

CAPES

**Edição Especial
Nº 2 - Maio
2012**

**Boletim
de serviço**

**PDE**

Presidência da CAPES

Portaria N° 066, de 16 de Maio de 2012

Aprova a Política de Segurança da Informação e Comunicações da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – CAPES.

O PRESIDENTE DA COORDENAÇÃO DE APERFEIÇOAMENTO DE PESSOAL DE NÍVEL SUPERIOR - CAPES, no uso das atribuições conferidas pelo artigo 26, incisos II e III do estatuto aprovado pelo Decreto n° 7.692, de 02 de março de 2012 e considerando:

- o disposto na norma complementar n° 03 do Gabinete de Segurança Institucional da Presidência da República, de 10 de junho de 2009 que define diretrizes para elaboração de política de segurança da informação e comunicações nos órgãos e entidades da administração pública federal;
- a portaria interna n° 04, de 07 de janeiro de 2010, alterada pela portaria interna n° 106, de 19 de maio de 2010, que institui o Comitê Gestor de Tecnologia da Informação e o Comitê de Segurança da Informação da CAPES;
- a portaria interna n° 178, de 03 de setembro de 2010, que disciplina a utilização dos recursos de tecnologia da informação nas unidades da CAPES.

RESOLVE:

Art. 1º Aprovar a Política de Segurança da Informação e Comunicações da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – CAPES.

CAPÍTULO I – DO ESCOPO

Art. 2º A Política de Segurança da Informação e Comunicações objetiva instituir diretrizes estratégicas, responsabilidades e competências a todos usuários da CAPES, visando viabilizar e assegurar disponibilidade, integridade, confidencialidade e autenticidade das informações da CAPES ou sob sua responsabilidade, contra ameaças, vulnerabilidades e falhas, inclusive as humanas, de modo a preservar os seus ativos de informação, como também sua imagem institucional.

CAPÍTULO II – DOS PRINCÍPIOS

Art. 3º A Política de Segurança da Informação e Comunicações obedecerá aos princípios constitucionais, administrativos e ao arcabouço legislativo vigente que rege a Administração Pública Federal.



CAPÍTULO III – DOS CONCEITOS E DEFINIÇÕES

- I. **Ameaça:** conjunto de fatores internos ou externos ou causa potencial de um incidente, que pode resultar dano para um sistema ou para a organização;
- II. **Ativo de informação:** meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso. Exemplo: banco de dados, dispositivos móveis, documentos, DVD, equipamentos, estações de trabalho, instalações, telefones, entre outros;
- III. **Autenticidade:** propriedade que certifica a produção, expedição, modificação e destruição da informação por determinada pessoa, sistema, órgão ou entidade;
- IV. **Celeridade:** todas as ações devem oferecer respostas dinâmicas e rápidas;-
- V. **Ciclo de vida da informação:** engloba o período desde a criação, o armazenamento, a consulta, o manuseio, o transporte até o descarte das informações;
- VI. **Confidencialidade:** disponibilidade da informação apenas à pessoa, sistema, órgão ou entidade autorizados;
- VII. **Dado:** conjunto de registros que organizados, agrupados, categorizados e padronizados, adequadamente, transformam-se em informação;
- VIII. **Disponibilidade:** propriedade de que a informação esteja acessível e utilizável;
- IX. **Gestor do ativo de informação:** tutor legal responsável pela classificação, manuseio, guarda e distribuição da informação;
- X. **Incidente:** qualquer evento que ameace ou comprometa a segurança da informação;
- XI. **Informação:** conjunto de dados, textos, imagens, métodos, sistemas ou quaisquer formas de representação dotadas de significado em determinado contexto, independentemente do suporte em que resida ou da forma pela qual seja veiculado;
- XII. **Informação da CAPES:** Toda informação ou conhecimento de cunho institucional relativo a CAPES, sob responsabilidade dos seus usuários;
- XIII. **Integridade:** propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;
- XIV. **Rede CAPES:** estrutura de recursos de tecnologia da informação e comunicações disponível aos usuários da CAPES;
- XV. **Risco:** potencial associado à exploração de vulnerabilidades de um ativo de informação por ameaças, com impacto negativo no negócio da organização;
- XVI. **Salvaguarda das informações:** cópias de segurança/*backup* das informações;
- XVII. **Sistema de informação:** Programa ou conjunto de programas de computador;
- XVIII. **Usuário:** todo servidor, consultor, terceirizado, estagiário ou pessoa autorizada;



XIX. Vulnerabilidade: fragilidade nos ativos de informação que pode ser explorada por uma ameaça.

CAPÍTULO IV – DAS DIRETRIZES GERAIS

Art. 4º Toda informação é considerada um patrimônio intangível e seu ativo deve ser protegido.

