Boletim de Serviço nº 010/2012
Setembro/ 2012
Suplementar

BOLETIM DE SERVIÇO

MINISTRO DE ESTADO DA CIÊNCIA, TECNOLOGIA E INOVAÇÃO
Marco Antonio Raupp

Subsecretário SCUP/MCTI:
Arquimedes Diógenes Ciloni

Diretor LNCC:
Pedro Leite da Silva Dias

LNCC – Laboratório Nacional de Computação Científica
Av. Getúlio Vargas, 333
Quitandinha - Petrópolis
25.651-070 - Rio de Janeiro - RJ
Fone: 0xx (24) 2233-6000

Organização e distribuição:

Serviço de Recursos Humanos

Coordenação de Administração – SRH/CAD/LNCC

BOLETIM DE SERVIÇO

SUMÁRIO

ATOS DO DIRETOR

PORTARIA N.º. 109 DE 11 DE SETEMBRO DE 2012

ACOMPANHAMENTO DE CONTRATO

O DIRETOR DO LABORATÓRIO NACIONAL DE COMPUTAÇÃO CIENTÍFICA DO MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÃO, no uso da competência que lhe foi delegada pela Portaria n.º. 407, de 29 de junho de 2006, do Ministro de Estado da Ciência e Tecnologia, publicada no Diário Oficial da União de 30/06/2006,

RESOLVE

I - Designar o servidor **ANTONIO CARLOS FEITOSA COSTA**, CPF/MF nº 056.[redacted]-30, matrícula no SIAPE nº 1520690, Técnico, lotado no Serviço de Redes da Coordenação de Sistemas e Redes, para acompanhar e fiscalizar a execução do Contrato nº 04/2012, referente ao Processo nº 36/2012, celebrado com a empresa **UNITÉCNICA REFRIGERAÇÃO LTDA** e nos seus impedimentos legais seu substituto **AMARILDO LOPES DE OLIVEIRA**, CPF/MF nº 785.[redacted]-30, matrícula no SIAPE nº 1709670, Assistente em Ciência e Tecnologia, lotado na Seção de Apoio Administrativo da Coordenação de Administração.

II – O Fiscal terá como atribuições aquelas estabelecidas no artigo 67 da Lei n.º 8.666, de 21/jun/1993, e Decreto nº 2.271, de 7/jul/1997.

III - Esta Portaria entra em vigor na data de sua publicação no Boletim Interno do LNCC.

PORTARIA N.º. 110 DE 11 DE SETEMBRO DE 2012

COMISSÃO DE PÓS-GRADUAÇÃO

O DIRETOR DO LABORATÓRIO NACIONAL DE COMPUTAÇÃO CIENTÍFICA DO MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÃO, no uso da competência que lhe foi delegada pela Portaria n.º. 407, de 29 de junho de 2006, do Ministro de Estado da Ciência e Tecnologia, publicada no Diário Oficial da União de 30/06/2006,

RESOLVE

1. **PROPÓSITO**

Constituir a Comissão de Pós-Graduação, conforme previsto no Artigo 37 do Regimento Interno aprovado pela Portaria n.º 969 de 15 de dezembro de 2006, para orientação e assessoramento ao Diretor nos assuntos inerentes as atividades de Pós-Graduação, de acordo com a Portaria 009/2003.

2. **CONSTITUIÇÃO DA COMISSÃO**

A Comissão será composta por 06 (seis) membros, conforme abaixo:

1. Membros Titulares:

- Chefe do SAAFRH – Gilson Antonio Giraldi
- Representante da CMC – Laurent Emmanuel Dardenne
- Representante da CCC – Jauvane Cavalcante de Oliveira
- Representante da CMA – Antonio André Novotny
- Representante da CSC – Paulo Antonio Andrade Esquef
- Representante do Corpo Discente – Caio Padoan de Sá Godinho

2. Membros Suplentes:

- Representante da CMC – Regina Célia Cerqueira de Almeida
- Representante da CCC – Bruno Richard Schulze
- Representante da CMA – Hélio José Correa Barbosa
- Representante da CSC – Paulo Cesar Marques Vieira
- Representante do Corpo Discente – Alan Alves Santana Amad

Na ausência do membro titular ou do suplente, o Coordenador ou seu substituto legal, participará da reunião com direito a voto.

Esta Portaria cancela a Portaria n.º 104 de 16 de agosto de 2012.

Esta Portaria entra em vigor na data de sua publicação no Boletim de Serviço.

PORTARIA N.º 111 DE 17 DE SETEMBRO DE 2012

O DIRETOR DO LABORATÓRIO NACIONAL DE COMPUTAÇÃO CIENTÍFICA DO MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÃO, no uso da competência que lhe foi delegada pela Portaria n.º 407, de 29 de junho de 2006, do Ministro de Estado da Ciência e Tecnologia, publicada no Diário Oficial da União de 30/06/2006, resolve:

Revisar a aposentadoria do servidor **SÉRGIO RICARDO ALVES DE SOUZA,** matrícula SIAPE nº 0673149, com base no Art. 40, § 1º, inciso I CF 88 e § 21, c/c o Art. 6-A da Emenda Constitucional nº 41/2003, incluído pela Emenda Constitucional nº 70/2012 e Art. 186, § 1º da Lei nº 8.112/90(Processo nº 10768.006439/2005-41).

PORTARIA N.º 113 DE 25 DE SETEMBRO DE 2012

TERMO CIRCUNSTANCIADO ADMINISTRATIVO

O DIRETOR DO LABORATÓRIO NACIONAL DE COMPUTAÇÃO CIENTÍFICA DO MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÃO, no uso da competência que lhe foi delegada pela Portaria n.º. 407, de 29 de junho de 2006, do Ministro de Estado da Ciência e Tecnologia, publicada no Diário Oficial da União de 30/06/2006,

RESOLVE:

I - Nomear o servidor **JAUVANE CAVALCANTE DE OLIVEIRA**, SIAPE nº 1467400, para atuar no procedimento dos atos necessários a sanar as impropriedades apontadas no Memo nº 133/2012-CAD/LNCC datado de 13 de setembro de 2012, objeto de Termo Circunstanciado Administrativo a ser aberto, conforme dados constantes do processo nº 01209.000223/2012-45,

II - Esta Portaria entra em vigor na data de sua publicação no Boletim Interno do LNCC.

PORTARIA N.º. 114 DE 25 DE SETEMBRO DE 2012

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

O DIRETOR DO LABORATÓRIO NACIONAL DE COMPUTAÇÃO CIENTÍFICA, no uso da competência que lhe foi delegada pela Portaria n.º. 407, de 29 de junho de 2006, do Ministro de Estado da Ciência, Tecnologia e Inovação, publicada no Diário Oficial da União em 30/06/2006 e considerando:

A **Norma Brasileira ABNT NBR ISO/IEC 27002:2005** que descreve um Código de práticas para a gestão da Segurança da Informação.

A **Norma Brasileira ABNT NBR ISO/IEC 27001:2006** que descreve os requisitos a serem adotados na elaboração de sistemas de gestão de segurança da informação.

A **Lei nº 9.983, de 14 de julho de 2000** que altera o **Decreto-Lei Nº 2.848, de 7 de Dezembro de 1940 – Código Penal** e dá outras providências.

O **Decreto nº 4.553, de 27 de dezembro de 2002**, que 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.

O **Decreto nº 3.505, de 13 de junho de 2000** que institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal.

A **Instrução Normativa GSI nº 1, de 13 de junho de 2008** que Disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências.

A **Instrução Normativa Nº 4 - SLTI/MPOG**, de 12 de novembro de 2010 que Dispõe sobre o processo de contratação de Soluções de Tecnologia da Informação pelos órgãos integrantes do Sistema de Administração dos Recursos de Informação e Informática (SISP) do Poder Executivo Federal. (Publicada no DOU Nº 218, de 16 Nov 2010- Seção 1)

A **Norma Complementar nº 01/IN01/DSIC/GSIPR** que define a atividade de Normatização. Publicada no DOU Nº 200, de 15 Out 2008 - Seção 1

A **Norma Complementar nº 02/IN01/DSIC/GSIPR**, que define a Metodologia de Gestão de Segurança da Informação e Comunicações. Publicada no DOU Nº 199, de 14 Out 2008 - Seção 1

A **Norma Complementar nº 03/IN01/DSIC/GSIPR**, de determina as Diretrizes para a Elaboração de Política de Segurança da Informação e Comunicações nos Órgãos e Entidades da Administração Pública Federal. Publicada no DOU Nº 125, de 03 Jul 2009 - Seção 1

A **Norma Complementar nº 04/IN01/DSIC/GSIPR**, e seu anexo, Diretrizes para o processo de Gestão de Riscos de Segurança da Informação e Comunicações - GRSIC nos órgãos e entidades da Administração Pública Federal. Publicada no DOU Nº 156, de 17 Ago 2009 - Seção 1

