UNIVERSIDADE FEDERAL RURAL DO RIO DE JANEIRO
CONSELHO UNIVERSITÁRIO
SECRETARIA DOS ÓRGÃOS COLEGIADOS

DELIBERAÇÃO Nº 96, DE 17 DE DEZEMBRO DE 2014

O CONSELHO UNIVERSITÁRIO DA UNIVERSIDADE FEDERAL RURAL DO RIO DE JANEIRO, tendo em vista a decisão tomada em sua 308ª Reunião Ordinária, realizada em 17 de dezembro de 2014, e considerando o que consta do processo nº 23083.011077/2014-41,

R E S O L V E:

I- aprovar a "Política de Segurança da Informação e Comunicações da UFRRJ", conforme consta no Anexo I a esta deliberação;

II- aprovar o "Regimento Interno do Comitê de Segurança da Informação e Comunicações da UFRRJ", conforme consta no Anexo II a esta deliberação.

EDUARDO MENDES CALLADO
Vice-presidente no exercício da Presidência

ANEXO I À DELIBERAÇÃO Nº 96/CONSU, DE 17 DE DEZEMBRO DE 2014

Política de Segurança da Informação e Comunicações (POSIC)

1 - Objetivo

Esta Política de Segurança da Informação e Comunicações (POSIC) tem como objetivo estabelecer diretrizes para o manuseio da informação, de forma eletrônica ou não, dentro do âmbito da Universidade Federal Rural do Rio de Janeiro (UFRRJ), observando os requisitos mínimos de confidencialidade, integridade, disponibilidade e autenticidade, além do atendimento à legislação pertinente, e normas definidas pelos órgãos reguladores.

2 - Abrangência e vigência

2.1 - A Política de Segurança da Informação e Comunicações (POSIC) se aplica a todas as unidades administrativas, servidores, estudantes, prestadores de serviço autorizados, e usuários de instituições conveniadas que operam dentro da rede da UFRRJ;

2.2 - A POSIC tem prazo de validade indeterminado, portanto, sua vigência se estenderá até a edição de outro marco normativo que a atualize ou a revogue, o que deverá ocorrer em prazo não superior a três anos.

3 - Conceitos e Definições

Os conceitos e definições constantes neste item se aplicam de forma a auxiliar a interpretação da Política de Segurança da Informação e Comunicações da UFRRJ.

a) Ameaça: Conjunto de fatores ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização;

b) Ativos de informação: Os meios de armazenamento, transmissão e processamento de informação, os sistemas de informação, bem como os locais onde se encontram esses meios, as pessoas que a eles têm acesso, a imagem institucional, os serviços e tudo aquilo que tem valor para a UFRRJ e que esteja relacionado com a informação e comunicações;

c) Contas de acesso: Permissões concedidas por autoridade competente da UFRRJ após o processo de credenciamento, que habilitam determinada pessoa, sistema ou organização ao acesso;

d) Incidente de segurança: Qualquer evento adverso, confirmado ou sob suspeita, ou ocorrência que promova uma ou mais ações tendentes a comprometer ou ameaçar a disponibilidade, a integridade, confidencialidade ou a autenticidade de qualquer ativo de informação da UFRRJ;

e) Quebra de segurança: Ação ou omissão, intencional ou acidental, que resulta no comprometimento da Segurança da Informação e Comunicações da UFRRJ;

f) Segurança da Informação e Comunicações (SIC): Ações que objetivam viabilizar e assegurar a disponibilidade, integridade, confidencialidade e autenticidade das informações, abrangendo não só aspectos tecnológicos, mas também recursos humanos e processos;

g) Tecnologia da Informação (TI): Conjunto de todas as atividades e soluções providas por recursos de computação. Serve para designar o conjunto de recursos tecnológicos e computacionais para geração e uso da informação;

