LNCC
www.lncc.br
Laboratório Nacional de Computação Científica

Av. Getúlio Vargas 333, Quitandinha, Petrópolis, RJ . CEP. 25651-075



# Boletim de Serviço nº 007/2019
# Julho/2019

# BOLETIM DE SERVIÇO

**MINISTRO DE ESTADO DA CIÊNCIA, TECNOLOGIA, INOVAÇÕES E COMUNICAÇÕES**
Marcos Pontes

**Diretor LNCC:**
Augusto Cesar Gadelha Vieira

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 Gestão e Desenvolvimento de Pessoas**

**Coordenação de Gestão e Administração – SEGEP/COGEA/LNCC**

# BOLETIM DE SERVIÇO

## SUMÁRIO

**BOLETIM DE SERVIÇO N.º 007/2019 31/07/2019**

# ATOS DO DIRETOR

## PORTARIA Nº 57/2019/SEI-LNCC de 06 de Junho de 2019

**SUBSTITUTO COPGA**

**O DIRETOR DO LABORATÓRIO NACIONAL DE COMPUTAÇÃO CIENTÍFICA DO MINISTÉRIO DA CIÊNCIA, TECNOLOGIA, INOVAÇÕES E COMUNICAÇÕES**, 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**

**Art. 1º** - Designar o servidor **LUIZ MANOEL ROCHA GADELHA JUNIOR** , CPF n.º 358.454.812-87, matricula SIAPE n.º 1467870, para substituir nos impedimentos ou afastamentos regulares, **ARTUR ZIVIANI**, Coordenador de Pós Graduação e Aperfeiçoamento - COPGA, código FCPE 101.3, do Laboratório Nacional de Computação Científica deste Ministério.

**Art. 2º** - Esta Portaria cancela a Portaria nº 024 de 23/02/2017.

**AUGUSTO CÉSAR GADELHA VIEIRA**

***Publicado no DOU de 21/06/2019***

## PORTARIA Nº 58/2019/SEI-LNCC de 06 de Junho de 2019

**SUBSTITUTO DA COMOD**

**O DIRETOR DO LABORATÓRIO NACIONAL DE COMPUTAÇÃO CIENTÍFICA DO MINISTÉRIO DA CIÊNCIA, TECNOLOGIA, INOVAÇÕES E COMUNICAÇÕES**, 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**

**Art. 1.º -** Designar o servidor **Laurent Emmanuel Dardenne,** CPF/MF Nº 498.094.311-04, matrícula SIAPE n.º 1356488, para substituir nos impedimentos ou afastamentos regulares, **Márcio Arab Murad**, Coordenador de Modelagem Computacional - COMOD, código FCPE 101.3, do Laboratório Nacional de Computação Científica deste Ministério.

**Art. 2.º -** Esta Portaria cancela a Portaria n.º 074/2016 de 16 de dezembro de 2016.

**AUGUSTO CESAR GADELHA VIEIRA**

***Publicado no DOU de 21/06/2019***

**PORTARIA Nº 38/2019/SEI-LNCC DE 18 DE MARÇO DE 2019**

**COMISSÃO DE EXAME DE QUALIFICAÇÃO**

**O DIRETOR DO LABORATÓRIO NACIONAL DE COMPUTAÇÃO CIENTÍFICA DO MINISTÉRIO DA CIÊNCIA, TECNOLOGIA, INOVAÇÕES E COMUNICAÇÕES**, 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:

**Art. 1º -** Constituir a Comissão do Exame de Qualificação, conforme previsto no Artigo 41 do Regimento Interno aprovado pela Portaria n.º 5.158 de 14 de novembro de 2016, publicada no DOU de 16/11/2016, para orientação e assessoramento ao Diretor, quando necessário.

**Art. 2º -** A Comissão será composta por 05 (cinco) membros, conforme abaixo:

- João Nisan Correia Guerreiro
- Renato Portugal
- Jack Baczynski
- Kary Ann del Carmen Ocaña Gautherot
- Pablo Javier Blanco

**Art. 3º -** Esta Portaria cancela a Portaria nº 075 de 16/11/2017.

**Art. 4º -** Esta Portaria entra em vigor na data de sua publicação no Boletim de Serviço do LNCC.

**AUGUSTO CESAR GADELHA VIEIRA**

**PORTARIA Nº 60/2019/SEI-LNCC de 06 de Junho de 2019**

**COMISSÃO DE BIBLIOTECA**

O **DIRETOR DO LABORATÓRIO NACIONAL DE COMPUTAÇÃO CIENTÍFICA – LNCC**, Unidade de Pesquisa do Ministério da Ciência, Tecnologia, Inovações e Comunicações, no uso da competência que lhe foi delegada pela Portaria MCT nº 407, de 28/jun/2006, e tendo em vista o disposto no artigo 41 do Regimento Interno deste Laboratório, aprovado pela Portaria MCTIC nº 5.158 de 14/11/2016,

**RESOLVE**

**Art. 1º** - Constituir a Comissão de Biblioteca para orientação e assessoramento ao Diretor.

**Art. 2º** - Para o cumprimento de sua finalidade, no respectivo campo de atuação, cabe à Comissão de Biblioteca**,** dentre outras, as seguintes atividades:

- elaborar a política de prestação de serviços;
- regulamentar a sua utilização;

- selecionar a aquisição de livros e periódicos no âmbito do LNCC;
- propor alterações ou atualizações dos serviços de informatização;
- viabilizar recursos adicionais para a Biblioteca.

**Art. 3º** - A Comissão será composta pelos membros abaixo:

- Antonio André Novotny
- Fábio Borges de Oliveira;
- Marcelo Trindade dos Santos;
- Paulo Antonio Andrade Esquef;
- Paulo Cesar Marques Vieira;
- Sandra Mara Cardoso Malta;
- Genilda Maria Machado Roli;
- Ligia de Oliveira Morais Machado,

**Art. 4º** - A Comissão será presidida pelo servidor Antonio André Novotny.

**Art. 5º** - As reuniões da Comissão serão realizadas sempre que convocadas pelo seu Presidente ou por pelo menos 2/3 (dois terços) de seus membros.

**Art. 6º** - Esta Portaria entra em vigor na data de sua publicação no Boletim Serviço do LNCC.

**AUGUSTO CESAR GADELHA VIEIRA**

**PORTARIA Nº 68/2019/SEI-LNCC de 01 de Julho de 2019**

**ACOMPANHAMENTO E FISCALIZAÇÃO**

**O DIRETOR DO LABORATÓRIO NACIONAL DE COMPUTAÇÃO CIENTÍFICA DO MINISTÉRIO DA CIÊNCIA, TECNOLOGIA, INOVAÇÕES E COMUNICAÇÕES**, 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, e tendo em vista o disposto no artigo 67 da Lei n.º 8.666, de 21/jun/1993, resolve:

**Art. 1º** - Instituir a Comissão de Acompanhamento e Fiscalização do Processo nº 01209.000070/2018-21, firmado com a empresa **KANTRO EMPREENDIMENTOS APOIO E SERVIÇOS LTDA**, Termo de Contrato nº 003/2019, referente contratação de pessoa jurídica do ramo pertinente para a prestação de serviços de limpeza, conservação e jardinagem para atender as necessidades do Laboratório Nacional de Computação Científica - LNCC.

**I - GESTOR DO CONTRATO**

a) Titular: **Amarildo Lopes de Oliveira**
CPF: 785.757.707-30
Matrícula SIAPE: 1709670
Lotação: NUCAM/COGEA

b) Substituto: **Anmily Paula dos Santos Martins**
CPF: 944.044.707-97
Matrícula SIAPE: 686227
Lotação: COGEA

**II - MEMBRO ADMINISTRATIVO**

a) Titular: **Márcia Aparecida Almeida Pereira**
CPF: 080.940.367-61
Matrícula SIAPE: 2711154
Lotação: SEGOF/COGEA

b) Suplente: **Barbara Paulo Cordeiro Elustondo**
CPF: 433.710.517-49
Matrícula SIAPE: 0673121
Lotação: SEGEP/COGEA

**Art. 2º -** O Gestor do Contrato deverá observar fielmente suas atribuições previstas no artigo 67 da Lei n.º 8.666, de 21/jun/1993.

