Institui a Política de Segurança da Informação (POSIC) no âmbito do Junta Comercial do Estado do Rio de Janeiro

O PRESIDENTE DA JUNTA COMERCIAL DO ESTADO DO RIO DE JANEIRO – JUCERJA, no exercício das suas atribuições que lhes conferem o Regimento Interno, aprovado pelo Decreto Estadual Nº 48.123 de 08 de junho de 2022, e tendo em vista o disposto na Instrução Normativa PRODERJ/PRE Nº 02 DE 28 DE ABRIL DE 2022,

CONSIDERANDO:

- a Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) e sua regulamentação pelo Decreto nº 43.597, de 17 de maio de 2012;

- a Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais);

- a Portaria PRODERJ/PRE Nº 825, de 26 de fevereiro de 2021, que institui a Estratégia da Governança de Tecnologia da Informação e Comunicação do Estado do Rio de Janeiro – EGTIC/RJ, notadamente o art. 1º, IV, que prevê a instituição de Instruções Normativas para a efetivação da Governança de Tecnologia da Informação e Comunicação no Estado do Rio de Janeiro, bem como o art. 11, do Anexo B, que trata de ações de governança voltadas à segurança da informação e à proteção de dados;

R E S O L V E M:

Art. 1º Fica instituída a Política de Segurança da Informação (POSIC) no âmbito do Junta Comercial do Estado do Rio de Janeiro.

CAPÍTULO I

DO ESCOPO

Art. 2º A Política de Segurança da Informação provê as diretrizes, princípios, competências e responsabilidades necessárias a viabilizar a Gestão de Segurança da Informação (GSI) na JUCERJA, visando assegurar a disponibilidade, integridade, confidencialidade e autenticidade das informações produzidas, transmitidas e custodiadas pelos sistemas de informação no âmbito do JUCERJA.

Parágrafo único. A POSIC é aplicável à toda a Instituição, devendo ser observada por todos os servidores, colaboradores, fornecedores, prestadores de serviço e por aqueles que, de alguma forma, executem atividades voltadas à atuação institucional da JUCERJA.

CAPÍTULO II

DOS CONCEITOS E DEFINIÇÕES

Art. 3º Para efeitos desta Política são estabelecidos os seguintes conceitos e definições:

I – **Ameaça**: conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou para o JUCERJA;

II – **Atividades Críticas**: atividades que devem ser executadas para garantir a prestação de serviços fundamentais da JUCERJA;

III – **Ativo de Informação**: recurso utilizado na produção, processamento, armazenamento, transmissão e recuperação da informação, incluindo a própria informação, sistemas de informação, locais onde se encontram esses meios e as pessoas que a eles têm acesso;

IV – **Autenticidade**: propriedade pela qual se assegura a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, equipamento, sistema, órgão ou entidade;

V – **Celeridade**: as ações relacionadas à segurança da informação deverão oferecer respostas ágeis para os incidentes e para as vulnerabilidades identificadas nos sistemas de informação da JUCERJA;

VI –**Superintendência de Informática** (SIF): trata-se da superintendência da JUCERJA responsável pela área de Tecnologia da Informação;

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

VIII – **Confidencialidade**: propriedade pela qual se assegura que a informação não esteja disponível ou não seja revelada a pessoa, a sistema, a órgão ou a entidade não autorizados nem credenciados;

IX – **Disponibilidade**: propriedade pela qual se assegura que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade devidamente autorizados;

X – **Dispositivos Móveis**: 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;

XI - **Gestor da Informação**: Gestor máximo de unidade organizacional, responsável pela administração de informações geradas em seu processo de trabalho e/ou sistemas de informação relacionados às suas atividades institucionais;

XII – **Gestor de Segurança da Informação**: responsável pelas ações de segurança da informação no âmbito da JUCERJA;

XIII – **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 autenticidade de qualquer ativo de informação da JUCERJA;

XIV – **Integridade**: propriedade pela qual se assegura que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

XV – **Quebra de Segurança**: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação;

XVI – **Recursos computacionais**: recursos que processam, armazenam e/ou transmitem informações, tais como aplicações, sistema de informação, estações de trabalho, notebooks, servidores de rede, equipamentos de conectividade e infraestrutura;

XVII – **Redes sociais**: estruturas sociais digitas compostas por pessoas ou organizações conectadas por um ou vários tipos de relações, que partilham valores e objetivos comuns;

XVIII – **Segurança da Informação (SI)**: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações em recursos de tecnologia da Informação;

XIX – **Tecnologia da Informação e Comunicações (TIC)**: ativo estratégico que apoia processos de negócios institucionais, mediante a conjugação de recursos, processos e técnicas utilizados para obter, processar, armazenar, disseminar e fazer uso de informações;

XX – **Usuário**: pessoa física, seja servidor ou equiparado, empregado ou prestador de serviços, habilitada pela administração para acessar os ativos de informação de um órgão ou entidade, formalizada por meio da ciência e aceita do Termo de Confidencialidade;

XXI – **Vulnerabilidade**: conjunto de fatores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para um sistema ou por uma organização, os quais podem ser evitados por uma ação interna de segurança da informação.

CAPÍTULO III

DOS PRINCÍPIOS

Art. 4º A POSIC deve obedecer aos seguintes princípios:

I o interesse público
II a preservação e a defesa do patrimônio público;
III a legalidade
IV a impessoalidade
V a moralidade
VI a transparência
VII a honestidade
VIII a integridade
IX a disponibilidade
X a publicidade
XI a autenticidade
XII a confidencialidade
XIII a responsabilidade
XIV o não-repúdio e
XV a prevenção

§ 1° Os bens de TIC cuja propriedade pertença a JUCERJA ou em nome dela tenham sido disponibilizados aos usuários são de livre acesso à SIF, sem necessidade de autorização ou ciência previa do usuário.

§ 2° As políticas, as normas e os procedimentos deverão ser atualizados, sempre que ocorrerem mudanças legais, sociais ou tecnológicas que venham a interferir na sua aplicabilidade no âmbito da JUCERJA.

§ 3° As atividades de SI levarão em consideração as atribuições regimentais, bem como as leis, normas e políticas organizacionais, administrativas, técnicas e operacionais da JUCERJA.

§ 4° O nível, a complexidade e os custos das ações de segurança da informação serão adequados ao atendimento administrativo e ao valor do ativo a se proteger.

CAPÍTULO IV

DAS DIRETRIZES GERAIS

Art. 5° A Gestão de Segurança da Informação (GSI) compreende ações e métodos ações e métodos que visam à integração das atividades de SI aos processos institucionais estratégicos, táticos e operacionais.

§1° Todos os sistemas, serviços e recursos computacionais estão sujeitos a monitoramento, controle de acesso e auditoria.

§ 2° As informações e registros obtidos pelo desenvolvimento das atividades da GSI poderão ser utilizados pela detecção de violações da POSIC e normas vigentes.

§ 3° A JUCERJA deverá adotar cláusulas de segurança da informação nos contratos com terceiros, de forma a resguardar o sigilo e a confidencialidade de toda e qualquer informação constante nos seus ativos tecnológicos, com as quais os prestadores de serviços venham a ter contato.