A **Norma Complementar nº 05/IN01/DSIC/GSIPR**, e seu anexo, que disciplina a criação de Equipes de Tratamento e Respostas a Incidentes em Redes Computacionais - ETIR nos órgãos e entidades da Administração Pública Federal. Publicada no DOU Nº 156, de 17 Ago 2009 - Seção 1

A **Norma Complementar nº 06/IN01/DSIC/GSIPR**, que 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. Publicada no DOU Nº 223, de 23 Nov 2009 - Seção 1

A **Norma Complementar nº 07/IN01/DSIC/GSIPR**, que 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. Publicada no DOU Nº 86, de 7 Maio 2010 - Seção 1

A **Norma Complementar nº 08/IN01/DSIC/GSIPR**, que estabelece as Diretrizes para Gerenciamento de Incidentes em Redes Computacionais nos órgãos e entidades da Administração Pública Federal. Publicada no DOU Nº 162, de 24 Ago 2010 - Seção 1

A **Norma Complementar nº 09/IN01/DSIC/GSIPR**, que 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. Publicada no DOU Nº 222, de 22 Nov 2010 - Seção 1

A **Norma Complementar nº 10/IN01/DSIC/GSIPR**, que 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. Publicada no DOU Nº 30, de 10 Fev 2012 - Seção 1

A **Norma Complementar nº 11/IN01/DSIC/GSIPR**, que 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. Publicada no DOU Nº 30, de 10 Fev 2012 - Seção 1

A **Norma Complementar nº 12/IN01/DSIC/GSIPR**, que 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. Publicada no DOU Nº 30, de 10 Fev 2012 - Seção 1

A **Norma Complementar nº 13/IN01/DSIC/GSIPR**, que 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). Publicada no DOU Nº 30, de 10 Fev 2012 - Seção 1

A **Norma Complementar nº 14/IN01/DSIC/GSIPR**, que 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. Publicada no DOU Nº 30, de 10 Fev 2012 - Seção 1

A **Norma Complementar nº 15/IN01/DSIC/GSIPR**, que 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. Publicada no DOU Nº 119, de 21 Jun 2012 - Seção 1

A **Portaria Nº 45 - GSI**, de 8 de setembro de 2009, que Institui, o Grupo Técnico de Segurança Cibernética e dá outras providências.

A **Portaria nº 018, de 02 de março de 2010** que estabelece responsabilidade no uso dos recursos computacionais do LNCC.

Resolve:

Art. 1º. Instituir a Política de Segurança da Informação e Comunicação no Laboratório Nacional de Computação Científica (LNCC) e demais órgãos, entidades e pessoas jurídicas vinculadas, nos termos do Anexo da presente Portaria, no âmbito do Ministério da Ciência, Tecnologia e Inovação.

Art. 2º. Esta Portaria entra em vigor na data de sua publicação no Boletim de Serviço.

Política de Segurança da Informação e Comunicação do Laboratório Nacional de Computação Científica

Capítulo I

DAS DISPOSIÇÕES GERAIS

O conteúdo e formato desta política baseia-se nos seguintes documentos:

A **Norma Brasileira ABNT NBR ISO/IEC 27002:2005** que descreve um Código de práticas para a gestão da Segurança da Informação.

A **Norma Brasileira ABNT NBR ISO/IEC 27001:2006** que descreve os requisitos a serem adotados na elaboração de sistemas de gestão de segurança da informação.

A **Lei nº 9.983, de 14 de julho de 2000** que altera o **Decreto-Lei Nº 2.848, de 7 de Dezembro de 1940 – Código Penal** e dá outras providências.

O **Decreto nº 4.553, de 27 de dezembro de 2002**, que 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.

O **Decreto nº 3.505, de 13 de junho de 2000** que institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal.

A **Instrução Normativa GSI nº 1, de 13 de junho de 2008** que Disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências.

A **Instrução Normativa Nº 4 - SLTI/MPOG**, de 12 de novembro de 2010 que Dispõe sobre o processo de contratação de Soluções de Tecnologia da Informação pelos órgãos integrantes do Sistema de Administração dos Recursos de Informação e Informática (SISP) do Poder Executivo Federal. (Publicada no DOU Nº 218, de 16 Nov 2010- Seção 1)

A **Norma Complementar nº 01/IN01/DSIC/GSIPR** que define a atividade de Normatização. Publicada no DOU Nº 200, de 15 Out 2008 - Seção 1

A **Norma Complementar nº 02/IN01/DSIC/GSIPR**, que define a Metodologia de Gestão de Segurança da Informação e Comunicações. Publicada no DOU Nº 199, de 14 Out 2008 - Seção 1

A **Norma Complementar nº 03/IN01/DSIC/GSIPR**, de determina as Diretrizes para a Elaboração de Política de Segurança da Informação e Comunicações nos Órgãos e Entidades da Administração Pública Federal. Publicada no DOU Nº 125, de 03 Jul 2009 - Seção 1

A **Norma Complementar nº 04/IN01/DSIC/GSIPR**, e seu anexo, Diretrizes para o processo de Gestão de Riscos de Segurança da Informação e Comunicações - GRSIC nos órgãos e entidades da Administração Pública Federal. Publicada no DOU Nº 156, de 17 Ago 2009 - Seção 1

A **Norma Complementar nº 05/IN01/DSIC/GSIPR**, e seu anexo, que disciplina a criação de Equipes de Tratamento e Respostas a Incidentes em Redes Computacionais - ETIR nos órgãos e entidades da Administração Pública Federal. Publicada no DOU Nº 156, de 17 Ago 2009 - Seção 1

A **Norma Complementar nº 06/IN01/DSIC/GSIPR**, que 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. Publicada no DOU Nº 223, de 23 Nov 2009 - Seção 1

A **Norma Complementar nº 07/IN01/DSIC/GSIPR**, que 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. Publicada no DOU Nº 86, de 7 Maio 2010 - Seção 1

A **Norma Complementar nº 08/IN01/DSIC/GSIPR**, que estabelece as Diretrizes para Gerenciamento de Incidentes em Redes Computacionais nos órgãos e entidades da Administração Pública Federal. Publicada no DOU Nº 162, de 24 Ago 2010 - Seção 1

A **Norma Complementar nº 09/IN01/DSIC/GSIPR**, que 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. Publicada no DOU Nº 222, de 22 Nov 2010 - Seção 1

A **Norma Complementar nº 10/IN01/DSIC/GSIPR**, que 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. Publicada no DOU Nº 30, de 10 Fev 2012 - Seção 1

A **Norma Complementar nº 11/IN01/DSIC/GSIPR**, que 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. Publicada no DOU Nº 30, de 10 Fev 2012 - Seção 1

A **Norma Complementar nº 12/IN01/DSIC/GSIPR**, que 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. Publicada no DOU Nº 30, de 10 Fev 2012 - Seção 1

A **Norma Complementar nº 13/IN01/DSIC/GSIPR**, que 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). Publicada no DOU Nº 30, de 10 Fev 2012 - Seção 1

A **Norma Complementar nº 14/IN01/DSIC/GSIPR**, que 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. Publicada no DOU Nº 30, de 10 Fev 2012 - Seção 1

A **Norma Complementar nº 15/IN01/DSIC/GSIPR**, que 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. Publicada no DOU Nº 119, de 21 Jun 2012 - Seção 1

A **Portaria Nº 45 - GSI, de 8 de setembro de 2009**, que Institui, o Grupo Técnico de Segurança Cibernética e dá outras providências.

A **Portaria nº 018, de 02 de março de 2010** que estabelece responsabilidade no uso dos recursos computacionais do LNCC.

Seção l

Dos Termos Utilizados

Lista dos principais termos utilizados neste documento:

1. **ABNT**: Associação de Normas Técnicas
2. **ACL**: *Access Control List* ou Lista de controle de acesso
3. **Ativo**: Os ativos de uma organização, são os bens móveis, imóveis e até mesmos intangíveis, como a informação armazenada em meios diversos
4. **API**: Application Programming Interface (ou Interface de Programação de Aplicativos) é um conjunto de rotinas e padrões estabelecidos por um software para a utilização das suas funcionalidades por aplicativos que não pretendem envolver-se em detalhes da implementação do software, mas apenas usar seus serviços
5. **CSIC**: Comitê de Segurança da Informação e Comunicações
6. **CSR**: Coordenação de Sistemas e Rede
7. **DSIC**: Departamento de Segurança da Informação e Comunicações
8. **NBR**: Denominação de norma da Associação Brasileira de Normas Técnicas
9. **ISO**: International Organization for Standardization
10. **IEC**: International Electrotechnical Commission
11. **P2P**: é uma arquitetura de sistemas distribuídos caracterizada pela descentralização das funções na rede, onde cada nodo realiza tanto funções de servidor quanto de cliente.
12. **PDCA**: Plan-Do-Check-Act
13. **POSIC**: Politica de Segurança da Informação e Comunicação
14. **Proprietário**: identifica um pessoa que tenha uma responsabilidade autorizada para controlar o ativo.