**Art. 3º -** Esta Portaria entra em vigor na data de sua publicação no Boletim de Serviço do LNCC.

**AUGUSTO CESAR GADELHA VIEIRA**

**PORTARIA Nº 69/2019/SEI-LNCC de 04 de JULHO de 2019**

**SUBSTITUTO SEDOC**

**O DIRETOR DO LABORATÓRIO NACIONAL DE COMPUTAÇÃO CIENTÍFICA DO MINISTÉRIO DA CIÊNCIA, TECNOLOGIA, INOVAÇÕES E COMUNICAÇÕES**, 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**

**Art. 1º** - Designar a servidora **LÍGIA DE OLIVEIRA MORAIS MACHADO** , CPF n.º 073.255.187-06, matricula SIAPE n.º 17051959, para substituir nos impedimentos ou afastamentos regulares, **GENILDA MARIA MACHADO ROLI**, Chefe do Serviço de Documentação e Biblioteca - SEDOC, código FCPE 101.1, do Laboratório Nacional de Computação Científica deste Ministério.

**Art. 2º** - Esta Portaria cancela a Portaria nº 068 de 15/12/2016.

**AUGUSTO CESAR GADELHA VIEIRA**

***Publicada no DOU de 09/07/2019***

**BOLETIM DE SERVIÇO N.º 007/2019 31/07/2019**

**PORTARIA Nº 70/2019/SEI-LNCC de 04 de JULHO de 2019**

**ACOMPANHAMENTO E FISCALIZAÇÃO**

**O DIRETOR DO LABORATÓRIO NACIONAL DE COMPUTAÇÃO CIENTÍFICA DO MINISTÉRIO DA CIÊNCIA, TECNOLOGIA, INOVAÇÕES E COMUNICAÇÕES**, 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, e tendo em vista o disposto no artigo 67 da Lei n.º 8.666, de 21/jun/1993, resolve:

**Art. 1º -** Instituir a Comissão de Acompanhamento e Fiscalização do Processo nº 01209.000069/2019-88, firmado com a empresa **GL ELETRO-ELETÔNICOS LTDA**, Contrato de Prestação de Serviços nº 006/2019, referente contratação de serviços continuados de manutenção preventiva e corretiva dos nobreaks, marca Legrand, que serão prestados nas condições estabelecidas no Projeto Básico para atendimento das necessidades da Coordenação de Tecnologia da Informação e Comunicação - COTIC do Laboratório Nacional de Computação Científica - LNCC.

**I - GESTOR DO CONTRATO**

a) Titular: **Wagner Vieira Léo**
CPF: 732.796.687-00
Matrícula SIAPE: 673173
Lotação: COTIC

b) Substituto: **Paulo Cabral Filho**
CPF: 636.363.607-87
Matrícula SIAPE: 0672429
Lotação: SERED/COTIC

**II** - **FISCAL ADMINISTRATIVO**

a) Titular: **Joaquim Lourenço Ferreira**
CPF: 292.662.971-00
Matrícula SIAPE: 671832
Lotação: SELEP/COGEA

**Art. 2º -** O Gestor e os Fiscais do Contrato deverão observar fielmente suas atribuições previstas no artigo 67 da Lei n.º 8.666, de 21/jun/1993.

**Art. 3º -** Esta Portaria entra em vigor na data de sua publicação no Boletim de Serviço do LNCC.

**AUGUSTO CESAR GADELHA VIEIRA**

**BOLETIM DE SERVIÇO N.º 007/2019 31/07/2019**

**PORTARIA Nº 71/2019/SEI-LNCC de 09 de Julho de 2019**

**APLICAÇÃO DE PENALIDADE**

**O DIRETOR DO LABORATÓRIO NACIONAL DE COMPUTAÇÃO CIENTÍFICA DO MINISTÉRIO DA CIÊNCIA, TECNOLOGIA, INOVAÇÕES E COMUNICAÇÕES**, no uso da competência que lhe foi delegada pela Portaria nº 407, de 29 de junho e 2006, do Ministro de Estado da Ciência e Tecnologia, publicada no Diário Oficial da União de 30/06/2006, e com fundamento no inciso II e III, do artigo 87, da Lei 8.666/93 e alterações, e

Considerando o descumprimento de obrigação contratual - Pregão Eletrônico nº 011/2018 - Empenho nº 2018NE800285 e pelo não cumprimento do estabelecido no ITEM 7 do Termo de Referência bem como do ítem 15 do Edital (Doc. SEI-LNCC nº 3484978 e 3553669, conforme consta nos autos do Processo nº 01209.000219/2018-72, firmado com à empresa **JP COMERCIO DE PRODUTOS ELETROELETRÔNICOS EIRELI**, inscrita no CNPJ/MF sob o nº 31.552.188/0001-04, resolve:

**Art. 1º** - Manter a penalidade de Advertência, aplicada em 10/04/2019, conforme Ofício nº 136/2019/SEI-LNCC.

**Art. 2º** - Aplicar a penalidade de multa compensatória no montante de 10% (dez por cento) sobre o valor do item 24, conforme Artigo 87, inciso II da Lei nº 8.666/93,

**Art. 3º** - Aplicar a penalidade de impedimento de licitar com o Laboratório Nacional de Computação Científica - LNCC, conforme artigo 87 inciso III da Lei nº 8.666/93, pelo prazo de 2 (dois) anos, conforme ofício nº 192/2018/SEI-LNCC constante dos autos do processo.

**Art. 4º** - Registrar as penalidades aplicadas no SICAF.

**Art. 5º** - Esta Portaria entra em vigor na data de sua publicação.

**AUGUSTO CESAR GADELHA VIEIRA**

**PORTARIA Nº 72/2019/SEI-LNCC de 10 de julho de 2019**

**APLICAÇÃO DE PENALIDADE**

**O DIRETOR DO LABORATÓRIO NACIONAL DE COMPUTAÇÃO CIENTÍFICA DO MINISTÉRIO DA CIÊNCIA, TECNOLOGIA, INOVAÇÕES E COMUNICAÇÕES**, no uso da competência que lhe foi delegada pela Portaria nº 407, de 29 de junho e 2006, do Ministro de Estado da Ciência e Tecnologia, publicada no Diário Oficial da União de 30/06/2006, e com fundamento no inciso II e III, do artigo 87, da Lei 8.666/93 e alterações, e

Considerando o descumprimento de obrigação contratual - Pregão Eletrônico nº 011/2018 - Empenho nº 2018NE800273, conforme consta nos autos do Processo nº 01209.000219/2018-72, firmado com à empresa **JVS COMÉRCIO E SERVIÇOS DE INFORMÁTICA LTDA**, inscrita no CNPJ/MF sob o nº 10.190.265/0001-53, resolve:

**Art. 1º** - Manter a penalidade de Advertência, aplicada em 15/02/2019, conforme Ofício nº 048/2019/SEI-LNCC (3856655).

**Art. 2º** - Aplicar a penalidade de impedimento de licitar com o Laboratório Nacional de Computação Científica - LNCC, conforme artigo 87 inciso III da Lei nº 8.666/93, pelo prazo de 2 (dois) anos, conforme ofício nº 102/2018/SEI-LNCC (4015496) constante dos autos do processo.