Art. 6° A presente POSIC apresenta diretrizes gerais sobre as seguintes disciplinas, assim como as regulamenta, conforme seus anexos:

I Tratamento da Informação;

II Controle de Acesso;

III Uso de E-mail Institucional;

IV Acesso à Internet

V Gestão de Recursos Computacionais e Uso de Dispositivos Móveis;

VI Uso de Software; e

VII Uso de Computação em Nuvem

Parágrafo único. Serão fixadas em normas complementares os procedimentos próprios e as diretrizes específicas para as seguintes disciplinas:

a) Tratamento e resposta a Incidentes de Rede;
b) Gestão de Riscos de SI;
c) Gestão de Continuidade de Negócios em SI;
d) Auditoria e Conformidade;
e) Serviço de Cópia de Segurança (backup);

Seção I

Do tratamento da Informação

Art. 7° Os ativos de informação serão protegidos contra ameaças e ações não autorizadas, acidentais ou não, com o objetivo de reduzir riscos e de garantir a disponibilidade, integridade, confidencialidade e autenticidade desses bens.

Parágrafo único. É vedado ao usuário o acesso a ativos de informação e sistemas que não tenha sido expressamente autorizado pelo Gestor da Informação.

Art. 8° Os documentos eletrônicos considerados imprescindíveis para as atividades da JUCERJA deverão ser armazenados nos sistemas de informação ou nos servidores de arquivos disponibilizados pela SIF.

Parágrafo único. A destruição de documentos eletrônicos deverá observar a sua classificação, adotando procedimentos de segurança que inviabilizem eventual recuperação e acesso não autorizado.

Art. 9° As informações criadas, armazenadas, manuseadas, transportadas ou descartadas na JUCERJA deverão ser classificadas segundo o grau de sigilo, quando necessário, e protegidas segundo a sua criticidade e outros critérios, conforme as normas e a legislação em vigor.

§ 1° As informações públicas a que se refere este artigo serão adequadamente disponibilizadas à sociedade por mecanismos próprios de transparência previstos na Lei de Acesso à Informação e em suas regulamentações infralegais.

§ 2° As informações pessoais e sigilosas geradas ou mantidas pela JUCERJA serão objeto de tratamento e proteção que lhes garantam a inviolabilidade.

Seção II

Do Tratamento e Resposta a Incidentes de Rede

Art. 10. As ocorrências de incidentes de segurança em redes computacionais, no âmbito da JUCERJA, deverão ser registradas com a finalidade de assegurar a manutenção de histórico das atividades desenvolvidas.

Seção III

Da Gestão de Riscos de Segurança da Informação

Art. 11. A Gestão de Riscos de SI deverá considerar, prioritariamente, a Política de Gestão de Riscos os objetivos estratégicos, os processos, os requisitos legais e a estrutura organizacional do JUCERJA.

§ 1° A Gestão de Riscos de Segurança da informação deverá identificar e implementar as medidas de proteção necessárias para o tratamento dos riscos.

§ 2° Deverá ser considerado o equilíbrio entre as medidas de proteção referidas no parágrafo precedente e os custos operacionais e financeiros envolvidos, evitando que as ameaças, de origem natural ou humana, de forma acidental ou não, explorem as vulnerabilidades dos ativos de informação e provoquem danos pela destruição não autorizada, revelação indevida, adulteração ou perda das informações da JUCERJA.

Seção IV

Da Gestão de Negócios em Segurança da Informação

Art. 12. A Gestão de Continuidade de Negócios em Segurança da Informação tem como finalidade evitar que os serviços institucionais, baseados em TIC, sejam interrompidos e, quando for o caso, assegurar o seu restabelecimento no tempo necessário.

Parágrafo único. A JUCERJA deverá definir quais são suas atividades críticas, com o objetivo de subsidiar a elaboração do Programa de Gestão de Continuidade de Negócios.

Seção V

Da Auditoria e Conformidade

Art. 13. A SIF deverá manter registros, como trilhas de auditoria que possibilitem a análise de conformidade através do rastreamento, monitoramento, controle e verificação de acessos aos sistemas e atividades críticas de TIC da JUCERJA.

Parágrafo único. A análise de conformidade será realizada de forma contínua – utilizando técnicas como entrevistas ou testes de invasão -, identificando possíveis violações às legislações pertinentes.

Seção VI

Dos Controles de Acesso

Art. 14. O controle de acesso físico tem como finalidade proteger os equipamentos, documentos e suprimentos contra ameaças e ações não autorizadas, acidentais ou não, com o objetivo de reduzir os riscos e de garantir a disponibilidade, integridade, confidencialidade e autenticidade desses bens.

Parágrafo único: O controle de acesso físico ao Data Center da JUCERJA está regulamentado no anexo I

Art. 15. O controle de acesso lógico tem como finalidade proteger os sistemas de informação e demais ativos de informação contra ameaças e ações não autorizadas, acidentais ou não, com o objetivo de reduzir os riscos e de garantir a disponibilidade, integridade, confidencialidade e autenticidade desses bens.

Art. 16. Os controles de acessos lógicos deverão observar o princípio da proporcionalidade, restringindo o conjunto de privilégios ao mínimo necessário para o desempenho das atribuições profissionais do usuário.

§ 1° Todo usuário receberá acessos com privilégios mínimos necessários ao desempenho das atribuições para as quais for designado.

§ 2° Situações excepcionais de acessos diferenciados deverão ser motivadas pelos gestores da informação, por tempo certo, na forma de regulamentação específica dessa disciplina.

§ 3° É reponsabilidade da unidade de Recursos Humanos informar a SIF o desligamento de qualquer servidor, colaborador, estagiário e outros, assim como as nomeações e exonerações para exercício de funções comissionadas ou de chefia para que sejam adotadas as providências de cancelamento dos acessos físicos e lógicos.

§ 4° Somente a Presidência poderá autorizar acesso a VPN e, excepcionalmente a SIF, desde que com prévia autorização da Presidência.

§ 5° A SIF disponibilizará ferramenta computacional ou e-mail para solicitações de acesso e/ou alteração de nível de acesso.

Secção VII

Do Uso do E-mail Institucional

Art. 17. A criação de contas de e-mail institucional necessita de solicitação, com validação e autorização da chefia imediata, demonstrando a necessidade desse serviço para o desempenho das atribuições profissionais de cada usuário.

Parágrafo único: O uso de e-mail institucional está regulamentado no anexo II.

Art. 18. A SIF deverá adotar mecanismos para reduzir o recebimento e o envio de mensagens indesejadas (SPAM ou Phishing) que representem risco ou estejam em desconformidade com os normativos vigentes.

Seção VIII

Do Acesso à Internet e rede

Art. 19. O acesso à Internet concedido aos usuários deverá observar o princípio da proporcionalidade, restringindo o perfil de acesso ao mínimo necessário para o desempenho das atribuições profissionais do usuário.

§ 1°. Situações excepcionais de acessos diferenciados deverão ser motivadas pelos gestores da informação, por tempo certo, na forma de regulamentação específica dessa disciplina.

§ 2°. O acesso à Internet e a rede está regulamentado no anexo III.

Art. 20. Os perfis institucionais em propriedades digitais deverão ser administrados e gerenciados pela Assessoria de Comunicação, segundo as diretrizes previstas na Política da JUCERJA e nas normas editadas.

