MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DE SERGIPE

# *PSI – Política de Segurança da Informação*

V.1.0

Maio 2012

# UNIVERSIDADE FEDERAL DE SERGIPE

Reitor

**Josué Modesto dos Passos Subrinho**

Vice-Reitor

**Ângelo Roberto Antoniolli**

## Comitê Gestor Provisório de Segurança da Informação - CGPSI

Presidente

**Ricardo José Paiva de Britto Salgueiro**

**Dilton Dantas de Oliveira**

**Rodrigus Oliveira Feitosa**

**Uriel Marx da Cunha Bispo**

# ÍNDICE

# POLÍTICA DE SEGURANÇA DA INFORMAÇÃO – PSI

## Apresentação

Este documento foi elaborado pelo Comitê Gestor Provisório da Política de Segurança da Informação da UFS, criado segundo Portaria nº 2003 de 05 de setembro de 2011, com as seguintes atribuições:

- Assessorar a Comissão de Tecnologia da informação da UFS (CTIn) na consecução de ações de Segurança da Informação que visem: proteção dos sistemas de informação contra a negação de serviço a usuários autorizados, assim como contra a intrusão, e a modificação desautorizada de dados ou informações, armazenados, em processamento ou em trânsito, abrangendo, inclusive, a segurança dos recursos humanos, da documentação e do material, das áreas e instalações das comunicações e computacional, assim como as destinadas a prevenir, detectar, deter e documentar eventuais ameaças a seu desenvolvimento;
- Apoiar todas as unidades da UFS no tratamento das questões de segurança da informação;
- Elaborar e apresentar para apreciação da CTIn uma proposta de documento visando o estabelecimento da Política de Segurança da Informação da UFS (PSI) num prazo máximo de 6 (seis) meses, em atendimento às solicitações da Controladoria Geral da União (CGU).

A PSI estabelece diretrizes definindo normas, procedimentos e instruções nos âmbitos estratégico, tático e operacional respectivamente, conforme a Norma ABNT NBR ISO 27001:2006 [ABNT, 2006].

A PSI deverá definir a composição, a organização, o funcionamento e a forma de designação do Comitê Gestor de Segurança da Informação da UFS definitivo.

# 1. Introdução

A UFS é composta pelos *campi* de São Cristóvão, da Saúde em Aracaju, Itabaiana, Laranjeiras e Lagarto, além de outras unidades de extensão em Aracaju. O *campus* de São Cristóvão é onde se localiza a Administração Central, o Centro de Processamento de Dados e o Ponto de Presença em Sergipe (PoP-SE) da Rede Nacional de Ensino e Pesquisa (RNP) que possibilita sua conexão a Internet. Os *campi* de São Cristóvão e Aracaju estão interligados pela Rede Metropolitana de Aracaju (MetroAju) que faz parte do projeto das Redes Comunitárias de Ensino e Pesquisa (Redecomep).

A rede da UFS oferece recursos computacionais e de redes para acesso aos Sistemas Integrados de Gestão – SIGs, permitindo a transmissão de um grande volume de comunicação, tanto interno quanto externo. Para isto, utiliza um grande número de ativos, essenciais para os negócios da universidade. Assim, os recursos computacionais e de rede da UFS e a informação através desses recursos precisam ser protegidos, como qualquer outro ativo importante para a UFS.

A PSI deverá proporcionar um ambiente computacional que se caracterize pela tentativa de manter a confidencialidade, integridade, legalidade e disponibilidade das informações, independentemente de onde elas estejam. Sua eficiência está diretamente ligada à adequação de suas diretrizes as características e necessidades peculiares a cada organização. Assim, este documento foi elaborado com base nas boas práticas já adotadas na UFS e em documentos disponibilizados por outras Instituições de Ensino Superior (IES) que representam os resultados de seus esforços no sentido de se obter uma boa PSI, tais como em [GSETI, 2011].

As demais seções da PSI apresentam na Seção 2 seus objetivos, na Seção 3, a definição de segurança da informação, na Seção 4, os aspectos da segurança da informação sob seus aspectos físico e lógico, na Seção 5, a definição de ativos de informação, na Seção 6, descreve sobre os incidentes de segurança, na Seção 7 estabelece os gestores da PSI, na Seção 8, decorre sobre a abrangência da segurança, na Seção 9, as penalidades e, finalmente, na Seção 10, a relação de documentos que compõem a PSI.

## 2. Objetivo

Este documento tem como objetivo específico definir uma Política de Segurança para a UFS, especialmente quanto à proteção dos seus ativos, estabelecendo procedimentos e recomendações visando prevenir e responder a incidentes de segurança.

## 3. Segurança da Informação

Considera-se como segurança da informação a preservação da autenticidade, confidencialidade, integridade, legalidade e disponibilidade da informação da universidade.

## 4. Aspectos da Segurança

A segurança pode ser enfocada sob dois aspectos: física e lógica.

Adota-se como segurança física o relacionado à proteção de edificações, infraestrutura e equipamentos, reduzindo as ameaças que possam colocar em risco o bom funcionamento dos sistemas.

Como segurança lógica, entende-se a segurança dos dados corporativos e acadêmicos da UFS armazenados nos servidores institucionais, tais como: servidores de redes, servidores de sistemas e de serviços à comunidade. Incluem-se ainda os dados gerados e armazenados em computadores de uso pessoal.

## 5. Ativos

São considerados Ativos qualquer coisa que tenha valor para a UFS. Alguns exemplos: banco de dados, *softwares*, equipamentos (computadores, *notebooks*), servidores, elementos de rede (roteadores, *switches*, entre outros), pessoas, processos e serviços [COELHO, 2010].

## 6. Incidentes de Segurança

Um incidente de segurança pode ser definido como qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de computação ou de redes de computadores. São exemplos de incidentes de segurança [CERT.br, 2011]:

- Tentativas de ganhar acesso não autorizado a sistemas ou dados;
- Ataques de negação de serviço;
- Uso ou acesso não autorizado a um sistema;
- Modificações em um sistema, sem o conhecimento, instruções ou consentimento prévio do dono do sistema;
- Desrespeito à política de segurança ou à política de uso aceitável de uma empresa ou provedor de acesso.

## 7. Componentes Gestores da Política de Segurança

A PSI da UFS estabelece os órgãos, comissões, grupos e pessoas responsáveis pela Política de Segurança e suas atribuições, como descritos nas subseções a seguir.

### 7.1 Comissão de Tecnologia da Informação – CTIn

A CTIn é responsável por formular as políticas da Universidade na área de informática e coordenar a execução dessas políticas pelos órgãos executivos.

### 7.2 Unidades Gestoras de TIC

A função das Unidades Gestoras de TIC é auxiliar a CTIn a formular as diretrizes gerais de informática e executar as políticas formuladas por esta comissão.

