Classificação*						Código	Revisão	Emissão	Folha
	C		R	X	P	P01/STI/UFC	05		1/17

*Confidencial; Restrito; Público.

Universidade Federal do Ceará
Secretaria de Tecnologia da Informação

Política de Segurança da Informação e Comunicação

ORIGEM

Secretaria de Tecnologia da Informação.

REFERÊNCIA NORMATIVA

Acórdão No 1608/2008 TCU-Plenário.
Acórdão No 2308/2010 TCU-Plenário.
Decreto 3505 de 13 de junho de 2000.
Decreto 7845 de 14 de novembro de 2012.
Instrução Normativa GSI No 1, de 13 de junho de 2008.
Instrução Normativa Conjunta CGU/MP No1, de 10 de maio de 2016.
Normativa Complementar 01/DSIC/GSIPR de 13 de outubro de 2008.
Normativa Complementar 02/IN01/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 15 de fevereiro de 2013.
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 14 de julho de 2014.
Normativa Complementar 08/DSIC/GSIPR de 19 de agosto de 2010.
Normativa Complementar 10/DSIC/GSIPR de 30 de Janeiro de 2012.
Normativa Complementar 11/IN01/DSIC/GSIPR, de 10 de Fevereiro de 2012
Normativa Complementar 18/IN01/DSIC/GSIPR, de 10 de Abril de 2013
NBR ISO/IEC 27001:2013
NBR ISO/IEC 27002:2013.
NBR ISO/IEC 27005:2011.

CAMPO DE APLICAÇÃO

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

INFORMAÇÕES ADICIONAIS

Não há.

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.

APROVAÇÃO

Henry de Holanda Campos
Reitor

Histórico de Mudanças

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 05/06/2013 na reunião do CATI. Atendendo sugestões da Auditoria Interna, enviados à STI via Solicitação de Auditoria no 022/2012.
	05	DSEG	

Tabela 1. Histórico de mudanças desta política.

Sumário

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 (SIC).

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

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) Artefato malicioso: qualquer programa de computador, ou parte dele, construído com a intenção de causar danos, obter informações não autorizadas ou interromper o funcionamento de sistemas e/ou redes de computadores;

b) Acesso: ato de ingressar, transitar, conhecer ou consultar a informação, bem como a possibilidade de usar os ativos de informação de um órgão ou entidade.

c) Agente responsável: é o servidor designado no documento de criação da ETIR e responsável pela mesma, é também o ponto de contato entre a ETIR e o CTIR Gov;

d) Ativo: qualquer bem, material ou não, que tenha valor para esta instituição;

e) Ativo custodiado: ativo de terceiro que é administrado e conservado por esta instituição;

f) Ativo de informação: ativo que guarda informação de valor para esta instituição;

g) Capacitação: atividade de ensino que tem como objetivo orientar sobre o que é SIC, fazendo com que os participantes saibam aplicar os conhecimentos em sua rotina pessoal e profissional, além de servirem como multiplicadores sobre o tema, estando aptos para atuar em suas organizações como Gestores de SIC;

h) Classificação do ativo: definição do nível de segurança adequado para um Ativo;

i) Conformidade em SIC: cumprimento das legislações, normas e procedimentos relacionados à Segurança da Informação e Comunicações da organização;

j) Conscientização em SIC: ações educativas que impactam na mudança de postura e de comportamento com relação a SIC.

k) Conteúdo ilegal: todo e qualquer dado, informação ou sistema que venha a infringir algum instrumento legal vigente no país;

l) 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;

m) CTIR Gov: Centro de Tratamento de Incidentes de Segurança de Redes de Computadores da Administração Pública Federal (APF). Responsável pelo atendimento aos incidentes em redes de computadores da APF;

n) Dados sensíveis: informações pessoais que são particularmente propensas a causar discriminação ao seu titular;

o) Diretriz: conjunto de orientações que devem ser observadas para a produção de Normas e Procedimentos específicos;

p) E-mail institucional: serviço de correio eletrônico oferecido por esta instituição para seus servidores como instrumento de trabalho.

q) Evento: qualquer ocorrência observável em um sistema ou rede de computadores;

r) Evento adverso: qualquer evento com consequências negativas, por exemplo: quebra de sistemas, inundação de pacotes, acesso não-autorizado, dentre outros;

s) Gestor do ativo: membro desta instituição responsável pela segurança de um determinado Ativo;

t) Hardening: é um processo de mapeamento das ameaças, mitigação dos riscos e execução das atividades corretivas, com foco na infraestrutura e tornando um sistema menos vulnerável à ameaças.