**Art. 3º** - Registrar as penalidades aplicadas no SICAF.

**Art. 4º** - Esta Portaria entra em vigor na data de sua publicação.

**AUGUSTO CESAR GADELHA VIEIRA**

**PORTARIA Nº 73/2019/SEI-LNCC de 15 de julho de 2019**

**EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO**

O DIRETOR DO LABORATÓRIO NACIONAL DE COMPUTAÇÃO CIENTÍFICA DO MINISTÉRIO DA CIÊNCIA, TECNOLOGIA, INOVAÇÕES E COMUNICAÇÕES, 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

**Art. 1º** - Instituir no âmbito do Laboratório Nacional de Computação Científica - LNCC, a Equipe de Planejamento da Contratação, conforme previsto no artigo 10 da Instrução Normativa nº 1, de 04/04/2019, em especial o inciso os incisos IV e §1º, com vistas à contratação de empresa especializada para o fornecimento de equipamentos de tecnologia da informação e comunicação (notebook, scanner de mesa e disco rígido externo), para atender as necessidades da Coordenação de Tecnologia da Informação e Comunicação - COTIC do LNCC, composta de 03 (três) membros:

1. **Integrante Requisitante:**
   Fábio Augusto Rosa – SIAPE nº 673185

2. **Integrante Técnico:**
   André Ramos Carneiro – SIAPE nº 2048721

3. **Integrante Administrativo:**
   Joaquim Lourenço Ferreira - SIAPE nº 671832

**Art. 2º -** Esta Portaria entra em vigor na data de sua publicação no Boletim Interno do LNCC.

**AUGUSTO CESAR GADELHA VIEIRA**

**BOLETIM DE SERVIÇO N.º 007/2019 31/07/2019**

**PORTARIA Nº 74/2019/SEI-LNCC de 24 de julho de 2019**

**SUBSTITUTO COMAC**

**O DIRETOR DO LABORATÓRIO NACIONAL DE COMPUTAÇÃO CIENTÍFICA DO MINISTÉRIO DA CIÊNCIA, TECNOLOGIA, INOVAÇÕES E COMUNICAÇÕES**, 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

**Art. 1º** - Designar o servidor **PABLO JAVIER BLANCO** , CPF n.º 059.766.107-30, matricula SIAPE n.º 1700670, para substituir nos impedimentos ou afastamentos regulares, **FREDERIC GERARD CHRISTIAN VALENTIN**, Coordenador de Métodos Matemáticos e Computacionais - COMAC, código FCPE 101.3, do Laboratório Nacional de Computação Científica deste Ministério.

**Art. 2º** - Esta Portaria cancela a Portaria nº 025 de 15/03/2017.

**AUGUSTO CESAR GADELHA VIEIRA**

***Publicada no DOU de 31/07/2019***

**PORTARIA Nº 75/2019/SEI-LNCC de 25 de Julho de 2019**

**SUBSTITUTO SERED/COTIC**

**O DIRETOR DO LABORATÓRIO NACIONAL DE COMPUTAÇÃO CIENTÍFICA DO MINISTÉRIO DA CIÊNCIA, TECNOLOGIA, INOVAÇÕES E COMUNICAÇÕES**, 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

**Art. 1º** - Designar o servidor **LUIS RODRIGO DE OLIVEIRA GONÇALVES** , CPF n.º 054.965.557-36, matricula SIAPE n.º 1700336, para substituir nos impedimentos ou afastamentos regulares, **PAULO CABRAL FILHO**, Chefe do Serviço do Serviço de Suporte de Sistemas e Redes - SERED, código FCPE 101.1, do Laboratório Nacional de Computação Científica deste Ministério.

**Art. 2º** - Esta Portaria cancela a Portaria nº 096 de 03/10/2019.

**AUGUSTO CESAR GADELHA VIEIRA**

***Publicada no DOU de 31/07/2019***

**PORTARIA Nº 76/2019/SEI-LNCC de 25 de julho de 2019**

**APLICAÇÃO DE PENALIDADE**

**O DIRETOR DO LABORATÓRIO NACIONAL DE COMPUTAÇÃO CIENTÍFICA DO MINISTÉRIO DA CIÊNCIA, TECNOLOGIA, INOVAÇÕES E COMUNICAÇÕES**, no uso da competência que lhe foi delegada pela Portaria nº 407, de 29 de junho e 2006, do Ministro de Estado da Ciência e Tecnologia, publicada no Diário Oficial da União de 30/06/2006, e com fundamento no inciso II e III, do artigo 87, da Lei 8.666/93 e alterações, e

Considerando o descumprimento de obrigação contratual - item 20 do Termo de Referência - Das obrigações da Contratada, bem como pela falta da entrega de material de limpeza, conforme consta nos autos do Processo nº 01209.000032/2014-45, firmado com à empresa **AJE SERVIÇOS TÉCNICOS ESPECIALIZADOS LTDA**, inscrita no CNPJ/MF sob o nº 01.435.248/0001-48, resolve:

**Art. 1º** - Manter a penalidade de Advertência, aplicada em 10/04/2019, conforme Ofício nº 134/2019/SEI-LNCC (4047812).

**Art. 2º** - Esta Portaria entra em vigor na data de sua publicação.

**AUGUSTO CESAR GADELHA VIEIRA**

**PORTARIA Nº 77/2019/SEI-LNCC de 25 de julho de 2019**

**APLICAÇÃO DE PENALIDADE**

**O DIRETOR DO LABORATÓRIO NACIONAL DE COMPUTAÇÃO CIENTÍFICA DO MINISTÉRIO DA CIÊNCIA, TECNOLOGIA, INOVAÇÕES E COMUNICAÇÕES**, no uso da competência que lhe foi delegada pela Portaria nº 407, de 29 de junho e 2006, do Ministro de Estado da Ciência e Tecnologia, publicada no Diário Oficial da União de 30/06/2006, e com fundamento no inciso II e III, do artigo 87, da Lei 8.666/93 e alterações, e

Considerando o descumprimento de obrigação contratual, conforme consta nos autos do Processo nº 01209.000246/2018-45, firmado com à empresa **CLARO S/A**, inscrita no CNPJ/MF sob o nº 40.432.544/0001-47, resolve:

**Art. 1º** - Manter a penalidade de Advertência, aplicada em 28/05/2019, conforme Ofício nº 097/2019/SEI-LNCC (3856655).

**Art. 2º** - Esta Portaria entra em vigor na data de sua publicação.

**AUGUSTO CESAR GADELHA VIEIRA**

LNCC
www.lncc.br
Laboratório Nacional de Computação Científica

Av. Getúlio Vargas 333, Quitandinha, Petrópolis, RJ . CEP. 25651-075



**PORTARIA Nº 79/2019/SEI-LNCC de 25 de Julho de 2019**

**APLICAÇÃO DE PENALIDADE**

**O DIRETOR EM EXERCÍCIO DO LABORATÓRIO NACIONAL DE COMPUTAÇÃO CIENTÍFICA DO MINISTÉRIO DA CIÊNCIA, TECNOLOGIA, INOVAÇÕES E COMUNICAÇÕES**, no uso da competência que lhe foi delegada pela Portaria nº 407, de 29 de junho e 2006, do Ministro de Estado da Ciência e Tecnologia, publicada no Diário Oficial da União de 30/06/2006, e com fundamento no inciso II e III, do artigo 87, da Lei 8.666/93 e alterações, e

Considerando o descumprimento de obrigação contratual e pelo não cumprimento do estabelecido no Item 1 - Objeto e Item 3 do Local e Prazo de Entrega do Objeto (docs. SEI-LNCC nº 4416777 e 4416795) - no Termo de Referência SEI nº 2216621, conforme consta nos autos do Processo nº 01209.000137/2017-47, Contrato nº 01.012.00.2017, firmado com à empresa **EPODONTO COMERCIO E SERVIÇOS LTDA**, inscrita no CNPJ/MF sob o nº 00.330.676/0001-43, resolve:

**Art. 1º** - Manter a penalidade de Advertência, aplicada em 17/07/2019, conforme Ofício nº 162/2019/SEI-LNCC (4417779).

**Art. 2º** - Esta Portaria entra em vigor na data de sua publicação.

**AUGUSTO CESAR GADELHA VIEIRA**

**PORTARIA Nº 80/2019/SEI-LNCC de 25 de julho de 2019**

**COMISSÃO PCI DO LNCC**

O **DIRETOR EM EXERCÍCIO DO LABORATÓRIO NACIONAL DE COMPUTAÇÃO CIENTÍFICA – LNCC**, Unidade de Pesquisa do Ministério da Ciência, Tecnologia, Inovações e Comunicações, no uso da competência que lhe foi delegada pela Portaria MCT nº 407, de 28/jun/2006, e tendo em vista o disposto no artigo 41 do Regimento Interno deste Laboratório, aprovado pela Portaria MCTIC nº 5.158 de 14/11/2016,

**RESOLVE**

**Art. 1º** - Constituir a Comissão do Programa de Capacitação Institucional do LNCC para orientação e assessoramento ao Diretor.

**Art. 2º** - A Comissão será composta pelos membros abaixo:

- Jauvane Cavalcante de Oliveira;
- Marcelo Dutra Fragoso;
- Frederic Gerar Christian Valentin;
- Laurent Emmanuel Dardenne;
- Marcio Arab Murad;
- Renato Portugal;

**Art. 3º** - A Comissão será coordenada pelo servidor Jauvane Cavalcante de Oliveira.

**Art. 4º** - Esta comissão também atuará como Comissão Permanente de Pré-Enquadramento, conforme descrito na PO/MCTIC nº. 2195, de 19 de abril de 2018.