Seção II

Da Instituição da Política de Segurança

A revisão e a aprovação desta política pelo Comitê de Segurança da Informação e Comunicações, instituído pelo Diretor do LNCC, através da Portaria n.º 098, de 19 de Outubro de 2011, resolve:

Art. 1º. Instituir a Política de Segurança da Informação e Comunicação no âmbito do Laboratório Nacional de Computação Científica (**LNCC**) e demais órgãos, entidades e pessoas jurídicas vinculadas.

Art. 2º. Os preceitos desta Portaria também estabelecem normas internas que cuidam dos acervos produzidos e armazenados em qualquer tipo de mídia pelo Laboratório Nacional de Computação Científica, bem como prover obrigações e responsabilidades decorrentes e correspondentes ao grau de importância atribuído a esses acervos.

Art. 3º. O conteúdo da Política de Segurança da Informação e Comunicação deve ser revisada anualmente.

Parágrafo único. O prazo para a publicação das revisões deverá ser contado a partir da data da publicação desta portaria e não deve ultrapassar 12(doze) meses.

Capítulo II

DOS PRINCÍPIOS

Art. 4º. Os mecanismos de segurança devem garantir os requisitos de segurança de forma que não interfiram na utilização de serviços prestados.

Art. 5º. A segurança das informações devem ser mantidas no meio da transmissão e nas extremidades.

Art. 6º. Todas as pessoas vinculadas direta ou indiretamente ao LNCC têm direito a confidencialidade de suas informações pessoais, conforme **Art. 5°, inciso XII da Constituição Federal**.

Parágrafo único. São invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação, **na forma do Art. 5°, inciso X da Constituição Federal.**

Art. 7º. São considerados originariamente sigilosos, e serão como tal classificados, dados ou informações cujo conhecimento irrestrito ou divulgação possa acarretar qualquer risco à segurança da sociedade, do Estado, na forma do art. 2º do **Decreto nº 4.553, de 27 de dezembro de 2002** bem como aqueles necessários ao resguardo da inviolabilidade da intimidade da vida privada, da honra e da imagem das pessoas.

Parágrafo único. O acesso a dados ou informações sigilosas é restrito e condicionado à necessidade de conhecer, conforme **Art. 2º do Decreto nº 4.553, de 2002**.

Art. 8º. Deve ser evitado o uso de protocolos sem criptografia.

Art. 9º. Não deve-se usar tecnologia cuja vulnerabilidade foi demonstrada.

Art. 10º. No intuito de manter a integridade e a autenticidade das informações, deve-se evitar redundâncias, exceto quando for necessário para garantir a segurança.

Art. 11º. Qualquer infração que venha a ocorrer será julgada pelo **Comitê de Segurança da Informação e Comunicações** (**CSIC**), de que trata o **Art. 5º, inciso VI da Instrução Normativa GSI Nº 1**, constituído pela **Portaria n.º 009, de 26 de janeiro de 2010**.

§1º. Observado o direito de defesa e o contraditório, o infrator ficará sujeito às sanções previstas no **inciso IV do art. 3º da Portaria n.º 018, de 02 de março de 2010**, quais sejam:

I – Solicitação de esclarecimentos;

II – Notificação;

III – Advertência;

IV – Notificação aos superiores responsáveis;

V – Restrição de acesso aos serviços de Tecnologia da Informação;

§2º. Os membros do Comitê de Segurança da Informação e Comunicações (**CSIC**) assegurarão no inquérito o sigilo necessário à elucidação do fato ou exigido pelo interesse do LNCC, conforme **Art. 20 do Código de Processo Penal**.

Parágrafo único. Se for necessário, será encaminhada denúncia às autoridades competentes.

Art. 12º. Conforme o **Art. 10 do Decreto nº 6.029/2007**, os trabalhos de todos os Comitês e Comissões de Ética devem ser desenvolvidos com celeridade e observância dos seguintes princípios:

I. proteção à honra e à imagem da pessoa investigada;

II. proteção à identidade do denunciante, que deverá ser mantida sob reserva, se este assim o desejar;

III. independência e imparcialidade dos seus membros na apuração dos fatos.

Art. 13º. A gestão de segurança da informação e comunicações baseia-se no processo de melhoria contínua, denominado ciclo PDCA (*Plan-Do-Check-Act*), referenciado pela norma **ABNT NBR ISO/IEC 27001:2006**, conforme **N.C. 02/IN01/DSIC/GSIPR, de 13 de outubro de 2008**.

Art. 14º. Todos os integrantes do LNCC, diretos ou indiretos, devem divulgar e informar sobre a existência desta Política de Segurança da Informação e Comunicações, estimulando o seu integral cumprimento.

Art. 15º. Os casos omissos à **POSIC** deverão ser tratados individualmente pelo **CSIC**.

Art. 16º. A Comissão Permanente de Avaliação de Documentos Sigilosos, instituída por ato do Diretor do Laboratório Nacional de Computação Científica, exercerá as atribuições previstas no **art. 35 e 36 do Decreto 4.553, de 2002.**

Art. 17º. Periodicamente os membros do LNCC serão informados sobre a Segurança da Informação onde esta política é apresentada e são dadas recomendações gerais baseadas nas auditorias.

Capítulo III

DA GESTÃO DOS ATIVOS

Art. 18º. Recomenda-se que todos os ativos sejam claramente identificados e que o inventário seja mantido.

Art. 19º. Recomenda-se que todas as informações e os ativos associados com os recursos de processamento da informação tenham um proprietário[1].

Art. 20º. Devem ser identificadas, documentadas e implementadas regras para que seja permitido o uso de informações e de ativos associados aos recursos de processamento da informação.

Art. 21º. Do ponto de vista do Sistema de Gestão de Segurança da Informação, a informação deve ser classificada em termos do seu valor, requisitos legais, sensibilidade e criticidade para a organização.

Capítulo IV

DA SEGURANÇA EM RECURSOS HUMANOS

Seção I

Das Considerações Gerais

Art. 22º. Os papéis e a responsabilidade pela segurança da informação de funcionários, fornecedores e terceiros devem ser definidos e documentados.

Art. 23º. Os funcionários e terceiros devem concordar e assinar os termos de confidencialidade e de responsabilidade.

Art. 24º. Os funcionários e terceiros devem participar dos treinamentos de conscientização e procedimentos organizacionais relacionados a Segurança da Informação.

Art. 25º. Deve existir um processo disciplinar formal para os funcionários e terceiros que tenham cometido uma violação da Segurança da Informação.

Art. 26º. Todos os funcionários e terceiros devem devolver todos os ativos da organização que estejam em sua posse antes do desligamento de suas atividades.

Art. 27º. O direito de acesso de todos os funcionários e terceiros às informações e aos recursos computacionais devem ser revogados após o desligamento de suas atividades.

Seção II

Das Divulgações de Segredo e Ações Não Autorizadas

Art. 28º. Constitui infração, sujeitando o infrator às penalidades previstas no Código Penal:

i. Divulgar, sem justa causa, conteúdo de documento particular ou de correspondência confidencial, de que é destinatário ou detentor, e cuja divulgação possa produzir dano a outrem;

ii. Divulgar, sem justa causa, informações sigilosas ou reservadas, assim definidas em lei, contidas ou não nos sistemas de informações ou banco de dados da Administração Pública;

iii. Revelar, sem justa causa, segredo, de que tem ciência em razão de função, ministério, ofício ou profissão, e cuja revelação possa produzir dano a outrem;

iv. Abusar dos privilégios para, no todo ou em parte, alterar o fluxo normal de correspondência, ou revelar a estranhos seu conteúdo;

v. Disponibilizar obras que violem os direitos autorais, mediante o programa de distribuição, cabo, fibra ótica, satélite, ondas ou qualquer outro sistema que permita ao usuário realizar a seleção da obra ou produção para recebê-la em um tempo e lugar previamente determinados por quem formula a demanda, com intuito de lucro, direto ou indireto, sem autorização expressa, conforme o caso, do autor, do artista intérprete ou executante, do produtor de fonograma, ou de quem os represente;

vi. Falsificar, no todo ou em parte, documento, ou alterar documento verdadeiro;

vii. Destruir, suprimir ou ocultar, em benefício próprio ou de outrem, ou em prejuízo alheio, documento público ou particular verdadeiro, de que não poderia dispor;

viii. Inserir ou facilitar a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou bancos de dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano;

ix. Modificar ou alterar sistema de informações ou programa de informática sem autorização ou solicitação de autoridade competente;

Art. 29º. Comunicar, entregar, auxiliar ou permitir a comunicação ou a entrega, a governo ou grupo estrangeiro, ou a organização ou grupo de existência ilegal, de dados, documentos ou cópias de documentos, planos, códigos, cifras ou assuntos que, no interesse do Estado brasileiro, são classificados como sigilosos, ou, obter ou revelar, para fim de espionagem, desenhos, projetos, fotografias, notícias ou informações a respeito de técnicas, de tecnologias, de componentes, de equipamentos, de instalações ou de sistemas de processamento automatizado de dados, em uso ou em desenvolvimento no País, que, reputados essenciais para a sua defesa, segurança ou economia, devem permanecer em segredo constitui infração, sujeitando o infrator às penalidades previstas na **Lei nº 7.170/83**.