u) Incidente de segurança: qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas ou redes de computadores. Nesse documento o termo “incidente” será utilizado com o mesmo significado de “incidente de segurança” aqui definido;

v) Log de dados: o processo de registro de eventos relevantes num sistema computacional;

w) Norma: conjunto de regras que devem ser seguidas por um grupo;

x) Membros: todo corpo docente, discente, técnico-administrativos e prestadores de serviços;

y) 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;

z) Ponto de acesso: dispositivo de hardware utilizado para prover acesso sem fio à uma rede computacional;

aa) Procedimento: conjunto de ações que devem ser realizadas por um grupo para produzir algo;

bb) Protocolo criptográfico: conjunto de ações que executam operações criptográficas sobre um dado ou informação;

cc) Público-alvo: é o conjunto de pessoas, setores, órgãos ou entidades atendidas por uma equipe;

dd) Serviços (ETIR): é o conjunto de procedimentos, estruturados em um processo bem definido, oferecido ao público-alvo da ETIR;

ee) Serviço de anonimato: ferramenta (programa) ou sítio utilizado para ocultar a origem de uma ação em redes computacionais;

ff) Sensibilização: atividade de ensino que tem como objetivo orientar sobre o que é Segurança da Informação e Comunicações (SIC) fazendo com que os participantes possam perceber em sua rotina pessoal e profissional ações que precisam ser corrigidas;

gg) Spam: termo usado para referir-se aos e-mails não solicitados, que geralmente são enviados para um grande número de pessoas;

hh) Spammer: aquele(a) que envia spam(s);

ii) Tratamento de incidentes de segurança em redes de computadores: conjunto de ações que visam receber, analisar e responder os incidentes de segurança ocorridos em uma rede e/ou sistema computacional;

jj) Usuário autenticado: usuário identificado como autêntico para um determinado ativo; e

kk) Vulnerabilidade: qualquer fragilidade dos sistemas e redes de computadores que permitam a exploração maliciosa e acessos indesejáveis ou não autorizados.

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 entidades declaradas;

b) Confidencialidade se baseia em conceitos que permitem assegurar que a informação não pode ser acessada por pessoas não autorizadas;

c) Disponibilidade é o princípio que garante que a informação estará sempre disponível para uso legítimo do destinatário;

d) Integridade diz respeito às técnicas que possibilitam verificar se os dados foram alterados ou suprimidos indevidamente;

e) Não-Repudiação são formas de impedir que uma entidade (emissor ou receptor) negue a participação em uma troca de informação;

f) Legalidade diz respeito à obediência aos princípios constitucionais, administrativos e à legislação vigente.

4. Diretrizes gerais

Esta política é regida 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 de ativos

Com relação ao tratamento dos ativos, que envolve a identificação, classificação, manipulação e conservação dos ativos, devem ser considerados os seguintes aspectos para todo ativo custodiado ou de propriedade desta instituição deve:

a) ser inventariado;

b) ser protegido segundo as diretrizes descritas nesta política e nas demais regulamentações em vigor;

c) ter um gestor do ativo, sobre quem recai a responsabilidade sobre a segurança do respectivo ativo;

d) ser autorizado pelo respectivo gestor do ativo;

e) 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;

f) ser cedido somente mediante autorização formal. Essa autorização deve observar a classificação do ativo e a legislação vigente;

g) ser feita a classificação e cessão 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 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;

b) 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;

c) 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 para o uso do Ativo:

a) deve gerar trilhas de auditoria que devem ser mantidas para efeito de análise; e

b) 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. Se eletrônico, deve dispor de cópia de segurança atualizada regularmente e com frequência adequada;

d) 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; e

e) ambientes críticos devem ter planos de contingência ou continuidade de negócios definidos, revisados e testados periodicamente.

4.5. Conscientização e Capacitação

Com relação à Conscientização e Capacitação em segurança da informação e comunicação, devem ser considerados os seguintes aspectos:

a) deve ser estabelecido ações contínuas de conscientização no âmbito desta instituição com o objetivo de minimizar os riscos relativos a falhas de natureza humana; e

b) deve ser incentivado a construção de uma cultura organizacional consciente em segurança da informação e comunicação.

4.6. Tratamento de incidentes de segurança em redes de computadores

Com relação ao tratamento de incidentes de segurança em redes de computadores nesta instituição, devem ser observados os seguintes aspectos:

a) deve ser instituído, sob a Divisão de Segurança da Informação (DSEG), a Equipe de Tratamento de Incidentes de Segurança em Redes de Computadores (ETIR);

b) devem ser estabelecidas ações e procedimentos formais para o tratamento de incidentes;

c) as ações e procedimentos devem guiar-se pelos padrões e procedimentos técnicos e normativos fornecidos pelo CTIR Gov, bem como nas melhores práticas de mercado, desde que não haja conflito com as instruções normativas desta política;

d) dentre os serviços de tratamento de incidentes, devem estar, no mínimo, as atividades de receber, analisar e responder os incidentes de segurança oriundos do âmbito desta instituição;

e) os incidentes recebidos devem ser devidamente registrados e classificados;

f) deve haver uma interface com o CTIR Gov e outras entidades relacionadas ao tratamento de incidentes nacionais e internacionais;

g) deve haver uma formalização para a troca de informações e a forma de comunicação entre a ETIR e demais entidades com as quais venha a estabelecer alguma forma de cooperação.

