



**UNIVERSIDADE FEDERAL DO CEARÁ**  
**REITORIA**  
**BIBLIOTECA UNIVERSITÁRIA**  
**COMISSÃO DE SERVIÇOS**



**DIRETRIZES PARA USO E MANUTENÇÃO DOS COMPUTADORES  
DESTINADOS AOS USUÁRIOS DO SISTEMA DE BIBLIOTECAS  
DA UNIVERSIDADE FEDERAL DO CEARÁ**

**FORTALEZA-CE**  
**2015**

**DIRETRIZES PARA USO E MANUTENÇÃO DOS COMPUTADORES  
DESTINADOS AOS USUÁRIOS DO SISTEMA DE BIBLIOTECAS  
DA UNIVERSIDADE FEDERAL DO CEARÁ**

**Reitor em Exercício**

Prof. Henry de Holanda Campos

**Diretor da Biblioteca Universitária**

Francisco Jonatan Soares

**Bibliotecários Colaboradores**

Diana Flor de Lima Rifane

Fabíola Maria Pereira Bezerra

Francisco Jonatan Soares

Nirlange Pessoa de Queiroz

**Membros da Comissão de Serviços**

Ana Rafaela Sales de Araújo

Érica Quadros do Amaral

Ericson Bezerra Viana

Francisco Edvander Pires Santos

Izabel Lima dos Santos

José Jairo Viana de Sousa

Juliana Soares Lima

Kalline Yasmin Soares Feitosa

## SUMÁRIO

<b>1 APRESENTAÇÃO.....</b>	<b>3</b>
<b>2 OBJETIVOS.....</b>	<b>4</b>
<b>3 PROCEDIMENTOS A SEREM ADOTADOS NAS BIBLIOTECAS.....</b>	<b>5</b>
<b>4 CONFIGURAÇÃO DOS COMPUTADORES DE PESQUISA.....</b>	<b>6</b>
<b>5 CONFIGURAÇÃO DOS COMPUTADORES DE ACESSO LIVRE.....</b>	<b>7</b>
<b>6 SUPORTE TÉCNICO.....</b>	<b>8</b>
<b>REFERÊNCIAS.....</b>	<b>9</b>
<b>APÊNDICES.....</b>	<b>10</b>
APÊNDICE A – Tutorial para solicitação de serviços à STI.....	10
<b>ANEXOS.....</b>	<b>13</b>
ANEXO A – Política de Segurança da Informação e Comunicação da UFC.....	13

## 1 APRESENTAÇÃO

A elaboração das diretrizes para uso e manutenção dos computadores destinados aos usuários do Sistema de Bibliotecas da Universidade Federal do Ceará (UFC) se deu a partir da necessidade de padronização no que se refere à configuração dos computadores disponibilizados para a comunidade acadêmica nas dependências das bibliotecas da UFC. Também houve a necessidade de a Biblioteca Universitária (BU) contribuir para a difusão da segurança da informação no Sistema de Bibliotecas, indo diretamente ao encontro da proposta da Política de Segurança da Informação e Comunicação ([POSIC](#)) da UFC.

As diretrizes foram traçadas depois de concluída a etapa de diagnóstico das máquinas disponíveis para acesso dos usuários em cada uma das bibliotecas que compõem o Sistema, na cidade de Fortaleza-CE. Por meio de uma análise feita *in loco*, foi possível constatar situações que foram desde o acesso desenfreado a sites que não correspondiam a pesquisas, prejudicando, assim, os usuários que necessitavam acessar o catálogo online e/ou os serviços oferecidos no site da biblioteca, até a manipulação de informações sigilosas numa das bibliotecas do Sistema.

Com base nos dados obtidos nessas visitas, a Comissão de Serviços da BU traçou como meta a elaboração de relatórios, com a finalidade de documentar a realidade encontrada nas bibliotecas visitadas. A partir desses relatórios, foram sugeridos procedimentos a serem adotados nas bibliotecas da UFC, visando solucionar os problemas encontrados e nortear futuras tomadas de decisão. Os procedimentos foram adotados e documentados com sucesso nas bibliotecas da capital, recebendo amplo apoio da Secretaria de Tecnologia da Informação (STI). Nesse ínterim, também houve a contribuição de algumas bibliotecas localizadas nos *campi* do Interior do Estado, por meio do envio de relatórios que comprovaram a aplicação das sugestões de procedimentos a serem adotados nas bibliotecas.

Assim, a elaboração deste documento resulta das diretrizes sugeridas e aplicadas nas bibliotecas da UFC, por meio do esforço conjunto da Comissão de Serviços, da Direção da BU e da Direção de cada biblioteca que compõe o Sistema, tendo em vista a consolidação das boas práticas na prestação de serviços ao usuário, recorrendo às medidas preventivas que norteiam a segurança da informação.

## 2 OBJETIVOS

Este documento tem como objetivo estabelecer diretrizes para a melhor utilização dos computadores de pesquisa e de acesso livre do Sistema de Bibliotecas da UFC, visando difundir a importância da segurança da informação na Universidade.