Art. 30º. É proibido obter ou tentar obter, indevidamente, acesso a sistema de tratamento automático de dados, a fim de alterar informações ou procedimentos, além disto, é proibido tentar desenvolver ou introduzir comando, instrução ou programa de computador, capaz de destruir, apagar, eliminar, alterar, gravar ou transmitir dado, instrução ou programa ou provocar qualquer outro resultado diverso do esperado em sistema de tratamento automático de dados, sujeitando o infrator às penalidades previstas na **Lei nº 9.100, de 29 de setembro de 1995.**

Art. 31º. É proibido realizar interceptação de comunicações telefônicas, de informática ou telemática, ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei, sujeitando o infrator às penalidades previstas na **Lei nº 9.296, de 24 de julho de 1996**.

Art. 32º. É proibido destruir, inutilizar ou deteriorar arquivo, registro, museu, biblioteca, pinacoteca, instalação científica ou similar, sujeitando o infrator às penalidades previstas na **Lei nº 9.605, de 1998**.

Art. 33º. É proibido desenvolver clandestinamente atividades de telecomunicação, sujeitando o infrator às penalidades previstas na **Lei nº 9.472, de 16 de julho de 1997**.

Art. 34º. É vedada a propaganda eleitoral nos domínios do LNCC, conforme **Resolução nº 22.718, de 28 de fevereiro de 2008, do TSE**.

Seção III

Das Obrigações Contratuais dos Contratos com Terceiros

Art. 35º. Entende-se por colaboradores as pessoas físicas ou jurídicas, fornecedoras ou prestadoras de serviços, contratados, empresas incubadas ou demais conveniados ao LNCC.

Art. 36º. Não é objeto de contratação nem delegação aos colaboradores a gestão de processos em Segurança da Informação e em Tecnologia da Informação, conforme **I.N. nº 4, de 12 de novembro de 2010**.

Art. 37º. Quando o contrato tiver requisitos de segurança deve haver um parecer do CSIC, conforme **Art. 12 da I.N. nº 4, de 2010**.

> **Parágrafo único.** O conhecimento da minuta do contrato por interessados na contratação está condicionado à assinatura do termo de compromisso de manutenção de sigilo, sem prejuízo de aplicação dos demais controles estabelecidos no **Decreto 4.553, de 2002**.

Art. 38º. Os colaboradores que estabeleçam algum vínculo contratual com o LNCC devem ser obrigados em contrato a seguir esta política.

> **Parágrafo único.** Todo colaborador deve assinar o termo de confidencialidade, responsabilidade e de uso dos recursos computacionais.

Art. 39º. Os colaboradores são obrigados a fornecer serviços adequados, eficientes, seguros.

Parágrafo único. Nos casos de descumprimento, total ou parcial, das obrigações referidas neste artigo, serão os responsáveis compelidos a cumpri-las e a reparar os danos causados, conforme contratos estabelecidos.

Art. 40º. Todos os procedimentos de segurança propostos por colaboradores devem passar por homologação da CSIC.

Seção IV

Da Prestação de Serviços e Fornecimento

Art. 41º. Periodicamente deve ser feita uma verificação dos recursos disponibilizados aos colaboradores.

§1º. Os colaboradores são obrigados a repor qualquer recurso que tenha sido extraviado, adulterado ou comprometido no todo ou em parte.

§2º. Não havendo reposição em tempo hábil implica em alteração maliciosa de processo.

Art. 42º. Caso alguma informação sigilosa referente ao LNCC seja revelada por terceiros, os responsáveis e co-responsáveis pelo vazamento da informação responderão por seus atos na Justiça.

Parágrafo único. Para os colaboradores, todas as informações referentes ao LNCC são sigilosas, a menos que o LNCC esteja fazendo divulgação pública.

Art. 43º. Os colaboradores responderão pelos danos que seus agentes, nessa qualidade, causarem a terceiros, assegurado o direito de regresso contra o responsável nos casos de dolo ou culpa, conforme dispõe o **Art. 37, §6º da Constituição Federal**.

Art. 44º. Os colaboradores devem informar a seus funcionários que a violação de segredo da empresa constitui justa causa para rescisão do contrato de trabalho pelo empregador, conforme dispõe o **Art. 482, alínea g da CLT - Consolidação das Leis do Trabalho**.

Capítulo V

DA SEGURANÇA FÍSICA E DO AMBIENTE

Art. 45º. Devem ser utilizados perímetros de segurança para proteger as áreas que contenham informações e recursos de processamento da informação.

Art. 46º. Recomenda-se que áreas seguras sejam protegidas de forma que somente pessoas autorizadas tenham acesso.

Art. 47º. Recomenda-se que “pontos de acesso”, tais como áreas de entrega e de carregamento e outros pontos onde pessoas não autorizadas possam entrar nas instalações, devem ser controladas e, se possível isolados dos recursos de processamento.

Art. 48º. Devem ser tomadas medidas de segurança para equipamentos que operam fora do LNCC, levando em conta os diferentes riscos decorrentes do fato de se trabalhar fora das dependências da organização.

Art. 49º. Equipamentos, informações ou softwares não devem ser retirados do LNCC sem autorização prévia.

Art. 50º. O objetivo do controle é sistematizar a concessão de acesso, a fim de evitar a quebra de segurança da informação e comunicações, conforme **N.C. 07/IN01/DSIC/GSIPR, de 06 de maio de 2010**.

Art. 51º. O Centro de Processamento de Dados , o sistema de refrigeração e de geração de energia estão localizados em áreas de acesso restrito.

Art. 52º. Ativos sigilosos devem ser alocados em áreas de acesso restrito.

Art. 53º. Todo acesso e manutenção em áreas restritas deve ser autorizados pelos responsáveis.

Art. 54º. É proibido retirar da repartição pública, sem estar legalmente autorizado, qualquer mídia, documento, livro ou bem pertencente ao patrimônio público, conforme **a alínea l, do inciso XV, da Seção III do Decreto nº 1.171/94, de 22 de junho de 1994**.

Art. 55º. Recomenda-se, sempre que possível, a utilização de câmeras que captam o movimento; principalmente no Centro de Processamento de Dados; laboratórios; salas públicas e corredores.

Art. 56º. As salas são de acesso exclusivo de seus titulares; convidados de seus titulares; zeladores com horário agendado pela administração do campus; da equipe de segurança patrimonial com anotação em relatório; chefes de suas respectivas coordenações.

Parágrafo único. Recomenda-se que o titular da sala a tranque e desligue todos os equipamentos, que não estejam em uso, ao se ausentar.

Art. 57º. É proibido alterar o aspecto ou estrutura de edificação do LNCC sem autorização da autoridade competente ou em desacordo com a concedida.

Art. 58º. A mudança de qualquer característica de hardware deve ser comunicada ao setor de patrimônio.

Art. 59º. Deve-se utilizar uma ferramenta automatizada de inventário de software e hardware.

i. Recomenda-se que em todas máquinas do LNCC ou de projetos hospedados no LNCC, a CSR mantenha instalado e configurado um software de inventário de hardware e software.

Art. 60º. A mudança de localização dos bens deve ser informada ao setor de patrimônio.

Art. 61º. É proibido adulterar ou remarcar número de série ou qualquer sinal identificador do patrimônio do LNCC, de seu componente ou equipamento.

Art. 62º. Deve-se informar ao setor de patrimônio toda a passagem de responsabilidade sobre os bens.

Capítulo VI

DO GERENCIAMENTO DAS OPERAÇÕES E COMUNICAÇÕES

Seção I

Aspectos Gerais

Art. 63º. Os procedimentos de operação devem ser documentados, mantidos atualizados e disponíveis para todos os usuários autorizados.

Art. 64º. Modificações nos recursos de processamento da informação e sistemas devem ser controlados.

Art. 65º. A utilização dos recursos deve ser monitoradas e ajustadas, e as projeções devem ser feitas para necessidades de capacidade futuras.

Art. 66º. Devem ser estabelecidos critérios para aceitação de novos sistemas.

Art. 67º. Devem ser implementados controles de detecção, prevenção e recuperação para proteger contra códigos maliciosos, assim como procedimentos para a devida conscientização dos usuários.

Art. 68º. Cópias de segurança das informações e dos softwares devem ser realizados e testados regularmente, conforme a política de geração de cópias e segurança definidas.

Art. 69º. A rede deve ser gerenciada e monitorada de forma a protegê-la contra ameaças e manter a segurança de sistemas e aplicações que utilizam esta rede.

Art. 70º. Devem existir procedimentos para o gerenciamento de mídias removíveis.

Art. 71º. A integridade das informações disponibilizadas em sistemas publicamente acessíveis devem ser protegida, para prevenir modificações não autorizadas.

Art. 72º. Registros de auditoria contendo atividade dos usuários, exceções e outros eventos de segurança da informação devem ser produzidos e mantidos por um período de tempo acordado.

Art. 73º. Devem ser estabelecidos procedimentos para o monitoramento do uso dos recursos computacionais.