Seção IX

Do Serviço de Cópia de Segurança

Art. 21. Todo ativo de informação corporativa deverá ser considerado para inclusão na política de cópia de segurança, observando-se os requisitos legais e a criticidade das informações relacionadas às atividades da JUCERJA.

§ 1°. Considera-se ativo de informação corporativa todos os dados armazenados, sistemas de informação, pastas de rede e arquivos digitalizados armazenados e /ou hospedados no Data Center da JUCERJA.

§ 2°. O serviço de cópia de segurança não tem amplitude sobre os dados e/ou informações armazenadas fora do Data Center.

§ 3°. O armazenamento e guarda de ativos de informações corporativas deverá ser realizado exclusivamente nas pastas de rede disponibilizadas às unidades da Instituição.

§ 4°. As cópias de segurança das informações e/ou dados armazenados fora do Data Center são de responsabilidade exclusiva do usuário.

Seção X

Da Gestão de Recursos Computacionais e Do Uso de Dispositivos Móveis

Art. 22. A gestão de recursos computacionais e o uso de dispositivo móveis deverá ser pautada por comportamento ético e profissional, observando as determinações da POSIC e normativos vigentes.

§ 1°. O uso de dispositivos móveis de propriedade do usuário somente será permitido nos sistemas ou serviços homologados e/ou autorizados pela SIF.

§ 2°. A utilização de dispositivos móveis, notebooks e outros equipamentos de propriedade do usuário nas redes da JUCERJA, deverá ser previamente autorizada pela SIF, mediante solicitação da chefia imediata do usuário, justificando a necessidade do serviço.

Seção XI

Do uso de Software

Art. 23. A instalação e a configuração de softwares pertencentes a JUCERJA ou de versões de testes e/ou gratuitas nos recursos computacionais e dispositivos móveis institucionais, deverão ser realizadas pela SIF, que se responsabilizará pela guarda das mídias e sua eventual desinstalação.

§ 1°. Para garantir a SI, todo software deverá ser previamente homologado pela SIF antes de sua utilização no ambiente da JUCERJA.

§ 2°. independente do perfil de acesso do usuário, somente a SIF poderá instalar softwares nos recursos computacionais e dispositivos móveis institucionais.

Seção XII

Do Uso de Computadores em Nuvem

Art. 24. O ambiente de computação em nuvem, sua infraestrutura e canal de comunicação devem possibilitar que todas as garantias legais atribuídas a JUCERJA sejam respeitadas.

Seção XIII

Do Uso da Internet WiFi

Art. 25. A rede WiFi corporativa é para uso exclusivo dos recursos computacionais e dispositivos móveis institucionais com a finalidade de apoiar e viabilizar atividades relacionadas aos serviços institucionais.

§ 1°. Acessos pessoais ou em recursos computacionais e dispositivos móveis que não sejam caraterizados como institucionais, com finalidades estranhas aos serviços da JUCERJA, somente poderão ser realizados pela rede WiFi para "visitantes".

§ 2°. O uso da Internet na rede WiFi está regulamentado no anexo IV.

CAPÍTULO V

DAS COMPETÊNCIAS E RESPONSABILIDADES

Art. 26. O Gestor de Segurança da Informação será designado pelo Presidente da JUCERJA dentre os servidores públicos ocupantes de cargos efetivos ou em comissão, desde que lotados na Instituição e com formação ou capacitação técnica compatível às suas atribuições e, terá as seguintes competências:

I- Promover a cultura de segurança da informação;
II- Acompanhar as investigações e as avaliações dos danos decorrentes de quebras de SI executadas;
III- Propor à autoridade máxima da JUCERJA os recursos necessários às ações de SI,
IV- Acompanhar estudos de novas tecnologias, quanto a possíveis impactos na SI;
V- Propor normas e procedimentos relativos à SI.

§1° A promoção de cultura da SI a que se refere o inciso I será atendida mediante campanhas de conscientização, palestras e treinamentos, assim como Interlocução permanente com a Presidência para garantir que os usuários tomem conhecimento da POSIC e assinem o Termo de Confidencialidade, constante o Anexo V, no ato da admissão.

Art. 27. O Responsável pelo Tratamento e Resposta a Incidentes será nomeado pelo Presidente da JUCERJA e a ele compete:

I - monitorar os recursos de TIC, detectar e realizar as análises dos incidentes de segurança da informação;

II - reportar ao Encarregado pelo Tratamento de Dados Pessoais os incidentes envolvendo tais dados;

III - identificar vulnerabilidades;

IV - receber e propor respostas a notificações relacionadas a incidentes de segurança da informação; e

V - coordenar e executar atividades de tratamento e resposta a eventos de segurança da informação.

Parágrafo único. O Responsável pelo Tratamento e Resposta a Incidentes será designado dentre os servidores desta autarquia ocupantes de cargos efetivos ou em comissão, desde que com formação ou capacitação técnica compatível às suas atribuições e, excepcionalmente, por indicação do GSI.

Art. 28. O Encarregado pelo Tratamento de Dados Pessoais será nomeado pelo Presidente da JUCERJA e ele compete:

I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;

II - receber comunicações da Autoridade Nacional de Proteção de Dados - ANPD e adotar providências;

III - orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais;

IV - executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares;

V - requerer relatório das áreas responsáveis por tratamento de dados pessoais no âmbito dos órgãos administrativos contendo, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados;

e VI - atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD), na forma da Lei nº 13.709/2018.

Art. 29. Aos usuários compete:

I- Utilizar os recursos de TIC da JUCERJA exclusivamente para atividades relacionadas com suas atribuições funcionais;

II- Responsabilizar-se pelas informações armazenadas na estação de trabalho e nos demais dispositivos móveis que utilizar para desempenho de suas funções; e

III- Armazenar informações estritamente corporativas no servidor de arquivos disponibilizados para sua unidade de lotação, respeitando o processo de controle de acesso regulamentado pela SIF.

IV- Não armazenar informações que não sejam estritamente corporativas no servidor de arquivos disponibilizado para sua unidade de lotação, respeitando o processo de controle de acesso regulamentado pela SIF.

Parágrafo único. É obrigatória a assinatura por todo usuário do Termo de Confidencialidade, constante do Anexo V, sobretudo para as concessões de primeiro acesso.

CAPÍTULO VI

DAS PENALIDADES

Art.30. O descumprimento de um ou mais itens da POSIC sujeita o infrator à aplicação de sanções administrativas, penais ou civis previstas na legislação vigente.

§ 1° Sempre que instada, a JUCERJA deverá cooperar ativamente com as autoridades competentes na apuração de possível prática de atividade ilícita realizada através dos seus recursos computacionais ou por usuário do Instituto.

§ 2° O usuário que tomar ciência de qualquer violação desta POSIC deverá comunicá-la à SIF, que será a responsável pela análise preliminar da infração, pelas medidas de restrição de acesso cabíveis e pelo eventual encaminhamento aos órgãos de apuração competentes.

CAPÍTULO VII

DA ATUALIZAÇÃO

Art. 31. A Política de Segurança da Informação deverá ser revisada ou ratificada sempre que se fizer necessário, não excedendo o período máximo de 3 (três) anos.

CAPÍTULO VIII

DAS CONTRATOS DE PRESTAÇÃO DE SERVIÇOS

Art. 32. Os contratos de prestação de serviços e demais ajustes celebrados pela JUCERJA deverão dispor de cláusula específica sobre a obrigatoriedade do cumprimento da presente Norma, bem como das penalidades decorrentes da sua inobservância.