**Art. 5º** - Esta Portaria cancela a Portaria nº 041 de 29/05/2017.

**Art. 6º** - Esta Portaria entra em vigor na data de sua publicação no Boletim Serviço do LNCC.

**WAGNER VIEIRA LÉO**

**PORTARIA Nº 81/2019/SEI-LNCC de 30 de Julho de 2019**

**POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO**

**O DIRETOR EM EXERCÍCIO 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 legislação existente e em vigor,

**RESOLVE:**

**Art. 1º.** Instituir a Política de Segurança da Informação e Comunicação do Laboratório Nacional de Computação Científica - LNCC, nos termos do Anexo da presente Portaria, disponível no endereço: http://sec.lncc.br.

**Art. 2º.** Esta Portaria cancela a Portaria nº 114 de 25/09/2012.

**Art. 3º** - Esta Portaria entra em vigor na data de sua publicação no Boletim de Serviço.

**WAGNER VIEIRA LÉO**

# 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 27002:2013** que descreve um Código de práticas para a gestão da Segurança da Informação.

A **Norma Brasileira ABNT NBR ISO/IEC 27001:2013** 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**[1], 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.

A **Instrução Normativa GSI nº 1, de 13 de junho de 2008**[2] que disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências.

A **Norma Complementar nº 01/IN01/DSIC/GSIPR**[3] 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**[4], 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**[5], 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**[6], 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 37, de **25 Fev 2013** - Seção 1

---

[1] http://sislex.previdencia.gov.br/paginas/23/2002/4553.htm
[2] http://dsic.planalto.gov.br/legislacao/in_01_gsidsic.pdf
[3] http://dsic.planalto.gov.br/legislacao/nc_1_normatizacao.pdf
[4] http://dsic.planalto.gov.br/legislacao/nc_2_metodologia.pdf
[5] http://dsic.planalto.gov.br/legislacao/nc_3_psic.pdf
[6] http://dsic.planalto.gov.br/legislacao/nc_04_grsic.pdf

A **Norma Complementar nº 05/IN01/DSIC/GSIPR**[78], 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**[9], 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**[10], (Revisão 01), 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 (APF), direta e indireta. Publicada no DOU Nº 134, de **16 Jul 2014** - Seção 1

A **Norma Complementar nº 08/IN01/DSIC/GSIPR**[11], 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**[12], (Revisão 02), que estabelece orientações específicas para o uso de recursos criptográficos em Segurança da Informação e Comunicações, nos órgãos ou entidades da Administração Pública Federal (APF), direta e indireta. Publicada no DOU Nº 134, de **16 Jul 2014** - Seção 1

A **Norma Complementar nº 10/IN01/DSIC/GSIPR**[13], 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**[14], 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**[15], 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

---

[7] http://dsic.planalto.gov.br/legislacao/anexo_nc_05_etir.pdf
[8] http://dsic.planalto.gov.br/legislacao/copy_of_nc_05_etir.pdf
[9] http://dsic.planalto.gov.br/legislacao/nc_6_gcn.pdf
[10] http://dsic.planalto.gov.br/legislacao/nc_07_revisao_01.pdf
[11] http://dsic.planalto.gov.br/legislacao/copy_of_nc_8_gestao_etir.pdf
[12] http://dsic.planalto.gov.br/legislacao/nc_09_revisao_02.pdf
[13] http://dsic.planalto.gov.br/legislacao/nc_10_ativos.pdf
[14] http://dsic.planalto.gov.br/legislacao/nc_11_conformidade.pdf
[15] http://dsic.planalto.gov.br/legislacao/nc_12_dispositivos.pdf

A **Norma Complementar nº 13/IN01/DSIC/GSIPR**[16], 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**[17], que estabelece princípios, diretrizes e responsabilidades relacionados à segurança da informação para o tratamento da informação em ambiente de computação em nuvem, nos órgãos e entidades da Administração Pública Federal, direta e indireta. Publicada no DOU 53, de **19 Mar 2018** - Seção 1, folhas 22 e 23

A **Norma Complementar nº 15/IN01/DSIC/GSIPR**[18], 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 **Norma Complementar nº 16/IN01/DSIC/GSIPR**[19], que estabelece as diretrizes para o Desenvolvimento e Obtenção de Software Seguro nos Órgãos e Entidades da Administração Pública Federal, direta e indireta. Publicada no DOU Nº 224, de **21 Nov 2012** - Seção 1

A **Norma Complementar nº 17/IN01/DSIC/GSIPR**[20], que estabelece diretrizes nos contextos de atuação e adequações para Profissionais da Área de Segurança da Informação e Comunicações (SIC) nos Órgãos e Entidades da Administração Pública Federal (APF). Publicada no DOU Nº 68, de **10 Abr 2013** - Seção 1

A **Norma Complementar nº 18/IN01/DSIC/GSIPR**[21], estabelece as diretrizes para as Atividades de Ensino em Segurança da Informação e Comunicações (SIC) nos Órgãos e Entidades da Administração Pública Federal (APF). Publicada no DOU Nº 68, de **10 Abril 2013** - Seção 1

A **Norma Complementar nº 19/IN01/DSIC/GSIPR**[22], que estabelece padrões mínimos de Segurança da Informação e Comunicações para os Sistemas Estruturantes da Administração Pública Federal (APF), direta e indireta. Publicada no DOU Nº 134, de **16 Jul 2014** - Seção 1

A **Norma Complementar nº 20/IN01/DSIC/GSIPR**[23]**, (Revisão 01)**, que estabelece as Diretrizes de Segurança da Informação e Comunicações para Instituição do Processo de Tratamento da Informação nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta. Publicada no DOU Nº 242, de **15 Dez 2014** - Seção 1

A **Norma Complementar nº 21/IN01/DSIC/GSIPR**[24], que estabelece as diretrizes para o Registro de Eventos, Coleta e Preservação de Evidências de Incidentes de Segurança em Redes nos órgãos e entidades da Administração Pública Federal, direta e indireta. Publicada no DOU Nº 196, de **10 Out 2014** - Seção 1

---

[16] http://dsic.planalto.gov.br/legislacao/nc_13_mudancas.pdf
[17] http://dsic.planalto.gov.br/arquivos/documentos-pdf/NC_14_R01.pdf
[18] http://dsic.planalto.gov.br/legislacao/nc_15_redes_sociais.pdf
[19] http://dsic.planalto.gov.br/legislacao/nc_16_software_seguro.pdf
[20] http://dsic.planalto.gov.br/legislacao/nc_17_profissionais_sic.pdf
[21] http://dsic.planalto.gov.br/legislacao/nc_18_atividades_ensino.pdf
[22] http://dsic.planalto.gov.br/legislacao/nc_19_SISTEMAS_ESTRUTURANTES.pdf
[23] http://dsic.planalto.gov.br/legislacao/copy_of_NC20_Revisao01.pdf
[24] http://dsic.planalto.gov.br/legislacao/nc_21_preservacao_de_evidencias.pdf

O **Decreto nº 7.845**[25], de 14 de novembro de 2012, publicado no DOU de **16 Nov 2012**, que regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento.

A **Instrução Normativa GSI Nº 2**[26], de 5 de fevereiro de 2013, que dispõe sobre o credenciamento de segurança para o tratamento de informação classificada, em qualquer grau de sigilo, no âmbito do Poder Executivo Federal. Publicada no DOU Nº 32, de **18 Fev 2013** - Seção 1

A **Instrução Normativa GSI Nº 3**[27], de 6 de março de 2013, que dispõe sobre os parâmetros e padrões mínimos dos recursos criptográficos baseados em algoritmos de Estado para criptografia da informação classificada no âmbito do Poder Executivo Federal. Publicada no DOU Nº 50, de **14 Mar 2013** - Seção 1

A **Instrução Normativa MP/SLTI Nº 4**[28], de **11 de setembro de 2014**, 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

O **DECRETO Nº 9.637**, DE **26 DE DEZEMBRO DE 2018**[29], que institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação, e altera o Decreto nº 2.295, de 4 de agosto de 1997, que regulamenta o disposto no art. 24, caput , inciso IX, da Lei nº 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional.