Art. 5º Na proteção dos ativos de informação da CAPES deve ser considerado todo o ciclo de vida da informação.

Art. 6º Toda a informação presente nos ativos de informação da CAPES deverá ser classificada e tratada de acordo com seu grau de sigilo.

Art. 7º As unidades da CAPES devem manter a documentação referente aos procedimentos e as rotinas operacionais de suas atividades atualizados e alinhados entre si.

Seção I – Gestão de Risco

Art. 8º Os ativos de informação da CAPES serão tratados por um processo contínuo de análise e avaliação de riscos que deve ser elaborado baseado na recomendação da Norma Complementar nº 04 do Gabinete de Segurança Institucional da Presidência da República ^[XII].

Parágrafo Único: Todo o usuário da CAPES deve comunicar ao Grupo de Resposta a Incidentes – GRI qualquer ameaça à segurança da informação e comunicação via formulário disponível na Intranet.

Seção II – Gestão de Continuidade

Art. 9º Os ativos de informação da CAPES devem ser protegidos contra impactos decorrentes de defeitos, desastres, indisponibilidades e falhas por meio de planos de continuidade conforme disposto na Norma Complementar nº 06 do Gabinete de Segurança Institucional da Presidência da República ^[XIV].

Seção III – Tratamento da Informação

Art. 10 Todas as informações da CAPES, classificadas com algum grau de sigilo, devem possuir mecanismos associados que garantam sua proteção adequada e acesso autorizado.



Art. 11 Os ativos de informação da CAPES devem ser classificados, conforme orientações da Norma Complementar nº 07 do Gabinete de Segurança Institucional da Presidência da República^[XVI].

Seção IV – Controles de Acesso

Art. 12 Todo o acesso aos ambientes físicos à Rede CAPES e aos sistemas de informação da CAPES deve possuir mecanismo de controle que assegure a sua rastreabilidade.

§1º Sempre que possível, os mecanismos de controle de acesso devem comunicar aos usuários as alterações realizadas nos seus perfis.

§2º O acesso aos ativos de informação da CAPES só é permitido a pessoas devidamente autorizadas.

Parágrafo Único: O acesso às dependências da CAPES é normatizado pela portaria nº 098, de 17 de agosto de 2009^[XXVI].

Art. 13 Todo tipo de permissão de acesso aos ativos de informação da CAPES, fornecido por senha, crachá, certificado digital, ou outros tipos de permissão, são pessoais e intransferíveis.

Seção V – Tratamento de Incidentes

Art. 14 As atividades de receber, analisar e responder notificações de incidentes deverão ser outorgadas ao Grupo de Resposta a Incidentes – GRI, esta diretriz considerará as recomendações da Norma Complementar nº 05 do Gabinete de Segurança Institucional da Presidência da República^[XIII].

Art. 15 Para um controle dos possíveis incidentes aos ativos de informação da CAPES, mecanismos de segurança específicos devem ser incorporados de acordo com as avaliações realizadas no processo de gestão de riscos, pelo Grupo de Resposta a Incidentes juntamente com os gestores de cada ativo.

CAPÍTULO V - DAS COMPETÊNCIAS E RESPONSABILIDADES

Art. 16 Cabe ao Comitê Gestor de Tecnologia da Informação prover os instrumentos necessários ao cumprimento das diretrizes estabelecidas nesta Política de Segurança da Informação e Comunicações.

Art. 17 Será de incumbência do Comitê de Segurança da Informação a revisão desta Política de Segurança da Informação e Comunicações, sempre que exigido e, caso necessário, propor modificações.



Seção I – Dos Usuários

Art. 18 A segurança das informações e comunicações da CAPES é de responsabilidade de todos os usuários.

Seção II – Das Universidades

Art. 19 A área responsável por fazer auditorias dos sistemas de informação e comunicações estará vinculada a Diretoria de Tecnologia da Informação – DTI.

