Política de Segurança da Informação e Comunicações do IBGE

IBGE
Instituto Brasileiro de Geografia e Estatística

Ministério do Planejamento, Orçamento e Gestão
Instituto Brasileiro de Geografia e Estatística – IBGE
Diretória de Informática - DI

Política de Segurança da Informação e Comunicações do IBGE

Rio de Janeiro
Outubro - 2014

Presidenta da República
Dilma Rousseff

Ministério do Planejamento, Orçamento e Gestão
Ministra do Planejamento, Orçamento e Gestão
Miriam Belchior

Instituto Brasileiro de Geografia e Estatística
Presidenta do IBGE
Wasmália Bivar

Diretoria Executiva (DE)
Fernando José de Araújo Abrantes

Diretoria de Informática (DI)
Paulo Cesar Moraes Simões

Diretoria de Pesquisas (DPE)
Roberto Luís Olinto Ramos

Diretoria de Geociências (DGC)
Wadih João Scandar Neto

Centro de Documentação e Disseminação de Informações (CDDI)
David Wu Tai

Escola Nacional de Ciências Estatísticas (ENCE)
Maysa Sacramento de Magalhães

Comitê de Tecnologia da Informação e Comunicação (CTIC)
Antonio Jose Ribeiro Dias
Arnaldo Lyrio Barreto – Secretário Executivo do CTIC
Bruno Freitas Cortez
Carlos José Lessa de Vasconcellos
Claudio Stenner
Edson Chun Ichi Ebara
Francisco Jose Pereira
Germano Augusto Zulchner G. Andrade
Ian Monteiro Nunes
Jose de Souza Pinto Guedes
Jose Sant Anna Bevilaqua
Luis Cesar Seixas de Oliveira
Luiz Fernando Pinto Mariano
Luiz Paulo do Nascimento
Marcio Imamura
Mauro dos Santos Mendonça
Nivia Regis di Maio Pereira
Patricia do Amorim Vida Costa
Paulo Cesar Moraes Simões – Presidente do CTIC
Paulo Vicente Mitchell
Pedro Luis do Nascimento Silva
Pedro Luiz de Sousa Quintslr

Equipe da Diretoria de Informática para Construção da POSIC
Andréia Fernandes da Silva
Arnaldo Lyrio Barreto
Carlos Alvaro de Macedo Soares Quintella
Sandra Martins Lino
Verônica dos Santos

Sumário

Apresentação

Este documento foi elaborado com objetivo de instituir a Política de Segurança da Informação e Comunicações (POSIC) definindo diretrizes estratégicas, responsabilidades e competências para garantir a confidencialidade, integridade, autenticidade e disponibilidade das informações, além de outros princípios aqui citados, difundindo as boas práticas e a cultura de segurança da informação no corpo de colaboradores do IBGE. Atualmente o IBGE é regido por um estatuto, estabelecido pelo Decreto nº 4.740 de 13/06/2003.

Cabe ao IBGE assegurar informações e estudos de natureza estatística, geográfica, cartográfica e demográfica necessários ao conhecimento da realidade física, econômica e social do País, visando especificamente ao planejamento econômico e social e à segurança nacional, conforme lei 5878/73.

Para que o IBGE alcance seus objetivos, foi instituído o Plano Geral de Informações Estatísticas e Geográficas como instrumento de orientação e coordenação das atividades de produção das informações. As informações necessárias para a execução do Plano serão prestadas obrigatoriamente por pessoas e empresas, e utilizadas exclusivamente para fins estatísticos, conforme definido na lei 5534/68.

A privacidade do informante e o sigilo das informações prestadas têm que ser garantidos para manutenção da relação de confiança e cooperação entre as partes, e impedir qualquer impacto negativo nas operações da Instituição causado pela violação do compromisso assumido.

Ressalta-se aqui a Lei de Acesso da Informação - LAI, nº 12.527/2011, que trata de assegurar a todos cidadãos o direito fundamental de acesso à informação, na qual o IBGE está submetido e que tem, em seu inciso I, a necessidade de "observância da publicidade como preceito geral e do sigilo como exceção".