Art. 74º. As falhas e incidentes ocorridos devem ser registados, analisados e devem ser adotadas as ações apropriadas.

Art. 75º. O relógio de todos os sistemas de processamentos de informações relevantes devem ser sincronizados com uma fonte de tempo precisa e acordada.

Art. 76º. A CSR não realiza manutenção nem efetua configurações ou instalação de hardware ou software em equipamentos particulares. No entanto, as máquinas particulares conectadas a internet pelo LNCC se submetem automaticamente a esta política.

Seção II

Dos Recursos Criptográficos

Art. 77º. Recomenda-se que as áreas de dados dos dispositivos móveis do LNCC sejam criptografados.

Art. 78º. O credenciamento de estrangeiros para uso e pesquisa de recurso criptográfico deve ser submetido ao Gabinete de Segurança Institucional da Presidência da República por intermédio do Departamento de Segurança da Informação e Comunicações – DSIC, conforme **N.C. 09/IN01/DSIC/GSIPR, de 19 de novembro de 2010.**

Art. 79º. A CSR deve monitorar e auditar os recursos criptográficos pertencentes ao LNCC, conforme N.C. 09/IN01/DSIC/GSIPR, de 19 de novembro de 2010.

Parágrafo único. É proibido impedir ou dificultar, de qualquer forma, a realização do monitoramento e da auditoria.

Art. 80º. É vedado ao usuário de recurso criptográfico do LNCC utilizar recursos criptográficos em desacordo com a **N.C. 09/IN01/DSIC/GSIPR, de 19 de novembro de 2010.**, bem como com a legislação em vigor.

Art. 81º. Também é vedado ao usuário de recurso criptográfico do LNCC utilizar os recursos:

i. para fins diversos dos funcionais ou institucionais;

ii. para interceptar ou tentar interceptar transmissão de dados ou informações não destinados ao seu próprio acesso por quaisquer meios;

iii. para tentar ou efetuar a interferência em serviços de outros usuários ou o seu bloqueio por quaisquer meios;

iv. para violar ou tentar violar os recursos de segurança dos equipamentos que utilizem recursos criptográficos;

v. para cifração ou decifração de informações ilícitas, entre os quais, materiais obscenos, ofensivos, ilegais, não éticos, ameaças, difamação, injúria, racismo ou qualquer outro que venha a causar molestamento, tormento ou danos a terceiros;

vi. de forma inadequada, expondo-o a choques elétricos ou magnéticos, líquidos ou outros fatores que possam vir a causar-lhes danos, incluindo testes de invasão/intrusão/penetração, teste de quebra de senhas, teste de quebra de cifração, e teste de técnicas de invasão e defesa entre outros;

Seção III

Do Conteúdo das Informações

Art. 82º. Todos os usuários devem adotar as práticas de segurança corretas para manterem os meios de transmissão e armazenamento livres de Software Malicioso, seja vírus ou qualquer coisa que possa interferir no serviço ou prejudicar outros usuários.

Parágrafo único. Os usuários não devem propagar ativamente qualquer tipo de software malicioso.

Art. 83º. Todos os usuários devem manter os meios de comunicação isentos de conteúdo promocional e comercial indesejado.

Parágrafo único. É expressamente proibido o envio de mensagens em massa que possam caracterizar a prática conhecida como *spam*.

Art. 84º. Postagens que sirvam para encaminhar o tráfego para materiais com nudez, pornografia infantil, representações gráficas de atos sexuais ou conteúdo explicitamente sexual não são permitidas.

Parágrafo único. Caso seja detectado quaisquer dos ilícitos acima citados, será bloqueado o acesso em todos os computadores do LNCC, bem como encaminhada denúncia às autoridades competentes.

Art. 85º. Serão bloqueados os conteúdos de ódio, ameaças, assédio, intimidação ou contraditórios à Legislação.

Art. 86º. Quando a Comissão de Segurança for notificada de atividades ilegais, esta deverá tomar as providências necessárias em um dia útil:

i. As providências devem incluir uma denúncia às autoridades competentes;

ii. A CSR deve bloquear as contas e o acesso do usuário à rede e demais sistemas computacionais;

iii. Quando constatado o crime ocorrerá ao Diretor a solicitação de denuncia às autoridades competentes.

Art. 87º. A violação de direitos de propriedade intelectual, inclusive direitos autorais, resultará no bloqueio da conta e ao acesso aos recursos computacionais.

Art. 88º. A falsificação de identidade ou de qualquer outro documento constitui crime previsto no Código Penal.

Art. 89º. É proibida a publicação não autorizada de informações pessoais ou confidenciais de terceiros, como números de cartão de crédito, números de documentos ou quaisquer informações que não sejam de acesso público.

Art. 90º. Recomenda-se que os documentos de normatização e procedimentos sejam disponibilizados em um repositório público.

Art. 91º. Os usuários dos sistemas computacionais poderão sofrer auditoria nas informações armazenadas e transmitidas.

Art. 92º. Os telefones são de uso exclusivo para serviço.

§ 1º. As ligações particulares devem ser declaradas e quitadas.

§ 2º. Todas as ligações serão registradas**.**

§ 3º. A violação de ligação telefônica constitui infração ao disposto **no artigo 5º, XII, da Constituição Federal,** sujeitando o infrator às penalidades previstas no Código Penal.

Art. 93º. A CSR deve divulgar os alertas de segurança e vulnerabilidades.

Art. 94º. Conforme **o inciso VIII do Art. 2º da Lei nº 7.232, de 29 de outubro de 1984**, recomenda-se que a CSR estabeleça os mecanismos e instrumentos legais, e técnicos para a proteção do sigilo dos dados armazenados, processados e veiculados, do interesse da privacidade e de segurança das pessoas físicas e jurídicas, privadas e públicas.

Art. 95º. O pedido de patente originário do LNCC cujo objeto interesse à defesa nacional será processado em caráter sigiloso, com base em parecer conclusivo do MCTI, não estará sujeito às publicações previstas, conforme **o art. 75 do Código de Propriedade Industrial,** e **o § 2º do art. 1º do Decreto nº 2.553, de 16 de abril de 1998**.

Art. 96º. Em caso de manutenção de equipamentos, recomenda-se que as mídias de armazenamento permaneçam com seus respectivos titulares no LNCC.

Art. 97º. No caso de descarte ou substituição de equipamento as mídias de armazenamento devem ser excluídos de forma segura.

Capítulo VII

DO CONTROLE DE ACESSO

Seção I

Do Gerenciamento do Acesso do Usuário

Art. 98º. Deve haver um procedimento formal de registro e cancelamento de usuário para garantir e revogar acessos em todos os sistemas de informação.

Art. 99º. A concessão e uso de privilégios deve ser restritos e controlados.

Art. 100º. A concessão de senhas deve ser controlada por meio de um processo de gerenciamento formal.

Art. 101º. É proibida a autenticação e transmissão de senhas através de protocolos sem criptografia.

Art. 102º. Deve-se existir apenas um ponto de cadastro e remoção de pessoas autorizadas ao acesso físico e lógico das propriedades do LNCC.

Art. 103º. Os administradores de sistemas devem redobrar o cuidado para manter o sigilo de suas senhas.

Parágrafo único. É proibido o envio de senhas por e-mail.

Art. 104º. Todas as senhas devem ser bloqueadas sempre que seu titular for oficialmente desligado da instituição.

Art. 105º. São expressamente proibidas senhas padrão, estas devem ser substituídas.

Art. 106º. Somente a **CSR** pode:

i. autorizar que uma conta tenha permissão de administrador nos computadores situados no Centro de Processamento de Dados;

ii. autorizar que uma conta tenha permissão de administrador nas estações de trabalho;

iii. autorizar que uma conta tenha permissão de administrador dos dispositivos de rede.

Art. 107º. As senhas das contas administrativas dos computadores situados no Centro de Processamento de Dados são exclusivas da **CSR**.

Art. 108º. As senhas das contas administrativas das estações de trabalho são exclusivas da **CSR**.

Art. 109º. Parágrafo único. Mediante justificativa, o responsável pela **CSR** pode autorizar que o usuário de uma estação de trabalho possua privilégio de administração da mesma.

Art. 110º. As senhas de contas administrativas dos dispositivos de rede são exclusivas da **CSR**.

Art. 111º. Periodicamente todas as senhas são testadas para detectar senhas fracas.

Parágrafo único. O titular de uma senha fraca será notificado e deverá trocar imediatamente de senha.

Art. 112º. A conta deve ser automaticamente bloqueada após o número de tentativas de conexão ultrapassar a quantidade permitida.

Art. 113º. A CSR manterá registros sigilosos das autenticações por senha por pelo menos por 1 (um) ano.

Seção II

Da Responsabilidade do Usuário

Art. 114º. Os usuários dos sistemas computacionais do LNCC têm o dever de denunciar quando acreditarem que esta política está sendo violada.

Parágrafo único. Cabe ao CSIC averiguar se a política foi realmente violada, e quando detectada uma violação, a CSCI deve tomar as devidas medidas e propor as devidas sanções.

