Classificação	Código	Revisão	Emissão	Folha
[ ] C [ ] R [X] P	P01/STI/UFC	04	05/06/2013	1/8

(C)onfidencial; (R)estrita; (P)úblico

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

INFORMAÇÕES ADICIONAIS

Não há

APROVAÇÃO

Professor Jesualdo Pereira Farias
Reitor da UFC

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;

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 irretratáveis, 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

informação circulante pode ser acessada;

c) Disponibilidade é o principio 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-Repudiação 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.

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:

a) todo uso dos Ativos deve ser autorizado pelo respectivo Gestor do Ativo e ocorrer mediante identificação única e intransferível do usuário;

b) 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;

c) 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

d) 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:

a) 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

b) 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:

a) 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;

b) deve ser elaborado plano de contingência para o restabelecimento das operações críticas interrompidas por falhas fortuitas dos Ativos desta instituição;

c) todo Ativo de Informação desta instituição, seja eletrônico ou não, deve ser armazenado em meio que ofereça salvaguarda adequada e segurança;

d) todo Ativo de informação desta instituição, se eletrônico, deve dispor de Cópia de Segurança atualizada regularmente e com frequência adequada; e

e) toda Cópia de Segurança deve ser mantida em lugar seguro e diferente do lugar onde o

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.

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.

6. Penalidades

As violações das Diretrizes, Normas ou Procedimentos, que juntas formam a Política de Segurança da Informação e Comunicação desta instituição, resultarão em sansões 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 sansões 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.