Este termo é comumente utilizado para designar o conjunto de recursos não humanos dedicados ao armazenamento, processamento e comunicação da informação, bem como o modo como esses recursos estão organizados em um sistema capaz de executar um conjunto de tarefas;

h) Usuário(s): Servidores, agentes públicos, terceirizados, colaboradores, consultores, auditores, estudantes, visitantes, estagiários e bolsistas que obtiveram autorização do responsável pela área interessada de acesso aos Ativos de Informação da UFRRJ, formalizada por meio da assinatura de um Termo de Responsabilidade;

i) Vulnerabilidade: Qualquer fragilidade dos sistemas computacionais e redes de computadores que permita a exploração maliciosa e acessos indesejáveis ou não autorizados. Também definida como conjunto de fatores internos ou causa potencial de um incidente indesejado, que pode resultar em risco para um ativo ou sistema e pode ser evitado por uma ação interna de SIC;

j) Dispositivos móveis: Consiste em equipamentos portáteis dotados de capacidade computacional, e dispositivos removíveis de memória para armazenamento, entre os quais se incluem, não se limitando a estes: *notebooks, netbooks, smartphones, tablets, pendrives, USB drives, HDs* externos e cartões de memória;

k) Computação em Nuvem: Modelo computacional que permite acesso por demanda, e independente da localização, a um conjunto compartilhado de recursos configuráveis de computação (rede de computadores, servidores, processamento, armazenamento, aplicativos e serviços), provisionados com esforços mínimos de gestão ou interação com o provedor de serviços;

l) Códigos maliciosos *(malware)*: são programas especificamente desenvolvidos para executar ações danosas e atividades maliciosas em um computador. Alguns tipos de *malware* são:

- **Vírus:** é um programa ou parte de um programa de computador, normalmente malicioso, que se propaga inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos;

- ***Worm*:** é um programa capaz de se propagar automaticamente pelas redes, enviando cópias de si mesmo de computador para computador;

- ***Bot*:** é um programa que dispõe de mecanismos de comunicação com o invasor que permitem que ele seja controlado remotamente (zumbi). Possui processo de infecção e

propagação similar ao do *worm*, ou seja, é capaz de se propagar automaticamente, explorando vulnerabilidades existentes em programas instalados em computadores;

- ***Botnet:*** é uma rede formada por centenas ou milhares de computadores zumbis e que permite potencializar as ações danosas executadas pelos *bots*;
- ***Spyware:*** é um programa projetado para monitorar as atividades de um sistema e enviar as informações coletadas para terceiros;

- ***Keylogger:*** *spyware* capaz de capturar e armazenar as teclas digitadas pelo usuário no teclado do computador. Sua ativação, em muitos casos, é condicionada a uma ação prévia do usuário, como o acesso a um site específico de comércio eletrônico ou de *Internet Banking;*

- ***Screenlogger:*** similar ao *keylogger*, capaz de armazenar a posição do cursor e a tela apresentada no monitor, nos momentos em que o mouse é clicado, ou a região que circunda a posição onde o mouse é clicado. É bastante utilizado por atacantes para capturar as teclas digitadas pelos usuários em teclados virtuais, disponíveis principalmente em sites de *Internet Banking;*

- ***Adware:*** projetado especificamente para apresentar propagandas. Pode ser usado para fins legítimos, quando incorporado a programas e serviços, como forma de patrocínio ou retorno financeiro para quem desenvolve programas livres ou presta serviços gratuitos. Também pode ser usado para fins maliciosos, quando as propagandas apresentadas são direcionadas, de acordo com a navegação do usuário e sem que este saiba que tal monitoramento está sendo feito;

- ***Backdoor:*** programa que permite o retorno de um invasor a um computador comprometido, por meio da inclusão de serviços criados ou modificados para este fim;

- **Cavalo de tróia *(Trojan)*:** programa que além de executar as funções para as quais foi aparentemente projetado, também executa outras funções, normalmente maliciosas, e sem o conhecimento do usuário;

- ***Rootkit:*** conjunto de programas e técnicas que permite esconder e assegurar a presença de um invasor ou de outro código malicioso em um computador comprometido.

4. Referências Legais e Normativas

4.1 - Lei nº 8.112, de 11 de dezembro de 1990, que dispõe sobre o regime jurídico dos servidores públicos civis da União, das autarquias e das fundações públicas federais;

4.2 - 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;

4.3 - Lei n° 9.983, de 14 de julho de 2000, que dispõe sobre a responsabilidade administrativa, civil e criminal de usuários que cometam irregularidades em razão do acesso a dados, informações e sistemas informatizados da Administração Pública;

4.4 - Decreto nº 4.553, de 27 de dezembro de 2002, que dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse de segurança da sociedade e do Estado, no âmbito da Administração Pública Federal, e dá outras providências;

