**SERVIÇO PÚBLICO FEDERAL**

**UNIVERSIDADE FEDERAL DA PARAÍBA**

**CONSELHO UNIVERSITÁRIO**

**RESOLUÇÃO Nº 32/2014**

Institui a política de segurança da informação da UFPB, normatiza procedimentos com esta finalidade e dá outras providências.

O Conselho Universitário (CONSUNI) da universidade Federal da Paraíba, no uso das atribuições que lhe confere o Estatuto da UFPB,

Considerando o disposto no Decreto nº 3.505, de 13 de junho de 2000, que institui a política de segurança da informação nos órgãos e nas entidades da Administração Pública Federal;

Considerando o disposto no Decreto nº 7.845, de 14 de novembro de 2012, que regulamenta procedimentos para o credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo no âmbito do Poder Executivo Federal;

Considerando a Instrução Normativa MPOG/SLTI nº 04/2010, que exige "normas de segurança vigentes no órgão ou entidade" para fins de aferição de comportamento do fornecedor/provedor de produtos e serviços em TI;

Considerando o Acórdão TCU nº 1.603/2008-Plenário, que define política de segurança da informação como "o documento que contém as diretrizes da instituição quanto ao tratamento da segurança da informação" e que

> "deve declarar explicitamente o comprometimento da direção da instituição com a segurança da informação. Além disso, deve também conter definições dos termos relacionados dentro do escopo da instituição e apontar os objetivos de controle, os controles, as estruturas que implementam esses controles, as responsabilidades e também as políticas e normas que disciplinam e complementam esse documento de diretrizes, incluindo referências à legislação e aos requisitos regulamentares e contratuais" (p. 15);

Considerando a necessidade da Universidade Federal da Paraíba adequar-se aos decretos, normativas e acórdãos citados:

Considerando a homologação prévia pelo Comitê de Gestão e Tecnologia da Informação (CGTI), conforme processo nº 23074.015468/2014-44, em atendimento à prerrogativa regimental do CGTI de "avaliar e emitir parecer sobre proposições de políticas [...]" (Regimento CGTI, Art. 2º); e, tendo em vista deliberação do plenário em reunião ordinária realizada no dia 21 de outubro de 2014 (Processo nº 23074.017164/2014-11),

**RESOLVE:**

**Art. 1º.** Instituir a Política de Segurança da Informação da UFPB (PSI/UFPB).

**Parágrafo único** A PSI/UFPB será executada na forma disposta no anexo a esta resolução.

**Art. 2º**. Os casos omissos serão resolvidos pelo CONSUNI.

**Art. 3º**. A presente resolução entra em vigor na data de sua publicação, revogadas as normas anteriores da Instituição relativas à matéria.

Conselho Universitário da Universidade Federal da Paraíba, João Pessoa, 22 de outubro de 2014.

**Margareth de Fátima Formiga de Melo Diniz**

Presidente

# ANEXO DA RESOLUÇÃO 32/2014 DO CONSUNI QUE INSTITUI A POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DA UFPB (PSI/UFPB)

## CAPÍTULO 1
## DO OBJETO

**Art.1**º. Fica estabelecida a Política de Segurança da Informação (PSI) da Universidade Federal da Paraíba (UFPB), contendo as diretrizes de segurança da informação a serem observadas no âmbito desta Universidade.

**Parágrafo Único**. As diretrizes estabelecidas na PSI/UFPB determinam as bases a serem seguidas pela UFPB com relação à segurança dos recursos de tecnologia da informação (TI) e informações geradas na UFPB.

**Art. 2º**. A PSI consiste em um quadro de referência contendo princípios que norteiam a gestão da segurança da informação e que devem ser observados por professores, alunos, servidores e demais usuários que interagirem com os "ativos" de TI da UFPB.

**Art. 3º**. Para fins da execução da PSI/UFPB, aplicam-se os seguintes conceitos referentes a ativos de TI:

**I**. Ativo de Informação – qualquer recurso que faça parte dos sistemas de informação (SI) e meios para geração de documentos que tenham valor para a UFPB;

**II**. Ativo de Sistema – patrimônio composto por todos os dados e informações geradas e manipuladas durante a execução de SIs e processos da UFPB;

**III**. Ativo de Processamento – patrimônio composto por todos os elementos de hardware, software, serviço, infraestrutura e instalações físicas necessárias para a execução dos SIs e processos da UFPB, incluindo tanto aqueles produzidos internamente quanto os adquiridos externamente por esta Universidade;

**IV**. Controle de Acesso – restrições ao acesso às informações de um SI, estabelecidas pela Gerência de Segurança da Informação (GSEGI) da Superintendência de Tecnologia da Informação (STI) da UFPB;

**V**. Custódia – consiste em restrição de acesso de ativo como forma de protege-lo para possível auditoria ou posterior análise judicial;

**VI**. Direito de Acesso – privilégio associado a um cargo, pessoa ou processo, que atribui permissão de acesso a um ativo de TI;

**VII**. Ferramentas – conjunto de equipamentos, programas, procedimentos, normas e demais recursos, por meio dos quais se aplica a PSI/UFPB;

**VIII**. Incidente de Segurança – qualquer evento ou ocorrência que promova uma ou mais ações que comprometam ou que sejam ameaça à integridade, autenticidade ou disponibilidade de qualquer ativo de TI da UFPB;

**IX**. Proteção de Ativos – processo pelo qual os ativos de TI recebem determinada classificação relacionada à restrição de acesso;

**X**. Responsabilidade – obrigações e deveres da pessoa que ocupa determinada função em relação ao acervo de ativos de TI.