A Lei nº 12.965/2014, conhecida como Marco Civil da Internet, estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil e determina as diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios foi observada na elaboração deste documento.

A publicação da POSIC atende às exigências legais e normativas do MPOG/SLTI, TCU, CGU e Gabinete de Segurança Institucional da Presidência da República (GSI/PR), assim como as metas estratégicas estabelecidas no Planejamento Estratégico 2012-2015 do IBGE.

A POSIC será atualizada anualmente a partir de Dezembro de 2014, sendo publicada a sua versão vigente tanto na Intranet do IBGE quanto na página institucional.

Os esforços empregados na criação desse documento permitirão que, cada vez mais, a cultura de segurança da informação e comunicações possa amadurecer e bem servir às necessidades institucionais.

Paulo Cesar Moraes Simões
Presidente do CTIC 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", define características importantes da informação prestada pela Instituição que só poderão ser garantidas se uma Política de Segurança da Informação e Comunicações estiver efetivamente implementada, e sendo conduzida com eficiência e eficácia.

A POSIC é uma das práticas listada pela Norma Brasileira ABNT NBR ISO/IEC 27002:2005 para auxiliar a gestão da segurança da informação, que também a estabelece como fator crítico de sucesso dentro de uma organização. A 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 POSIC 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 implementação da POSIC é sustentada por planos (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.

Os principais planos que serão produzidos a partir da implantação desta POSIC são:

- Plano de Capacitação Contínua em Segurança da Informação;
- Plano de Continuidade do Negócio;
- Plano de Gerenciamento de Riscos em Tecnologia da Informação e Comunicações; e
- Plano de Gerenciamento e Tratamento de Incidentes em Tecnologia da Informação e Comunicações.

A elaboração da POSIC está alinhada ao Planejamento Estratégico 2012-2015 do IBGE, conforme os seguintes objetivos estratégicos:

- **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 pela Norma Brasileira ABNT NBR ISO/IEC 27002:2005 como crítico para o sucesso da POSIC.

Seguindo a recomendação da Norma Complementar 03/IN01/DSIC/GSIPR, este documento possuí os seguintes tópicos: Escopo, Conceitos e Definições, Princípios, Diretrizes Gerais, Penalidades e

Competências e Responsabilidades e o anexo com as Referências Legais e Normativas.

Esta Política será complementada pelos seguintes documentos:

- Nível Estratégico
  - Política de Acesso à Internet;
  - Política de Classificação de Ativos de Informação; e
  - Política sobre o Uso do Correio Eletrônico no IBGE.
- Nível Tático
  - Norma de Mensageria Instantânea e Videoconferência; e
  - Norma para Desenvolvimento de Sistemas.
- Nível Operacional
  - Ordem de Serviço de Acesso à Internet;
  - Ordem de Serviço de Back-up;
  - 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 Aquisição de Sistemas;
  - 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 Dispositivos Móveis;
  - 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;
  - Termo de Confidencialidade; e
  - Termo de Responsabilidade sobre Ativo de Tecnologia.

1.3 Conceitos e Definições

Ameaça – causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização (ISO/IEC 13335-1:2004).

Ativo - qualquer coisa que tenha valor para a organização. (Norma Brasileira ABNT NBR ISO/IEC 27002:2005).

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 conceder ou bloquear o acesso, baseados nos requisitos de segurança e nas atividades do usuário.

Credenciais ou Contas de Acesso - identificação única, concedida de forma pessoal e intransferível a uma pessoa, em conjunto com uma senha que garante a sua 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 – funcionários 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 pelo Conselho Diretor, 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.

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.

Política – intenções e diretrizes globais, formalmente expressas pela direção da Instituição.

Risco – possibilidade de ocorrência de evento adverso à Instituição ou projeto.

Sigilo – confidencialidade, segredo.