§ 1° Os gestores dos contratos novos, em ato contínuo a assinatura, deverão assegurar que todos os colaboradores alocados na Instituição assinem os Termos de Confidencialidade (Anexo V) e os insira nos respectivos processos administrativos;

§ 2° Os contratos em vigor na data de publicação desta Norma deverão, oportunamente, quando aditados, incluir no respectivo Termo Aditivo, cláusula específica sobre a obrigatoriedade do cumprimento da presente Norma, bem como das penalidades decorrentes da sua inobservância.

I – Cabe aos fiscais de contratos, independente de aditamento:

a) providenciar o recolhimento da assinatura do Termo de Confidencialidade (Anexo V) de todos os colaboradores alocados na Instituição, assim como a juntada dos documentos no respectivo processo administrativo;

b) informar à SIF, imediatamente, sobre desligamentos e/ou substituições de colaboradores para fins de revogação de permissões de acesso e bloqueio de contas de e-mails.

c) No encerramento dos contratos, informar à SIF, imediatamente, sobre desligamentos e/ou substituições de colaboradores para fins de revogação de permissões de acesso e bloqueio de contas de e-mails.

§ 3° No que tange aos estagiários, cabe a unidade de Recursos Humanos:

a) Providenciar o recolhimento da assinatura do Termo de Confidencialidade (Anexo V) de todos os novos colaboradores alocados na Instituição, assim como promover o devido registro;

b) informar à SIF, imediatamente, sobre desligamentos e/ou substituições de colaboradores para fins de revogação de permissões de acesso e bloqueio de contas de e-mails.

CAPÍTULO IX

DISPOSIÇÕES FINAIS

Art. 33. A elaboração da POSIC adotou por referência o disposto na legislação e normatização elencada no preâmbulo.

Art. 34. Os casos omissos e as dúvidas sugeridas na aplicação desta Política serão dirimidos pelo Presidente da JUCERJA.

Art. 35. Esta portaria entra em vigor na data de sua publicação.

ANEXO I

Segurança de acesso físico ao Data Center

O presente regulamento estabelece normas e procedimentos específicos para entrada no Data Center da JUCERJA.

Art. 1º – Para os efeitos desta Norma são estabelecidos os seguintes conceitos e definições:

I – Data Center da JUCERJA: Local onde estão concentrados os equipamentos responsáveis pelo processamento e armazenamento de dados, responsáveis pela hospedagem e funcionamento dos sistemas e bancos de dados corporativos, cruciais para o negócio da instituição;

II – Horário Comercial**:** Período compreendido entre 08:00h e 18:00h dos dias úteis.

III – Sala-Segura**:** Local específico onde está localizado o Data Center da JUCERJA. A Sala-Segura da JUCERJA é um ambiente que protege o *Data Center* contra calor, umidade e acesso indevido;

IV – O ambiente da Sala-Segura é composto pelas seguintes áreas:

- Acesso – Único pela entrada principal
- Saída alternativa de emergência – Acesso ao corredor interno do prédio.
- Sala do Data Center:

IV – Autorização formal: Autorização por escrito, via e-mail ou memorando.

Art. 2° – Em horário comercial, o acesso ao ambiente da Sala-Segura somente será realizado pelas pessoas credenciadas e autorizadas pela Superintendência de Informática - SIF.

Art. 3° – Fora do horário comercial, fins de semana e feriados, o acesso ao ambiente da Sala-Segura somente será realizado para manutenções preventivas agendadas ou ações corretivas emergenciais, por pessoas credenciadas e autorizadas pela Superintendência de Informática - SIF.

Art. 4° – Quando autorizado o acesso ao ambiente da Sala-Segura, a liberação de acesso será feita formalmente junto a Vigilância da JUCERJA e, dependendo da necessidade e conveniência, para acompanhamento de procedimentos e/ou atividades, sempre com o acompanhamento de um membro da equipe de infraestrutura da SIF previamente credenciado.

Art. 5° – Os membros da equipe de infraestrutura da SIF previamente credenciados terão livre acesso ao ambiente, sem prejuízo da identificação e registros pelos agentes de vigilância da JUCERJA.

§ 1° A Vigilância deverá manter registro de todos os acessos à Sala-Segura, no qual conste horário de entrada, identificação da pessoa e horário de saída, assim como relacionar todo e qualquer material que entrar ou sair das dependências da Sala-Segura;

§ 2° Não é permitida a entrada e ou a saída de peças, equipamentos e acessórios da Sala-Segura sem o prévio conhecimento e autorização da Superintendência de Informática - SIF;

§ 3° Não é permitida a entrada com qualquer tipo de bebida ou alimento na Sala-Segura.

Art. 6° – Todas as entradas na Sala-Segura deverão ser registradas no livro de ocorrências,descrevendo o motivo da entrada e tarefas executadas, ficando este sob guarda da vigilância da JUCERJA, disponível a área de infraestrutura da Superintendência de Informática - SIF.

Art. 7° – É de competência da Área de Infraestrutura a geração de relatórios sobre qualquer ocorrência na Sala-Segura, ou sempre que solicitado pela Administração da JUCERJA.

Art. 8° – Para os casos de intervenções e serviços na Sala-Segura por equipes de manutenção e/ou por equipes de prestação de serviços contratadas para intervenções pontuais e/ou programadas pela JUCERJA, o acesso também deverá seguir o mesmo fluxo de autorização e validação exposto acima.

Art. 9° – Todos os serviços de engenharia e manutenção a serem realizados no ambiente da Sala-Segura deverão ser previamente agendados e comunicados à SIF com antecedência mínima de uma semana, sendo necessário identificar a empresa e o(s) profissional(s) que realizará(ão) o(s) serviço(s).

§ Único - Manutenções e/ou intervenções emergenciais de engenharia (Civil, elétrica, hidráulica e de refrigeração), fora dos dias e horários de expediente normal, poderão ser realizadas sem prejuízo do acompanhamento dos serviços pela equipe de vigilância da JUCERJA, até que um membro da equipe da SIF chegue ao local.

Art. 10º – As dúvidas e os casos omissos serão resolvidos pelo Presidente, mediante proposta do Superintendente de Informática.

ANEXO II

Uso do e-mail corporativo

O presente regulamento estabelece normas e procedimentos específicos para uso do e-mail corporativo.

Art. 1º A disponibilização do serviço de correio eletrônico corporativo da Junta Comercial do Estado do Rio de Janeiro, por meio da Superintendência de Informática, bem como sua utilização pelos usuários, devem observar o disposto nesta Norma.

Art. 2º O serviço de correio eletrônico tem como finalidade o envio e o recebimento eletrônico de mensagens e documentos relacionados com as funções institucionais da JUCERJA, como instrumento de intercâmbio de ideias e informações, racionalização do trabalho, de forma a promover o aumento de produtividade.

Parágrafo único. É admitida a utilização do correio eletrônico institucional para fins pessoais, dentro dos limites da ética, do bom senso e da razoabilidade, e desde que sem prejuízo ao serviço, atendidos ainda os demais requisitos estabelecidos nesta Norma.

Art. 3º São usuários do serviço de correio eletrônico corporativo os colaboradores e servidores da JUCERJA, seus órgãos e unidades, os estagiários e os demais agentes públicos ou particulares que oficialmente executem atividade vinculada à atuação institucional da JUCERJA.