### 7.3 Unidades de Ensino, Pesquisa e Extensão e Órgãos da Administração

Responsável por formular e coordenar a execução das normas de segurança da informação específicas em consonância com as normas estabelecidas nesta política de segurança nos casos que a CTIn julgar necessário.

### 7.4 Procuradoria Geral – PGE

A PGE participa da PSI auxiliando o CGSI, Unidades e Órgãos quanto aos aspectos legais de modo a avaliar os incidentes de segurança causados por funcionários da Universidade, recomendando as penalidades cabíveis.

### 7.5 Comitê Gestor de Segurança da Informação – CGSI

O CGSI possui a função de assessorar a CTIn, o CPD e as demais Unidades Gestoras de TIC da UFS no tratamento de questões de segurança. Adicionalmente o comitê deve:

- Manter e aprimorar a Política de Segurança vigente visando à sustentação das atividades de proteção da informação eletrônica da UFS;
- Ser o canal de comunicação entre a PGE, a CTIn e as Unidades Gestoras de TIC nas questões de segurança;
- Receber pareceres do GSI e, quando necessário, solicitar parecer jurídico da PGE.

### 7.6 Gestor de Segurança da Informação – GSI

O GSI é o responsável por monitorar e avaliar o cumprimento da Política de Segurança, auditar e indicar responsabilidades na ocorrência de incidentes, assessorando o CGSI. No caso de incidentes deverá receber as notificações do AdmA e emitir pareceres para o CGSI.

### 7.7 Administrador de Ativos – AdmA

O AdmA é a pessoa indicada pela Unidade com a responsabilidade de zelar pelo cumprimento das Normas de Segurança, atuando na solução e notificando o GSI nas ocorrências de incidentes.

### 7.8 Usuários dos Recursos de TIC

Estes usuários são os alunos, funcionários e demais pessoas que utilizam os recursos de TIC da UFS que devem seguir as determinações da Política de Segurança da UFS.

## 8. Abrangência da Segurança

A abrangência da segurança é definida pelo CTIn, no tocante as responsabilidades das Unidades Gestoras de TIC da capital e do interior.

No escopo definido pela CTIn, os quesitos da PSI devem ser aplicados de maneira mandatória. Fora desse escopo, eles devem servir de recomendações, podendo ser aplicados pelas Unidades, Centros, Departamentos, Núcleos ou outros setores integrantes da UFS.

## 9. Penalidades

As penalidades poderão advir resultantes de incidentes de segurança. Nestes casos, o CGSI, após receber o parecer do GSI, deverá, caso julgue necessário, consultar a PGE e encaminhar a recomendação de penalidade para os gestores das unidades responsáveis.

## 10. Documentos da Política de Segurança

Os documentos que integram a PSI da UFS são:

Anexo I - **Normas de Segurança da UFS**. Criado em 16/12/2011. Última revisão em 21/12/2011.

Anexo II - **Normas de Acesso à Rede Sem Fio da UFS**. Criado em 11/11/2011. Última revisão em 11/11/2011.

Anexo III - **Normas do Portal da UFS**. Criado em 11/11/2011. Última revisão em 11/11/2011.

Anexo IV - **Relação de Ativos de Criticidade Máxima da UFS**. Criado em 20/12/2011. Última revisão em 20/12/2011.

## Referências Bibliográficas

ABNT, NBR 27001- Norma ABNT NBR ISSO 27001:2006 – Tecnologia da Informação – Técnicas de segurança – Código de prática para gestão da segurança da informação – Requisitos, 2006.

COELHO, Flávia., Governança em TI - Gestão da Segurança da Informação. – NBR 27001 e NBR 27002. Escola Superior de Redes, 2010.

CERT.br, FAQ: Perguntas Freqüentes ao CERT.br . Disponível em: <http://www.cert.br/docs/certbr-faq.html#6>. Último acesso em: 20/12/2011.

GSETI, Grupo de Segurança em TI. Política de Segurança da USPnet. Disponível em: <http://www.security.usp.br/normas_pseg00.html>. Último acesso em: 21/12/2011.

# ANEXO I

## NORMAS DE SEGURANÇA DA UFS

# NORMAS DE SEGURANÇA DA UFS

## 1. Introdução

A Política de Segurança da Informação (PSI) da Universidade Federal de Sergipe (UFS) estabelece a criação de normas que busquem a garantia de mecanismos para proteção dos sistemas de informação contra a negação de serviço a usuários autorizados, assim como contra a intrusão, e a modificação desautorizada de dados ou informações, armazenados, em processamento ou em trânsito, abrangendo, inclusive, a segurança dos recursos humanos, da documentação e do material, das áreas e instalações das comunicações e computacional, assim como as destinadas a prevenir, detectar, deter e documentar eventuais ameaças a seu desenvolvimento. Deste modo, as Normas de Segurança da UFS devem garantir a parte estratégica da PSI.

As demais seções estão organizadas da seguinte forma: na Seção 2 são apresentados os objetivos das normas, na Seção 3 a abrangência das normas, na Seção 4 é abordada a segurança física das instalações, na Seção 5 a segurança ambiental, na Seção 6 a segurança de acesso às instalações, na Seção 7 a segurança dos equipamentos, na Seção 8 a segurança lógica ou segurança da informação, na Seção 9 a segurança administrativa, na Seção 10 as diretrizes gerais para lidar com incidentes e na Seção 11 são apresentadas diretivas sobre auditoria.

## 2. Objetivo

As Normas de Segurança da Informação para a UFS têm o objetivo de fornecer um conjunto de regras e recomendações aos administradores de rede e usuários, visando à proteção e segurança dos equipamentos, dados, pessoas e instalações da Universidade, a saber:

- Estabelecer procedimentos para a instalação e manutenção de ferramentas, *hardware* e *software*, visando a segurança dos sistemas computacionais e de comunicação da UFS interligados à rede de computadores.
- Orientar, por meio de suas diretrizes, todas as ações de segurança das Unidades de Ensino e Pesquisa e Órgãos de Administração para minimizar os

riscos de segurança e garantir autenticidade, confidencialidade, integridade, legalidade e disponibilidade da informação.

- Estabelecer procedimentos visando prevenir e responder a incidentes de segurança.

## 3. Abrangência

Esta Norma tem abrangência para toda Universidade, em relação às instalações, equipamentos, informação e pessoal.

Em conformidade com a PSI da UFS, esta norma abrange os seguintes aspectos:

- Segurança física dos dispositivos de rede e da infra-estrutura;
- Segurança lógica dos equipamentos de rede;
- Segurança da informação;
- Segurança administrativa;
- Segurança do funcionário e do usuário.

## 4. Segurança física das instalações de processamento

A Segurança Física tem como objetivos específicos:

- proteger edificações e equipamentos;
- prevenir perda, dano ou comprometimento dos ativos;
- manter a continuidade das atividades dos negócios;
- reduzir as ameaças que coloquem em risco o bom funcionamento dos sistemas.