1

Art. 20 Caberá a cada unidade da CAPES manter atualizada as permissões de acesso aos seus sistemas de informações e às instalações sob sua responsabilidade e informar ao Grupo de Resposta a Incidentes - GRI quando houver perda ou roubo das formas de acesso, além de outras medidas cabíveis.

Art. 21 A Diretoria de Tecnologia da Informação – DTI é responsável por:

- I. Assegurar a disponibilidade e a integridade de todos os sistemas de informação da CAPES;
- II. Definir os prazos de retenção para a salvaguarda das informações digitais em consonância com os gestores dos ativos de informação;
- III. Mitigar os riscos existentes na rede CAPES;
- IV. Manter atualizados os controles de acesso aos sistemas de informação e;
- V. Fazer periodicamente análises de vulnerabilidades na rede CAPES.

CAPÍTULO VI - DAS PENALIDADES

Art. 22 O descumprimento ou violação desta Política de Segurança da Informação e Comunicações e demais normas e procedimentos estabelecidos relativos a ela terá implicação administrativa, civil e/ou penal, segundo as normas e legislações vigentes e de acordo com a gravidade do ato praticado.-

CAPÍTULO VII - SENSIBILIZAÇÃO, CONSCIENTIZAÇÃO E CAPACITAÇÃO

Art. 23 Todas as unidades da CAPES deverão manter um processo permanente de divulgação de suas normas e procedimentos para capacitar, conscientizar e sensibilizar seus usuários à correta conduta na utilização das informações da CAPES.



Seção I – Divulgação

Art. 24 Após a publicação desta Política de Segurança da Informação e Comunicações ela estará disponível permanentemente nos canais de comunicação interno, externo da CAPES e no D.O.U. a todos os usuários.

Parágrafo Único: Cabe ao Comitê de Segurança da Informação garantir a divulgação desta Política de Segurança da Informação e Comunicações.

CAPÍTULO VIII - DA ATUALIZAÇÃO

Art. 25 Esta Política de Segurança da Informação e Comunicações será revisada e/ou atualizada a cada 2 anos ou quando eventos ou mudanças significativas assim a exigirem.

Art. 26 Todo usuário poderá propor mudanças a esta Política de Segurança da Informação e Comunicações e em suas normas e procedimentos relacionados, desde que devidamente embasadas, para avaliação do Comitê de Segurança da Informação.

CAPÍTULO IX – VIGÊNCIA

Art. 27 Esta Política de Segurança da Informação e Comunicações entrará em vigor da data de sua publicação.

CAPÍTULO X – AS REFERÊNCIAS LEGAIS E NORMATIVAS

Decretos

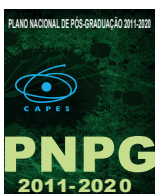
- [I] **Decreto nº 1.171 de 22/06/1994** – Aprova o Código de Ética Profissional do Servidor Público Civil do Poder Executivo Federal.
- [II] **Decreto nº 3.505 de 13/06/2000** – Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal
- [III] **Decreto nº 4.553 de 27/12/2002** – Dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da APF.
- [IV] **Decreto nº 5.482 de 30/06/2005** – Dispõe sobre a divulgação de dados e informações pelos órgãos e entidades da APF, por meio da rede mundial de computadores – Internet.
- [V] **Decreto nº 6.029 de 01/02/2007** – Institui o Sistema de Gestão da Ética do Poder Executivo Federal.

**Leis**

- [VI] **Lei nº 8.159 de 08/01/1991** – Dispõe sobre a Política Nacional de Arquivos Públicos e Privados.
- [VII] **Lei nº 9.609 de 19/02/1998** - Dispõe sobre a proteção da propriedade intelectual de programa de computador, sua comercialização no País, e dá outras providências.
- [VIII] **Lei nº 9.610 de 19/02/1998** - Altera, atualiza e consolida a legislação sobre direitos autorais e dá outras providências.
- [IX] **Lei nº 9.983 de 14/07/2000** – Código Penal e dá outras providências.