§ 1º A concessão da utilização de contas de correio eletrônico, na última hipótese referida no caput, depende de pedido fundamentado da autoridade responsável pela respectiva área, demonstrando a necessidade para a Instituição da utilização do serviço pelo agente.

§ 2º Os titulares de órgão ou unidade da JUCERJA podem solicitar a criação de listas de distribuição, restritas aos seus respectivos âmbitos de atuação.

§3º Cada unidade da JUCERJA poderá manter uma conta de correio eletrônico, destinada às comunicações institucionais.

Art. 4º É vedado o acesso ao conteúdo das mensagens tramitadas de terceiros por meio do serviço de correio eletrônico corporativo, salvo nas hipóteses previstas em lei, desde que existente fundado receio de descumprimento desta Norma, e mediante prévio procedimento administrativo cercado das devidas garantias constitucionais.

§1º A autoridade competente poderá determinar cautelarmente a manutenção das informações contidas nos ambientes de resguardo (backup), até a decisão acerca do procedimento de que trata o caput, sem que isso importe conhecimento de seu conteúdo.

§ 2º O conhecimento não autorizado às informações tramitadas, por meio do serviço de correio eletrônico corporativo da JUCERJA ou contidas em seus ambientes, será punido na forma da lei.

Art. 5º O acesso ao serviço de correio eletrônico dar-se-á por meio de senha de uso pessoal e intransferível, vedada sua divulgação.

Art. 6º É vedado ao usuário o uso do serviço de correio eletrônico corporativo com o objetivo de:

I – praticar crimes e infrações de qualquer natureza;

II – executar ações nocivas contra outros recursos computacionais da JUCERJA ou de redes externas;

III – distribuir material obsceno, pornográfico, ofensivo, preconceituoso, discriminatório, ou de qualquer forma contrário à lei e aos bons costumes;

IV – disseminar anúncios publicitários, mensagens de entretenimento e mensagens do tipo "corrente", vírus ou qualquer outro tipo de programa de computador que não seja destinado ao desempenho de suas funções ou que possam ser considerados nocivos ao ambiente de rede da JUCERJA;

V – emitir ou retransmitir comunicados gerais com caráter iminentemente associativo, sindical ou político-partidário;

VI – enviar arquivos de áudio, vídeo ou animações, salvo os casos que tenham relação com as funções institucionais desempenhadas pela JUCERJA;

VII – divulgar, no todo ou em parte, os endereços eletrônicos corporativos constantes do catálogo de endereços do serviço; e

VIII – executar outras atividades lesivas, tendentes a comprometer a intimidade de usuários, a segurança e a disponibilidade do sistema, ou à imagem institucional.

Art. 7º O usuário que fizer uso de forma indevida ou não-autorizada dos recursos de tecnologia da informação, em desacordo com os termos desta Norma, fica sujeito à aplicação das penalidades, sem prejuízo de outras eventualmente aplicáveis.

Art. 8º Compete à SIF disponibilizar o serviço de correio eletrônico corporativo, diretamente ou mediante contrato, competindo-lhe, ainda, o seguinte:

I – zelar pelo atendimento aos princípios da segurança, integridade, sigilo e disponibilidade dos serviços e dados transmitidos por meio do sistema de correio eletrônico;

II – prover meios tecnológicos necessários à adequada utilização do serviço;

III – definir os padrões e requisitos para cadastramento, concessão, utilização, suspensão ou exclusão das contas de correio eletrônico e listas de distribuição, atendidas as diretrizes definidas por esta Resolução;

IV – manter, em local seguro e restrito, informações dos serviços de correio eletrônico, no sentido de garantir a recuperação das mesmas em caso de necessidade, como por exemplo, em caso de danos ao ambiente de rede, recuperação eventualmente comunicada aos usuários dos serviços;

V – suspender motivadamente o acesso à conta de correio quando constatado o uso indevido dos recursos, dando imediata ciência ao respectivo titular e ao responsável pela apuração formal;

VI – manter proteção contra vírus e mensagens não solicitadas (spam) nos servidores do correio eletrônico;

VII – restringir a transmissão de arquivos que, em tese, possam significar comprometimento do serviço;

VIII – monitorar o uso do ambiente virtual, por meio de ferramentas sistêmicas, a fim de preservar a integridade das informações e identificar possíveis violações ao disposto nesta Resolução;

IX – divulgar esta norma aos usuários, bem como suas respectivas normas de execução;

X – capacitar, sempre que necessário, os usuários no uso da ferramenta de correio eletrônico; e

XI – manter à disposição do usuário do serviço ferramenta permanente para atualização de dados cadastrais.

Art. 9º Os contratos de prestação de serviço celebrados pela JUCERJA deverão ter cláusula específica obrigando os seus servidores ao cumprimento da presente Norma, bem como prevendo as penalidades decorrentes da sua inobservância.

Parágrafo único. Os contratos em vigor na data de publicação desta Norma deverão ser oportunamente aditados com inclusão da cláusula referida no caput.

Art.10 Cabe à unidade de Recursos Humanos informar à SIF, em até três dias úteis, as ocorrências de afastamentos ou desligamentos de usuários do serviço, que importem a necessidade de suspensão ou exclusão de contas de correio eletrônico.

ANEXO III

Uso da Internet e Rede

O presente regulamento estabelece normas e procedimentos específicos para uso da Internet e rede de dados da JUCERJA.

Art. 1º Estabelece normas e procedimentos específicos para uso da Internet.

Art. 2º – Para os efeitos desta Norma são estabelecidos os seguintes conceitos e definições:

1. **Código Malicioso –** Programa ou algoritmo que replica a si próprio através da Rede e, normalmente, executa ações maliciosas, tais quais utilizar os recursos computacionais, podendo fazer com que a máquina fique indisponível (***worm***) ou programa de computador com utilidade aparente ou real que contém funções escondidas e adicionais, explorando secretamente as informações armazenadas e provocando perda da segurança (cavalo de tróia).

2. **Vírus** – Programa desenvolvido com intenção nociva que, se inserido em um computador, pode causar queda do seu desempenho, destruição de arquivos e disco rígido, ocupar espaço livre de memória, entre outros danos.

3. ***Download*** – É a transferência de um arquivo de outro computador para o seu computador, através da *Internet*.

4. ***Upload*** – É a transferência de um arquivo do seu computador para outro computador, através da *Internet*.

5. **Incidente de Segurança da Informação** – É uma indicação de eventos, indesejados ou inesperados, que podem ameaçar a Segurança da Informação.

6. ***Internet*** – Rede mundial de computadores.

7. **Rede da JUCERJA** – São computadores e outros dispositivos interligados que compartilham informações ou recursos da JUCERJA.

8. **Senha** – Validação da identidade do usuário para obtenção de acesso a um sistema de informação ou serviço.

9. ***Software*** – Programa de computador.

10. **Usuário** – É todo aquele que exerça, ainda que transitoriamente e sem remuneração, por eleição, nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função pública na JUCERJA.

11. **Proxy** - Servidor intermediário que atende a requisições repassando os dados do usuário à frente, assim como possibilita navegar com o IP do servidor, escondendo a sua identidade.

12. **Navegador** - Ferramenta utilizada para acessar e visitar os diversos sítios daInternet.