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

Vulnerabilidade – fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças.

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 Brasileira ABNT NBR ISO/IEC 27002:2005 e também dos Princípios Fundamentais das Estatísticas Oficiais estabelecidos pela Organização das 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

As diretrizes de segurança da informação estabelecidas nesta POSIC 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 Política de Segurança da Informação e Comunicação do IBGE (POSIC) deve ser realizada continuamente.

Para garantir que os colaboradores tenham ciência da POSIC e sejam sempre comunicados das alterações, será apresentada uma mensagem no momento do acesso à Rede do IBGE.

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 deste plano nas intranets.

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 – DI, pelo Comitê de Segurança da Informação e Comunicações – CSI e pela Gerência de Segurança da Informação e Comunicações, a ser criada na DI.

O CSI deverá ser instituído pelo Conselho Diretor por portaria específica. O Conselho Diretor indicará nomes de especialistas das áreas setoriais para este comitê e sugere-se a seguinte composição:

I- Gestor de Segurança da Informação e Comunicações (Diretor de Informática);

II- 3 representantes da Diretoria de Informática (DI);

III- 1 representante da Diretoria Executiva (DE);

IV- 1 representante da Diretoria de Geociências (DGC);

V- 1 representante da Diretoria de Pesquisas (DPE);

VI- 2 representante do Centro de Documentação e Disseminação (CDDI);

VII- 1 representante da Coordenação Operacional do Censo (COC);

VIII- 1 representante da Auditoria (GPR);

IX- 1 representante da Escola Nacional de Ciências Estatísticas (ENCE); e

X- 1 representante do Gabinete da Presidência (GPR).

Os substitutos eventuais das unidades às quais pertencem os integrantes titulares do CSI, integrarão o grupo, na qualidade de suplentes. Esses serão indicados pelos respectivos membros das Diretorias e Coordenações Gerais. O CSI poderá convidar para assessorá-lo, quando necessário, qualquer servidor do IBGE, bem como, consultar especialistas e representantes de outras instituições.

A efetividade desta política de segurança 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 Instituição.

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, de acordo com a *Ordem de Serviço para Uso de Dispositivos Móveis e a Ordem de Serviço para Armazenamento de Dados*. Esta última 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 da Instituição 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 elaboração da *Ordem de Serviço de Back-up* 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 á Gerência de Segurança da Informação e Comunicações, através de um processo a ser definido por esta gerência.

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 usuário 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 funcionários, estagiários e 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, somente ser permitido 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 de usuários 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 estão 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 funcionário. A restrição de acesso deve estar alinhada aos riscos identificados.

A *Ordem de Serviço de Controle de Acesso Físico* definirá para cada área de hospedagem dos equipamentos os possíveis controles de acesso a serem estabelecidos, 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 usuário da máquina, sendo somente realizadas com o consentimento da unidade gestora de infraestrutura de tecnologia da informação.

Já a garantia da conformidade com a política de 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 3 (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.

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 agentes 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 organização, 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 organização.

Este plano deve prioritariamente indicar a forma de eliminação do risco, caso isso não seja possível podem se adotar estratégias para reduzir o risco, transferir o risco ou ainda aceitar a sua existência, e neste caso deve ser preparado um plano de contingência no caso de sua ocorrência. A atualização do mesmo deve ser feita periodicamente.

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 serão direcionados e/ou detectados pela Gerência de Segurança da Informação e Comunicações. Esta gerência irá coletar todas as informações relacionadas à ocorrência do incidente, como trilhas de auditoria, e avaliá-las para tomar as devidas providências para 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. A Gerência de Segurança da Informação e Comunicações pode demandar a participação de outras gerências na solução dos problemas causados pelo incidente. 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* a ser definido, que determinará os procedimentos para tratamento e resposta aos diferentes tipos de incidente, 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

As 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.

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 a POSIC e/ou por necessidade de serviço.