Além disso, também faz parte do seu escopo:

- Definir responsabilidades, visando promover as boas práticas frente ao público interno e externo da UFC;
- Permitir a otimização dos recursos;
- Assegurar a integridade, disponibilidade, confidencialidade e segurança da informação;
- Preservar a propriedade intelectual e os direitos sobre dados.

### 3 PROCEDIMENTOS A SEREM ADOTADOS NAS BIBLIOTECAS

Levando em consideração as decisões tomadas em conjunto pela Comissão de Serviços e pela Direção da BU, ficam definidos os seguintes procedimentos a serem adotados nas bibliotecas da UFC:

- Acionar a STI **sempre** que houver a necessidade de instalação, manutenção e/ou reparo nos computadores destinados à pesquisa e ao acesso livre dos usuários;
- Adequar o sistema operacional dos computadores (Windows ou Linux) à necessidade da biblioteca;
- Reservar uma quantidade específica de computadores exclusivamente para pesquisa ao catálogo online, acesso aos recursos e serviços disponíveis no site da biblioteca e no domínio UFC;
- Disponibilizar pelo menos um computador com softwares e/ou recursos específicos para possibilitar o acesso a pessoas com deficiência.

## 4 CONFIGURAÇÃO DOS COMPUTADORES DE PESQUISA

A configuração de acesso para os computadores destinados **exclusivamente** à pesquisa ao catálogo online e aos recursos e serviços oferecidos pelo Sistema de Bibliotecas da UFC está condicionada às seguintes recomendações:

- Instalar o sistema operacional Linux nas máquinas de pesquisa, dependendo da configuração de fábrica do computador;
- Manter instalados e atualizados os antivírus e os navegadores de Internet;
- Criar conta e senha de administrador e de convidado em cada uma das máquinas (a senha de administrador ficará sob a responsabilidade da Direção da biblioteca);
- Bloquear a instalação de softwares piratas e/ou não autorizados e também as páginas externas ao domínio UFC;
- Instalar o DosVox (programa para deficientes visuais), leitores de tela NVDA (para Windows) ou Orca (para Linux), além de outros recursos de acessibilidade disponíveis em ambos os sistemas operacionais (Linux e Windows);
- Providenciar adesivos especiais para teclados, a fim de torná-los acessíveis para usuários com baixa visão e/ou com outros problemas oculares parciais.

Para qualquer dúvida e/ou informação acerca dos computadores a serem configurados para os usuários com algum tipo de deficiência, recorrer à STI, à Comissão de Acessibilidade e/ou à Comissão de Serviços do Sistema de Bibliotecas da UFC.

## 5 CONFIGURAÇÃO DOS COMPUTADORES DE ACESSO LIVRE

Computadores de acesso livre são aqueles cujo acesso a domínios externos (tais como contas de e-mail, redes sociais, buscadores web, dentre outros) à UFC ou a recursos e serviços oferecidos pelo Sistema de Bibliotecas está liberado. A existência de computadores com essa configuração **não** é obrigatória em nenhuma biblioteca do Sistema, e mesmo aquelas que os possuem podem suspender a oferta desse serviço a qualquer momento.

Nesse sentido, a configuração de acesso para os computadores destinados ao acesso livre dos usuários do Sistema de Bibliotecas da UFC está condicionada às seguintes recomendações:

- A quantidade de computadores reservados ao acesso livre dos usuários, bem como o seu tempo de permanência nos computadores, ficará a cargo da Direção de cada biblioteca;
- Dependendo da configuração de fábrica do computador, poderá haver máquinas com sistema operacional Linux ou Windows;
- Manter instalados e atualizados os antivírus e os navegadores de Internet;
- É permitido o acesso a sites que não pertençam ao domínio UFC, desde que respeitadas as condições de segurança da informação adotadas pelo Sistema de Bibliotecas e pela Universidade, tendo em vista a [POSIC](#) da UFC.



## 6 SUPORTE TÉCNICO

As bibliotecas deverão recorrer sempre à STI para solucionar problemas relativos ao uso e/ou à manutenção dos computadores. As alterações na configuração dos computadores devem ser feitas **exclusivamente** pelos servidores da STI, acionados por meio do [Sistema de Solicitação de Serviços](#), localizado na aba UFC Digital do site da Universidade (vide APÊNDICE A).

## REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27001**: Tecnologia da informação: Técnicas de segurança: Sistemas de gestão da segurança da informação: Requisitos. Rio de Janeiro, 2013.

\_\_\_\_\_. **NBR ISO/IEC 27002**: Tecnologia da informação: Técnicas de segurança: Código de prática para a gestão da segurança da informação. Rio de Janeiro, 2013.

BRASIL. Decreto nº 3505, de 13 de junho de 2000. Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal. Disponível em: <[http://www.planalto.gov.br/ccivil\\_03/decreto/D3505.htm](http://www.planalto.gov.br/ccivil_03/decreto/D3505.htm)>. Acesso em: 22 abr. 2015.

\_\_\_\_\_. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. **Diário Oficial [da] República Federativa do Brasil**, Brasília, DF, 24 abr. 2014. Disponível em: <[http://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2014/lei/l12965.htm](http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm)>. Acesso em: 22 abr. 2015.