Art 3° Disposições Gerais:

I - O acesso à Internet, via Rede dados, disponibilizado pela JUCERJA aos usuários da rede, deve ser utilizado para os interesses de trabalho da Instituição;

II - JUCERJA permite o uso da Internet para fins particulares dos usuários da Rede, desde que este uso não exceda os limites da ética, do bom senso e da razoabilidade;

III - É atribuição exclusiva da SIF definir os softwares homologados para o uso da Internet em sua Rede;

IV – O dispositivo conectado à Rede de dados do JUCERJA, dentro das dependências do órgão, somente deverá realizar o acesso à Internet pela própria rede de dados da Instituição.

Art 4° Permissão de Acesso à Internet:

I - A todo usuário da Rede da JUCERJA é facultado o acesso à Internet, em conformidade com os termos estabelecidos nesta norma.

Art 5° Cancelamento e Bloqueio do Acesso à Internet:

I - O acesso à Internet pelo usuário da Rede será obrigatoriamente cancelado quando do término do seu vínculo com a JUCERJA;

II - O cancelamento, o bloqueio e o desbloqueio do acesso à Internet seguem as condições descritas na Seção VIII da POSIC, que estabelece regras específicas para credenciamento e acesso de usuários aos ativos de rede de informação.

Art 6° Uso da Internet:

I - O acesso à Internet concedido ao Usuário da Rede da JUCERJA é pessoal e intransferível, sendo seu titular o único e total responsável pelas ações e danos causados à Instituição por meio de seu uso;

II - O acesso à Internet, quando realizado pela Rede disponibilizada pela JUCERJA e por meio do navegador homologado e disponibilizado nas estações de trabalho, não poderá ser feito mediante *proxies* externos, que permitam burlar as regras de acesso estabelecidas;

III - O Usuário da Rede deverá utilizar a Internet de forma a não causar tráfego desnecessário na Rede da JUCERJA ou em Redes de outras instituições;

IV - Todo serviço disponibilizado via Internet deverá ser avaliado previamente pela SIF, quanto às questões relativas à tecnologia da informação.

V - A SIF poderá publicar na Intranet, de forma consolidada, relatórios que demonstrem o uso da Internet no ambiente da JUCERJA, ficando vedada a divulgação de dados de acesso individualizados.

VI - É vedada a utilização da Internet para:

a)Acessar sítios com códigos maliciosos e vírus de computador;

b) Acessar sítios ou arquivos com conteúdo de incitação à violência, com materiais pornográficos, atentatórios à moral e aos bons costumes ou ofensivos;

c) Acessar sítios ou arquivos com conteúdo ilegal, criminoso, de incitação à violência ou que façam apologia ao crime, incluindo os de pirataria;

d) Realizar *download* ou *upload* de arquivos que não estejam relacionados às necessidades de trabalho da JUCERJA, em especial arquivos que contenham materiais ilegais ou que não respeitem os direitos autorais;

e) Infringir qualquer normativa local, estadual, nacional ou internacional aplicável;

f) Mostrar, armazenar ou transmitir texto, imagens ou sons que possam ser considerados ofensivos ou abusivos;

g) Utilizar o acesso à Internet para instigar, ameaçar ou ofender, abalar a imagem, invadir a privacidade ou prejudicar outros membros da comunidade Internet;

h) Efetuar ou tentar qualquer tipo de acesso não autorizado aos recursos computacionais da instituição;

i) Interceptar ou tentar interceptar a transmissão de dados através de monitoração;

j) Efetuar ou tentar qualquer tipo de acesso não autorizado aos recursos computacionais da instituição;

k) Provocar interferência em serviços de outros usuários ou o seu bloqueio, provocando congestionamento da Rede de dados, inserindo vírus ou tentando a apropriação indevida dos recursos computacionais da instituição;

l) Desenvolver, manter, utilizar ou divulgar dispositivos que possam causar danos aos sistemas e às informações armazenadas, tais como criação e propagação de vírus e *worms*, criação e utilização de sistemas de criptografia que causem ou tentem causar a indisponibilidade dos serviços e/ou destruição de dados, e ainda, se engajar em ações que possam ser caracterizadas como violação da segurança computacional;

m) Praticar atos que violem as regras de uso da Rede e os sistemas de segurança, estando, portanto, sujeito às sanções cabíveis;

n) Utilizar os recursos da Rede sem fio da instituição para fins comerciais ou políticos, tais como mala direta, *spams* ou propaganda política;

o) Se fazer passar por outra pessoa ou dissimular sua identidade quando utilizar o acesso à Internet;

p) Praticar atos que violem as regras de uso da Rede e os sistemas de segurança, estando, portanto, sujeito às sanções cabíveis;

q) Transferir para e armazenar informações sensíveis da JUCERJA em sites com os quais não haja um contrato ou acordo de responsabilidade estabelecido com esta Instituição;

r) Escutar música ou assistir programas de TV, exceto nos casos em que tais ações sejam condizentes com atividades de trabalho da JUCERJA e justificadas pela chefia mediata e autorizadas pela Presidência da JUCERJA.

VII - O usuário sempre deverá se certificar da procedência do sítio, verificando, quando cabível, seu certificado digital, principalmente para realizar transações eletrônicas via Internet, digitando o endereço do sítio diretamente no navegador da estação de trabalho, devendo evitar clicar em um link existente em uma página ou em uma mensagem de correio eletrônico, principalmente, se lhe parecer suspeito;

VIII - A SIF deverá homologar softwares, serviços de mensagens instantâneas, de voz, de videoconferência e de transferência de arquivos via Internet;

X - É vedado aos usuários disponibilizar informações de propriedade da JUCERJA em sites da Internet sem autorização da Instituição;

XI - Só será permitido o acesso à Internet via Rede por máquinas autorizadas e homologadas pela SIF, e que atendam a todos os requisitos de segurança da informação estabelecidos pela SIF;

XII - A conexão de equipamentos pessoais à Rede de dados da JUCERJA para acesso à Internet é proibida, exceto nos casos de trabalhos específicos da JUCERJA, desde que devidamente autorizados;

Art 7° Monitoramento:

I - O acesso à Internet será monitorado para fins de estudo, segurança, auditoria, desempenho e controle, quando for o caso;

II - O superior imediato pode solicitar formalmente um relatório com as informações de acesso à Internet dos seus subordinados, em casos em que haja suspeita de infração às regras de acesso desta norma, à Política de Segurança da Informação em vigor e normas correlatas;

Art. 8º Há três categorias de acesso à Internet, a saber:

I – acesso padrão;
II – acesso parcialmente liberado; e
III – acesso liberado.

Parágrafo Único: será respeitado o princípio do menor privilégio para configurar as contas de acesso dos usuários e colaboradores à Internet da JUCERJA, sendo inicialmente ousuário cadastrado na categoria Padrão.

Art. 9º O acesso padrão consiste na liberação de todas as categorias de sites, exceto aquelas listadas na Tabela 1, Anexo III, que serão bloqueadas.

Art. 10 O acesso parcialmente liberado consiste no acesso padrão, mais os acessos à vídeos, redes sociais, rádios e músicas.

Art. 11 O acesso liberado consiste no acesso a todos os sites e serviços, salvo aqueles de conteúdo ilícito e imoral e/ou potencialmente ofensivos, controversos, violação de segurança, conforme Tabela 1, Anexo III.