O acesso à Internet será regulamentado pela *Política de Acesso à Internet* que disciplinará a utilização dos recursos de acesso à Internet e listará os casos em que o acesso pode ser bloqueado e/ou revogado. Esse documento será complementado pela *Ordem de Serviço de Acesso à Internet* que definirá aspectos operacionais relacionados a política citada.

2.11 Sistema de Mensageria

A utilização de qualquer sistema de mensageria deve estar em consonância com as atividades desempenhadas pelo profissional no IBGE, e durante sua utilização os colaboradores do IBGE devem 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 servidores para a comunicação, intercâmbio de dados, ideias e informações e para o apoio às atividades da Fundação Instituto Brasileiro de Geografia e Estatística (IBGE).

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 POSIC; e
- garantir 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 funcionários e estagiários sob sua gestão;
- incorporar as diretrizes da POSIC nos processos de trabalho de suas unidades de gestão; e
- exigir o cumprimento da POSIC pelos funcionários e estagiários sob sua gestão.

Ao Gestor de Segurança da Informação e Comunicações compete:

- presidir o 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 **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;
- 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 a disseminação e conscientização da importância da segurança da informação e comunicações entre todos os colaboradores;
- revisar anualmente, ou em caráter extraordinário, a POSIC e seus documentos complementares, submetendo as alterações à avaliação do Comitê de Tecnologia da Informação e Comunicação - CTIC;

- publicar a versão vigente da POSIC e seus documentos complementares na Intranet do IBGE;
- acompanhar os trabalhos da Gerência de Segurança da Informação e Comunicações, operacionalizada pela Diretoria de Informática;
- avaliar os processos de segurança da informação no IBGE apontados pelo Comitê de Tecnologia da Informação e Comunicação - CTIC e sugerir medidas de curto, médio e longo prazo; e
- encaminhar à área competente as informações de violação da segurança da informação e comunicações.

À área de **Recursos Humanos** compete:

- garantir a todos os funcionários e estagiários, admitidos a partir da vigência da política, o conhecimento do conjunto de documentos que compõem a POSIC;
- garantir a assinatura e a guarda do *Termo de Confidencialidade* dos funcionários e estagiários; e
- notificar a Diretoria de Informática a admissão, demissão, exoneração, afastamentos, aposentadoria ou qualquer outra movimentação referente a funcionários e estagiários, com vistas a regularizar o acesso aos ativos de tecnologia.

À **Gerência de Segurança da Informação e Comunicações** compete:

- analisar e responder a incidentes relacionados à segurança da informação e comunicações;
- avaliar novas tecnologias, quanto à aderência à POSIC, propostas pelo Comitê de Tecnologia da Informação e Comunicação - CTIC antes de sua inclusão no PDTI;
- prospectar novas tecnologias que permitam a melhoria nos processos de segurança previstos na POSIC;
- elaborar, em conjunto com outras áreas do IBGE, o *Plano de Gerenciamento e Tratamento de Incidentes* com vistas a garantir a continuidade dos processos de negócio do IBGE;
- identificar e solicitar os recursos humanos, financeiros e materiais necessários à POSIC;
- 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;
- implantar e acompanhar os processos de segurança da informação e comunicações;
- promover a melhoria contínua dos processos de gestão de segurança da informação e

comunicações na Instituição;

- monitorar e acompanhar os ativos de tecnologia de informação com vistas a atuar preventivamente na ocorrência de incidentes; e
- verificar a conformidade da aplicação da POSIC.

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;
- exigir da Gerência de Segurança da Informação e Comunicações os requisitos de segurança da informação e comunicações pertinentes aos ativos de acordo com a sua classificação;
- avaliar, regularmente, se os requisitos de segurança da informação e comunicações estão sendo aplicados corretamente; e
- repassar a custódia dos ativos a outros funcionários da instituição em caso de afastamentos, aposentadorias e mudanças de responsabilidade.

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 a admissão, demissão, exoneração, afastamentos ou qualquer outra movimentação referente a prestadores de serviço com vistas a regularizar o acesso aos ativos de tecnologia.