A **Portaria Nº 45 - GSI**[30], 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 I

## 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

[25] http://sislex.previdencia.gov.br/paginas/23/2012/7845.htm
[26] http://dsic.planalto.gov.br/legislacao/instrucao_normativa_nr2.pdf
[27] http://dsic.planalto.gov.br/legislacao/instrucao_normativa_nr3.pdf
[28] https://www.governodigital.gov.br/documentos-e-arquivos/legislacao/1%20-%20IN%204%20%2011-9-14.pdf
[29] http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Decreto/D9637.htm
[30] http://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?jornal=1&pagina=2&data=09/09/2009

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. **COTIC**: Coordenação de Tecnologia da Informação e Comunicação
7. **CSIRT** - Computer Security Incident Response Team (grupo técnico responsável por resolver incidentes relacionados à segurança em sistemas computacionais)
8. **CTIR Gov** - Centro de Tratamento de Incidentes de Segurança em Redes de Computadores da Administração Pública Federal
9. **DSIC**: Departamento de Segurança da Informação e Comunicações
10. **ISO**: *International Organization for Standardization*
11. **IEC**: *International Electrotechnical Commission*
12. **LNCC –** Laboratório Nacional de Computação Científica
13. **MCTIC**: Ministério da Ciência, Tecnologia, Inovações e Comunicações
14. **NBR**: Denominação de norma da Associação Brasileira de Normas Técnicas
15. **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.
16. **PDCA**: *Plan-Do-Check-Act*
17. **POSIC**: Política de Segurança da Informação e Comunicação
18. **Proprietário**: identifica o indivíduo 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 e de Segurança Física (CSIC), instituído pelo Diretor do LNCC, através da Portaria n.º 064/2019/SEI-LNCC, de 18 de Junho de 2019, resolve:

**Art. 1º.** Instituir a Política de Segurança da Informação e Comunicação (**POSIC**) 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 (**LNCC**), bem como prover obrigações e responsabilidades decorrentes e correspondentes ao grau de importância atribuído a esses acervos.

**Art. 3º.** Recomenda-se que, o conteúdo da Política de Segurança da Informação e Comunicação (**POSIC**) seja revisada a cada três anos, ou em intervalo inferior.

§1º O prazo para a publicação das revisões deverá ser contado a partir da data da publicação desta portaria.

§2º Esta revisão permanece válida até a publicação de uma nova.

## 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 deve ser mantida 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**.

§1º 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**[31]

§2º Recomenda-se que, sejam definidos formalmente, e em documento próprio, o período e a forma da retenção dos dados relevantes as atividades do **LNCC**, de seus servidores e de seus colaboradores, sejam eles diretos ou indiretos.

**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, bem como aqueles necessários ao resguardo da inviolabilidade da intimidade da vida privada, da honra e da imagem das pessoas. DECRETO Nº 7.845, DE 14 DE NOVEMBRO DE 2012 - DOU DE 16/11/2012[32]

**Parágrafo único.** O acesso a dados ou informações sigilosas é restrito e condicionado à necessidade de conhecer.

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

**Art. 9º** Deve ser evitado o uso de 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 e de Segurança Física (CSIC)**, de que trata o **Art. 5º, inciso VI da Instrução Normativa GSI Nº 1**[33]**.**

**§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;

---

[31] https://www.jusbrasil.com.br/topicos/10730704/inciso-x-do-artigo-5-da-constituicao-federal-de-1988
[32] http://sislex.previdencia.gov.br/paginas/23/2012/7845.htm
[33] http://dsic.planalto.gov.br/legislacao/in_01_gsidsic.pdf

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**[34]

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

**Art. 12º.** Conforme o **Art. 10 do Decreto nº 6.029/2007**[35], 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 27001:2013**, conforme **N.C. 02/IN01/DSIC/GSIPR**[36]**, 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**. O procedimento aplicado, à cada um destes casos, deve ser documentado e divulgado de forma apropriada.

**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**[37]**.**

**Art. 17º.** Periodicamente os membros do LNCC devem ser informados sobre Segurança da Informação, onde, recomenda-se que a POSIC seja divulgada e sejam dadas recomendações gerais baseadas nas auditorias e levantamentos realizados.

§1º. Recomenda-se que, todos os usuários recebam a POSIC quando da abertura de conta.

§2º. Recomenda-se que, ao ocorrerem mudanças na POSIC e nos procedimentos de segurança, os usuários sejam informados e que lhes seja disponibilizada a nova versão do documento.

---

[34] https://www.jusbrasil.com.br/topicos/10677389/artigo-20-do-decreto-lei-n-3689-de-03-de-outubro-de-1941
[35] http://www.planalto.gov.br/ccivil_03/_Ato2007-2010/2007/Decreto/D6029.htm
[36] http://dsic.planalto.gov.br/legislacao/nc_2_metodologia.pdf
[37] http://sislex.previdencia.gov.br/paginas/23/2002/4553.htm

## 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 servidores e colaboradores às informações e aos recursos computacionais devem ser revogados de acordo com procedimento específico.

### 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**[38].

**Art. 30º.** É proibido obter ou tentar obter, indevidamente, acesso ao 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**[39]**.**

**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**[40].

**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**[41].

---

[38] https://presrepublica.jusbrasil.com.br/legislacao/104071/lei-de-seguranca-nacional-lei-7170-83
[39] http://www.planalto.gov.br/ccivil_03/Leis/L9100.htm
[40] http://www.planalto.gov.br/ccivil_03/LEIS/L9296.htm
[41] http://www.planalto.gov.br/ccivil_03/LEIS/L9605.htm

**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**[42].

**Art. 34º.** É vedada a propaganda eleitoral nos domínios do LNCC, conforme **Resolução nº 22.718, de 28 de fevereiro de 2008, do TSE**[43].

## 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 11 de setembro de 2014**[44].

**Art. 37º.** Quando o contrato tiver requisitos de segurança deve haver um parecer do **CSIC**, conforme **I.N. nº 4, de 2014**.

> **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 Nº 7.845, de 14 de novembro de 2012**[45]**.**

**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.

---

[42] http://www.planalto.gov.br/ccivil_03/Leis/L9472.htm
[43] http://www.tse.jus.br/legislacao-tse/res/2008/RES227182008.htm
[44] https://www.governodigital.gov.br/documentos-e-arquivos/legislacao/1%20-%20IN%204%20%2011-9-14.pdf
[45] http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Decreto/D7845.htm

**§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 corresponsáveis 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**[46].

**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**[47].

## 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 16 Jul 2014**[48].

**Art. 51º.** As áreas onde estão localizados os centros de processamento de dados, os sistemas de refrigeração e de geração de energia, devem ser consideradas como 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 autorizado pelos responsáveis.

---

[46] https://www.jusbrasil.com.br/topicos/10710882/paragrafo-6-artigo-37-da-constituicao-federal-de-1988
[47] https://www.jusbrasil.com.br/topicos/10709394/artigo-482-do-decreto-lei-n-5452-de-01-de-maio-de-1943
[48] http://dsic.planalto.gov.br/legislacao/nc_07_revisao_01.pdf

**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**[49].

**Art. 55º.** Recomenda-se, sempre que possível, a utilização de câmeras que captam o movimento; principalmente nos centros 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.** Recomenda-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 **COTIC** 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 monitorada e ajustada, 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.

---

[49] http://www.planalto.gov.br/ccivil_03/decreto/D1171.htm

**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 deve 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 registrados, analisados e devem ser adotadas as ações apropriadas.

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

**Art. 76º.** A **COTIC** 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 criptografadas.

**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 (Revisão 02), de 16 jullho 2014**[50]**.**

**Art. 79º.** A **COTIC** deve monitorar e auditar os recursos criptográficos pertencentes ao LNCC, conforme **N.C. 09/IN01/DSIC/GSIPR (Revisão 02), de 16 julho 2014**.

> **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 (Revisão 02), de 16 julho 2014**, bem como com a legislação em vigor.

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

---

[50] http://dsic.planalto.gov.br/legislacao/nc_09_revisao_02.pdf

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 cifrar ou decifrar 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 cifra, 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.** O armazenamento e a divulgação de pornografia não são permitidos.

**Parágrafo único.** Caso seja detectado, deve ser bloqueado o acesso em todos os computadores do **LNCC;** quando o ilícito a cima envolver pornografia infantil, deve-se encaminhar denúncia às autoridades competentes.