4.5 - Decreto nº 5.482, de 30 de junho de 2005, que dispõe sobre a divulgação de dados e informações pelos órgãos e entidades da administração pública federal, por meio da Rede Mundial de Computadores (Internet);

4.6 - Instrução Normativa GSI/PR 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;

4.7 - Norma Complementar nº 07/IN01/DSIC/GSI/PR, de 06 de maio de 2010, que estabelece 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;
4.8 - Decreto nº 8.135 de 4 de novembro de 2013, que dispõe sobre as comunicações de dados da administração pública federal direta, autárquica e fundacional, e sobre a dispensa de licitação nas contratações que possam comprometer a segurança nacional.

5. Classificação da Informação e de Ativos de Informação

5.1 - É de responsabilidade dos dirigentes de setor/departamento a classificação das informações manuseadas em seu setor, observando a legislação e regulamentações pertinentes, considerando também os critérios de sigilo, valor e criticidade;

5.2 - Os servidores e demais colaboradores de cada setor devem ser orientados sobre a classificação das informações a que têm acesso, bem como os cuidados necessários no tratamento das mesmas;

5.3 - Os ativos de informação devem ser classificados em níveis de criticidade, considerando o tipo de ativo de informação, o provável impacto no caso de quebra de segurança, tomando como base a gestão de risco e a gestão de continuidade de negócios relativas aos aspectos da segurança da informação e comunicações da APF;

5.4 - Os ativos de informação classificados como sigilosos requerem procedimentos especiais de controles de acesso físico em conformidade com a legislação vigente.

6. Gestão de ativos de Informação

6.1 - A gestão dos ativos de informação deverá observar normas operacionais e procedimentos específicos, a fim de garantir sua operação segura e contínua;

6.2 - Os ativos de informação da UFRRJ deverão ser inventariados, atribuídos aos respectivos responsáveis e seu uso deve estar em conformidade com os princípios e normas operacionais de SIC e são destinados ao uso corporativo e acadêmico, sendo vedada a utilização para fins em desconformidade com os interesses institucionais;

6.3 - O usuário deve ter acesso aos ativos necessários e indispensáveis ao seu trabalho, respeitando as recomendações de sigilo de normas e legislação específica de classificação de informação;

6.4 - Os ativos de informação disponibilizados pela UFRRJ ao usuário devem ser devolvidos pelo mesmo após o seu desligamento da Instituição.

7. Cópias de segurança *(backup)*

7.1 - Deverão ser adotados procedimentos de cópias de segurança e recuperação de sistemas e dados armazenados em servidores;

7.2 - É de responsabilidade do setor de Tecnologia da Informação e Comunicações da UFRRJ os procedimentos relacionados à política de *backup*:

- Documentar, testar e avaliar regularmente as tarefas de backup;
- Aplicar testes de recuperação e validação dos backups bimestralmente;
- Alocar o servidor de *backup* em local seguro, visando à segurança, integridade e inviolabilidade dos dados;

7.3 - A política de *backups*, de acordo com o serviço, deverá ocorrer da seguinte maneira:

- Diário, nos servidores de banco de dados e de e-mail;
- Semanal do conteúdo dos demais servidores;
- Esses *backups* devem ser automáticos, e devem ocorrer preferencialmente em períodos de menor atividade na rede;

7.4 - Antes do descarte de discos e outros meios de armazenamento, deverá ser assegurado de que foi feito *backup* das informações importantes e que os mesmos sejam definitivamente destruídos, sem risco de comprometer a confidencialidade das informações da UFRRJ;

7.5 - O tempo de armazenamento das informações em *backup* deverá atender às regulamentações pertinentes e aos requisitos da área responsável pela utilização desses sistemas.

8. Controles contra *malware*

8.1 - Computadores, *notebook*s e demais equipamentos conectados à rede da UFRRJ devem utilizar sempre que possível, softwares para controle de *malware (anti-vírus)*;

8.2 - O setor de Tecnologia da Informação e Comunicações da UFRRJ será responsável pelo fornecimento, instalação e manutenção dos *softwares* para controle de *malware* nos computadores, servidores de rede, *notebooks* e demais equipamentos que sejam de propriedade da UFRRJ e que sejam compatíveis com o *software* contratado;

8.3 - O setor de Tecnologia da Informação e Comunicações da UFRRJ será responsável por minimizar a propagação na rede dos malwares identificados pelas ferramentas disponíveis e eventuais notificações por parte das entidades competentes;

8.4 - Os usuários devem ser orientados a utilizar o *software* de controle de *malware* para verificar unidades externas de armazenamento de arquivos (*pen-drives*, *cd-rom* etc) antes de sua utilização. Também devem ser verificados os arquivos recebidos por e-mail e outras modalidades de transferência de arquivos;

9. Controle de acesso à rede e sistemas

9.1 - O acesso à rede e demais sistemas da UFRRJ estará disponível a usuários previamente credenciados.