À área de **Auditoria Interna** compete:

- verificar a conformidade dos procedimentos internos em relação à POSIC.

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.

4. Penalidades

O descumprimento da Política Corporativa de Segurança da Informação e Comunicações e/ou de suas normas e procedimentos acarretará na aplicação de sanções administrativas, cíveis e penais previstas no Estatuto do Servidor Público Federal (Lei no. 8112/1990), e pela avaliação da Comissão de Ética do IBGE, no Código Penal (Decreto-Lei no. 2848/1940, com as alterações da Lei no. 9983/2000 e do Decreto no. 2910/1998) e no Código Civil (Lei no. 10.406/2002), 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.

Anexo - Referências Legais e Normativas

Documento	*Descrição*
Lei 5.534, de 14 de novembro de 1968	Dispõe sobre a obrigatoriedade de prestação de informações estatísticas e dá outras providências.
Lei Nº 5.878, de 11 de maio de 1973	Dispõe sobre a Fundação Instituto Brasileiro de Geografia e Estatística - IBGE, e dá outras providências
Lei Nº 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.
Lei 8.159, de 8 de janeiro de 1991	Dispõe sobre a política nacional de arquivos públicos e privados e dá outras providências.
Lei 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.
Lei 9.610, de 19 de fevereiro de 1998	Altera, atualiza e consolida a legislação sobre direitos autorais e dá outras providências.
Lei 9.609, de 19 de fevereiro de 1998	Dispõe sobre a proteção da propriedade intelectual de programa de computador, sobre sua comercialização no País, e dá outras providências.
Lei 9.983, de 14 de julho de 2000	Altera o Decreto Lei 2848, de 7 de dezembro de 1940 – Código Penal e dá outras providências. Dispõe sobre tipificação de crimes por computador contra a APF.
Lei Complementar 105, de 10 de janeiro 2001	Dispõe sobre o sigilo das operações de instituições financeiras e dá outras providências.
Lei 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 no 8.112, de 11 de dezembro de 1990; revoga a Lei no 11.111, de 5 de maio de 2005, e dispositivos da Lei no 8.159, de 8 de janeiro de 1991; e dá outras providências.
Lei 12.965, de 23 de abril de 2014	Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.
Decreto-lei 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
Decreto 73177, de 20 de novembro de 1973	Regulamenta a Lei nº 5.534, de 14 de novembro de 1968, modificada pela Lei nº 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.
Decreto 1171/1994	Código de Ética do Funcionalismo Público Federal
Decreto 3.505, de 13 de junho de 2000	Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal.
Decreto 4.073, de 3 de janeiro de 2002	Regulamenta a Lei no 8.159, de 8 de janeiro de 1991, que dispõe sobre a política nacional de arquivos públicos e privados.
Decreto 4.553, de 27 de dezembro de 2002	Dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da Administração Pública Federal, e dá outras providências.
Decreto 7845/2012	Regulamenta procedimentos para o credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo no âmbito do Poder Executivo federal, e dispõe sobre o Núcleo de Segurança e Credenciamento, conforme o

	disposto nos arts. 25, 27, 29, 35, § 5º, e 37 da Lei nº 12.527, de 18 de novembro de 2011.
Decreto 7.724, de 16 de maio de 2012	Regulamenta a Lei no 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. 37 e no § 2o do art. 216 da Constituição.
ISO/IEC 13335-1:2004	Information technology – Security techniques – Management of information and communications technology security – Part 1: Concepts and models for information and communications technology security management.
ABNT NBR ISO/IEC 27002:2005	Tecnologia da Informação – Técnicas de Segurança – Código de Prática para a Gestão de Segurança da Informação. 2005
Norma Complementar Nº 01/IN01/DSIC/GSIPR, de 13 de outubro de 2008.	Estabelece critérios e procedimentos para elaboração, atualização, alteração, aprovação e publicação de normas complementares sobre Gestão de Segurança da Informação e Comunicações, no âmbito da Administração Pública Federal, direta e indireta.
Norma Complementar Nº 02/IN01/DSIC/GSIPR, de 13 de outubro de 2008	Metodologia de Gestão de Segurança da Informação e Comunicações.
Norma Complementar Nº 03/IN01/DSIC/GSIPR, de 30 de junho de 2009.	Diretrizes para a Elaboração de Política de Segurança da Informação e Comunicações nos Órgãos e Entidades da Administração Pública Federal.
Norma Complementar Nº 05/IN01/DSIC/GSIPR, de 14 de agosto de 2009.	Disciplina a criação de Equipes de Tratamento e Respostas a Incidentes em Redes Computacionais - ETIR nos órgãos e entidades da Administração Pública Federal.