### 4.1 Sistema de Proteção contra Descargas Atmosféricas (SPDA) e aterramento

Recomenda-se que as edificações onde se encontram instalações de processamento, estejam protegidas por um sistema contra descargas atmosféricas (pára-raios) e possuam sistema de aterramento eficiente, observando-se o seguinte:

- Todo sistema de proteção deve receber manutenção preventiva e inspeção anualmente.
- O projeto, instalação e manutenção do sistema deve estar em conformidade com a norma NBR-5419-2005.

- A função do pára-raios é proteger edificações e pessoas, não abrangendo necessariamente equipamentos eletro-eletrônicos.
- Recomenda-se a utilização de protetores para os equipamentos considerados essenciais, tais como varistores de óxido de zinco ou similares, adequados para cada tipo de equipamento.
- Em relação à rede elétrica, aconselha-se o uso dos pára-raios de baixa tensão, do tipo pastilhas de Óxido de Zinco, nos quadros elétricos de entrada do edifício.
- A inspeção e medição do sistema de aterramento também devem ser anuais, conforme a norma vigente.
- Antes da instalação de equipamentos que possam ocasionar sobrecarga na rede elétrica, recomenda-se a realização de um diagnóstico energético das instalações.

### 4.2 Fornecimento de energia

Os equipamentos devem estar protegidos contra falhas de alimentação elétrica, observando-se as especificações do fabricante do equipamento quanto ao fornecimento de energia:

- É altamente recomendado o uso de *no-break* em equipamentos que suportam atividades críticas e para todos os componentes do *backbone* da UFS.
- O uso de grupo-gerador em instalações estratégicas e áreas do núcleo e de distribuição da rede é fortemente recomendado.
- Para o caso dos ativos classificados com criticidade máxima o uso de grupo-gerador é obrigatório.
- Para outros equipamentos em áreas sujeitas a corte do fornecimento de energia frequente, o seu uso deve ser estudado, sendo uma boa alternativa a aquisição de no-break com maior autonomia.
- Tanto para os casos de uso de *no-break* como para o de grupo-gerador, convém que seja firmado um contrato de manutenção para que as peças e componentes do sistema estejam sempre em perfeito estado e de acordo com as recomendações do fabricante. A Comissão de Controle Interno (CCI) deve ser consultada sobre este assunto.
- Equipamento de rede classificado com criticidade máxima deverá dispor de N+1 fontes de alimentação, onde N é igual ao número mínimo de fontes para suportar

a carga imposta pela configuração do equipamento. A fonte redundante deverá estar operacional, no modo *load sharing* (balanceamento de carga), de modo que a falha de uma das fontes seja imperceptível.

- Para equipamentos com mais de uma fonte de alimentação recomenda-se alimentação múltipla de circuitos elétricos, de modo a evitar um único ponto de falha, correspondendo um circuito para cada fonte.
- É importante que as salas de equipamentos do *backbone* recebam alimentação de circuitos totalmente independentes, ou seja, diferentes dos circuitos que alimentam os prédios vizinhos. Esses circuitos devem estar interligados diretamente à rede elétrica primária do campus.
- Convém ainda que as salas contendo os equipamentos possuam iluminação de emergência e interrúptores elétricos de emergência que permitam o desligamento em caso de necessidade.
- A instalação elétrica deve seguir a norma NBR-5410/2004 "Instalações Elétricas de Baixa Tensão".

### 4.3 Segurança do cabeamento

A segurança do cabeamento é tão importante quanto a segurança dos equipamentos de rede. Assim, é importante observar o seguinte:

- O cabeamento de fibra óptica deve ser preferencialmente subterrâneo e, neste caso, o encaminhamento do mesmo deve ser através do sistema de dutos de uso exclusivo do campus.
- A instalação de cabeamento de fibra óptica com gel em seu núcleo deve seguir as recomendações das normas vigentes.
- O cabeamento de fibra óptica do núcleo do *backbone* da UFS deve possuir proteção anti-roedor, sendo que a norma NBR 14773 pode ser consultada.
- As rotas do cabeamento de fibra óptica devem receber sinalização específica para evitar acidentes e/ou danos de terceiros. Cabe ao Gestor de Tecnologia da Informação e Comunicação (TIC) local tomar as providências para manter a relação e identificação das rotas dos cabos ópticos do *backbone*.
- As caixas de passagem devem ser mantidas adequadas ao uso e possuir tampas de ferro com identificação.

- A instalação de cabeamento, tanto em cobre quanto em fibra óptica, deve seguir as recomendações da norma NBR 14565 e TIA/EIA 568-B.2-1.

## 5. Segurança ambiental

A Segurança Ambiental tem por objetivo adotar medidas que evitem risco às instalações e equipamentos por ocorrência dos seguintes fatores:

- Incêndio;
- Fumaça;
- Poeira;
- Vibração;
- Umidade;
- Água.

Recomenda-se que:

- Sensores de controle destes fatores estejam integrados a um sistema que permita a monitoração remota, assim como o disparo de alarmes.
- Sejam adotados, ainda, procedimentos restringindo comida, bebida e fumo dentro das instalações de processamento.
- De forma a promover condições ao que se refere às Medidas de Segurança e Medicina do Trabalho, deve ser seguida a norma NR10 sobre Instalações e Serviços em Eletricidade.

## 6. Segurança do acesso às instalações

A Segurança das instalações com relação ao acesso físico tem como objetivos específicos:

- Prevenir e controlar o acesso não autorizado a informações e instalações físicas da Unidade/Departamento;
- Prevenir perda, dano ou comprometimento dos ativos;
- Evitar a exposição ou roubo de informação.

## 6.1 Controle de acesso

As instalações de processamento ou outras áreas de segurança devem ser equipadas com controles de entrada apropriados, de forma que somente pessoal autorizado tenha acesso liberado.

O controle de acesso depende dos requisitos de segurança próprios da área considerada e pode se dar através de:

- Controle de entrada (métodos de acesso físico);
- Crachás de identificação e procedimentos pelos quais o acesso é concedido, modificado ou negado;
- Chaves e/ou controles eletrônicos, tais como métodos biométricos e cartão inteligente;
- Restrições de acesso baseadas no *status* do funcionário e horas de operação;
- Pontos de contato para acesso;
- Combinação dos itens anteriores.

## 6.2 Segurança do acesso à instalação

Convém que cada Unidade crie normas ou procedimentos que complementem os sistemas de segurança adotados e sugeridos:

- Recomenda-se que o Controle de Acesso utilize como validação um sistema de cartão com PIN (*personal identification number* - número de identificação pessoal). Eventualmente, em locais mais críticos, pode-se optar também pela validação biométrica (impressão digital, por exemplo).
- O fornecimento dos cartões de acesso deve ser através do gestor responsável pela segurança da unidade.
- O extravio ou roubo de cartões de acesso deve ser informado imediatamente à unidade responsável.
- Os cartões de acesso devem ser mantidos pelos seus respectivos proprietários todo o tempo, e nunca devem ser emprestados para qualquer pessoa ou deixados desprotegidos.
- Mesmo durante o horário comercial o acesso com cartão é necessário para os funcionários.