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

**Art. 86º.** Quando a **CSIC** for notificada de atividades ilegais, inclusive os previstos neste documento, esta deverá tomar as providências necessárias em caráter de urgência:

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

ii. A **COTIC** 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 denúncia às autoridades competentes.

**Art. 87º.** A violação de direitos de propriedade intelectual, inclusive direitos autorais, resultará no bloqueio da conta e do 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**[51]**,** sujeitando o infrator às penalidades previstas no **Código** Penal.

**Art. 93º.** A **COTIC** 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**[52], recomenda-se que a **COTIC** 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**[53]**,** e **o § 2º do art. 1º do Decreto nº 2.553, de 16 de abril de 1998**[54].

**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 excluídas de forma segura.

## Capítulo VII

[51] https://www.jusbrasil.com.br/topicos/10730639/inciso-xii-do-artigo-5-da-constituicao-federal-de-1988
[52] http://www.planalto.gov.br/ccivil_03/Leis/L7232.htm
[53] https://www.jusbrasil.com.br/topicos/10590519/artigo-75-da-lei-n-9279-de-14-de-maio-de-1996
[54] http://www.planalto.gov.br/ccivil_03/decreto/D2553.htm

## 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 restrita e controlada.

**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 **COTIC** 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 **COTIC**.

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

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

**Art. 109º.** As senhas de contas administrativas dos dispositivos de rede são exclusivas da **COTIC**.

**Art. 110º.** Periodicamente todas as senhas devem ser testadas para detectar senhas fracas.

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

**Art. 111º.** Recomenda-se que a conta seja automaticamente bloqueada após o número de tentativas de conexão ultrapassar a quantidade de 3, exceto caso excepcional.

**Art. 112º.** A **COTIC** manterá registros sigilosos das autenticações por senha por pelo menos por 1 (um) ano.

## Seção II

## Da Responsabilidade do Usuário

**Art. 113º.** 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 **CSIC** deve tomar as devidas medidas e propor as devidas sanções.

**Art. 114º.** 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. 115º.** A senha representa a autenticação de cada usuário sendo de seu exclusivo controle, uso e conhecimento, devendo ser gerada pelo próprio usuário.

**Art. 116º.** É dever de todo usuário notificar através de *e-mail* para a **Coordenação de Tecnologia da Informação e Comunicação** (**COTIC**) as contas que não estejam sendo usadas para que sejam excluídas.

**Art. 117º.** Os usuários são responsáveis pelos *softwares* por eles instalados.

**Art. 118º.** Todo *software* que não tenha sido instalado pela COTIC é de responsabilidade do usuário do equipamento.

**Art. 119º.** Os usuários devem ser orientados a seguir as boas práticas de segurança da informação.

**Art. 120º.** 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.** Recomenda-se que os usuários não mantenham sobre suas mesas ou estações de trabalho, documentos de conteúdo restrito.

**Art. 121º.** 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. 122º.** Os usuários devem utilizar apenas os serviços e os recursos de rede a que foram autorizados.

**Art. 123º.** Recomenda-se que grupos de serviços de informação, usuários e sistemas de informação devem ser segregados em redes distintas.

**Art. 124º.** Para todo projeto classificado como sigiloso, o tratamento e o controle de acesso será conforme o **Decreto Nº 7.845, de 2012**[55].

**Art. 125º.** A **COTIC** pode bloquear temporariamente o acesso, parcial ou completo, à um serviço para garantir a disponibilidade de serviços prioritários.

**Art. 126º.** No intuito de garantir a continuidade do serviço, a **COTIC** pode bloquear ou limitar, temporariamente, a conectividade de usuários ou de serviços.

**Art. 127º.** É proibido prover acesso remoto não autorizado.

**Art. 128º.** É proibido manter-se conectado à rede do **LNCC** e ao mesmo tempo utilizar outro provedor de acesso à *Internet*.

**Art. 129º.** Todo serviço de rede hospedado em máquinas conectadas à rede interna do **LNCC**, por padrão, deve estar inacessível para máquinas e usuários externos à rede do **LNCC**.

**Art. 130º.** As solicitações para liberação de acessos aos recursos computacionais devem ser encaminhadas à **COTIC** por um servidor público federal lotado no **LNCC,** através de formulário próprio.

**Art. 131º.** A COTIC efetuará registros de todas as conexões à *Internet*, mantendo-os em sigilo.

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

**Art. 132º.** 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. 133º.** A **COTIC**, deve controlar a liberação de acesso aos serviços hospedados, nas máquinas conectadas à rede.

[55] http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Decreto/D7845.htm

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

**§2.** Quando ocorrer uma solicitação de liberação de serviço hospedado na rede do **LNCC** para acesso externo à rede da instituição, a comissão de segurança, ou equipe por ela delegada, deve explicitamente autorizar tal liberação.

**Art. 134º.** Para que a segurança na rede interna seja mantida, a **COTIC** deve manter registro e supervisionar os serviços providos pela rede.

**Art. 135º.** Deve-se configurar em toda máquina ou dispositivo que provê algum serviço de rede um controle de acesso baseado em *ACL*s ou algo similar.

**Parágrafo Único**: Recomenda-se que a ferramenta de controle de acesso mantenha um registro das tentativas de conexão.

**Art. 136º.** Todas as máquinas administradas pela **COTIC** devem ter um pacote de segurança devidamente instalado e configurado.

**Art. 137º.** Recomenda-se que todas as máquinas conectadas à rede do **LNCC** tenham um pacote de segurança devidamente instalado, configurado e autorizado pela COTIC

**Art. 138º.** Toda correspondência eletrônica direcionada ao **LNCC** deve ser verificada com ferramentas para remoção de programas maliciosos.

**Art. 139º.** Os computadores e dispositivos dos centros de processamento de dados devem encaminhar os registros de eventos críticos ao sistema de log.

**Art. 140º.** Recomenda-se que as impressoras, ou o ambiente de impressão, contabilize o número de páginas utilizadas por cada um dos seus usuários.

**Art. 141º**. A **COTIC** 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 **COTIC**;

ii. Todos dispositivos devem ser cadastrados pela **COTIC** antes de serem conectados à rede **cabeada** 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 **COTIC** poderão ser conectados a rede cabeada do **LNCC**.

**Art. 142º**. 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. 143º**. Recomenda-se que o e-mail institucional não seja utilizado para fins pessoais.

**Art. 144º**. Por padrão, não é permitido o uso de aplicações baseadas em protocolos ***P2P*** na rede do **LNCC**.

i. Quando a utilização destas aplicações for necessária 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. 145º.** Devem ser especificados os requisitos de segurança para novos sistemas de informação ou melhorias em sistemas existentes.

**Art. 146º.** Procedimentos para controlar a instalação de *softwares* em sistemas operacionais devem ser implementados.

**Art. 147º.** Implementação de mudanças deve ser controlada utilizando procedimentos formais.

**Art. 148º.** Recomenda-se que as novas bases de dados devem ter possibilidade de integração com as bases de dados existentes.

**Art. 149º.** Recomenda-se que os novos sistemas devem manter a interoperabilidade com os sistemas computacionais existentes.

**Art. 150º.** Recomenda-se que o software não deve conter código oculto que possa causar qualquer alteração de comportamento.

**Art. 151º.** 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. 152º.** 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**[56].

**Art. 153º.** Cabe à **COTIC**, 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. 154º.** Deve-se reduzir os riscos resultantes da exploração de vulnerabilidades técnicas conhecidas.

**Art. 155º.** Os eventos de segurança devem ser relatados através dos canais apropriados o mais rapidamente possível.

**Art. 156º.** 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. 157º.** Deve-se assegurar um enfoque consistente e efetivo à gestão de incidentes de segurança da informação.

**Art. 158º.** Com fundamento no **Decreto 7.845, de 14 de novembro de 2012**[57], e no Código de Ética do Servidor Público Civil do Poder Executivo Federal, aprovado pelo **Decreto 1.171, de 22 de junho de 1994**[58], 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. 159º.** A equipe responsável pela Resposta e 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**[59].

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

**Art. 160º.** 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**[60]**,** que regulamenta sua atividade.

**Art. 161º.** A equipe da **COTIC** responsável pelos equipamentos da área de armazenamento pode usar programas para detectar irregularidades, desde que não infrinja o **Art. 6 da N.C. 09/IN01/DSIC/GSIPR (Revisão 02), de 15 de julho de 2014**[61].