Art. 115º. Todos os usuários dos sistemas computacionais do LNCC se comprometem a:

i. não fornecer sua senha que é pessoal e intransferível;

ii. não responder a e-mails ou mensagens que venham a solicitar senhas ou dados sigilosos;

iii. não usar senhas fracas;

iv. trocar de senha com periodicidade máxima de um ano;

v. não se afastar dos objetivos declarados do projeto ao qual está vinculado ou utilizar o sistema para finalidades diferentes das declaradas na ocasião do cadastramento;

vi. respeitar as diretrizes de uso das redes às quais o LNCC está conectado;

vii. não se afastar do computador deixando sessões abertas sem bloqueio;

Art. 116º. A senha representa a autenticação de cada usuário sendo de seu exclusivo controle, uso e conhecimento, devendo ser gerada pelo próprio usuário.

Art. 117º. É dever de todo usuário notificar através de e-mail para a **Coordenação de Sistemas e Rede** (**CSR**) as contas que não estejam sendo usadas para que sejam excluídas.

Art. 118º. Os usuários são responsáveis pelos softwares por eles instalados.

Art. 119º. Todo software instalado que não tenha sido de inciativa da CSR deve ser de responsabilidade do usuário do equipamento.

Art. 120º. Os usuários devem ser orientados a seguir as boas práticas de segurança da informação.

Art. 121º. Recomenda-se que seja adotada a política de mesa limpa de papéis e mídias de armazenamento removíveis.

§1. Recomenda-se aos usuários que mantenham devidamente protegidos todo e qualquer tipo de documento ou de informação.

§2. Todos os usuários não devem manter sobre suas mesas ou estações de trabalho, documentos e informações relacionadas as atividades do LNCC.

Art. 122º. Recomenda-se que seja adotada a política de tela limpa para os recursos de processamento da informação.

§1. Recomenda-se que todos os computadores, utilizados nas dependências, dos LNCC adotem um sistema de proteção que seja acionado quando as máquinas ficarem inativas por um determinado período de tempo.

§2. Recomenda-se que o sistema de proteção, solicite algum tipo de autenticação do usuário antes de liberar o acesso ao sistema.

Seção III

Controle de Acesso à Rede

Art. 123º. Os usuários devem utilizar apenas os serviços e os recursos de rede a que foram autorizados.

Art. 124º. Recomenda-se que grupos de serviços de informação, usuários e sistemas de informação devem ser segregados em redes distintas.

Art. 125º. Para todo projeto classificado como sigiloso, o tratamento e o controle de acesso será conforme o **Decreto nº 4.553, de 2002**.

Art. 126º. A CSR pode bloquear temporariamente o acesso, parcial ou completo, à um serviço para garantir a disponibilidade de serviços prioritários.

Art. 127º. No intuito de garantir a continuidade do serviço, a CSR pode bloquear ou limitar, temporariamente, a conectividade de usuários ou de serviços.

Art. 1287º. É proibido prover acesso remoto não autorizado.

Art. 129º. É proibido manter-se conectado à rede do LNCC e ao mesmo tempo utilizar outro provedor de acesso à Internet.

Art. 130º. Todo serviço de rede hospedado em máquinas conectadas à rede do LNCC, por padrão, não deve ser acessado por máquinas externas a rede do LNCC.

Art. 131º. As solicitações para liberação de serviços devem ser encaminhada à CSR por um servidor público federal lotado no LNCC. Toda solicitação deverá ser encaminhada através de formulário próprio.

Art. 132º. A CSR efetuará registros, desde que sigilosos, de todas as conexões à internet.

Parágrafo único. O dispositivo de segurança pode bloquear automaticamente conteúdo incompatível com esta política.

Art. 133º. A Rede de dados deverá ser segmentada.

i. Caso algum projeto de pesquisa necessite, recomenda-se que seja criada uma sub-rede exclusiva para o mesmo;

ii. Recomenda-se que cada segmento tenha um conjunto de endereços IPs próprio;

iii. Recomenda-se que o fluxo de dados entre os segmentos seja isolado e controlado.

Art. 134º. Deve-se controlar a liberação de acesso aos serviços hospedados mas máquinas conectadas à rede.

i. Recomenda-se que o controle e a liberação de acesso sejam baseados nos protocolos usados.

ii. Quando ocorrer uma solicitação de liberação de serviço hospedado na rede do LNCC para acesso externo à rede da instituição, a comissão de segurança deve explicitamente autorizar tal liberação.

Art. 135º. Para que a segurança na rede interna seja mantida a CSR deve manter registro e supervisionar os serviços providos pela rede.

Art. 136º. Deve-se configurar em toda máquina ou dispositivo que prove algum serviço de rede um controle de acesso baseado em ACLs ou algo similar.

i. Recomenda-se que a ferramenta de controle de acesso mantenha um registro das tentativas de conexão.

Art. 137º. Todas as máquinas administradas pela CSR devem ter um pacote de segurança devidamente instalado e configurado.

Art. 138º. Recomenda-se que todas as máquinas conectadas à rede do LNCC devem ter um pacote de segurança devidamente instalado e configurado.

Art. 139º. Toda correspondência eletrônica direcionada ao LNCC deve ser verificada com ferramentas para remoção de programas maliciosos.

Art. 140º. Os computadores e dispositivos do Centro de Processamento de Dados devem encaminhar os registros de eventos críticos ao sistema de log.

Art. 141º. Recomenda-se que as impressoras sejam conectadas à um servidor de impressão que contabilize o número de páginas por usuários.

Art. 142º . A CSR deve controlar a conexão física de equipamentos à rede interna do LNCC.

i. Equipamentos não devem ser conectados a rede cabeada do LNCC sem prévia autorização da CSR;

ii. Todos dispositivos devem ser cadastrados pela CSR antes de serem conectados a rede do LNCC;

iii. Dispositivos móveis, pessoais, não devem ser conectados a rede cabeada do LNCC;

iv. Somente os dispositivos móveis patrimoniados e com prévia autorização da CSR poderão ser conectados a rede cabeada do LNCC.

Art. 143º. É permitido o uso de programas de comunicação para vídeo conferência, VoIP, mensagens instantâneas e redes sociais, desde que estejam relacionadas as atividades do LNCC.

Art. 144º. Recomenda-se que o e-mail institucional não seja utilizado para fins pessoais.

Art. 145º. Por padrão, não é permitido o uso de aplicações baseadas em protocolos P2P na rede do LNCC.

i. Quando a utilização destas aplicações forem necessárias para a realização de atividades relacionadas ao LNCC, deve-se encaminhar ao CSIC uma solicitação acompanhada de justificativa.

ii. Somente após autorizado pelo CSIC é que o usuário poderá fazer uso deste tipo de aplicação.

Capítulo VIII

DA AQUISIÇÃO, DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMAS

Art. 146º. Devem ser especificados os requisitos de segurança para controles de segurança para novos sistemas de informação ou melhorias em sistemas existentes.

Art. 147º. Procedimentos para controlar a instalação de softwares em sistemas operacionais devem ser implementados.

Art. 148º. Implementação de mudanças deve ser controlada utilizando procedimentos formais.

Art. 149º. Recomenda-se que as novas bases de dados devem ter possibilidade de integração com as bases de dados existentes.

Art. 150º. Recomenda-se que os novos sistemas devem manter a interoperabilidade com os sistemas computacionais existentes.

Art. 151º. Recomenda-se que o programa não deve conter código oculto que possa causar qualquer alteração de comportamento.

Art. 152º. Recomenda-se que os programas devem ser concebidos para:

i. validar os dados de entrada e impedir a injeção de código;

ii. proibir a construção dinâmica de requisições (*queries*) usando dados fornecidos pelo usuário;

iii. auditar e registrar procedimentos críticos;

iv. ter autenticidade de sua origem através de assinatura digital;

v. ter mecanismos de não repúdio;

vi. que os identificadores de sessão (*cookies*) sejam validados, cifrados e imprevisíveis;

vii. ter o conteúdo do código fonte livre de senhas ou outros segredos que possam ser lidos diretamente ou por engenharia reversa;

viii. impedir o armazenamento de senhas ou segredos em memória temporária;

ix. impedir ataques de disfarce;

x. impedir ataques de monitoramento das mensagens;

xi. tratar ataques que sobrecarregam o sistema;

xii. tratar exceções e erros de forma explícita e adequada;

xiii. impedir o excesso de informações nos erros e revelar apenas o necessário ao usuário;

xiv. usar funcionalidades e algoritmos comprovados sem reinventar padrões estabelecidos;

xv. usar algoritmos criptográficos reconhecidamente seguros;

xvi. armazenar, se necessário, as chaves criptográficas cifradas e *hash* de senhas;

xvii. não usar API banida, funções e rotinas inseguras, desatualizadas ou não utilizadas no código;

xviii. ter requisitos mínimos de privilégios ao ser executado.