- Todas as portas externas devem ter acesso controlado fora do horário de expediente normal.
- Qualquer pessoa dentro de uma área de segurança deverá dispor de identificação de acordo com a função por ela exercida.
- Os funcionários não podem permitir a estranhos o acesso aos recursos de rede.
- Os visitantes ou funcionários sem permissão deverão ganhar autorização e identificação especial para ter acesso e permanecer nos locais de segurança, devendo estar explícito qual o propósito de adentrar ao local, quais as atividades que serão desenvolvidas e a quais recursos estas pessoas terão acesso.
- Serviços de terceiros em Instalações de Processamento devem ser agendados previamente, deve ser fornecido o nome das pessoas que executarão o serviço, assim como o detalhamento da atividade a ser desenvolvida.
- Tanto para o caso de terceiros quanto para visitantes, uma pessoa da Unidade/Depto deve sempre acompanhar o trabalho, de forma que um estranho nunca fique sozinho nas instalações.
- Adicionalmente, convém que o Controle de Acesso utilize sistemas eletrônicos complementares, tais como Circuito Fechado de TV nas áreas consideradas estratégicas, havendo registro da imagem local por meio de câmeras de vídeo, que deverão estar sendo armazenadas em alguma mídia, de forma a poderem ser resgatadas em caso de alguma ocorrência ou auditoria.

### 6.3 Segurança para o sistema de telefonia

Semelhante às Instalações de Processamento, o sistema de telefonia requer cuidados e procedimentos que visem a segurança:

- O acesso físico ao *hardware* do sistema de telefonia e aos terminais de configuração de sistema é restrito aos administradores do sistema de telefonia e ao pessoal da companhia provedora do serviço.
- O sistema de telefonia deve estar em uma área segura que necessite de métodos de acesso especializados via chaves e/ou controles eletrônicos de acesso.
- A instalação de novos modems deve ser coordenada pelo grupo responsável, a fim de fornecer a segurança necessária e infraestrutura de rede para manter a segurança.

## 7. Segurança dos equipamentos

A segurança dos equipamentos está diretamente relacionada aos procedimentos de instalação e proteção, atentando-se ao seguinte:

- A instalação de equipamentos deve seguir o procedimento recomendado pelo fabricante e/ou normas específicas existentes, na falta destes, deverá ser consultado o setor responsável pela instalação elétrica da Unidade.
- Os equipamentos devem ser instalados de modo a permitir fácil acesso à equipe de manutenção de rede.
- Recomenda-se que a instalação garanta boa ventilação a seus componentes.
- Terminais públicos devem estar fixados via dispositivos de alarme antifurto e cabos com travas;
- Equipamento instalado fora das áreas de segurança deverá dispor de proteção física, como armário, gaiola, ou equivalente, com trava mecânica e/ou eletrônica, chave ou outro dispositivo que permita barrar o acesso de pessoas não autorizadas.
- A instalação, manutenção e atualização de equipamentos no *backbone* de cada campus da UFS é de responsabilidade de cada Gestor de TIC.

### 7.1 Manutenção de equipamentos

Em relação à manutenção dos equipamentos, deve-se observar o seguinte:

- A manutenção de equipamentos deve ser de acordo com intervalos e especificações do fabricante. Se essas recomendações não forem conhecidas, procedimentos de manutenção devem ser elaborados e aplicados.
- Apenas profissionais autorizados podem fazer manutenção nos equipamentos, ou seja, o próprio fabricante, empresas autorizadas por ele e equipes de manutenção.
- Devem ser mantidos registros de todas as falhas suspeitas ou ocorridas em toda manutenção preventiva e corretiva. É recomendado o uso de um sistema computacional com um banco de dados para estas informações, preferencialmente com acesso via web.

- Equipamentos enviados para manutenção de terceiros e que possuem meios de armazenamento (disco rígido, fitas, etc) devem ter seus itens checados para assegurar que toda informação sensível, sigilosa e *software* licenciado foi removido ou sobreposto antes da alienação do equipamento.
- Um *hardware* sobressalente deve estar disponível caso a criticidade do equipamento seja alta.
- Dispositivos de armazenamento danificados, assim como equipamentos, devem sofrer uma avaliação de riscos para verificar se eles devem ser destruídos, reparados ou descartados. Recomenda-se que cada ativo ou parte dele seja avaliado pelo Gestor da Unidade ou por uma Comissão por ele criada, à qual caberá dar o devido destino.

## 8. Segurança lógica ou segurança da informação

Tão importante quanto a segurança física é a segurança da informação.

Recomenda-se a adoção das seguintes medidas que visem proteger a integridade das informações da Universidade:

- Sugere-se a utilização de cofres especiais para a guarda das mídias contendo as cópias de segurança (*back-up*). Estes cofres especiais são resistentes a incêndio, umidade, interferências eletromagnéticas, poeira, fumaça e vandalismo.
- O acesso às mídias de *back-up* deve ser restrito ao pessoal autorizado.
- O acesso ao aplicativo de *back-up* deve ser restrito ao pessoal autorizado.
- Equipamentos, informações ou *software* não devem ser retirados da organização sem autorização.
- Toda informação, quer em mídia eletrônica ou papel, deve ficar sempre guardada em locais apropriados e de acesso restrito, especialmente fora dos horários de trabalho normal.
- É recomendado que outra cópia seja guardada fora do site, semanalmente, por meio do gerente ou um funcionário autorizado.
- Os sistemas devem estar armazenados em repositórios com controle de versão.
- Aconselha-se que seja feita uma vez por semana o *back-up* completo do repositório dos sistemas e, diariamente, de preferência à noite ou madrugada, a cópia incremental, ou seja, o que foi modificado. A restauração deve ocorrer da

última cópia completa até as cópias com as alterações incrementais (*layered over*) até o momento do evento.

- Os *back-ups* das bases de dados devem ser testados diariamente.
- Recomenda-se, para fins de auditoria e de responsabilização, que as aplicações permitam sempre verificar em que contexto as informações foram modificadas durante o uso normal do sistema, registrando os *logs* de acesso dos usuários.