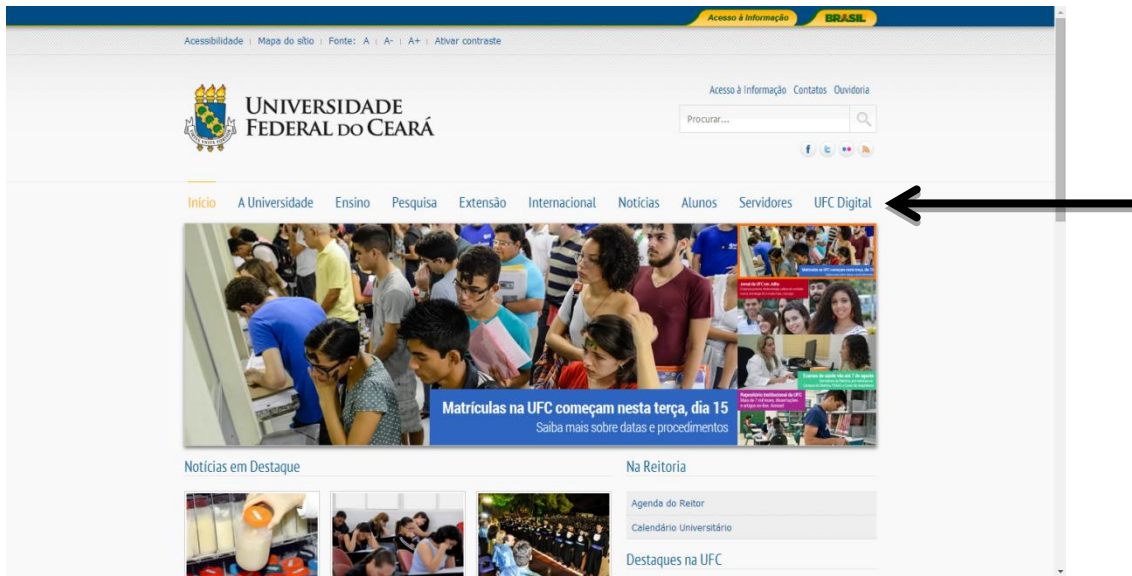
\_\_\_\_\_. Tribunal de Contas da União. **Boas Práticas em Segurança da Informação**. 4. ed. Brasília, DF, 2012. 108 p. Disponível em: <<http://portal2.tcu.gov.br/portal/pls/portal/docs/2511466.PDF>>. Acesso em: 22 abr. 2015.

UNIVERSIDADE FEDERAL DO CEARÁ. **Política de Segurança da Informação e Comunicação – POSIC**. Disponível em: <<http://www.sti.ufc.br/govti/seginfo/posic.php>>. Acesso em: 22 abr. 2015.

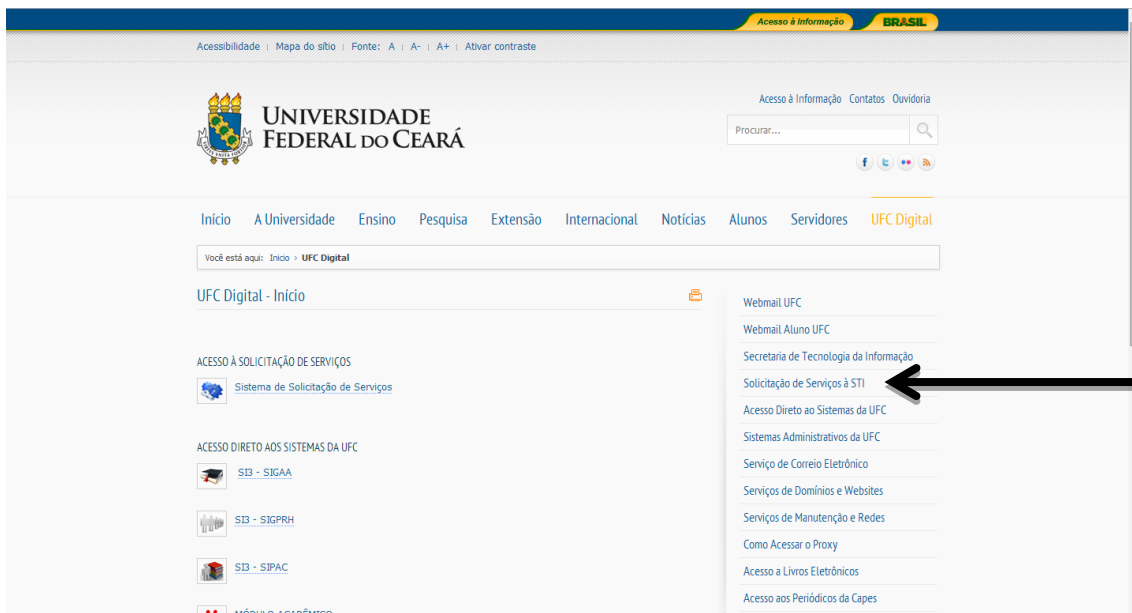
## APÊNDICES

### APÊNDICE A – Tutorial para solicitação de serviços à STI

1) Acesse o site da UFC: [www.ufc.br](http://www.ufc.br) e clique em “UFC Digital”.



2) Clique em “Solicitação de Serviços à STI”.