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

---

[56] http://www.planalto.gov.br/ccivil_03/_Ato2004-2006/2006/Lei/L11419.htm
[57] http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Decreto/D7845.htm
[58] http://www.planalto.gov.br/ccivil_03/decreto/d1171.htm
[59] http://dsic.planalto.gov.br/legislacao/copy_of_nc_05_etir.pdf
[60] http://dsic.planalto.gov.br/legislacao/copy_of_nc_8_gestao_etir.pdf
[61] http://dsic.planalto.gov.br/legislacao/nc_09_revisao_02.pdf

ii. A **COTIC** 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. 162º.** 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. 163º.** 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. 164º.** Deve-se fazer por escrito uma detalhada análise de impacto nas mudanças e manutenções.

**Art. 165º.** 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. 166º.** 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 (Revisão 1), de 25 de fevereiro de 2013**[62]**.**

**Art. 167º.** 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**[63].

## Capítulo XI

## DA CONFORMIDADE COM REQUISITOS LEGAIS

[62] http://dsic.planalto.gov.br/legislacao/nc_04_grsic.pdf
[63] http://dsic.planalto.gov.br/legislacao/nc_6_gcn.pdf

## Seção I

## Da Auditoria

**Art. 168º.** 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 da equipe de resposta à incidente de segurança.

**Art. 169º.** O coordenador da **COTIC** 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** e ao Gestor da Segurança da Informação.

**Art. 170º** Recomenda-se que a **Equipe de Resposta a Incidente (CSIRT)** seja indicada pelo **CSIC** e deve ser nomeada por ato do **Diretor**.

§1. Recomenda-se que a equipe seja formada apenas por servidores públicos**;** salvo quando não houver servidor com conhecimento técnico adequado para a realização da função.

§2. Recomenda-se que, cada uma das áreas técnicas do **LNCC** seja representada por um membro do **CSIRT**;

**Art. 171º** A **CSIRT** deve acompanhar os alertas de vulnerabilidades e ameaças; assim como, deve:

i. Desenvolver a normatização de reforço de segurança.

ii. Documentar e divulgar os procedimentos técnicos que apoiem as atividades técnicas relacionadas à segurança da informação.

**Art. 172º** São tarefas periódicas da **CSIRT**:

i. Analisar os alertas de integridade de dados;

ii. Analisar os registros de sistema;

iii. Analisar o relatório de varredura de vulnerabilidades;

iv. Sugerir e solicitar a aplicação da correção das vulnerabilidades constatadas;

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

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

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

**Art. 173º** Sempre que ocorrer um incidente de segurança, a CSIRT deve notificar ao responsável pelo ativo e ao gestor de segurança sobre o ocorrido.

**Parágrafo único.** As tentativas de intrusão provenientes da *Internet* também devem ser comunicadas aos respectivos centros de atendimento a incidente de segurança, como o CAIS da RNP e o CTIR Gov.

**Art. 176º** Todas as atividades da **CSIRT** devem gerar relatórios à **CSIC e o gestor de segurança**.

**Parágrafo único.** Quando solicitado pela CSIC ou pelo gestor de segurança, deve-se gerar documentação que poderá ser utilizada pela equipe técnica do **LNCC**.

**PORTARIA Nº 82/2019/SEI-LNCC de 31 de julho de 2019**

**ACOMPANHAMENTO E FISCALIZAÇÃO**

**O DIRETOR EM EXERCÍCIO DO LABORATÓRIO NACIONAL DE COMPUTAÇÃO CIENTÍFICA DO MINISTÉRIO DA CIÊNCIA, TECNOLOGIA, INOVAÇÕES E COMUNICAÇÕES**, no uso da competência que lhe foi delegada pela Portaria nº 407, de 29 de junho e 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:

**Art. 1º -** Instituir a Comissão de Acompanhamento e Fiscalização do Processo nº 01209.000280/2019-09 da empresa **PETROVERA DERIVADOS DE PETROLEO LTDA**, conforme Nota de Empenho NE nº 800271, referente contratação de empresa especializada para o fornecimento de óleo diesel, com o objetivo de abastecer os Grupos Geradores de energia deste LNCC -Laboratório Nacional de Computação Científica.

**I - GESTOR DO CONTRATO**

a) Titular: **Paulo Cabral Filho**
CPF: 636.363.607-87
Matrícula SIAPE: 672429
Lotação: SERED/COTIC

b) Suplente: **Bruno Alves Fagundes**
CPF: 095.929.227-64
Matrícula SIAPE: 2049245
Lotação: SERED/COTIC

**Art. 2º -** O Gestor do Contrato deverá observar fielmente suas atribuições previstas no artigo 67 da Lei n.º 8.666, de 21/jun/1993.

**Art. 3º -** Esta Portaria entra em vigor imediatamente independentemente da data de sua publicação no Boletim de Serviço do LNCC.

**WAGNER VIEIRA LÉO**

**REFERÊNCIA :** Processo nº 012009.000041/2017-89
**INTERESSADO: JOAQUIM LOURENÇO FERREIRA**
**ASSUNTO :** Abono de Permanência

De acordo. Autorizo a concessão do abono de permanência ao servidor **JOAQUIM LOURENÇO FERREIRA**, matrícula SIAPE n° 671832, ocupante do cargo efetivo de Assistente de Ciência e Tecnologia, Classe R, Padrão III, pertencente ao quadro deste Laboratório, a contar de 22 de janeiro de 2019, de acordo com o disposto no Artigo 2º da Emenda Constitucional nº 41/2003.

Petrópolis, 06/02/2019

**Augusto Cesar Gadelha Vieira - Diretor**

**EXTRATO DE ACORDO DE ACORDO DE COOPERAÇÃO TÉCNICA**

**PARTES:**

LABORATÓRIO NACIONAL DE COMPUTAÇÃO CIENTÍFICA (LNCC) CNPJ: 04.079.233/0001-82

UNIVERSIDADE FEDERAL FLUMINENSE (UFF) CNPJ: 28.523.215/0001-06

**OBJETO:** O presente Acordo tem por objetivo permitir ao LNCC e a UFF desenvolverem atividades de cooperação científica e tecnológica numa base de reciprocidade, com a participação em projetos de pesquisa e programas de interesse comum, com a implementação de Projetos conforme planos de Trabalho, que, uma vez aprovados pelas partes, constituirão como parte integrante deste instrumento. Data de assinatura: 12/04/2019.

**EXTRATO DE APOSTILAMENTO**

**CTIS TECNOLOGIA S/A**

Objeto: Prestação de serviço de manutenção corretiva, adaptativa e perfectiva do sistema Intranet e Internet do LNCC.

O presente Termo de Apostilamento tem por objeto equilibrar o preço anual do Contrato, passando do valor mensal de R$ 260.406,53 (duzentos e sessenta mil e quatrocentos e seis reais e cinquenta e três centavos) para R$

273.272,12 (duzentos e setenta e três mil e duzentos e setenta e dois reais e doze centavos), conforme análise financeira do LNCC (4408291) e documentação pertinente encaminhada pela empresa..

A partir de 12/04/2019, o Contrato passou do valor mensal de R$ 260.406,53 (duzentos e sessenta mil e quatrocentos e seis reais e cinquenta e três centavos) para R$ 273.272,12 (duzentos e setenta e três mil e duzentos e setenta e dois reais e doze centavos).

Ratificamos que todas as demais cláusulas e condições do Contrato ora apostilado permanecem válidas e inalteradas aquelas não expressamente modificadas por este Instrumento, que doravante passa a fazer parte integrante do Contrato para todos os fins legais e de direito.

Processo nº 01209.000169/2017-42 Contrato: 01.007.00/2018
Data da Assinatura: 06 de junho de 2018 Data da Publicação: 27 de junho de 2018
Contratante: MCTIC/Laboratório Nacional de Computação Científica LNCC
Contratada: CTIS TECNOLOGIA S/A
C.N.P.J: 01.644.731/0001-32

**EXTRATO DE APOSTILAMENTO**

**KANTRO SERVIÇOS TERCEIRIZADOS LTDA.**

C.N.P.J / MF: 01.436.782/0001-79

Objeto: Prestação dos serviços de assistência técnica operacional, de apoio e conservação da infraestrutura à gestão administrativa.