## 8.1 Contas de acesso aos sistemas

Sobre o acesso aos sistemas, segue:

- Cada usuário deve possuir uma conta individual. Não deve haver contas coorporativas ou contas compartilhadas por mais de um usuário, a não ser em situações específicas e prazos determinados.
- A solicitação de abertura de contas em quaisquer dos sistemas se dará em concordância com um Termo de Identificação e Compromissos.
- Após receber uma conta, cujas identificações foram criadas pelos administradores dos sistemas ou de redes, o proprietário da conta tem um mês para alterar a seu critério essas identificações.
- A autorização e o nível da conta serão concedidos pelo gestor e/ou administrador do sistema, ou se for o caso, pelo administrador de rede.
- Contas de usuários que venham a se desligar da UFS, tais como alunos formados, professores e funcionários, serão canceladas após um período máximo de 30 dias da data do desligamento, salvo casos excepcionais que serão analisados pelo Gestor da Unidade.
- Funcionários demitidos pela universidade terão suas contas canceladas no ato da demissão. A Gerência de Recursos Humanos (GRH) deve comunicar ao responsável de segurança para as providências.
- O usuário é responsável por qualquer atividade a partir de sua conta e também por seus atos no uso dos recursos computacionais oferecidos. Assim, o mesmo responderá por qualquer ação legal apresentada à UFS e que o envolva.

## 8.2 Segurança para rede de dados

A segurança para a rede sob o aspecto da segurança lógica deve considerar filtros e protocolos habilitados nos ativos. Deste modo:

- Devem ser implantadas regras de proteção nos roteadores e/ou *firewall* para proteger as redes de uma forma restritiva (método de exceção).
- Para os roteadores do *backbone*, os filtros e regras deverão ser obrigatórios e estudados para cada caso.
- Os filtros e regras no *firewall* devem permitir apenas conexões entrantes para servidores WWW, de correio eletrônico e de nomes (DNS), sendo que exceções devem ser estudadas pelo CPD e pelo GSI.
- O acesso lógico aos equipamentos de rede (roteadores, *switches*, modems, servidores, ou outros) deve sempre ser protegido por senhas não-padrão (*default* ou inicial), quer para suporte, configuração ou gerenciamento e, preferencialmente, a partir de um número restrito de equipamentos.
- As senhas de acesso lógico aos equipamentos devem ser trocadas periodicamente, a cada 180 dias no máximo, ou quando o administrador ou funcionário que as detenha venha a se desligar da Universidade ou da função, ou quando do Gestor de TIC e a Comissão de Segurança definir como necessário.
- Os responsáveis devem manter um registro (*log*) para as alterações de configuração dos equipamentos de rede.
- É recomendado o uso de aplicativos de gerenciamento para os equipamentos de rede e servidores, que notifiquem o administrador em casos de anomalias.
- Para o caso do gerenciamento via protocolo SNMP (*Sample Network Management Protocol*), não deve estar habilitado se não estiver em uso, do contrário, garantir acesso estritamente aos administradores responsáveis.
- A gerência dos equipamentos de redes e servidores deve ser feita exclusivamente em uma rede lógica separada das demais e com acesso restrito.
- Também é recomendada a utilização de antivírus que monitorem as mensagens de correio eletrônico.
- As informações de configuração dos equipamentos devem estar armazenadas em servidores administrativos, nunca em servidores públicos ou de produção.

- Sempre que possível, os equipamentos de rede devem fazer *back-up* de sua configuração em servidores administrativos, buscando aumentar a segurança e confiabilidade.
- Os equipamentos devem ter habilitados somente os protocolos necessários.

### 8.3 Segurança de acesso remoto

- Somente o CPD pode fornecer acesso remoto à rede da UFS, sendo que a configuração do *hardware* deverá seguir as orientações de segurança contidas nesta política.
- A permissão para o acesso remoto é fornecida pelo CPD, que deve preencher formulários, assinados pelos usuários deste serviço, atestando a ciência às normas.

### 8.4 Segurança para servidores

Além das recomendações, um plano de contingência deve ser criado para a recuperação de desastres.

- Os servidores devem ser configurados para suportar apenas os serviços necessários.
- Os servidores devem ser fisicamente seguros, permitindo acesso restrito.
- Os administradores dos servidores devem estar atentos a atualizações e correções de vulnerabilidades dos sistemas operacionais e *softwares*.

### 8.5 Segurança para equipamentos de usuários

- Os usuários jamais devem deixar sessões abertas, efetuando o *logout* quando ele não estiver em uso.
- Recomenda-se que dados importantes sejam protegidos por senhas e criptografia.
- É fortemente recomendado que o usuário utilize senhas diferentes para os sistemas e equipamentos, defendendo-se em caso de roubo de alguma senha.

- Recomenda-se para equipamentos portáteis o uso de cabos, correntes ou outro dispositivo de segurança, ou ainda, trancá-los em gavetas ou armários quando fora de uso.

## 9. Segurança administrativa

Cabe ao Administrador de Ativos (AdmA) cumprir as seguintes diretrizes visando a segurança administrativa:

- É proibido o acesso aos arquivos e informações do usuário, exceto em caso de segurança ou apuração de algum fato envolvendo o próprio usuário, sempre com a ciência do gerente ou responsável pela rede.
- A monitoração de dados e voz que circulam através dos meios só deverá ser praticada visando a detecção de invasão ou outro assunto relacionado à segurança.
- O administrador que incorrer em alguma não-conformidade ou evento que resulte em parada ou prejuízo de serviços deve estar ciente que haverá investigação que poderá resultar em alguma ação contra ele.
- Os usuários, por sua vez, devem atender às seguintes diretivas básicas:
- A utilização dos recursos de rede da Universidade só é concedida mediante a adesão dos usuários às normas e diretivas de segurança vigentes, lendo, entendendo e assinando o termo adequado.
- É responsabilidade do usuário criar e trocar as senhas de acordo com as recomendações da norma, tendo ciência de que as contas são pessoais e intransferíveis.
- Os recursos jamais devem ser utilizados de maneira inadequada, de forma a comprometer os sistemas ou a segurança da rede, ou agindo de forma ofensiva.
- O usuário deve estar ciente de que atos impróprios resultarão em investigação, podendo acarretar punição.
- Os terminais devem ser bloqueados ou ter a sessão finalizada quando fora de uso.
- *Notebooks*, PDAs ou outros dispositivos portáteis estão sujeitos a inspeção pelo administrador.
- Os usuários devem concordar em participar de auditorias, em conformidade com as diretivas de segurança.

- Cabe ao usuário notificar ao Gestor da Unidade, qualquer observação em relação a defeitos, acesso não autorizado, falhas de segurança ou afins.

## 10. Diretrizes gerais para lidar com incidentes

Os usuários devem ler e entender as seguintes diretrizes para lidar com incidentes:

- Todos os incidentes e suas soluções devem ficar registrados, sendo submetidos ao gerente de rede, ou ao administrador de rede ou alguém responsável pela rede, e este ao CGSI.
- A análise do incidente deverá ser discutida em uma reunião do CGSI para identificar os pontos fracos, visando prevenir incidentes futuros, procurando sempre contar com o apoio do CPD e do GSI.

