

_____. Portaria P.PR n. 552/2015, de 22. out. 2015. Designa os membros do Comitê de Segurança da Informação e Comunicações do IBGE (CSI). Boletim de Serviço, Rio de Janeiro, n. 2788, p. 3-4, 23 out. 2015.

_____. Resolução RCD n. 22/2014, de 05 nov. 2014. Define política sobre o uso do Correio Eletrônico da Fundação Instituto Brasileiro de Geografia e Estatística (IBGE) e dá outras providências. Boletim de Serviço, Rio de Janeiro, n. 2738, p. 1-3, 07 nov. 2014.

_____. Resolução RCD n. 26/2015, de 21 de outubro de 2015. Cria o Comitê de Segurança da Informação e Comunicações do IBGE - CSI. Boletim de Serviço, Rio de Janeiro, n. 2789, p. 1-2, 30 out. 2015.

_____. Resolução RCD n. 30/2014, de 29 de dezembro de 2014. Define política de acesso à internet da Fundação Instituto Brasileiro de Geografia e Estatística (IBGE) e dá outras providências. Boletim de Serviço, Rio de Janeiro, n. 2746, p. 1-5, 2 jan. 2015.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. ISO/IEC 27000: information technology: security techniques information security management systems: overview and vocabulary. 3 rd. Vernier, Geneva, 2014. Disponível em: <http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html>. Acesso em: jan. 2016.

Equipe técnica responsável

1. Comitê de Segurança da Informação e Comunicações - CSI

   Paulo Cesar Moraes Simões (Gestor de Segurança da Informação e Comunicações)

   Andréia Fernandes da Silva (Secretária Executivo do CSI)

   Bruno Cesar Barbosa Alves(DI)

   José Luiz Thomaselli Nogueira(DI)

   Jose Sant Anna Bevilaqua(DI)

   Jose de Souza Pinto Guedes(DE)

   Francisco Jose Pereira(DE)

   Rafael Lopes Silva(DGC)

   Celso José Monteiro Filho(DGC)

   Antônio Agra Lopes Neto(DPE)

   Cristina Maria Castanheira(DPE)

   Ian Monteiro Nunes(CDDI)

   Marise Maria Ferreira(CDDI)

   Carlos Jose Lessa de Vasconcellos(CDDI)

   Marcio Imamura(COC)

   Germano Augusto Z. Goncalves Andrade(COC)

   Edson Chun Ichi Ebara(AUD)

   Adilson da Silva Marques(AUD)

   Mauro dos Santos Mendonça(ENCE)

   Jose André de Moura Brito(ENCE)

   Luis Cesar Seixas de Oliveira(GPR)

   Daniel Alves Moreira(GPR)

2. Equipe da Diretoria de Informática para Construção da POSIC

   Arnaldo Lyrio Barreto

   Sandra Martins Lino