4.7. Gestão de Riscos

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 desta política, ficam instituídas as seguintes competências e responsabilidades nesta instituição:

5.1. Autoridade máxima

São responsabilidades da Autoridade Máxima desta instituição:

a) instituir e atualizar o Comitê Gestor de Segurança da Informação e Comunicação;

b) designar o Dirigente da Divisão de Segurança da Informação;

c) instituir a Divisão de Segurança da Informação;

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 da Divisão de Segurança da Informação

São responsabilidades do Dirigente da Divisão de Segurança da Informação desta instituição:

a) dirigir as atividades da Divisão de Segurança da Informação;

b) coordenar 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) tratar de assuntos relacionados à Segurança da Informação e Comunicação na instituição.

f) designar, dentre os membros da DSEG, o Gestor de Risco que acompanhará o desenvolvimento do projeto de Gestão de Riscos de SIC;

g) designar, dentre os membros da DSEG, o Agente Responsável pela ETIR e seu substituto;

h) assessorar as atividades da DSEG;

i) intermediar a garantia dos recursos necessários para as atividades da DSEG; e

j) instituir a Gestão de Riscos de Segurança da Informação e Comunicação.

5.4. Divisão de Segurança da Informação

São responsabilidades da Divisão de Segurança da Informação desta instituição:

a) desenvolver ações para capacitar e conscientizar os membros desta instituição sobre Segurança da Informação;

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) definir processo formal para tratar e responder os Incidentes de Segurança identificados ou reportados;

f) desenvolver ações relacionadas à Gestão de Continuidade, conforme previsto nesta política;

g) propor normas e procedimentos seguindo as diretrizes desta política;

h) auditar o cumprimento desta política bem como das normas e procedimentos ligadas esta POSIC;

5.5. Membros da Instituição

São responsabilidades dos Membros desta instituição:

a) estar ciente e seguir esta política e as demais regulamentações em vigor relacionadas à segurança da informação;

b) comunicar à Divisão 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;

c) cumprir e difundir as regulamentações descritas nesta política;

d) cabe ao usuário reportar descumprimentos desta política; e

e) todos os agentes públicos têm a responsabilidade de contribuir para a melhoria dos níveis de segurança da informação e comunicação.

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 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.

Anexo I

Normas Complementares

CAPÍTULO I
NORMATIZA O USO DE INTERNET

TÍTULO I
DO OBJETIVO

Art. 1º Este capítulo visa normatizar as diretrizes referentes ao uso da internet.

TÍTULO I
DAS NORMAS PARA O USO DA INTERNET

Art. 2º Para acessar o serviço de Internet o usuário deverá ser autenticado.

Art. 3º É bloqueado o acesso a sítios com conteúdos indevidos ou inadequados ao ambiente de trabalho.

§ 1º Em caso de necessidade de acesso a um sítio que esteja bloqueado, a solicitação de liberação deve ser feita formalmente à STI.

§ 2º Embora um site com conteúdo ilegal não esteja bloqueado, não implica dizer que o acesso ao mesmo seja permitido.

§ 3º Todos os usuários devem utilizar o acesso à internet respeitando o código de ética desta universidade.

Art. 4º A divulgação e/ou compartilhamento de informações desta Universidade deverá ser feita respeitando a classificação da informação em questão.

Art. 5º É proibida a utilização de software P2P (tais como µTorrent, BitTorrent, Emule e similares).

Parágrafo único. Em casos excepcionais a solicitação de liberação deve ser feita formalmente à STI.

Art. 6º É proibida a realização de download de software que infringe os direitos autorais.

Art. 7º É proibida a utilização de serviços de anonimato para acesso à internet.

Art. 8º É necessário ter os mesmos cuidados no uso da rede sem fio desta universidade:

Parágrafo único. É permitido somente o uso de pontos de acesso homologados pela instituição.

Art. 9º Todos os funcionários, contratados, terceirizados e outros agentes que utilizam os recursos de rede são responsáveis pela segurança, zelo e bom uso das informações às quais têm acesso, sejam elas do próprio governo, do cidadão ou de outro órgão.

Art. 10º Deverão ser gerados registros dos acessos realizados por usuários.