### 10.1 Em relação ao acesso físico

- No caso de um visitante não autorizado, o funcionário deve notificar imediatamente a Divisão de Vigilância (DIVIG) e solicitar auxílio para remoção do mesmo.
- Caso o visitante seja pego cometendo furto, ataque ou destruição da propriedade, deve-se notificar a DIVIG para que sejam contactadas as autoridades competentes.
- Todas as testemunhas devem fornecer aos responsáveis pela segurança um depoimento detalhado do incidente que indique a presença de um visitante não autorizado e devem estar disponíveis para interrogatório posterior pela segurança e pelas autoridades competentes.
- Todas as portas, fechaduras e métodos de acesso que não estejam funcionando devem ser informados a DIVIG e ao Departamento de Manutenção (DEMAN) para correção do equipamento defeituoso.
- Os gerentes devem ser notificados quando um funcionário estiver envolvido em uma vulnerabilidade de segurança.

### 10.2 Em relação aos ativos de rede

- Sempre tentar identificar a causa do incidente.

- Se uma invasão causar parada ou ruptura de serviços, a prioridade é restabelecer os serviços, porém sempre que possível, os administradores devem tentar identificar a origem do problema, preservando as evidências.
- No caso de uma invasão é aconselhável rever as regras implementadas, modificando-as para controlar os efeitos.
- Em caso de incidente que resulte em perda de informações, o responsável deve ser notificado imediatamente, e o gerente de rede deve notificar o incidente ao Comitê Gestor de Segurança.
- Em caso de incidentes como comprometimento do sistema ou invasões de um servidor ou outro ativo, deve-se removê-lo da rede e deixá-lo em seu estado atual a fim de permitir um trabalho de investigação eficiente.

## 11. Auditoria

É importante que se adote um esquema de auditorias. Neste caso, os funcionários devem ler, entender e cooperar com os procedimentos e diretivas adotadas.

- As auditorias serão realizadas principalmente em servidores e equipamentos de rede para assegurar a configuração e atualização adequadas.
- Os auditores devem indicados pelo Comitê Gestor de Segurança.
- As auditorias em sistemas seguirão as diretivas adotadas.
- As auditorias podem ser notificadas ou não.

### 11.1 Auditorias notificadas

São anunciadas previamente aos funcionários, de modo que tenham tempo para preparar o ambiente e rever suas práticas. Seus propósitos são:

- Analisar os sistemas em relação aos componentes de segurança.
- Verificar se as práticas dos usuários não são impróprias ou desafiam a segurança.
- Assegurar que as informações são apropriadas e cumprem aos objetivos.

### 11.2 Auditorias não anunciadas

São aleatórias, buscando a identificação de vulnerabilidades e a constante conscientização com a segurança. Podem ser implementadas na forma de ataques simulados, desde que permaneçam no escopo da rede local.

# ANEXO II

## NORMAS DE ACESSO À REDE SEM FIO DA UFS

# NORMAS DE ACESSO À REDE SEM FIO DA UFS

## 1. Descrição

A rede sem fio do projeto Wi-Fi UFS foi concebida para complementar a rede cabeada. Ela não deve ser vista como uma rede exclusiva ou substituta à rede cabeada atual. O propósito da infraestrutura da rede sem fio é permitir acesso a rede de dados e a Internet através de dispositivos móveis e também cobrir certas áreas com ausência de infraestrutura de rede cabeada.

Ela é adequada ao uso em pequenos intervalos de tempo, como consultas de e-mail ou navegação na web. O uso para transferência de grandes arquivos, aplicações ou de conexões constantes não é recomendado na rede sem fio. Estas atividades terão melhor desempenho através da rede cabeada.

O serviço estará disponível 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana, entretanto poderá, eventualmente, sofrer quedas de desempenho ou interrupções devido as seguintes circunstâncias externas:

- Manutenções técnicas e/ou operacionais que exijam o desligamento temporário do sistema ou impossibilitem o acesso;
- Falta de fornecimento de energia elétrica;
- Defeitos, falhas ou panes nos equipamentos;
- Ocorrências de falhas no link de acesso à Internet;
- Em função de condições técnicas e/ou ambientais que podem interferir com o sinal emitido pelos roteadores, não há garantia na manutenção do mesmo em condições adversas e os usuários devem estar cientes da possibilidade de perda de comunicação ou de informações.

## 2. Público Alvo

A rede sem fio da UFS visa atender os professores, alunos, funcionários administrativos e visitantes respaldados pela instituição.

## 3. Objetivo

A política de utilização da rede sem fio tem como objetivo estabelecer regras e normas de utilização e ao mesmo tempo desenvolver um comportamento ético e profissional aos usuários desta rede nas dependências da universidade.

## 4. Normas Gerais

Para assegurar a qualidade na prestação dos serviços da rede sem fio, faz-se necessária a especificação de uma política de utilização.

Nos termos da política de utilização da rede, quanto ao aspecto de "violação" e uso indevido dos recursos, a Coordenação de Redes do CPD poderá proceder o bloqueio de acesso ou cancelamento da conta do usuário, caso seja detectado e evidenciado o uso em desconformidade com o estabelecido ou que tenha causado prejuízo aos serviços da rede sem fio.

Ao aceitar os termos para o uso da rede sem fio, o usuário aceita expressamente, sem reservas ou ressalvas, todas as condições estipuladas neste documento.

O usuário é responsável por todos os atos oriundos da utilização deste serviço, quer seja de acesso, visualização, divulgação, legal ou ilegal, devendo manter seu login e senha em absoluto sigilo.

O usuário compromete-se a fazer uso da senha de forma segura e confidencial, zelando por sua guarda e confidencialidade, declarando-se ciente de que não poderá vender, transferir, ceder ou emprestar a outrem, a qualquer título, a senha que é de caráter pessoal e intransferível.

A instituição poderá suspender ou cancelar o acesso do usuário, sem prévio aviso, na hipótese de identificar o mesmo como divulgador de imagens de pedofilia, crimes financeiros, disseminação de vírus, malwares, trojans, que violem direitos autorais ou práticas ilícitas, que induzam ou provoquem riscos a terceiros, práticas enganosas, etc.

Em locais sem cobertura da rede sem fio do projeto WiFi UFS somente será permitida a instalação de dispositivos para rede sem fio com a orientação do responsável pela rede local na instituição, e desde que se respeite as regras de uso desta política.

Essas redes não serão administradas pelo CPD da instituição, e, portanto, o suporte à conexão e as garantias de segurança não são de responsabilidade deste centro.

## 5. Regras Para Usuários

O acesso à rede WiFi da UFS somente será permitido aos usuários devidamente cadastrados nos Sistemas Integrados da UFS.

O usuário deve conhecer as regras e penalidades, sendo elas:

- Não se fazer passar por outra pessoa ou dissimular sua identidade quando utilizar os recursos computacionais;
- Responsabilizar-se pela sua identidade eletrônica, senha, credenciais de autenticação, autorização ou outro dispositivo de segurança, negando revelá-la a terceiros.
- Responder pelo mau uso dos recursos computacionais em qualquer circunstância.
- O usuário deve manter seus computadores pessoais com software e com antivírus atualizados;
- Se necessário, os usuários devem procurar a Coordenação de Redes do CPD da UFS para esclarecimentos.