O presente Termo de Apostilamento tem por objeto equilibrar o preço mensal do presente Contrato, que passa do mensal de R$ 64.937,10 para R$ 67.127,85, a partir de 01 de junho de 2019, conforme análise financeira do LNCC (SEI4431296) e documentação pertinente encaminhada pela empresa.

Ratificamos que todas as demais cláusulas e condições do Contrato ora apostilado permanecem válidas e inalteradas aquelas não expressamente modificadas por este Instrumento, que doravante passa a fazer parte integrante do Contrato para todos os fins legais e de direito.

Processo nº 01209.00003-2015/64 Contrato: 01.015.00/2014
Data da Assinatura:22 de setembro de 2014 Data da Publicação: 02 de outubro de 2014
Contratante: MCTIC/Laboratório Nacional de Computação Científica - LNCC
Contratada: KANTRO SERVIÇOS TERCEIRIZADOS LTDA.
C.N.P.J: 01.436.782/0001-79

LNCC
www.lncc.br
Laboratório Nacional de Computação Científica

Av. Getúlio Vargas 333, Quitandinha, Petrópolis, RJ . CEP. 25651-075

**BOLETIM DE SERVIÇO N.º 007/2019 31/07/2019**

## ATOS DO SERVIÇO DE GESTÃO E DESENVOLVIMENTO DE PESSOAS

## RELAÇÃO PESSOAL AFASTADO ATIVIDADES – JULHO 2019

### AFASTAMENTOS

| LOTAÇÃO | NOME | PERÍODO | | FUNDAMENTO |
|---|---|---|---|---|
| COMAC | Fernanda Maria Pereira Raupp | 28/05/2014 | | Art. 93 |
| COMAC | Frederic Gerard Christian Valentin | 18/05/2019 | 02/08/2019 | Art. 98 |
| COMAC | Pablo Javier Blanco | 28/06/2019<br>17/07/2019 | 12/07/2019<br>08/08/2019 | Art.98 |

**No Boletim de Serviço nº 006 – JUNHO Suplementar as folhas 05 onde se lê: RELAÇÃO DOS SERVIDORES EM FÉRIAS NO MÊS DE MAIO/JUNHO 2019, leia-se RELAÇÃO DOS SERVIDORES EM FÉRIAS NO MÊS DE JULHO 2019.**

### RELAÇÃO DOS SERVIDORES EM FÉRIAS NO MÊS DE AGOSTO 2019

| NOME | EXERCÍCIO | PERÍODO | | |
|---|---|---|---|---|
| | | PARCELA | ÍNICIO | TÉRMINO |
| Antonio Tadeu Azevedo Gomes | 2019 | 2ª | 22/07/19 | 02/08/19 |
| Augusto Cesar Gadelha Vieira | 2018 | 1ª | 29/07/19 | 07/08/19 |
| Fábio Borges de Oliveira | 2019 | 1ª | 29/07/19 | 09/08/19 |
| Gilson Antonio Giraldi | 2019 | 2ª | 01/08/19 | 12/08/19 |
| Kary Ann Del Carmen Ocana Gautherot | 2019 | 3ª | 07/08/19 | 16/08/19 |
| Laurent Emmanuel Dardenne | 2019 | 1ª | 15/07/19 | 03/08/19 |
| Marcelo Dutra Fragoso | 2019 | 2ª | 23/07/19 | 11/08/19 |
| Paulo Cesar de Freitas Honorato | 2019 | 2ª | 22/07/19 | 04/08/19 |
| Sanda Mara Cardoso Malta | 2019 | 1ª | 15/08/19 | 24/08/19 |
| Simone Santana Rodrigues Elias | 2019 | 1ª | 21/07/19 | 19/08/19 |
| Anmily Paula dos Santos Martins | 2019 | 3ª | 01/08/19 | 10/08/19 |

### DIÁRIAS JULHO

| Beneficiário | Natureza | Motivo do Deslocamento | Itinerário |
|---|---|---|---|
| HANNELE TARJA RUOHOLA-BAKER (CANCELADO) | Colaborador | A pesquisadora Hannele Rouhola-Baker é professora adjunta do Departament of Biology da University of Washington e tem uma atuação extremamente expressiva na área de Biologia de sistemas. Atua na área de | São Paulo/Rio de Janeiro/São Paulo |

| | | | |
|---|---|---|---|
| | | modelagem dinâmica e diferenciação de células tronco. | |
| BENNO SCHWIKOWSKI (CANCELADO) | Colaborador | O pesquisador Benno Schwikowski é atualmente o chefe da estrutura de Biologia de Sistemas do Instituto Pasteur - Paris. O referido grupo tem sido responsável pela produção de importantes ferramentas computacionais para análise de redes biológicas, como o Cytoscape. Uma das mais populares ferramentas para análise e visualização de grafos. | São Paulo/Rio de Janeiro/São Paulo |
| JEAN-MARC CHRISTIAN SCHWARTZ | Colaborador | O professor Jean-Marc Schwartz, Senior Lecturer na University of Manchester é um antigo colaborador do LNCC, sendo a parte europeia de um acorde entre a University of Manchester e o LNCC. Sua contribuição para a área de Biologia de sistemas é notória. | São Paulo/Rio de Janeiro/São Paulo |
| WAGNER VIEIRA LEO | Servidor | Participar como expositor da EXPOTEC / 71ª SBPC em Campo Grande - MS, no período de 21 a 27/05/2019 | Rio de Janeiro/Campo Grande/ Rio de Janeiro |
| AUGUSTO CESAR GADELHA VIEIRA | Servidor | Participar como expositor na EXPOTEC / 71ª SBPC em Campo Grande - MS no período de 21 à 27/07/2019. | Rio de Janeiro/Campo Grande/ Rio de Janeiro |
| FABIO LIMA CUSTODIO | Servidor | Participar da 71ª Reunião Anual da SBPC como expositor representando o LNCC e o grupo de pesquisas GMMSB sobre o projeto DockThor. | Rio de Janeiro/Campo Grande/Rio de Janeiro |
| CARLA OSTHOFF FERREIRA DEBARROS | Servidor | Participar da 71ª Reunião Anual da Sociedade Brasileira para o Progresso da Ciência (SBPC) sediado na Universidade Federal de Mato Grosso do Sul(UFMS) | Rio de Janeiro/Campo Grande/ Rio de Janeiro |
| EMERSON CORREIA FREITAS LIMA | Colaborador | Participará da 71ª Reunião Anual da SBPC como expositor representando o LNCC e o grupo de pesquisas GMMSB sobre o projeto DockThor. | Rio de Janeiro/Campo Grande/Rio de Janeiro |

| | | | |
|---|---|---|---|
| LIGIA DE OLIVEIRA MORAIS MACHADO | Servidor | Participar da 71ª Reunião Anual da Sociedade Brasileira para o Progresso da Ciência (SBPC) sediado na Universidade Federal de Mato Grosso do Sul(UFMS | Rio de Janeiro/Campo Grande/ Rio de Janeiro |
| GENILDA MARIA MACHADO ROLI | Servidor | Participação como expositora do Laboratório Nacional de Computação Científica (LNCC) na 71ª Reunião Anual da SBPC, de 21 a 27 de julho de 2019, na Universidade Federal do Mato Grosso do Sul, em Campo Grande/MS | Rio de Janeiro/Campo Grande/ Rio de Janeiro |
| ISABELLA ALVIM GUEDES | Colaborador | A profa. Isabella Alvim Guedes participará da 71ª Reunião Anual da SBPC onde ministrará uma palestra representando o grupo de pesquisas GMMSB sobreo projeto DockThor do LNCC, coordenado pelo prof. Laurent E. Dardenne que não poderá participar do evento já que estará em férias | Rio de Janeiro/Campo Grande/ Rio de Janeiro |
| ANDERSON CHAVES DA SILVA | Colaborador | Participar da 71ª Reunião Anual da SBPC como expositor representando o LNCC e o grupo de DEXL. | Rio de Janeiro/Campo Grande/Rio de Janeiro |

LNCC
www.lncc.br
Laboratório Nacional de Computação Científica

Av. Getúlio Vargas 333, Quitandinha, Petrópolis, RJ . CEP. 25651-075

# BOLETIM DE SERVIÇO N.º 007/2019 31/07/2019