Normas Complementares

- [X] **Instrução normativa GSI nº1 de 13/06/2008** – Disciplina a Gestão de Segurança da Informação e Comunicações na APF, direta e indireta.
- [XI] **Norma Complementar nº 03/IN01/DSIC/GSIPR de 30/06/2009** - Diretrizes para elaboração de política de segurança da informação e comunicações nos órgãos e entidades da administração pública federal.
- [XII] **Norma Complementar nº 04/IN01/DSIC/GSIPR de 14/08/2009** - Diretrizes para o processo de Gestão de Riscos de Segurança da Informação e Comunicações - GRSIC nos órgãos e entidades da Administração Pública Federal.
- [XIII] **Norma Complementar nº 05/IN01/DSIC/GSIPR de 14/08/2009** - Disciplina a criação de Equipes de Tratamento e Respostas a Incidentes em Redes Computacionais - ETIR nos órgãos e entidades da Administração Pública Federal.
- [XIV] **Norma Complementar nº06/IN01/DSIC/GSIPR de 11/11/2009** - 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.
- [XV] **Norma Complementar nº07/IN01/DSIC/GSIPR de 06/05/2010** - 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.
- [XVI] **Norma Complementar nº08/IN01/DSIC/GSIPR de 19/08/2010** - Estabelece as Diretrizes para Gerenciamento de Incidentes em Redes Computacionais nos órgãos e entidades da Administração Pública Federal.
- [XVII] **Norma Complementar nº09/IN01/DSIC/GSIPR de 19/11/2010** - 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.

**PDE**

- [XVIII] **Norma Complementar nº10/IN01/DSIC/GSIPR de 30/01/2012** - Inventário e Mapeamento de Ativos de Informação nos Aspectos Relativos à Segurança da Informação e Comunicações nos órgãos e entidades da Administração Pública Federal
- [XIX] **Norma Complementar nº11/IN01/DSIC/GSIPR de 30/01/2012** - Diretrizes para Avaliação de Conformidade nos aspectos relativos à Segurança da informação e Comunicações.
- [XX] **Norma Complementar nº12/IN01/DSIC/GSIPR de 30/01/2012** - Uso de Dispositivos Móveis nos Aspectos relativos à Segurança da Informação e Comunicações nos órgãos e entidades da Administração Pública Federal.
- [XXI] **Norma Complementar nº13/IN01/DSIC/GSIPR de 30/01/2012** - Diretrizes para Gestão de Mudanças nos aspectos relativos à Segurança da Informação e Comunicações nos órgãos e entidades da Administração Pública Federal.
- [XXII] **Padrão de Interoperabilidade de Governo Eletrônico de 03/12/2010** – E-PING.
- [XXIII] **ABNT NBR ISO/IEC 27001 de 2006** – Norma de sistemas de gestão de segurança da informação.
- [XXIV] **ABNT NBR ISO/IEC 27002 de 2005** – Norma de código de prática para a gestão da segurança da informação.
- [XXV] **ABNT NBR ISO/IEC 27005 de 2008** – Norma de gestão de riscos de segurança da informação.

Portarias

- [XXVI] **Portaria Normativa nº 098, de 17/08/2009** – Institui sistema de Controle de Acesso de Pessoas e de Veículos às dependências da CAPES, abrangendo a identificação, o registro de entrada e saída e o uso de instrumentos de identificação, bem como o controle de acesso aos gabinetes das Diretorias e da Presidência.
- [XXVII] **Portaria Normativa nº 004, de 07/01/2010** - Institui o Comitê Gestor de Tecnologia da Informação e o Comitê de Segurança da Informação da CAPES.
- [XXVIII] **Portaria Normativa nº 106, de 19/05/2010** - Institui o Comitê Gestor de Tecnologia da Informação e o Comitê de Segurança da Informação da Capes.
- [XXIX] **Portaria Normativa nº 178, de 03/09/2010** - Disciplina a utilização dos recursos de Tecnologia da Informação nas unidades da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - CAPES.



Regimentos

[XXX] **Regimento Interno CAPES de 20/05/2008** - Regimento Interno CAPES, Portaria nº 609.

Resoluções

[XXXI] **Resolução nº 7, de 29/07/2002** - Estabelece regras e diretrizes para os sítios na internet da Administração Pública Federal.