3) Digite o seu CPF e o número de matrícula no SIAPE. Clique em “Entrar”.

**UNIVERSIDADE FEDERAL DO CEARÁ**

Secretaria de Tecnologia da Informação - STI

**Solicitação de Atendimento**

Para efetuar sua solicitação de atendimento, siga os seguintes passos:

- CPF  
Preencha este campo com os 11 números do seu CPF (apenas números, sem espaços, pontos ou hífen).
- SIAPE  
Preencha este campo com os 7 números do seu SIAPE (apenas números, sem espaços, pontos ou hífen).

> DSM-STI: Regras para abertura de solicitação de serviços.

1. Abra 01 (Uma) solicitação para cada equipamento. **Informe o número patrimonial.**
2. Não realizamos manutenção em impressoras.
3. Não Realizamos Backup de informações.
4. Monitores/Estabilizadores/No-Breaks:
  - o Os equipamentos devem ser entregues e retirados no setor de atendimento da STI, Campus do Pici, bloco 901, primeiro andar.
  - o Não abra ordem de serviço. A ordem de serviço vai ser aberta no momento da entrega do seu equipamento.

**Evite o cancelamento do seu pedido. Observe sempre as regras acima.**

5. Solicitações "URGENTES" - CPU/Desktops com defeito podem ser enviados diretamente ao setor de atendimento da STI para diagnóstico imediato, evitando espera.
6. A STI somente instala software licenciado. (Não sendo apresentada licença de uso para WINDOWS, estaremos instalando LINUX).
7. Problema causados pelo uso indevido de roteadores sem fio em nossa rede é de responsabilidade do usuário responsável pelo equipamento.
8. Não realizamos manutenção de hardware em notebooks - somente SOFTWARE.

© 2007 Projeto e desenvolvimento: STI - UFC. Todos os direitos reservados.

4) Preencha os campos com as informações solicitadas. No campo de “Assunto/Descrição” você deve informar qual é o serviço que deseja solicitar. Digite o código da imagem e clique em “Enviar”.

**OBSERVAÇÃO:** Deve ser aberto um chamado por máquina, e o número de patrimônio deve ser informado. Se a máquina não tiver plaqueta de número patrimonial, deverá ser descrita nesse campo como “sem número de patrimônio”.

**UNIVERSIDADE FEDERAL DO CEARÁ**

Secretaria de Tecnologia da Informação - STI

**Solicitação de Atendimento**

Preencha o formulário abaixo com as informações solicitadas.

Nome: JULIANA SOARES LIMA

Email:

Telefone(s):

Departamento:

Setor:

Tipo:  Solicito instalar software anti-virus  
 prédio sem internet  
 computador não acessa a internet  
 problema no correio eletrônico  
 computador não liga ou está travando  
 solicito registro de domínio  
 solicito restabelecer primeiro acesso ao módulo acadêmico  
 Outros

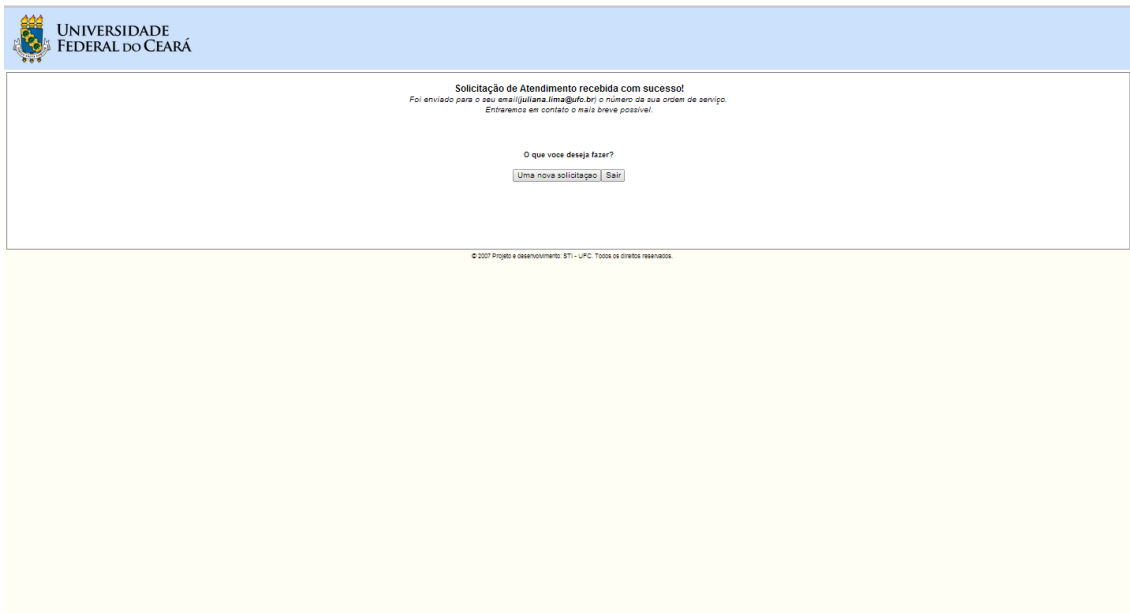
Assunto/Descrição:

Cadastre a solicitação, informando se for o caso, o horário e o local para visita (pale. laboratório), e plaqueta patrimonial etc.