9.1.1 - Poderão ser credenciados servidores (docentes ou técnico-administrativos), estudantes, prestadores de serviço autorizados, e usuários de instituições conveniadas que operam dentro da rede da UFRRJ, observando-se a necessidade de utilização dos mesmos para a realização de suas atividades, e a respectiva autorização por parte dos responsáveis por estes sistemas;

9.2 - Para acesso aos recursos da rede corporativa da UFRRJ, o usuário deverá ser cadastrado, possuindo assim conta de acesso (usuário e senha) para efetuar o processo de *login* nos computadores disponibilizados, e consequentemente, ter acesso aos recursos de rede necessários à sua atividade profissional.

9.2.1 - O usuário deverá assinar o Termo de Responsabilidade, estando ciente, dessa forma, que será responsabilizado pela quebra de segurança ocorrida com a utilização de sua conta de acesso;

9.2.2 - Será disponibilizado ao usuário, que não exerce funções de administração da rede local, somente uma única conta institucional de acesso, pessoal e intransferível;

9.2.3 - Contas de acesso no perfil de administrador serão fornecidas somente a usuários cadastrados para execução de tarefas como configuração, instalação ou manutenção de ativos de informação;

9.2.4 - Em caso de usuário visitante, poderá ser feito o cadastro de conta de acesso para o mesmo desde que solicitado pelo responsável do setor onde realizará suas atividades, informando o prazo de validade para a conta criada.

9.3 - Será fornecida aos usuários da rede da UFRRJ conta de e-mail institucional, devendo ser utilizada pelos servidores e prestadores de serviço autorizados exclusivamente para fins corporativos, sendo vedado aos setores administrativos da UFRRJ a utilização de e-mail de outros provedores para este fim;

9.4 - Alunos terão acesso à rede sem fio disponibilizada nas áreas de estudo, além do acesso em computadores dos laboratórios de ensino, sendo necessário sua identificação através conta de acesso, definidos previamente pela área responsável pela administração da rede corporativa da UFRRJ, para acesso à internet.

9.4.1 - O acesso à rede sem fio disponibilizada em áreas de estudo também estará disponível aos demais usuários da UFRRJ, sendo necessário sua identificação através de

conta de acesso, definidos previamente pela área responsável pela administração da rede corporativa da UFRRJ, para acesso à internet;

9.4.2 - A rede sem fio disponibilizada deverá estar separada da rede corporativa, não sendo recomendada sua utilização para tráfego de informações corporativas da UFRRJ.

9.5 - A conta de acesso do usuário poderá ser bloqueada, em casos de incidentes de segurança da informação e comunicações causados pelo mesmo. A conta será restabelecida após a solução dos problemas causados e reorientação do usuário, desde que não existam outros impedimentos;

9.6 - As credenciais de acesso à rede e demais sistemas devem ser canceladas imediatamente após o desligamento do usuário da UFRRJ, devendo este cancelamento ser providenciado pelo setor responsável pelo processo de desligamento;

9.7 - Serão armazenados registros de utilização da rede *(logs)* pelo prazo mínimo de 12 meses, que permitirão a rastreabilidade e a identificação dos usuários e ativos de informação, para fins de auditoria de rede e resposta às solicitações de autoridades responsáveis pela investigação de crimes eletrônicos.

9.7.1 - Os sistemas disponibilizados pela UFRRJ na rede corporativa, deverão guardar registros de utilização *(logs)* pelo prazo estipulado acima, ou por prazo superior caso definido em legislação ou regulamentação específica.

9.8 - O acesso fornecido a instituições que utilizarem a rede da UFRRJ, será fornecido de acordo com o convênio firmado, sendo necessário definir controles que garantam a responsabilização dos seus usuários por incidentes causados, e a adoção de procedimentos favoráveis à segurança da informação e comunicações, atendendo no mínimo aos controles definidos na Política de Segurança da Informação e Comunicações da UFRRJ.