## CAPÍTULO II
## DOS OBJETOS E DO ESCOPO

**Art. 4º**. A PSI/UFPB tem os seguintes objetivos:

**I**. Definir o escopo da segurança da informação da UFPB;

**II.** Orientar as ações de segurança com o intuito de reduzir riscos e garantir a confidencialidade, integridade e disponibilidade dos ativos de TI da UFPB;

**III.** Incentivar o uso de soluções integradas de segurança;

**IV.** Servir de referência para auditoria, apuração e avaliação de responsabilidades;

**Art. 5º.** A PSI/UFPB abrange os seguintes aspectos:

**I.** Requisitos de segurança criptográficos: define padrões e princípios sobre quando e como recursos criptográficos devem (ou não devem) ser utilizados sobre dados institucionais;

**II.** Requisitos de segurança no manuseio e tratamento de informação: define padrões e princípios relacionados ao manuseio de informações, o que inclui inventários, administração e propriedade sobre dados, eliminação e remoção de informação, informações disponíveis em mesas de trabalho, telas de computador, material impresso, etc.

**III.** Requisitos de segurança de redes e dispositivos móveis: define padrões e princípios relacionados à segurança de redes, por cabos e sem fio, tais como administração, design e configuração da rede, segurança física e redundância, conexão de dispositivos, serviços e protocolos:

**IV.** Requisitos de segurança em operações de sistemas de informação: define padrões e princípios relacionados à operação dos sistemas de informação, tais como procedimentos operacionais, controles, responsabilidades sobre senhas, contas de usuários, uso de correio eletrônico, relato de incidentes de segurança da informação e falhas de software;

**V.** Requisitos de segurança contratual e acordo de nível de serviço: define padrões e princípios relacionados à manutenção da segurança dos ativos de TI que são acessados ou fornecidos por terceiros;

**VI.** Requisitos de segurança em recursos humanos: define padrões e princípios de segurança relacionados a ações realizadas por ou eventos ocorridos com servidores 9docentes e técnico-administrativos), gestores, pessoal em cargos de chefia, estagiários, tais como procedimentos a realizar quando um servidor é exonerado, quando sofre relotação, quando está em licença, etc.;

**VII.** Requisitos de segurança em gestão de software: define padrões e princípios relacionados à administração de softwares instalados nos computadores da UFPB, tais como gerenciamento de licenças, uso de “software livre”, riscos relacionados ao desenvolvimento de software por parte dos usuários, atualização de versão, etc.;

**VIII.** Requisitos de segurança para aquisição de ativos de TI: define padrões e princípios relacionados à seleção, aquisição, instalação e gestão de contratos de fornecimento/provimento de ativos de TI.

**Parágrafo Único.** A responsabilidade sobre os ativos de TI e os requisitos de segurança dos itens supracitados serão regulamentados por meio de normas específicas elaboradas pela GSEGI/STI, baseadas em padrão ABNT específico e submetidas à homologação pelo Comitê de Gestão e Tecnologia da Informação (CGTI) e aprovação final pelo CONSUNI.

## CAPÍTULO III
## DO GERENCIMANTO DE RISCOS E INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

**Art. 6º.** Entende-se como gerenciamento de riscos o processo que visa à proteção dos serviços de TI da UFPB por meio da aceitação, redução, eliminação ou transferência de riscos, conforme seja econômica e estrategicamente viável. Os seguintes pontos principais devem ser identificados:

I. Escopo - ativos de TI a serem protegidos;

II. Riscos - áreas em que a segurança da informação pode ser comprometida, considerando-se o escopo estabelecido;

III. Análise de Riscos - considera a probabilidade de determinado risco se concretizar e o potencial dano dele advindo, assim como a decisão que deve ser tomada de acordo com escopo e riscos.

**Art. 7º.** O processo de gerenciamento de riscos será instituído e revisto periodicamente pela GSEGI/STI com o intuito de agir proativamente contra riscos advindos de novas tecnologias e ameaças externas, visando à constante elaboração de planos de ação apropriados para proteção dos ativos ameaçados.

**Parágrafo Único.** Todos os ativos de TI da UFPB deverão ser inventariados e classificados de acordo com as instruções no Decreto Nº 7.845 de 14 de Novembro de 2012.

**Art. 8º.** A GSEGI/STI apresentará planos de gerenciamento de incidentes e ação de reposta a incidentes a serem avaliados e aprovados pelas instâncias competentes na STI e submetidos à aprovação pelo CGTI.