Art. 153º. Recomenda-se desenvolver e usar, preferencialmente, programas com código aberto, acessíveis ininterruptamente por meio da rede mundial de computadores, priorizando-se a sua padronização, conforme **Art. 14. Lei Nº 11.419, de 19 de dezembro de 2006**.

Art. 154º. Cabe à CSR fornecer as orientações necessárias ao fiel cumprimento das normas vigentes, que estabelece regras e diretrizes para os sítios na internet da Administração Pública Federal.

Capítulo IX

DA GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

Art. 155º. Deve-se reduzir os riscos resultantes da exploração de vulnerabilidades técnicas conhecidas.

Art. 156º. Os eventos de segurança devem ser relatados através dos canais apropriados o mais rapidamente possível.

Art. 157º. Todos os usuários devem ser instruídos a registar e notificar, através dos canais apropriados, qualquer observação ou suspeita de fragilidade em sistemas e serviços.

Art. 158º. Deve-se assegurar um enfoque consistente e efetivo à gestão de incidentes de segurança da informação.

Art. 159º. Com fundamento no **Decreto 4.553, de 27 de dezembro de 2002**, e no Código de Ética do Servidor Público Civil do Poder Executivo Federal, aprovado pelo **Decreto 1.171, de 22 de junho de 1994**, a comunicação ao público, por qualquer meio de comunicação, sobre eventual ocorrência de incidentes, será de exclusiva competência do Diretor do LNCC ou de seu delegatário para esse fim.

Art. 160º. A equipe responsável pela Resposta a Tratamento de Incidentes de Segurança fica responsável por localizar a origem dos incidentes, remediar e aplicar esta política, conforme **N.C. 05/IN01/DSIC/GSIPR, de 14 de agosto de 2009**.

Parágrafo único. A equipe responsável pela Resposta a Tratamento de Incidentes de Segurança deve comunicar e fornecer estatística sobre os incidentes ao CSIC.

Art. 161º. A equipe responsável pela Resposta a Tratamento de Incidentes de Segurança deve cumprir a **N.C. 08/IN01/DSIC/GSIPR, de 19 de agosto de 2010,** que regulamenta sua atividade.

Art. 162º. A equipe da CSR responsável pelos equipamentos da área de armazenamento pode usar programas para detectar irregularidades, desde que não infrinja o Art. 3 da **N.C. 09/IN01/DSIC/GSIPR, de 19 de novembro de 2010**.

i. É proibido o armazenamento de conteúdos ilegais, particulares e que não estejam relacionados às atividades do LNCC.

ii. A CSR deve solicitar esclarecimentos sobre o conteúdo citado no item anterior e eventualmente promover sua remoção.

iii. Caso alguma irregularidade seja detectada deve-se imediatamente comunicar à Comissão de Segurança para averiguar se a política foi realmente violada e tomar as devidas medidas e propor as devidas sanções.

Art. 163º. Também são consideradas confidenciais as senhas, códigos de acesso, número de séries e arquivos de licenças.

Capítulo X

DA GESTÃO DA CONTINUIDADE DO NEGÓCIO

Art. 164º. Recomenda-se implementar controles para impedir a interrupção das atividades do negócio e proteger os processos críticos contra efeitos de falhas, assim como assegurar, quando for o caso, sua retomada em tempo hábil.

Art. 165º. Deve-se fazer por escrito uma detalhada análise de impacto nas mudanças e manutenções.

Art. 166º. O objetivo dos planos de contingência é proteger o LNCC acima de tudo. Os ativos devem ser protegidos na seguinte ordem de prioridade:

i. pessoas;

ii. informações armazenadas em mídia;

iii. informações armazenadas em papel;

iv. estrutura predial;

v. equipamentos eletrônicos;

vi. veículos;

vii. demais ativos.

Art. 167º. Deve haver planos de contingência, cujo alcance será definido pela Comissão de Segurança.

Parágrafo único. Os planos de contingência devem seguir a Gestão de Riscos de Segurança da Informação e Comunicações apresentada na **N.C. 04/IN01/DSIC/GSIPR, de 14 de agosto de 2009**.

Art. 168º. O Plano de Gestão de Continuidade de Negócios deve buscar redundâncias e seguir a **N.C. 06/IN01/DSIC/GSIPR, de 11 de novembro de 2009**.

Capítulo XI

DA CONFORMIDADE COM REQUISITOS LEGAIS

Seção I

Da Auditoria

Art. 169º. A auditoria intrusiva é confidencial e somente pode ser feita com a autorização do diretor do LNCC e na presença de no mínimo três servidores sendo:

i. o presidente da Comissão de Segurança;

ii. um membro da Comissão de Segurança;

iii. um membro do Grupo de resposta à incidente de segurança.

Art. 170º. O coordenador da CSR pode autorizar a realização a qualquer momento, sem aviso prévio, de auditoria não-intrusiva e remota de sistemas (*scanner*) para descoberta de vulnerabilidades externas em todas as máquinas que ela provê conexão.

Parágrafo único. Recomenda-se que os resultados sejam divulgados ao CSIC.

Art. 171º A equipe de resposta a incidente deve ser nomeada por ato do Diretor.

Parágrafo único. A equipe deve ser formada apenas por servidores públicos.

Art. 172º A Equipe de resposta à incidentes deve acompanhar os alertas de vulnerabilidades e ameaças e desenvolver normatização de reforço de segurança.

Art. 173º São tarefas semanais do Grupo de resposta à incidente de segurança:

i. Analisar os alertas de integridade de dados;

ii. Analisar os registros de sistema;

iii. Analisar o relatório de varredura de vulnerabilidades;

iv. Corrigir as vulnerabilidades constatadas;

v. Gerar estatísticas e relatórios sobre os incidentes de segurança.

Art. 174º São tarefas diárias do Grupo de resposta à incidente de segurança:

i. Acompanhamento de versões e correções (*patches*);

ii. Análise dos alertas do Sistema de Detecção de Intruso.

Art. 175º Sempre que ocorrer um incidente de segurança, o Grupo de resposta à incidente de segurança deve notificar ao responsável pelo ativo sobre o ocorrido.

Parágrafo único. As tentativas de intrusão provenientes da internet também são comunicadas a centros de atendimento a incidente de segurança.

Art. 176º Todas as atividades do Grupo de resposta à incidente de segurança devem gerar relatórios à Comissão de Segurança.

PORTARIA N.º. 115 DE 28 DE SETEMBRO DE 2012

ACOMPANHAMENTO DE CONTRATO

O DIRETOR DO LABORATÓRIO NACIONAL DE COMPUTAÇÃO CIENTÍFICA DO MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÃO, no uso da competência que lhe foi delegada pela da Portaria n.º. 407, de 29 de junho de 2006, do Ministro de Estado da Ciência e Tecnologia, publicada no Diário Oficial da União de 30/06/2006, e tendo em vista o disposto no artigo 67 da Lei n.º 8.666, de 21/jun/1993,

RESOLVE

I - Designar o servidor **AMARILDO LOPES DE OLIVEIRA,** CPF/MF nº 785.[redacted]-30, SIAPE nº 1709670, Assistente em Ciência e Tecnologia, lotado na Coordenação de Administração, para acompanhar e fiscalizar a execução do Contrato nº 01.012.00/2012, referente a contratação de serviços de vigilância e segurança patrimonial armada celebrado com a **TRANSEGUR VIGILÂNCIA E SEGURANÇA LTDA**, e nos seus impedimentos legais seu substituto **PAULO SÉRGIO ALBERTASSI**, CPF/MF nº 440.[redacted]-15, matrícula no SIAPE nº 673131, Assistente em Ciência e Tecnologia, lotado na Coordenação de Administração.

II – O Fiscal terá como atribuições aquelas estabelecidas no artigo 67 da Lei n.º 8.666, de 21/jun/1993.

III – Esta Portaria cancela a Portaria nº 091 de 30 de setembro de 2011.

IV - Esta Portaria entra em vigor na data de sua publicação no Boletim Interno do LNCC.

PORTARIA N.º. 116 DE 28 DE SETEMBRO DE 2012

ACOMPANHAMENTO DE CONTRATO

O DIRETOR DO LABORATÓRIO NACIONAL DE COMPUTAÇÃO CIENTÍFICA DO MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÃO, no uso da competência que lhe foi delegada pela da Portaria n.º. 407, de 29 de junho de 2006, do Ministro de Estado da Ciência e Tecnologia, publicada no Diário Oficial da União de 30/06/2006, e tendo em vista o disposto no artigo 67 da Lei n.º 8.666, de 21/jun/1993,

RESOLVE

I - Designar o servidor **PAULO CÉSAR FARIA,** CPF/MF nº 657.[redacted]-91, SIAPE nº 673164, Analista em Ciência e Tecnologia, lotado na Diretoria, para acompanhar e fiscalizar a execução da Ordem de Serviço nº 004, objeto do processo nº 132/2011, referente a prestação de serviços de Hotelaria celebrado com a empresa **MIKONOS EVENTOS E SERVIÇOS LTDA**, e nos seus impedimentos legais seu

substituto **ANTONIO CARLOS FEITOSA COSTA**, CPF/MF nº 056.[redacted]-30, matrícula no SIAPE nº 1520690, Técnico, lotado no Serviço de Redes da Coordenação de Sistemas e Redes.