10. Controle de Acesso Físico

10.1 - Os ativos de rede devem ser protegidos contra acesso físico não autorizado;

10.2 - Em caso de intervenção técnica nos ativos de rede, o profissional que realizar o serviço deve ser identificado através de uso de crachá ou identidade funcional;

10.3 - Caso a intervenção técnica não esteja relacionada a atendimento de chamado aberto pelo usuário ou setor, a legitimidade da intervenção deve ser confirmada com o setor de Tecnologia da Informação e Comunicações da UFRRJ;

10.4 - Locais considerados críticos com relação à SIC devem possuir métodos de controle de acesso que registrem esses acessos e verifiquem a validade da autorização dos usuários, preferencialmente de forma eletrônica, através de biometria ou cartões de acesso e senha.

11. Monitoramento

11.1 - É de responsabilidade do setor de Tecnologia da Informação e Comunicações da UFRRJ monitorar o acesso à rede e sistemas para identificar problemas relativos à SIC;

11.2 - Os registros de auditoria *(logs)* devem conter as informações de monitoramento por tempo acordado para atender às regulamentações pertinentes e servir de auxílio em caso de investigações pelas autoridades competentes;

11.3 - Os registros de auditoria *(logs)* devem ser protegidos contra falsificação e acesso não autorizado;

11.4 - Os relógios de todos os sistemas e ativos de rede devem ser sincronizados de acordo com a hora oficial.

12. Penalidades

12.1 - O descumprimento ou violação, pelo usuário, das regras previstas na Política de Segurança da Informação e Comunicações (POSIC) poderá resultar na aplicação das sanções previstas em regulamentações internas e legislação em vigor;

12.2 - O usuário responderá disciplinarmente e/ou civilmente pelo prejuízo que vier a ocasionar à UFRRJ, podendo culminar em abertura de Processo Administrativo Disciplinar e eventuais processos criminais, se aplicáveis.

ANEXO II À DELIBERAÇÃO Nº 96/CONSU, DE 17 DE DEZEMBRO DE 2014

REGIMENTO INTERNO DO COMITÊ DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES DA UFRRJ

CAPÍTULO I
DA CATEGORIA E FINALIDADE

Art. 1º O COMITÊ DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES da UFRRJ (CSIC/UFRRJ) possui suas atribuições e incumbências definidas no Art. 3º da Deliberação 009 do Conselho Universitário, de 30 de março de 2011.

I – assessorar na implementação das ações de segurança da informação e comunicações;
II – constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação e comunicações;
III – propor alteração na Política de Segurança da Informação e Comunicações;
IV – propor normas relativas à segurança da informação e comunicações.

CAPÍTULO II
DA ORGANIZAÇÃO DO COMITÊ DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES DA UFRRJ

Seção I
Da Composição

Art. 2º O COMITÊ DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES funcionará nos termos do Art. 4º da Deliberação 009 do Conselho Universitário, de 30 de março de 2011. Terá um representante de cada uma das seguintes unidades organizacionais:

I – Assessoria Especial da Reitoria;
II – Coordenadoria de Informática (COINFO);
III – Assessoria de Comunicação (ASCOM);
IV – Divisão de Guarda e Vigilância (DGV);
V – Representante da Câmara de Pesquisa e Pós-Graduação;
VI – Representante da Câmara de Graduação;
VII – Representante da Câmara de Extensão;
VIII – Auditoria Interna (AUDIN).

Seção II
Do Funcionamento

Art. 3º A Coordenação do COMITÊ DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES da UFRRJ será exercida pelo Gestor de Segurança da Informação e

Comunicações, nomeado pelo Reitor da UFRRJ. Possui suas atribuições definidas no Art. 2º da Deliberação 009 do Conselho Universitário, de 30 de março de 2011.

I – promover cultura e segurança da informação e comunicações;
II – acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;
III – propor recursos necessários às ações de segurança da informação e comunicações;
IV – coordenar o Comitê de Segurança da Informação e Comunicações e a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETRIRC);
V – realizar e acompanhar estudos de novas tecnologias, quanto a possíveis impactos na segurança da informação e comunicações;
VI – manter contato direto com o DSIC (Departamento de Segurança da Informação e Comunicações) para o trato de assuntos relativos à segurança da informação e comunicações;
VII – propor normas relativas à segurança da informação e comunicações.