**Art. 9º.** Os incidentes de segurança da informação identificados por quaisquer servidores, alunos ou professores deverão ser prontamente reportados ao responsável do setor onde o incidente ocorreu, bem como à STI:

## CAPÍTULO IV
## DOS DEVERES E DAS RESPONSABILIDADES

**Art. 10.** É dever de todo usuário dos ativos de TI da UFPB:

**I.** Preservar a integridade e guardar sigilo das informações de que fazem uso, bem como zelar e proteger os ativos de TI;

**II.** Cumprir a PSI/UFPB, sob pena de sanções disciplinares e legais cabíveis, previstas no Art. 13 desta Resolução.

**III.** Utilizar os SIs da UFPB e os recursos a eles relacionados apenas para os fins previstos por esta Universidade;

**IV.** Abster-se de instalar, utilizar, inspecionar, copiar, armazenar ou fornecer ativos de TI (incluindo, enfaticamente, programas de computador/software) em violação à legislação de propriedade intelectual vigente;

**V.** Responder por todo e qualquer acesso realizado aos ativos de TI da UFPB realizado por meio de sua credencial individual ou por meio de credencial pública ou de grupo;

**VI.** Comunicar ao seu superior imediato quaisquer irregularidades ou desvios de uso dos ativos de TI identificados, para que o mesmo possa relatar à GSEGI.

**Art. 11.** É dever de todo ocupante de cargo de chefia na UFPB:

**I.** Verificar o atendimento às regras de proteção dos ativos de TI da UFPB por parte de seus subordinados;

**II.** Aplicar medidas em caso de violação das regras estabelecidas de acordo com as Normas e Procedimentos de Segurança da Informação da STI;

**III.** Atualiza-se periodicamente quanto às políticas, normas e procedimentos de segurança da informação vigentes na UFPB;

**IV.** Identificar, registrar e comunicar à STI as violações ou tentativas de acesso a ativos de TI não autorizadas;

**V.** Manter o devido registro e controle ao autorizar e fornecer acesso aos ativos de TI sob sua responsabilidade a servidores, professores, alunos ou terceiros.

**Art.12.** Entende-se como responsabilidade de quem elabora contratos relativos à TI em nome da UFPB a observação das normas que estabelecem requisitos de segurança contratual e acordos de nível de serviço (SLA, na sigla original em inglês).

## CAPÍTULO V
## DAS SANÇÕES E PENALIDADES

**Art. 13.** Em caso de descumprimento de termos estabelecidos por esta Resolução, serão aplicadas as sanções e penalidades previstas na legislação em vigor, em especial no Código de Ética do Servidor Público Civil do Poder Executivo Federal, aprovado pelo Decreto n º 1.171/1994 e na Lei nº 8.112/1990, que instituiu o Regime Jurídico dos Servidores Públicos Civis da União, das autarquias, inclusive as em regime especial, e das fundações públicas federais.

## CAPÍTULO VI
## DAS AUDITORIAS E FISCALIZAÇÕES

**Art. 14.** Cabe à GSEGI/STI responder às diligências relativas à segurança da informação promovidas por meio de auditoria interna ou externa.

## CAPÍTULO VII
## DO GERENCIAMENTO DE RISCOS

**Art. 15.** As normas e procedimentos para implantação do gerenciamento de riscos referentes aos ativos de TI serão definidos em norma específica, a ser elaborada pela GSEGI/STI e submetida à aprovação pelo CGTI.

## CAPÍTULO VIII
## DO PLANO DE CONTINUIDADE DE NEGÓCIOS

**Art. 16.** O Plano de Continuidade de Negócios (PCN) tem como objetivo manter em funcionamento os serviços e processos críticos da UFPB, na eventualidade de ocorrência de desastres, atentados, falhas e intempéries.

**Art. 17.** O PCN da UFPB será definido pela STI, levando em consideração as normas e procedimentos para gerenciamento de riscos referentes aos ativos de TI, e submetido à aprovação pelo CGTI.

## CAPÍTULO IX
## DAS DISPOSIÇÕES FINAIS

**Art. 18.** A PSI da UFPB se aplica a todos os integrantes do quadro de pessoal, recursos administrativos e tecnológicos, e tem abrangência sobre os recursos ligados a esta Universidade em caráter permanente ou temporário.

**Art. 19.** A PSI resultante contida nesta Resolução deverá ser publicada e amplamente promovida, garantindo que a comunidade universitária tenha conhecimento da mesma para adequado usufruto dos benefícios e assunção das responsabilidades sobre os ativos de TI da UFPB.

**Art. 20.** Os processos de aquisição de bens e serviços relacionados a ativos de TI na UFPB deverão observar conformidade com esta PSI.

**Art. 21.** A PSI será revisada anualmente pela GSEGI/STI, apreciada pelo CGTI e submetida à aprovação do CONSUNI.

**Art. 22.** Os casos omissos nesta Resolução serão resolvidos pelo CONSUNI ouvidos a GSEGI/STI e o CGTI.