Parágrafo Único: À equipe de infraestrutura e ao Superintendente de Informática é facultado o acesso irrestrito à internet para fins de pesquisa, rastreio e outros atinentes às rotinas técnicas da área de tecnologia da informação.

Art. 12 As mudanças de categoria de acesso serão realizadas de acordo com os seguintes procedimentos:

I - Autorização por meio de formulário eletrônico/sistema de atendimento, com a devida justificativa da chefia imediata, que deverá ser convalidado pela respectiva superintendência ou unidade equivalente;

II - Deverão ser informados o nome e *login* de Rede do usuário, além do período em que o acesso permanecerá na categoria indicada.

Art. 13 Disposições Finais:

I - Os usuários da Rede que descumprirem as regras estabelecidas por esta norma poderão ter seu acesso à Rede e à Internet bloqueados até a apuração de responsabilidades, sem prejuízo das sanções legais cabíveis;

II - A SIF poderá adotar, a qualquer momento, medidas excepcionais que sejam necessárias para garantir a segurança, a disponibilidade, a integridade, a confidencialidade e aestabilidade da Rede;

III - Os casos omissos serão resolvidos pela SIF.

ANEXO III

Tabela 1: Categoria de Acesso Bloqueados

Categorias Bloqueadas	Conteúdos Bloqueados
Potencialmente ofensivos	Drogas ilícitas
	Hacking
	Ilegal ou anti-ético
	Racismo e ódio
	Violência
	Burla de proxy
	Phishing
	Abuso de crianças
Controversos	Material Adulto
	Apostas
	Grupos extremistas
	Nudez
	Pornografia
Potencialmente não produtivos	Jogos
	Bate-papo (chat)
	Instant messaging
	Rádio e TV pela internet
Potencialmente consumidores de banda	Compartilhamento peer-to-peer
	Rádio e TV pela internet
	Rede Social, relacionamento pessoal
	Rádio e TV pela internet
Potencial de violação de segurança	**Spyware**
	Malware
Outros	com base nas análises do fabricante da solução de firewall

Política de Segurança da Informação e Comunicação

ANEXO IV

Uso da Internet na rede WiFi

O presente regulamento estabelece normas e procedimentos específicos para uso da Internet na Rede Sem Fio corporativa da JUCERJA.

Art. 1º Estabelece normas e procedimentos específicos para uso da Internet na Rede Sem Fio corporativa da JUCERJA.

Art. 2º A rede Sem Fio corporativa consiste em infraestrutura computacional de pontos de acessode Rede Sem Fio (*wireless Access Points* ou *wireless* AP's) e controlador de pontos de acesso, cuja finalidade é prover o acesso aos recursos da Rede mundial de computadores (Internet) e sistemas internos, por meio de desktops internos e dispositivos móveis.

Parágrafo único. Entende-se por dispositivos móveis os computadores portáteis (*notebooks*, *netbooks*, *laptops*) e outros equipamentos compatíveis com conexões a Redes Sem Fio (*tablets*, *smartphones*, PDAs, celulares e etc.).

Art 3° A Rede Sem Fio corporativa da JUCERJA será implementada no mesmo regime da rede lógica cabeada.

Art. 4º – Para os efeitos desta Norma são estabelecidos os seguintes conceitos e definições:

1. **Código Malicioso –** Programa ou algoritmo que replica a si próprio através da Rede e, normalmente, executa ações maliciosas, tais quais utilizar os recursos computacionais, podendo fazer com que a máquina fique indisponível (*worm*) ou programa de computador com utilidade aparente ou real que contém funções escondidas e adicionais, explorando secretamente as informações armazenadas e provocando perda da segurança (cavalo de tróia).

2. ***Download*** – É a transferência de um arquivo de outro computador para o seucomputador, através da *Internet*.

3. ***Upload*** – É a transferência de um arquivo do seu computador para outro computador, através da *Internet*.

4. **Incidente de Segurança da Informação** – É uma indicação de eventos, indesejados ou inesperados, que podem ameaçar a Segurança da Informação.

5. **Internet** – Rede mundial de computadores.

6. **Rede do JUCERJA** – São computadores e outros dispositivos interligados que compartilham informações ou recursos da JUCERJA.

7. **Senha** – Validação da identidade do usuário para obtenção de acesso a um sistemade informação ou serviço.

8. ***Software*** – Programa de computador.

9. **Usuário** – É todo aquele que exerça, ainda que transitoriamente e sem remuneração, por eleição, nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função pública na JUCERJA.

10. **Vírus** – Programa desenvolvido com intenção nociva que, se inserido em um computador, pode causar queda do seu desempenho, destruição de arquivos e disco rígido, ocupar espaço livre de memória, entre outros danos.

11. **Proxy** - Servidor intermediário que atende a requisições repassando os dados do cliente à frente, como possibilita navegar com o IP do servidor, esconde a sua identidade.

12. **Navegador** – Ferramenta utilizada para acessar e visitar os diversos sítios da Internet.

Art 5° O acesso à Rede Sem Fio corporativa da JUCERJA é facultado aos servidores e colaboradores da JUCERJA devidamente cadastrados na Rede de dados da JUCERJA e no sistema de controle de acesso à Rede Sem Fio.

§ 1º Os servidores e colaboradores deverão utilizar o seu *login* e senha de rede para acessar a Rede Sem Fio, mediante concordância com o termo de responsabilidade, disponibilizado no momento do *login*.

§ 2º Aos visitantes será disponibilizado acesso à rede sem fio específica, em contexto e ambiente apartado da rede sem fio corporativa da JUCERJA, também, mediante identificação do usuário por meio de login e senha disponibilizados pela SIF.

§ 3º Durante a visitação ou em eventos promovidos no âmbito do prédio da JUCERJA no Rio de Janeiro, serão providenciados *login* e senha de acesso específicos, que serão fornecidos pela SIF, mediante solicitação do servidor responsável pelo(s) visitante(s) e/ ou evento;

§ 4º Na primeira vez em que o visitante se conectar à Rede Sem Fio, após informação do *login* e senha pela SIF, o mesmo deverá realizar o cadastramento online, mediante fornecimento do nome e identificação válida;

§ 5º O cadastramento será realizado em sistema próprio da Rede Sem Fio;

§ 6º O *login* e senha de acesso para visitantes terão validade apenas para o dia da visita e, após este prazo, expirarão automaticamente;

§ 7º A utilização da Rede Sem Fio será exclusiva para acesso à Internet, sendo vedado o acesso à Rede de Dados da JUCERJA por esta Rede sob qualquer hipótese;

§ 8º O usuário é o responsável por sua identidade eletrônica, senha, credenciais de

autenticação, autorização ou outro dispositivo de segurança.

Art 6º O Uso da Internet na Rede Sem Fio corporativa da JUCERJA:

I - O acesso à Internet na Rede Sem Fio corporativa da JUCERJA concedido ao Usuário é pessoal e intransferível, sendo o titular do acesso o responsável pelas ações e danos eventuais causadosà Instituição pelo seu acesso;

II - O usuário será responsável pela configuração e segurança do seu aparelho móvelde acesso, assim como pelos acessos realizados, devendo manter todos os sistemas de segurança, tais como, Sistema Operacional, antivírus, antispyes, antimalware, etc, atualizados.