II – O Fiscal terá como atribuições aquelas estabelecidas no artigo 67 da Lei n.º 8.666, de 21/jun/1993.

III - Esta Portaria entra em vigor na data de sua publicação no Boletim Interno do LNCC.

PORTARIA N.º. 117 DE 28 DE SETEMBRO DE 2012

ACOMPANHAMENTO DE CONTRATO

O DIRETOR DO LABORATÓRIO NACIONAL DE COMPUTAÇÃO CIENTÍFICA DO MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÃO, no uso da competência que lhe foi delegada pela da Portaria n.º. 407, de 29 de junho de 2006, do Ministro de Estado da Ciência e Tecnologia, publicada no Diário Oficial da União de 30/06/2006, e tendo em vista o disposto no artigo 67 da Lei n.º 8.666, de 21/jun/1993,

RESOLVE

I - Designar o servidor **PAULO CÉSAR FARIA,** CPF/MF nº 657.[redacted]-91, SIAPE nº 673164, Analista em Ciência e Tecnologia, lotado na Diretoria, para acompanhar e fiscalizar a execução da Ordem de Serviço nº 003, objeto do processo nº 132/2011, referente a prestação de serviços de Hotelaria celebrado com a empresa **BARRA LIVRE EVENTOS E PROMOÇÕES LTDA**, e nos seus impedimentos legais seu substituto **ANTONIO CARLOS FEITOSA COSTA**, CPF/MF nº 056.[redacted]-30, matrícula no SIAPE nº 1520690, Técnico, lotado no Serviço de Redes da Coordenação de Sistemas e Redes.

II – O Fiscal terá como atribuições aquelas estabelecidas no artigo 67 da Lei n.º 8.666, de 21/jun/1993.

III - Esta Portaria entra em vigor na data de sua publicação no Boletim Interno do LNCC.

PEDRO LEITE DA SILVA DIAS

ATOS DO SERVIÇO DE RECURSOS HUMANOS

RELAÇÃO PESSOAL AFASTADO ATIVIDADES – SETEMBRO 2012

1. À disposição de outros órgãos – art. 93

1.1. Miriam Barbuda Fernandes Chaves – Pesquisador Adjunto
Casa Civil de 14/10/2003 a 17/01/2011
Ministério do Planejamento, Orçamento e Gestão a partir de 18/01/2011

2. Licença sem vencimentos para trato de interesses particulares – art. 91

2.1. Fernanda Maria Pereira Raupp – Tecnologista Sênior
De 01/10/2007 a 30/09/2013

2.2. Rizza Castelo Branco – Analista em C&T
De 15/09/2010 a 14/09/2013

3. Afastamento para estudo ou missão no exterior (c/remuneração) Pesquisador – art. 95

3.1. Fábio Borges de Oliveira – Tecnologista Pleno
De 01/08/2011 a 01/08/2014

3.2. Renato Portugal – Pesquisador Associado
De 02/09/2012 a 09/09/2012

3.3. Paulo Cabral Filho - Tecnologista Sênior
De 08/09/2012 a 15/09/2012

3.4. Eduardo Lúcio Mendes Garcia – tecnologista Sênior
De 22/09/2012 a 01/11/2012

3.5. Luiz Gonzaga Paula de Almeida – Tecnologista Pleno 3
De 30/09/2012 a 07/10/2012

3.6. Marisa Fabiana Nicolás – Pesquisadora Associada
De 17/09/2012 a 23/09/2012

4. Licença com Remuneração para tratamento da saúde (servidor) – arts 202 a 206

4.1 Maria Cristina Albuquerque Almeida – Tecnologista Sênior
De 28/07/2012 a 25/10/2012

RELAÇÃO DOS SERVIDORES EM FÉRIAS NO MÊS DE AGOSTO 2012

MAT. SIAPE	NOME	EXERCÍCIO	PARCELA	ÍNICIO	TÉRMINO	N° DIAS DIREITO
673143	JOÃO NISAN CORREIA GUERREIRO	2012	3º	01/10/12	09/10/12	09
673143	JOÃO NISAN CORREIA GUERREIRO	2012	4º	15/10/12	26/10/12	12
1700403	MÁRCIO RENTES BORGES	2012	ÚNICA	01/10/12	30/10/12	30
664037	LEON ROQUE SINAY	2012	2 º	16/10/12	30/10/12	15
673131	PAULO SÉRGIO ALBERTASSI	2012	2º	15/10/12	03/11/12	20
1804260	SILVIA SILVEIRA SOARES	2012	1º	01/10/12	10/10/12	10
6673167	NORMA FERREIRA RUSSO ROMANO	2012	2º	09/10/12	18/10/12	10

CANCELAMENTO FÉRIAS

MAT. SIAPE	NOME	EXERCÍCIO	PARCELA	ÍNICIO	TÉRMINO	N° DIAS DIREITO
1467857	ANTÔNIO ANDRÉ NOVOTNY	2012	2º	10/09/12	29/09/12	20

REPROGRAMAÇÃO FÉRIAS

MAT. SIAPE	NOME	EXERCÍCIO	PARCELA	ÍNICIO	TÉRMINO	N° DIAS DIREITO
1467857	ANTÔNIO ANDRÉ NOVOTNY	2012	2º	18/02/13	09/03/13	20

DIÁRIAS SERVIDORES/COLABORADORES

Beneficiário	Natureza	Motivo do Deslocamento	Itinerário
ANTONIO TADEU AZEVEDO GOMES	SERVIDOR	Atender convite do Secretário de Política de Informática do MCTI para participar da reunião sobre o Tema Computação em Nuvem dia 04/09/2012 as 15:00hs no MCTI	Rio de Janeiro/ Brasília / Rio de Janeiro.
JACK BACZYNSKI	SERVIDOR	Visita técnica a São Carlos para desenvolvimento de trabalhos de pesquisa em conjunto com o Prof. Dorival Leão.	Rio de Janeiro/São Carlos (SP)/Rio de Janeiro
FLAVIO BARBOSA TOLEDO	SERVIDOR	Participar do XXII Seminário Nacional da ANPROTEC no Parque Tecnológico de Itaipu em Foz do Iguaçu, PR, de 16 a 21 de setembro de 2012.	Rio de Janeiro/ Foz do Iguaçu (PR)/ Rio de Janeiro
CARLA OSTHOFF FERREIRA DE BARROS	SERVIDOR	Participação no "XVII Congresso Brasileiro de Meteorologia - CBMet", que será realizado na cidade de Gramado RS, de 27 a 29 de setembro.	Rio de Janeiro/ Porto Alegre (RS)/ Gramado (RS)/ Porto Alegre (RS)/ Rio de Janeiro
JAIRO ROCHA DE FARIA	SERVIDOR	Participar de atividades de pesquisa e de banca de seminário obrigatório no LNCC.	João Pessoa (PB)/Rio de Janeiro/ Petrópolis/ Rio de Janeiro
MAICON RIBEIRO CORREA	COLABORADOR EVENTUAL	Participar de atividades de pesquisa e de banca de mestrado no LNCC.	Campinas (SP)/ Petrópolis (RJ) Campinas (SP)
HÉLIO PEDRO AMARAL SOUTO	COLABORADOR EVENTUAL	Participar de banca de mestrado no LNCC.	Nova Friburgo (RJ)/ Petrópolis (RJ)/ Nova Friburgo (RJ)
ESTEVÃO ROSALINO JUNIOR	COLABORADOR EVENTUAL	Participar de atividades de pesquisa no ICMC da USP.	Rio de Janeiro/ Campinas (SP)/ Rio de Janeiro.
ANTONIO CARLOS PAVÃO	COLABORADOR EVENTUAL	Apresentar a palestra Aprendendo Sobre o Cérebro com os Pássaros durante o Ciclo Fique por Dentro	Rio de Janeiro/Petrópolis/Rio de Janeiro
KARINA ACOSTA BARBOSA	COLABORADOR EVENTUAL	A Sr.ª Karina vira em visita técnica ao LNCC para desenvolver trabalhos de pesquisa cientifica em colaboração com o Prof. Carlos Emanuel de Souza.	Porto Alegre (RS)/Rio de Janeiro/Petrópolis/Rio de Janeiro/ Porto Alegre (RS)

JUAN DEL CARMEN GRADOS VASQUEZ	COLABORADOR EVENTUAL	Apresentar trabalho no CNMAC 2012.	Rio de Janeiro/ São Paulo (SP)/ Águas de Lindóia (SP)/ São Paulo (SP) /Rio de Janeiro
ALAN ALVES SANTANA AMAD	COLABORADOR EVENTUAL	Apresentar trabalho no CNMAC2012.	Rio de Janeiro/ São Paulo (SP)/ Águas de Lindóia (SP)/ São Paulo (SP) /Rio de Janeiro)

BOLETIM DE SERVIÇO N.º 010/2012 **28/09/2012**