JORGE ALMEIDA GUIMARÃES

Presidente

**PDE****Diretoria de Gestão - DGES****Coordenação-Geral de Gestão de Pessoas - CGGP****Portaria nº 65, de 14 de maio de 2012**

O Diretor de Gestão da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – CAPES, usando das atribuições que lhe são conferidas pelo Estatuto aprovado pelo Decreto nº 7.692, de 02 de março de 2012, publicado no Diário Oficial da União de 06 de março de 2012, e pela Portaria CAPES nº 164, de 31/08/2011, publicada no Diário Oficial da União de 16/09/2011, com base na Lei nº 8.691, de 28/07/93 e na MP nº 210, de 31/08/04, convertida na Lei nº 11.094, de 13/01/05, e em conformidade com a Resolução nº 03, de 20/12/94, do Conselho do Plano de Carreiras de Ciência e Tecnologia, e tendo em vista, ainda, o Parecer da Coordenação-Geral de Elaboração, Sistematização e Aplicação das Normas, da Secretaria de Recursos Humanos, do Ministério do Planejamento, Orçamento e Gestão, de 23/12/2008, exarado no Processo nº 23038.004252/2005-17, e o que consta do artigo 4º da Portaria CAPES nº 069, de 10/06/2009, resolve:

Art. 1º Conceder aos servidores constantes do Anexo desta Portaria progressão funcional, com efeitos financeiros a partir das datas especificadas.

Art. 2º Esta Portaria entra em vigor na data de sua assinatura.

FÁBIO DE PAIVA VAZ

Diretor

Anexo – Portaria nº 65, de 14 de maio de 2011

SERVIDOR	CARGO	SITUAÇÃO ATUAL		PROMOÇÃO		A PARTIR DE
		CLASSE	PADRÃO	CLASSE	PADRÃO	
Bruno Martini Bonaldo	Assistente em C & T	Assistente 1	II	Assistente 1	III	13/05/12
Patrícia Reis Paiva	Analista em C & T	Junior	II	Junior	III	16/04/12



Coordenação-Geral de Recursos Logísticos - CGLOG

Portaria n° 69, de 16 de maio de 2012.

O Diretor de Gestão da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – CAPES, usando das atribuições que lhe são conferidas pelo Estatuto aprovado pelo Decreto n° 7.692, de 2/3/2012, publicado no Diário Oficial da União de 6/3/2012, e pela Portaria CAPES n° 164, de 31/8/2011, publicada no Diário Oficial da União de 16/9/2011, resolve:

Art. 1º Designar **JORGE MELO DE OLIVEIRA SOUZA JÚNIOR**, Assistente em C&T, matrícula SIAPE n° 1671984, CPF n° 035.376.347-06, **SEBASTIÃO DE ARAUJO COSTA**, Assistente em C&T, matrícula SIAPE n° 435715, CPF n° 280.996.131.04, e **IZAEL ALVES DE SOUZA**, Assistente em C&T, matrícula SIPAE n° 45833, CPF n° 292.672.341-53, para Constituírem Comissão de Alienação e Desfazimento dos Bens Patrimoniais da CAPES.

Art. 2º Fixar prazo de trinta dias para a conclusão dos trabalhos.

Art. 3º Esta Portaria entra em vigor na data de sua assinatura.

FÁBIO DE PAIVA VAZ

Diretor

Boletim de Serviço

Edição Especial Nº 2

Maio - 2012

Coordenação de Aperfeiçoamento de Pessoal de Nível Superior

Expediente

Ministério da Educação
Coordenação de Aperfeiçoamento de Pessoal de Nível Superior

Boletim de Serviço, Edição Especial, Nº 2 - Maio de 2012

Editado, composto e impresso pela:
Diretoria de Gestão
Coordenação de Gestão de Documentos
Divisão de Tratamento da Informação

Data da publicação: Brasília, 16 de Maio de 2012

Ministro da Educação
ALOIZIO MERCADANTE OLIVA

Presidente da CAPES
JORGE ALMEIDA GUIMARÃES

Diretor de Gestão
FÁBIO DE PAIVA VAZ

Diretor de Avaliação
LIVIO AMARAL

Diretor Substituto de Programas e Bolsas no País
ADALBERTO GRASSI CARVALHO

Diretor de Relações Internacionais
MARCIO DE CASTRO SILVA FILHO

Diretora de Formação dos Professores da Educação Básica
CARMEN MOREIRA DE CASTRO NEVES

Diretor de Educação a Distância
JOÃO CARLOS TEATINI DE SOUZA CLÍMACO

Diretor de Tecnologia da Informação
SÉRGIO DA COSTA CÔRTEZ

Equipe Técnica
Astrogildo Brasil - CGD
Claudia Barbosa Santos - CGGP

Composição Gráfica
Astrogildo Brasil - CGD



Ministério da
Educação