Art. 4º O COMITÊ DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES CSIC/UFRRJ reunir-se-á, ordinariamente, uma vez por mês, no Campus Seropédica, e extraordinariamente por convocação de seu Coordenador.

§ 1º Deverá ser observado, para a convocação de reunião extraordinária, o prazo mínimo de dois dias úteis de antecedência em relação à data de sua realização, a qual, para ser subscrita pelos membros do Comitê, deverá conter a pauta a ser tratada.

§ 2º As reuniões do Comitê serão instaladas com a presença de, no mínimo, cinco membros, dentre eles o Coordenador.

§ 3º As reuniões terão sua pauta preparada pelo Coordenador do Comitê, em consonância com as matérias encaminhadas pelos demais membros.

§ 4º As pautas das reuniões juntamente com documentos técnicos de referência, e demais documentos para apreciação, quando for o caso, serão encaminhadas aos membros do Comitê, preferencialmente através de e-mail, respeitados os seguintes prazos mínimos de antecedência em relação à data de realização das reuniões:

I – Cinco dias úteis para os temas de pauta de reuniões ordinárias;
II – Dois dias úteis para convocação de reuniões extraordinárias.

Art. 5º Os trabalhos durante as reuniões terão a seguinte sequência:

I - instalação:
a) verificação de presença e de existência de quórum para instalação;

II - expediente:
a) aprovação da ata da reunião anterior;
b) apresentação e discussão das matérias;

c) considerações dos membros;
d) elaboração de documento para apreciação do CTIC/UFRRJ, quando houver demanda;
e) definição de atividades futuras;
f) encerramento.

Art. 6º Por aprovação do Comitê ou indicação de seu Coordenador poderão ser convidados a participar das reuniões outros servidores, empregados ou representantes de empresas que possam contribuir para o esclarecimento das matérias a serem apreciadas.

Art. 7º As decisões serão tomadas por maioria simples dos membros presentes, observado o quórum exigido para a realização das reuniões, § 2º do Art. 4º deste Regimento.

Parágrafo único – Em caso de empate, o Coordenador do Comitê dará o voto de decisão.

Seção III
Das Atribuições dos Membros do Comitê

Art. 8º. Aos membros do CSIC/UFRRJ incumbe:

I - encaminhar matérias e minuta de documentos para análise e posterior encaminhamento à apreciação do CTIC/UFRRJ;
II - propor ao Coordenador a convocação de reuniões extraordinárias;
III – propor ao Coordenador, em caso de urgência ou relevância, alteração da pauta da reunião;
IV - debater a matéria em discussão;
V - assinar os documentos a serem encaminhados ao CTIC/UFRRJ;
VI - sugerir servidores, empregados ou representantes de empresas que possam contribuir para esclarecimento das matérias em discussão no Comitê;
VII - assinar os documentos gerados pelo Comitê;
VIII - propor as datas para realização das reuniões ordinárias.

Art. 9º. Ao Coordenador do CSIC/UFRRJ incumbe:

I - convocar e coordenar as reuniões do Comitê, observado o disposto no art. 8;
II - aprovar a pauta da reunião;
III - propor, em caso de urgência ou relevância, alteração da pauta da reunião;
IV - ordenar o uso da palavra;
V - manter a dinâmica das reuniões, organizando os debates e a apreciação das matérias;
VI - assinar os documentos a serem encaminhados à apreciação do CTIC/UFRRJ;
VII - indicar servidores, empregados ou representantes de empresas que possam contribuir para esclarecimento das matérias em discussão no Comitê;
VIII - Definir as datas para realização das reuniões ordinárias;
IX - Realizar a convocação das reuniões extraordinárias nos termos dispostos nesse regimento.

CAPÍTULO III
DAS DISPOSIÇÕES FINAIS

Art. 10. O presente Regimento Interno poderá ser alterado mediante aprovação de seus membros em reunião extraordinária convocada especificamente para este fim, com quórum mínimo de 5 membros, além do coordenador.

Art. 11. Este Regimento, após aprovado pelo CONSU, entra em vigor a partir da data de sua publicação.