Número mostrado ao lado:

© 2007 Projeto e desenvolvimento: STI - UFC. Todos os direitos reservados.

- 5) Após o preenchimento e após clicar em “Enviar”, surgirá a mensagem de que a sua solicitação foi realizada com sucesso.



The screenshot shows a web page header for the Universidade Federal do Ceará. The main content area contains a confirmation message in Portuguese, stating that the request was received successfully and that the user will be contacted as soon as possible. Below the message are two buttons: 'Uma nova solicitação' and 'Sair'. At the bottom of the page, there is a small copyright notice: '© 2007 Projeto e desenvolvimento: STI - UFCE. Todos os direitos reservados.'

 UNIVERSIDADE  
FEDERAL DO CEARÁ

**Solicitação de Atendimento recebida com sucesso!**  
Foi enviado para o seu e-mail [guiliana.lima@ufce.br](mailto:guiliana.lima@ufce.br) o número de sua ordem de serviço.  
Entraremos em contato o mais breve possível.

O que você deseja fazer?

[Uma nova solicitação](#) | [Sair](#)

© 2007 Projeto e desenvolvimento: STI - UFCE. Todos os direitos reservados.



Classificação	Código	Revisão	Emissão	Folha
<input type="checkbox"/> C <input type="checkbox"/> R <input checked="" type="checkbox"/> P	P01/STI/UFC	04	05/06/2013	1/8

(C)onfidencial; (R)estrita; (P)ública

**Universidade Federal do Ceará**  
Secretaria de Tecnologia da Informação

**Política de Segurança da Informação e  
Comunicação**

## ORIGEM

Secretaria de Tecnologia da Informação

## REFERENCIA NORMATIVA

Decreto 3505 de 13 de junho de 2000.  
Decreto 4553 de 27 de dezembro de 2002.  
Normativa Complementar 01/DSIC/GSIPR de 13 de outubro de 2008.  
Normativa Complementar 03/DSIC/GSIPR de 30 de junho de 2009.  
Normativa Complementar 04/DSIC/GSIPR de 14 de agosto de 2009.  
Normativa Complementar 05/DSIC/GSIPR de 14 de agosto de 2009.  
Normativa Complementar 06/DSIC/GSIPR de 11 de novembro de 2009.  
Normativa Complementar 07/DSIC/GSIPR de 06 de maio de 2010.  
Normativa Complementar 08/DSIC/GSIPR de 19 de agosto de 2010.  
NBR ISO/IEC 27002:2005.  
NBR ISO/IEC 27005:2008.

## CAMPO DE APLICAÇÃO

Esta Política aplica-se no âmbito da Universidade Federal do Ceará

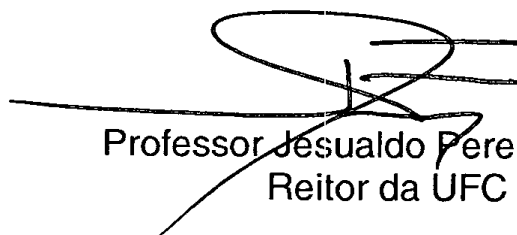
## SUMÁRIO

- Introdução
1. Escopo
  2. Conceitos e Definições
  3. Princípios
  4. Diretrizes Gerais
  5. Competências e Responsabilidades
  6. Penalidades
  7. Atualização
  8. Histórico de Mudanças

## INFORMAÇÕES ADICIONAIS

Não há

## APROVAÇÃO

  
Professor Jesualdo Pereira Farias  
Reitor da UFC

Classificação	Código	Revisão	Emissão	Folha
<input type="checkbox"/> C <input type="checkbox"/> R <input checked="" type="checkbox"/> P	P01/STI/UFC	04	05/06/2013	2/8

(C)onfidencial; (R)estrita; (P)ública

## Introdução

A Segurança da Informação, ou simplesmente SI, é a proteção da informação nas suas mais diversas formas. Não importa se ela é escrita, impressa ou armazenada digitalmente. Nem se ela é transmitida pelo correio ou por e-mail. Por envolver também os aspectos relacionados à comunicação, usa-se comumente o termo Segurança da Informação e Comunicação, ou simplesmente o acrônimo SIC.

Essa proteção é contra vários tipos de ameaças que, se efetivadas, podem gerar prejuízos à organização. A segurança da informação pode ser obtida a partir da implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e soluções de TI.

A Segurança da Informação é fundamental para os negócios, inclusive do setor público. Nesse caso, a segurança da informação assume papel importante nos serviços de governo eletrônico (e-gov), ao evitar ou reduzir os riscos de fraude, sabotagem, vandalismo, incêndios e inundações, além de proteger as infraestruturas críticas das organizações.

A Política de Segurança da Informação e Comunicação é um documento que contém um conjunto de princípios e diretrizes que norteiam a gestão da segurança da informação e que devem ser observados pelo corpo técnico e gerencial da organização, bem como por seus usuários internos e externos, a fim de garantir que os Ativos sejam assegurados. Os Ativos são qualquer bem, material ou não, que tenha valor para a organização.