## 6. Violação das Regras

Considera-se violação das regras:

- Mostrar, armazenar ou transmitir texto, imagens ou sons que possam ser considerados ofensivos ou abusivos;
- Utilizar o acesso à internet para instigar, ameaçar ou ofender, abalar a imagem, invadir a privacidade ou prejudicar outros membros da comunidade internet;
- Efetuar ou tentar qualquer tipo de acesso não autorizado aos recursos computacionais da UFS;
- Utilizar os recursos computacionais da UFS para acesso não autorizado a recursos de terceiros;

- Violar ou tentar violar os sistemas de segurança, quebrando ou tentando adivinhar a identidade eletrônica de outro usuário, senhas ou outros dispositivos de segurança;
- Interceptar ou tentar interceptar a transmissão de dados através de *software* de monitoração, exceto quando solicitado explicitamente à Coordenação de Redes do CPD pelo chefe do departamento e com finalidade exclusiva de pesquisa;
- Provocar interferência em serviços de outros usuários ou o seu bloqueio, provocando congestionamento da rede de dados, inserindo vírus ou tentando a apropriação indevida dos recursos computacionais da UFS;
- Desenvolver, manter, utilizar ou divulgar dispositivos que possam causar danos aos sistemas e às informações armazenadas, tais como criação e propagação de vírus e *worms*, criação e utilização de sistemas que causem ou tentem causar a indisponibilidade dos serviços e/ou destruição de dados, e ainda, engajar-se em ações que possam ser caracterizadas como violação da segurança computacional;
- Utilizar os recursos computacionais da UFS para fins comerciais ou políticos, tais como mala direta ou propaganda política;
- Utilizar os recursos computacionais da UFS para ganho indevido;
- Utilizar os recursos computacionais da UFS para intimidar, assediar, difamar ou aborrecer qualquer pessoa;
- Consumir inutilmente os recursos computacionais da UFS de forma intencional.

O usuário é responsável por qualquer atividade a partir de sua conta (login) e também por seus atos no uso dos recursos computacionais oferecidos. Assim, o mesmo responderá por qualquer ação legal apresentada à UFS e que o envolva.

Caso alguma violação de regra seja identificada, através do sistema de monitoramento, o usuário será bloqueado e notificado pelo e-mail de contato.

## 7. Considerações Finais

A Coordenação de Redes do CPD, visando preservar a segurança da rede UFS global, poderá, a seu critério, restringir o acesso da rede sem fio aos recursos da rede cabeada.

O login de acesso à rede Wi-Fi só terá validade enquanto perdurar o vínculo do aluno ou servidor com a UFS.

Medidas de segurança como antivírus, firewall, anti-spyware, em equipamento pessoal, são de responsabilidade do próprio usuário. Em nenhum caso a UFS se responsabilizará por qualquer dano e/ou prejuízo que o usuário possa sofrer ao utilizar o serviço.

A UFS se reserva o direito de cancelar este serviço sem prévio aviso.

# ANEXO III

## NORMAS DO PORTAL DA UFS

# NORMAS DO PORTAL DA UFS

Este documento estabelece termos e condições de utilização do Portal da Universidade Federal de Sergipe pela comunidade universitária, aí incluídos todos os setores administrativos e acadêmicos, servidores públicos e alunos, bem como para todos aqueles da comunidade civil que pretendam usar o Portal.

Ao usar o Portal UFS o usuário está obrigado a aceitar os Termos e Condições que estiverem em vigor, devendo respeitá-lo, sob pena de responsabilização pelo uso inadequado.

Toda página vinculada ao Portal UFS de unidade administrativa da Universidade Federal de Sergipe integrante de seu Subsistema de Administração Geral ou Subsistema de Administração Acadêmica deverá ter um gerente responsável que responderá pela integridade do conteúdo e pela adequação da página às normas definidas.

Os Termos e Condições de utilização do Portal UFS subordinam-se ao disposto no art. 5º e 220 da Constituição Federal, à Lei nº 9.610/98 (Lei de Direitos Autorais), ao Código Penal Brasileiro, ao Regimento Geral e ao Estatuto da Universidade Federal de Sergipe.

O nome fantasia "Portal UFS" será adotado para fins de citação e aplicação em documento ou peças publicitárias vinculados no Portal.

O Portal da Universidade Federal de Sergipe tem como objetivos:

I. facilitar a comunicação e o trabalho dos diversos sistemas de gestão que compõem a UFS;
II. fixar e viabilizar a política de comunicação social da UFS;
III. divulgar as atividades de ensino, pesquisa e de extensão da UFS;
IV. divulgar informações ao público interno e externo;
V. servir como instrumento de cidadania, mediando as relações entre a UFS e a sociedade.

O Portal da Universidade Federal de Sergipe será administrado por um Núcleo de Gerenciamento, presidido pelo Gerente Geral e com a seguinte composição:

I. 1 (um) Gerente Geral e suplente, indicados pelo Reitor;
II. o Assessor de Comunicação da UFS e seu suplente por ele indicado. Caso o Assessor de Comunicação já tenha sido indicado como Gerente Geral, o próprio

Assessor de Comunicação indicará o titular e o suplente, ambos representantes e pertencentes aos quadros da Assessoria de Comunicação da UFS;

III. 1 (um) representante e suplente do Centro de Processamento de Dados;

IV. 1 (um) representante e suplente do CONSU;

Cabe ao CONSU a designação de seu representante e suplente no Núcleo de Gerenciamento, ambos com mandato de 01 (um) ano.

Nos casos de vaga, ausência e impedimento dos membros titulares, assumirá o respectivo suplente.

Compete ao Gerente Geral:

I. convocar e presidir as reuniões do Núcleo de Gerenciamento;

II. executar ou auxiliar nas ações aprovadas pelo Núcleo de Gerenciamento;

III. manter contatos internos com os gerentes responsáveis pelos domínios ou páginas vinculadas ao Portal UFS, com o propósito de promover ou executar ações com vistas ao uso correto do Portal, dos seus sistemas e serviços.

O Núcleo de Gerenciamento é o órgão gestor do Portal UFS competindo-lhe:

I. determinar as linhas gerais de atuação do Portal UFS, respeitando as normas superiores;

II. analisar e deliberar acerca do conteúdo veiculado nos domínios, páginas ou blogs vinculados ao Portal UFS ou que adotem a URL //ufs.br

III. cumprir e fazer cumprir estas normas.

Os materiais, conteúdos e software do Portal UFS produzidos ou desenvolvidos pela Universidade Federal de Sergipe ou por terceiros são susceptíveis de serem protegidos através de direitos de propriedade intelectual.