Norma Complementar Nº 06/IN01/DSIC/GSIPR, de 11 de novembro de 2009.	Estabelece Diretrizes para Gestão de Continuidade de Negócios, nos aspectos relacionados à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF.
Norma Complementar Nº 07/IN01/DSIC/GSIPR, de 06 de maio de 2010.	Estabelece as Diretrizes para Implementação de Controles de Acesso Relativos à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF.
Norma Complementar Nº 08/IN01/DSIC/GSIPR, de 19 de agosto de 2010.	Estabelece as Diretrizes para Gerenciamento de Incidentes em Redes Computacionais nos órgãos e entidades da Administração Pública Federal.
Norma Complementar Nº 04/IN01/DSIC/GSIPR, de 25 de fevereiro de 2013.	Diretrizes para o processo de Gestão de Riscos de Segurança da Informação e Comunicações - GRSIC nos órgãos e entidades da Administração Pública Federal.
Norma Complementar Nº 09/IN01/DSIC/GSIPR, de 21 de março de 2013.	Estabelece orientações específicas para o uso de recursos criptográficos como ferramenta de controle de acesso em Segurança da Informação e Comunicações, nos órgãos ou entidades da Administração Pública Federal, direta e indireta.
Norma Complementar Nº 10/IN01/DSIC/GSIPR, de 30 de janeiro de 2012.	Estabelece diretrizes para o processo de Inventário e Mapeamento de Ativos de Informação, para apoiar a Segurança da Informação e Comunicações (SIC), dos órgãos e entidades da Administração Pública Federal, direta e indireta – APF.
Norma Complementar Nº 11/IN01/DSIC/GSIPR, de 10 de fevereiro de 2012.	Estabelece diretrizes para avaliação de conformidade nos aspectos relativos à Segurança da Informação e Comunicações (SIC) nos órgãos ou entidades da Administração Pública Federal, direta e indireta – APF.
Norma Complementar Nº 12/IN01/DSIC/GSIPR, de 10 de fevereiro de 2012.	Estabelece diretrizes e orientações básicas para o uso de dispositivos móveis nos aspectos referentes à Segurança da Informação e Comunicações (SIC) nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta.

Norma Complementar Nº 13/IN01/DSIC/GSIPR, de 10 de fevereiro de 2012.	Estabelece diretrizes para a Gestão de Mudanças nos aspectos relativos à Segurança da Informação e Comunicações (SIC) nos órgãos e entidades da Administração Pública Federal, direta e indireta (APF).
Norma Complementar Nº 14/IN01/DSIC/GSIPR, de 10 de fevereiro de 2012.	Estabelece diretrizes para a utilização de tecnologias de Computação em Nuvem, nos aspectos relacionados à Segurança da Informação e Comunicações (SIC), nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta.
Norma Complementar Nº 15/IN01/DSIC/GSIPR, de 21 de junho de 2012.	Estabelece diretrizes de Segurança da Informação e Comunicações para o uso de redes sociais, nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta.
Norma Complementar Nº 16/IN01/DSIC/GSIPR, de 21 de novembro de 2012.	Estabelece as Diretrizes para o Desenvolvimento e Obtenção de Software Seguro nos Órgãos e Entidades da Administração Pública Federal, direta e indireta.