## 1. Escopo

Fazem parte do escopo desta política:

- a) Apresentar de forma clara a visão desta instituição, e de sua administração superior, relacionada à segurança da informação e comunicação;
- b) Definir diretrizes que orientarão a criação de normas e procedimentos relacionados à segurança da informação e comunicação no âmbito desta instituição; e
- c) Prover meios para atingir a excelência na qualidade dos serviços prestados por esta instituição, no que tange à confidencialidade, integridade, disponibilidade, autenticidade e não-repúdio das informações.

## 2. Conceitos e Definições

Para efeito desta política, serão adotadas as seguintes definições:

- a) Ativo: qualquer bem, material ou não, que tenha valor para esta instituição;
- b) Ativo Custodiado: Ativo de terceiro que é administrado e conservado por esta instituição;
- c) Ativo de Informação: Ativo que guarda informação de valor para esta instituição;

Classificação	Código	Revisão	Emissão	Folha
<input type="checkbox"/> C <input type="checkbox"/> R <input checked="" type="checkbox"/> P	P01/STI/UFC	04	05/06/2013	3/8

(C)onfidencial; (R)estrita; (P)ública

- d) Autenticidade: garantia da veracidade da identidade dos usuários e da origem das informações;
- e) Classificação do Ativo: definição do nível de segurança adequado para um Ativo;
- f) Confidencialidade: garantia de que uma informação estará disponível apenas para os usuários devidamente autorizados;
- g) Cópia de Segurança: cópia reserva que deve ser utilizada no processo de restauração, caso a cópia original seja perdida ou danificada. Também conhecida como Backup.
- h) Diretriz: conjunto de orientações que devem ser observadas para a produção de Normas e Procedimentos específicos;
- i) Disponibilidade: garantia de que uma informação estará disponível sempre que os usuários autorizados necessitarem;
- j) Gestor do Ativo: membro desta instituição responsável pela segurança de um determinado Ativo;
- k) Incidente de Segurança: evento identificado em um Ativo que indica uma violação da Política de Segurança da Informação e Comunicação;
- l) Integridade: garantia de que uma informação estará disponível de forma correta e completa, sem adulterações;
- m) Não-repúdio: garantia de que os atos de um usuário são irrefutáveis, ou seja, não poderão ser negados;
- n) Norma: conjunto de regras que devem ser seguidas por um grupo;
- o) Política de Segurança da Informação e Comunicação: conjunto de princípios que norteiam a gestão da segurança da informação e que devem ser observados pelo corpo técnico e gerencial da instituição, bem como por seus usuários internos e externos, a fim de garantir que os Ativos sejam assegurados; e
- p) Procedimento: conjunto de ações que devem ser realizadas por um grupo para produzir algo.

### 3. Princípios

O crescente uso de recursos tecnológicos para controle e transmissão da informação, vem transformando os conceitos de comunicação no mundo. Entretanto, este crescimento trouxe vários problemas/ataques relativos à segurança da informação e comunicação cujos Princípios devem ser observados:

- a) Autenticidade diz respeito ao conjunto de meios que permite assegurar que os dados enviados e recebidos provêm das entidade declaradas. Problema que originou este princípio: Informações digitais de identificação podem ser falsificadas;
- b) Confidencialidade se baseia em conceitos que permitem assegurar que a informação não pode ser acessada por pessoas não autorizadas. Problema que originou este princípio: Toda



Classificação	Código	Revisão	Emissão	Folha
<input type="checkbox"/> C <input type="checkbox"/> R <input checked="" type="checkbox"/> P	P01/STI/UFC	04	05/06/2013	4/8

(C)onfidencial; (R)estrita; (P)ública

informação circulante pode ser acessada;

- c) Disponibilidade é o princípio que garante que a informação vai estar sempre disponível para uso legítimo do destinatário. Problema que originou este princípio: Ataque para deixar indisponível a informação;
- d) Integridade diz respeito às técnicas que possibilitam verificar se os dados foram alterados ou suprimidos. Problema que originou este princípio: Dados podem ser capturados e modificados; e
- e) Não-Repudição são formas de impedir que uma entidade (emissor ou receptor) negue a participação em uma troca de informação. Problema que originou este princípio: Em determinadas trocas de informações em rede, não existe testemunha de participação.
- f) Legalidade diz respeito à obediência aos princípios constitucionais, administrativos e à legislação vigente.

## 4. Diretrizes Gerais

Esta política e seus documentos complementares são regidos pelas Diretrizes apresentadas a seguir. Elas devem orientar a definição de Normas e Procedimentos específicos relacionados à segurança da informação e comunicação.