É vedado ao usuário ou gerente responsável reproduzir, alterar, copiar, usar, distribuir, comercializar, aproveitar, descarregar ou empregar outros meios não previstos para utilizar e explorar os materiais e conteúdos do Portal UFS (incluindo, expressamente, o seu desenho, configuração e forma de apresentação) sem a autorização prévia, por escrito, do Portal UFS ou dos terceiros titulares dos direitos em causa.

É dispensada a autorização prévia por escrito para a reprodução ou aproveitamento do conteúdo jornalístico produzido pela Assessoria de Comunicação e disponibilizado no Portal UFS, estando seu uso sujeito ao disposto na Lei nº 9.610 (Lei de Direitos Autorais) e no Código de Ética dos Jornalistas Brasileiros.

É vedado ao usuário ou gerente responsável qualquer ato ou tentativa de alteração de materiais, conteúdos ou de software, de carregamento de informação, de acesso não autorizado ou outra ação que possa causar danos ou colocar em risco a integridade, continuidade ou qualidade dos serviços do Portal UFS.

O Portal UFS, através do Núcleo de Gerenciamento, terá o direito de, em qualquer momento e sem necessidade de aviso prévio, tomar todas as providências necessárias, incluindo restrições ou limitações de acesso, para assegurar a integridade, segurança, continuidade ou qualidade do Portal.

É dever do gerente responsável cumprir e fazer cumprir o disposto nas Normas do Portal UFS.

O gerente é o responsável direto por todos os conteúdos, informações, dados, comunicações, incluindo os respectivos anexos, materiais, etc., que tenha disponibilizado, por qualquer forma, através do Portal UFS ou ainda que tenha armazenado nos servidores do Portal.

O gerente responsável obriga-se a obter as necessárias autorizações antes da utilização ou disponibilização, por qualquer forma, de materiais sujeitos ao direito de propriedade intelectual ou a direitos de diferente natureza, a exemplo dos direitos de imagem da UFS ou de terceiros.

O Portal UFS, através do Núcleo de Gerenciamento reserva-se o direito de monitorar todas as seções do Portal e assim:

I. excluir conteúdos disponibilizados no Portal UFS ou armazenado nos seus servidores cuja ilicitude for manifesta ou quando tal for requerido por uma entidade competente nos termos legais;
II. excluir conteúdos falsos, ambíguos, inexatos que possam induzir a erro sobre seu objeto ou sobre as intenções ou propósitos do comunicante; que se encontrem protegidos por quaisquer direitos de propriedade intelectual, de imagem ou industrial pertencentes a terceiros; constituam propaganda publicitária fora do contexto educativo e cultural, ilícita ou enganosa; que possuam vírus ou outros elementos físicos ou eletrônicos que possam impedir o funcionamento normal do Portal e de seus sistemas ou que possam causar danos a equipamentos ou documentos eletrônicos da Universidade Federal de Sergipe ou de terceiros;
III. suspender, parcial ou totalmente, o acesso a qualquer parte do Portal UFS, em especial para operações de gestão, manutenção, reparação, alteração ou

modernização das mesmas. No caso de operações programadas, e caso seja possível, o Portal UFS divulgará um aviso prévio sobre a data e duração da intervenção ou suspensão temporária de seus serviços;

IV. de encerrar, definitiva ou temporariamente, parcial ou totalmente, qualquer parte do Portal.

O Portal UFS não se responsabiliza:

I. pela licitude, fidedignidade ou qualidade de qualquer conteúdo disponibilizado em websites, blogs ou documentos externos ao Portal UFS para onde remetam os links do Portal, nem pelo cumprimento das regras legais aplicáveis em relação aos conteúdos ali disponíveis.

II. pela utilização que terceiros possam dar aos conteúdos, quaisquer que sejam, que o gerente responsável tenha disponibilizado ou tornado acessível através do Portal.

O Portal UFS, através do Núcleo de Gerenciamento, empreenderá os melhores esforços para manter o Portal em boas condições de funcionamento.

# ANEXO IV

## RELAÇÃO DE ATIVOS DE CRITICIDADE MÁXIMA DA UFS

# RELAÇÃO DE ATIVOS DE CRITICIDADE MÁXIMA DA UFS

| | Ativo | Impacto | Responsável |
|---|---|---|---|
| 1 | Servidor de Firewall | Perda de conectividade, afetando todos os outros ativos que utilizem-se da rede. | Coordenação de Redes |
| 1.1 | Firewall | Perda de conectividade, afetando todos os outros ativos que utilizem-se da rede. | Coordenação de Redes |
| 2. | Servidor de Proxy | Perda de conectividade, afetando todos os outros ativos que utilizem-se da rede. | Coordenação de Redes |
| 2.1 | Proxy | Perda de conectividade, afetando todos os outros ativos que utilizem-se da rede. | Coordenação de Redes |
| 3. | Servidor de DNS | Perda de conectividade, afetando todos os outros ativos que utilizem-se da rede. | Coordenação de Redes |
| 3.1 | DNS | Perda de conectividade, afetando todos os outros ativos que utilizem-se da rede. | Coordenação de Redes |
| 4. | Roteador | Perda de conectividade, afetando todos os outros ativos que utilizem-se da rede. | Coordenação de Redes |
| 5. | Switch Core | Perda de conectividade, afetando todos os outros ativos que utilizem-se da rede. | Coordenação de Redes |
| 6. | Servidor de Banco de Dados DB2 | Perda do serviço de Banco DB2 (6.1) | Coordenação de Sistemas |
| 6.1 | Banco de dados DB2 | Perda das aplicações do DAA (8.1) e de diversas outras aplicações (SOS, SGSM, Sistema de Processos, Sistema de Requisição de Veículos, PIBIC, PIBID, PIBIX) | Coordenação de Sistemas |
| 7. | Servidor de Banco de Dados para Postgres | Perda dos serviços de Banco Postgres (7.1) e (7.2) e do Portal da UFS | Coordenação de Sistemas |
| 7.1 | Banco de dados das aplicações SIG | Perda das aplicações SIG | Coordenação de Sistemas |
| 8. | Servidor das aplicações do DAA | Perda do Sistema do DAA | Coordenação de Sistemas |
| 8.1 | Aplicações do DAA | Impossibilidade de gerenciamento de todas as informações acadêmicas da graduação | Coordenação de Sistemas |

| | | | |
|---|---|---|---|
| 9. | Servidor das Aplicações SIG | Perda das aplicações SIG | Coordenação de Sistemas |
| 9.1 | Aplicações SIG | Impossibilidade de gerenciamento de todas as informações da Pós Graduação, de Recursos Humanos, Ensino médio, Ensino à Distância, Pesquisa, Extensão, Patrimônio, Contratos e Almoxarifado. | Coordenação de Sistemas |
| 10. | Cluster de Virtualização (Blades) | Indisponibilidade de todos os sistemas e serviços em rede. | Coordenação de Redes |
| 10.1 | Software de Virtualização | Indisponibilidade de todos os sistemas e serviços em rede. | Coordenação de Redes |