III - O usuário é responsável por qualquer ato (legal ou ilegal) decorrente do uso da Internet utilizando seu *login* e senha;

IV – O usuário habilitado será responsável por seu dispositivo de acesso, devendo manter atualizados todos os requisitos de configuração necessários para o acesso;

V – Em hipótese nenhuma a SIF será responsável pela configuração e manutenção do dispositivo utilizado pelo usuário para o acesso à Rede Sem Fio corporativa, cabendo ao próprio usuário efetuar a conexão e navegação na Rede;

VI - O acesso à Internet pela Rede Sem Fio corporativa da JUCERJA não poderá ser feito mediante *proxies* externos, que permitam burlar as regras de acesso estabelecidas;

VII - É vedada a utilização da Internet para:

a) Acessar sítios com códigos maliciosos e vírus de computador;
b) Acessar sítios ou arquivos com conteúdo de incitação à violência, com materiais pornográficos, atentatórios à moral e aos bons costumes ou ofensivos;
c) Acessar sítios ou arquivos com conteúdo ilegal, criminoso, de incitação à violência ou que façam apologia ao crime, incluindo os de pirataria;
d) Realizar *download* ou *upload* de arquivos que contenham material ilegal ou que não respeitem os direitos autorais;
e) Infringir qualquer lei ou regulamento local, estadual, nacional ou internacionalaplicável;
f) Mostrar, armazenar ou transmitir texto, imagens ou sons que possam ser considerados ofensivos ou abusivos;
g) Utilizar o acesso à Internet para instigar, ameaçar ou ofender, abalar a imagem, invadir a privacidade ou prejudicar outros membros da comunidade Internet;
h) Efetuar ou tentar qualquer tipo de acesso não autorizado aos recursos computacionais da instituição;
i) Interceptar ou tentar interceptar a transmissão de dados através de monitoração;
j) Efetuar ou tentar qualquer tipo de acesso não autorizado aos recursos computacionais da instituição;
k) Provocar interferência em serviços de outros usuários ou o seu bloqueio, provocando congestionamento da Rede de dados, inserindo vírus ou tentando a apropriação indevida dos recursos computacionais da instituição;
l) Desenvolver, manter, utilizar ou divulgar dispositivos que possam causar danos aos

sistemas e às informações armazenadas, tais como criação e propagação de vírus e *worms*, criação e utilização de sistemas de criptografia que causem ou tentem causar a indisponibilidade dos serviços e/ou destruição de dados, e ainda, se engajar em ações que possam ser caracterizadas como violação da segurança computacional;

m) Praticar atos que violem as regras de uso da Rede e os sistemas de segurança, estando, portanto, sujeito às sanções cabíveis;

n) Utilizar os recursos da Rede Sem Fio da instituição para fins comerciais ou políticos, tais como mala direta, *spams* ou propaganda política;

o) Se fazer passar por outra pessoa ou dissimular sua identidade quando utilizar o acesso à Internet;

p) Praticar atos que violem as regras de uso da Rede e os sistemas de segurança, estando, portanto, sujeito às sanções cabíveis.

q) Transferir para e armazenar informações sensíveis da JUCERJA em sites com os quaisnão haja um contrato ou acordo de responsabilidade estabelecido com esta Instituição.

Art 7° É permitido o uso da Internet na Rede Sem Fio corporativa da JUCERJA para fins particulares dos usuários, desde que este uso não exceda os limites da ética, do bom senso e da razoabilidade.

Art. 8º Por medida de controle para evitar tráfego excessivo e para efeitos de segurançade Rede Sem Fio corporativa, é facultado à SIF a intervenção imediata na gerência da Rede Sem Fio, podendo esta aplicar controle de tráfego, restrição de banda e qualquer outra ação necessária.

Parágrafo Único: O processo de encerramento da conexão (*Logoff*) na Rede Sem Fio é de responsabilidade do usuário.

Art. 9º Cancelamento e Bloqueio do Acesso à Internet na Rede Sem Fio da JUCERJA:

I - O acesso à Internet na Rede Sem Fio corporativa da JUCERJA pelo usuário será obrigatoriamente cancelado quando do término do seu vínculo com o JUCERJA;

II - Caso seja detectada propagação de alguma ameaça à Rede Sem Fio corporativa pelo usuário, tal como vírus, spam, etc, a SIF estará autorizada a intervir imediatamente, bloqueando o acesso do usuário automaticamente.

III - O desbloqueio será realizado quando resolvido o problema.

Art. 10 O acesso à Rede Sem Fio corporativa será monitorado para fins de estudo, segurança, auditoria, desempenho e controle, quando for o caso.

Art. 11 Os privilégios de acesso de qualquer usuário, cujas atividades estejam em desconformidade com este documento ou demais normas e políticas de Segurança da Informação e Comunicação vigentes na JUCERJA, estarão sujeitos à suspensão temporária ou permanente.

Art. 12 A Rede Sem Fio corporativa, devido à sua própria natureza, poderá sofrer

quedas de desempenho ou interrupções, devendo os usuários estarem cientes da possibilidade de perda de comunicação ou de informações.

Art. 13 Disposições Finais:

I - A SIF poderá adotar, a qualquer momento, medidas excepcionais que sejam necessárias para garantir a segurança, a disponibilidade, a integridade, a confidencialidade e a estabilidade da Rede Sem Fio corporativa da JUCERJA;

II - Os casos omissos serão resolvidos pela SIF.

ANEXO V

TERMO DE CONFIDENCIALIDADE

Nome:

Empresa:

Cargo/ Função / Vínculo:

Matrícula / CPF:

Data:

Cláusula 1ª - Declaro ter conhecimento da Política de Segurança da Informação (POSIC) adotada pela JUCERJA para utilização dos bens e recursos de tecnologia da informação e comunicação (TIC), e me comprometo ao seu fiel cumprimento e observância.

Cláusula 2ª – Responsabilizo-me pelo correto uso dos recursos de TIC da JUCERJA, comprometendo-me a utilizá-los somente para fins institucionais, cumprindo as determinações e recomendações contidas na POSIC e normativos vigentes.

Cláusula 3ª – Comprometo-me a manter sigilo absoluto sobre os sistemas e informações a mim confiados, bem como aos que venha ter conhecimento em função da execução de atividades desenvolvidas para atendimento dos objetivos da instituição.

Cláusula 4ª – Estou ciente e concordo que a utilização do e-mail institucional, da internet e demais acessos devem ocorrer em consonância com o disposto na POSIC e normativas vigentes.

Cláusula 5ª – Estou ciente de que a Jucerja pode monitorar o uso das informações e recursos de TIC, conforme previsto na POSIC e em suas normas complementares, sem prejuízo das ações preventivas, corretivas ou disciplinares que possam ser tomadas.

Cláusula 6ª – Estou ciente de que as senhas de acesso aos sistemas e a ambientes físicos têm caráter confidencial, pessoal e intransferível, sendo minha responsabilidade zelar pelo seu sigilo.

Cláusula 7ª – Declaro, finalmente, que tenho pleno conhecimento de que todas as minhas ações no ambiente da TIC da JUCERJA podem ser registradas, ciente de que o uso indevido ou fraudulento das informações e dos recursos ensejará apuração de responsabilidade, nos termos da legislação Vigente.