### 4.1. Tratamento dos Ativos

Com relação ao Tratamento dos Ativos, que envolve a Identificação, Classificação, Manipulação e Conservação dos Ativos, devem ser considerados os seguintes aspectos:

- a) todo Ativo Custodiado ou de propriedade desta instituição deve ser inventariado;
- b) todo Ativo Custodiado ou de propriedade desta instituição deve ser protegido segundo as Diretrizes descritas nesta política e nas demais regulamentações em vigor;
- c) todo Ativo Custodiado ou de propriedade desta instituição deve ter um Gestor do Ativo, sobre quem recai a responsabilidade sobre a segurança do respectivo Ativo;
- d) todo Ativo de Informação custodiado ou de propriedade desta instituição deve ser classificado quanto aos aspectos de confidencialidade, integridade, autenticidade, não-repúdio e disponibilidade, de forma explícita ou implícita. Esse processo de classificação deve ser implementado e mantido, em conformidade com a legislação vigente, visando estabelecer os controles de segurança necessários a cada Ativo de Informação;
- e) todo Ativo Custodiado ou de propriedade desta instituição deve ser cedido somente mediante autorização formal. Essa autorização deve observar a classificação do ativo e a legislação vigente; e
- f) toda classificação e cessão dos Ativos deve ser feita pelo respectivo Gestor do Ativo.

Classificação	Código	Revisão	Emissão	Folha
<input type="checkbox"/> C <input type="checkbox"/> R <input checked="" type="checkbox"/> P	P01/STI/UFC	04	05/06/2013	5/8

(C)onfidencial; (R)estrita; (P)ública

## 4.2. Controle de Acesso

Com relação ao Controle de Acesso, que envolve o Acesso Lógico e Físico aos Ativos, devem ser considerados os seguintes aspectos:

- todo uso dos Ativos deve ser autorizado pelo respectivo Gestor do Ativo e ocorrer mediante identificação única e intransferível do usuário;
- todo uso dos Ativos deve ser controlado e limitado ao mínimo necessário para o cumprimento das atividades de cada usuário. Qualquer outra forma de uso deve ser previamente autorizada formalmente pelo respectivo Gestor do Ativo;
- sempre que houver a admissão, mudança das atribuições ou desligamento de membros desta instituição, será responsabilidade da chefia imediata notificar aos Gestores dos Ativos utilizados por esse membro. Os Gestores dos Ativos deverão providenciar os ajustes necessários dos privilégios de acesso dos respectivos Ativos; e
- todo ambiente deve ser classificado e protegido com mecanismos adequados de segurança de acordo com a criticidade e o sigilo dos Ativos que são mantidos naquele local.

## 4.3. Auditoria e Conformidade

Com relação à Auditoria e Conformidade devem ser considerados os seguintes aspectos:

- todo uso de Ativo, sempre que possível, deve gerar trilhas de auditoria que devem ser mantidas para efeito de análise segundo as diretrizes descritas nesta política e as demais regulamentações em vigor; e
- todo uso de Ativo é passível de monitoramento e auditoria e, sempre que possível, deve ser analisado em busca de indícios de descumprimento desta política.

## 4.4. Gestão de Continuidade

Com relação à Gestão de Continuidade, que envolve o Backup, Plano de Contingência, Testes, Treinamentos e Documentação de procedimentos, devem ser considerados os seguintes aspectos:

- deve ser estabelecida a gestão de continuidade no âmbito desta instituição com o objetivo de minimizar os impactos de falhas fortuitas dos Ativos que suportam as operações desta instituição;
- deve ser elaborado plano de contingência para o restabelecimento das operações críticas interrompidas por falhas fortuitas dos Ativos desta instituição;
- todo Ativo de Informação desta instituição, seja eletrônico ou não, deve ser armazenado em meio que ofereça salvaguarda adequada e segurança;
- todo Ativo de informação desta instituição, se eletrônico, deve dispor de Cópia de Segurança atualizada regularmente e com frequência adequada; e
- toda Cópia de Segurança deve ser mantida em lugar seguro e diferente do lugar onde o

Classificação	Código	Revisão	Emissão	Folha
<input type="checkbox"/> C <input type="checkbox"/> R <input checked="" type="checkbox"/> P	P01/STI/UFC	04	05/06/2013	6/8

(C)onfidencial; (R)estrita; (P)ública

respectivo Ativo de Informação está localizado. O lugar escolhido deve garantir a segurança da cópia, caso alguma ameaça a que está sujeito o respectivo Ativo de Informação se concretize.

## 4.5. Gestão de Risco

Com relação à Gestão de Risco, que envolve o Inventariamento dos Ativos, Análise, Avaliação, Tratamento, Aceitação, Comunicação e Monitoramento dos Riscos, devem ser considerados os seguintes aspectos:

- a) todo impacto associado aos Ativos deve ser avaliado e, se possível, minimizado; e
- b) toda ação de segurança da informação deve ser feita com base na avaliação da criticidade dos Ativos.

## 5. Competências e Responsabilidades

Para o efetivo cumprimento das diretrizes estabelecidas por esta política, ficam instituídas as seguintes competências e responsabilidades nesta instituição:

### 5.1. Autoridade Máxima

São responsabilidades da Autoridade Máxima desta instituição:

- a) instituir o Comitê Gestor de Segurança da Informação e Comunicação;
- b) designar o Dirigente do Departamento de Segurança da Informação e Comunicação;
- c) instituir o Departamento de Segurança da Informação e Comunicação;
- d) aprovar a Política de Segurança da Informação e Comunicação; e
- e) garantir os recursos necessários para implementação destas diretrizes.