Art. 11º Os registros citados no item anterior deverão ser devidamente classificados e tratados.

Art. 12º Deverão ser utilizados mecanismos automáticos para inibir que equipamentos externos se conectem à rede corporativa.

Art. 13º Realizar processo de Hardening nos servidores e ativos de rede;

§ 1º Todos os sítios e sistemas que lidam com dados sensíveis devem implementar protocolo criptográfico forte.

§ 2º Realizar a configuração dos serviços e dispositivos ligados a monitoramento, autenticação, firewall, filtros de conteúdo;

Art. 14º Realizar processo de hardening nos computadores institucionais e nos ativos de redes.

Art. 15º Nas configurações das redes sem fio desta instituição:

§ 1º Deverá ser utilizado um sistema de autenticação de usuários para o acesso ao serviço;

§ 2º Deverá ser utilizado um protocolo criptográfico forte para o tráfego dos dados da rede sem fio;

§ 3º Deverá ser utilizado um sistema que gerencie os pontos de acessos.

Art. 17º As informações e os recursos de TI para acesso à rede desta instituição e seus recursos agregados devem ser disponibilizados, única e exclusivamente àqueles que necessitem deles para o exercício de suas funções.

Art. 18º Os acessos aos dados e informações devem ser registrados, de modo que a qualquer momento estejam disponíveis as informações sobre acesso ou tentativas de acesso, frustradas ou não.

Art. 19º É de responsabilidade da instituição promover a filtragem de acessos indevidos provenientes de suas redes, com destino a outra(s) rede(s) de outros órgãos, ou para a Internet. Esses acessos indevidos podem ser gerados por ataques direcionados, códigos maliciosos (malware) e ataques de negação de serviço (DDoS), dentre outros.

CAPÍTULO II
NORMATIZA O USO DO E-MAIL INSTITUCIONAL

TÍTULO I
DO OBJETIVO

Art. 1º Este capítulo visa normatizar as diretrizes referentes ao uso do e-mail institucional.

TÍTULO II
DAS NORMAS PARA O USO DO E-MAIL INSTITUCIONAL

Art. 2º Para acessar o serviço de E-mail institucional o usuário deverá ser autenticado.

Art. 3º Os serviços de correio eletrônico hospedados nos servidores da UFC são oferecidos como um recurso profissional com o intuito de apoiar os usuários no cumprimento de seus objetivos institucionais.

Art. 4º Cada usuário é responsável por utilizar os serviços de correio eletrônico de maneira profissional, ética e legal.

Art. 5º Não devem ser solicitadas informações pessoais dos usuários através de correio eletrônico.

§1º O usuário não deve clicar em links que solicitem a atualização de suas informações pessoais.

§2º O usuário deve reportar a Divisão de Segurança da Informação (DSEG) sobre o recebimento de mensagens suspeitas ou que viole esta norma.

§3º É proibido o envio de grande quantidade de mensagens do tipo spam, ficando os spammers sujeitos à penalidade prevista nesta norma.

§4º O usuário tem total responsabilidade pelo envio de anexos nas mensagens, ficando o mesmo também responsável pela garantia da não violação do princípio da legalidade.

Art. 6º A divulgação e o compartilhamento de informações desta Universidade deverá ser feita respeitando a classificação da informação em questão.

Art. 7º É proibida a utilização do E-mail Institucional para fins que não caracterizem ou prestem suporte às atividades de pesquisa, ensino e extensão.

Art. 8º Deverão ser gerados registros dos acessos realizados por usuários.

Art. 9º Configuração dos serviços e dispositivos ligados a monitoramento, autenticação, filtros anti-spam.

CAPÍTULO III
NORMATIZA O USO DE SENHAS

TÍTULO I
DO OBJETIVO

Art. 1º Este capítulo visa normatizar o uso de senha para os serviços e sistemas que o requererem.

TÍTULO II
DAS DIRETRIZES GERAIS

Art. 2º Para acessar os serviços, o usuário deverá ser autenticado.

Art. 3º A senha é de uso pessoal e intransferível, e tudo que for acessado é de responsabilidade do usuário.

Art. 4º Nunca armazenar usuários e senhas ou chaves criptográficas de sua aplicação no código fonte. Procurar utilizar serviços de autenticação.

Art. 5º A senha deve seguir as seguintes orientações:

§ 1º Deve ter comprimento mínimo de 8 caracteres;

§ 2º Obrigatoriamente a senha deve ser composta por letras, números e caracteres especiais;

§ 3º Não utilizar nenhuma das quatro senhas anteriores;

§ 4º Após tentativas frustradas, o sistema bloqueará temporariamente o acesso.

§ 5º A mudança de senha deve ser realizada, a cada 180 dias.