### 5.2. Comitê Gestor de Segurança da Informação e Comunicação

São responsabilidades do Comitê Gestor de Segurança da Informação e Comunicação desta instituição:

- a) propor, analisar e aprovar normas, procedimentos e soluções específicas que atendam às necessidades de segurança da informação e comunicação;
- b) apoiar a implementação das ações de segurança da informação e comunicação; e
- c) analisar os casos relacionados à segurança da informação e comunicação omissos nesta política.

Classificação	Código	Revisão	Emissão	Folha
<input type="checkbox"/> C <input type="checkbox"/> R <input checked="" type="checkbox"/> P	P01/STI/UFC	04	05/06/2013	7/8

(C)onfidencial; (R)estrita; (P)ública

### 5.3. Dirigente do Departamento de Segurança da Informação e Comunicação

São responsabilidades do Dirigente do Departamento de Segurança da Informação e Comunicação desta instituição:

- a) dirigir as atividades do Departamento de Segurança da Informação e Comunicação;
- b) assessorar e contribuir com as atividades do Comitê Gestor de Segurança da Informação e Comunicação;
- c) promover a cultura institucional de Segurança da Informação e Comunicação;
- d) propor recursos necessários às ações de Segurança da Informação e Comunicação; e
- e) tratar de assuntos relacionados à Segurança da Informação e Comunicação na instituição.

### 5.4. Departamento de Segurança da Informação e Comunicação

São responsabilidades do Departamento de Segurança da Informação e Comunicação desta instituição:

- a) desenvolver ações para capacitar e conscientizar os membros desta instituição sobre Segurança da Informação e Comunicação;
- b) desenvolver ações relacionadas à Gestão de Risco, conforme previsto nesta política;
- c) desenvolver ações relacionadas à Auditoria e Conformidade, conforme previsto nesta política.
- d) monitorar, sempre que possível, os Ativos de forma a identificar a ocorrência de Incidentes de Segurança; e
- e) definir processo formal para tratar e responder os Incidentes de Segurança identificados ou reportados.

### 5.5. Membros

São responsabilidades dos Membros desta instituição:

- a) estar ciente e seguir esta política e as demais regulamentações em vigor relacionadas à segurança da informação; e
- b) comunicar ao Departamento de Segurança da Informação e Comunicação qualquer Incidente de Segurança de que venha a tomar conhecimento, seja suspeito ou confirmado. A comunicação deve ocorrer por meio de processo formal.

Classificação	Código	Revisão	Emissão	Folha
<input type="checkbox"/> C <input type="checkbox"/> R <input checked="" type="checkbox"/> P	P01/STI/UFC	04	05/06/2013	8/8

(C)onfidencial; (R)estrita; (P)ública

## 6. Penalidades

As violações das Diretrizes, Normas ou Procedimentos, que juntas formam a Política de Segurança da Informação e Comunicação desta instituição, resultarão em sanções não só disciplinares, mas também cíveis e penais, tendo em vista que atos ilícitos praticados em desacordo com essa política podem ter também sanções definidas na legislação brasileira, como é o caso, por exemplo, da Lei nº 9.601/98 (lei de proteção aos direitos autorais); dos artigos 153, §1º-A (divulgação de segredo), 154-A (Invasão de dispositivo informático), 168 (apropriação indébita), 266 (Interrupção ou perturbação de serviço informático), 313-A (inserção de dados falsos em sistemas de informação) e 313-B (modificação ou alteração não autorizada de sistema de informação), do Código Penal Brasileiro; e do art. 927 (ato ilícito e reparação de dano) do Código Civil Brasileiro de 2002.

As sanções disciplinares deverão ser previstas em documento normativo específico aprovado pelo Comitê Gestor de Segurança da Informação e Comunicação. Os casos não previstos deverão ser avaliados individualmente pelo mesmo Comitê.

## 7. Atualização

Esta política e os instrumentos normativos gerados a partir dela devem ser revisados sempre que necessário, contanto que não exceda o período máximo de 2 (dois) anos.

## 8. Histórico de Mudanças

Na Tabela 1 devem ser registradas todas as alterações realizadas nesta política.

Data	Revisão	Responsável	Detalhes
19/07/2011	00	Márcio Correia	Produção da versão inicial para aprovação.
22/07/2011	01	Márcio Correia	Realizados ajustes aprovados na reunião do comitê dirigente da STI. Basicamente questões relacionadas à redação do documento.
10/11/2011	02	Márcio Correia	Realizados ajustes aprovados na reunião com os Diretores Geral e Adjunto da STI. Correções ortográficas. Ajustes nos conceitos e definições utilizados. Realizadas também melhorias no detalhamento e adequação das Competências e Responsabilidades.
31/05/2012	03	Márcio Correia	Realizados ajustes aprovados em 27/04/2012 na reunião do CATI. Ajustes de alguns princípios, definições e termos utilizados. O item “3. Princípios” foi reescrito com foco na comunicação com o usuário e perdeu o caráter regulatório. Foi removido o item “4.1 b” que tratava da propriedade das informações produzidas na instituição.
05/06/2013	04	Márcio Correia	Realizados ajustes aprovados em 05/06/2012 na reunião do CATI. Atendendo sugestões da Auditoria Interna, enviados à STI via Solicitação de Auditoria nº 022/2012.

**Tabela 1** – Tabela de histórico de mudanças desta política.