FACELI
FUNDAÇÃO FACULDADES INTEGRADAS DE ENSINO SUPERIOR DO MUNICÍPIO DE LINHARES
"A Marca do Ensino Público de Linhares"

# PORTARIA Nº 071, DE 03/05/2018

**INSTITUI A POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DA FUNDAÇÃO FACELI – PSI/FACELI, E DÁ OUTRAS PROVIDÊNCIAS**

A Presidente da Fundação Faculdades Integradas de Ensino Superior do Município de Linhares – Faceli, no uso das suas atribuições que lhe são conferidas pela Lei nº 3.501/2015, e pelo Decreto Nº 016, de 02 de janeiro de 2017,

**RESOLVE**

**Art. 1º** Instituir a Política de Segurança da Informação da Fundação Faceli – PSI/Faceli disposta no **Anexo I**, que orienta e estabelece princípios, normas, diretrizes e objetivos para a proteção e utilização dos ativos de informação, de acordo com os ordenamentos vigentes.

**Art. 2º** A PSI/Faceli tem por objetivo estabelecer diretrizes que permitam aos seus colaboradores seguirem padrões de comportamento relacionados à segurança da informação adequados às necessidades de proteção legal da instituição e do indivíduo, abrangendo os aspectos estratégicos, táticos e operacionais, norteando a definição de controles, por meio de normas e procedimentos específicos, a fim de preservar a integridade, confidencialidade, disponibilidade e autenticidade das informações produzidas ou custodiadas pela Fundação Faceli.

**Art. 3º** Toda informação gerada, transmitida, adquirida ou custodiada em qualquer área ou equipamento da Fundação Faceli, é considerada um ativo e, assim sendo, de sua propriedade.

**Art. 4º** Compete ao Coordenador de Teconologia da Informação – TI da Fundaçao Faceli:

I. Coordenar e acompanhar a implementação da PSI/Faceli e suas normas complementares;
II. formular e conduzir diretrizes e procedimentos para a PSI/Faceli, monitorar e avaliar periodicamente sua efetividade, propor normas e mecanismos institucionais para a sua melhoria contínua;
III. promover ações permanentes de divulgação, treinamento, educação e conscientização dos usuários, em relação aos conceitos e às práticas de segurança da informação;

IV. configurar os equipamentos, ferramentas e sistemas utilizados na Fundação Faceli, com todos os controles necessários para cumprir os requisitos de segurança estabelecidos pela PSI/Faceli e pelas normas e procedimentos dela decorrentes, bem como pelas normalizações reguladoras de segurança da informação, quando aplicáveis;
V. informar os incidentes de segurança da informação evidenciados à Diretoria Administrattiva e Financeira para as providências cabíveis.

**Art. 5º** Compete à Diretoria Administrativa e Financeira fazer cumprir a presente PSI/Faceli e suas normas complementares.

**Art. 6º** A não observância aos dispositivos da presente política acarretará, isolada ou cumulativamente, nos termos da legislação aplicável, sanções administrativas, civis e penais.

**Art. 7º** Esta portaria entra em vigor na data da sua assinatura.

**Art. 8º** Revogam-se as disposições em contrário.

**Original assinado**
**Me. Jussara Carvalho de Oliveira**
Presidente da Fundação Faculdades Integradas de Ensino Superior do Município de Linhares - Faceli

Fundação  Faculdades Integradas de Ensino Superior do Município de Linhares

# Política de Segurança da Informação

## Documento de Normas e Diretrizes

**Versão 1.0**

# Sumário

# 1. INTRODUÇÃO

A Política de Segurança da Informação, também referida como PSI, é o documento que orienta e estabelece as normas e diretrizes da FACELI (Faculdade de Ensino Superior de Linhares) para a proteção dos ativos de informação e a prevenção de responsabilidade legal para todos os usuários. Deve, portanto, ser cumprida e aplicada em todas as áreas da instituição.

A presente PSI está baseada nas recomendações propostas pela norma **NBR ISO/IEC 27002**, reconhecida mundialmente como um código de prática para a gestão da segurança da informação, bem como está de acordo com as leis vigentes em nosso país.

Todo e qualquer usuário de recursos computadorizados da Instituição tem a responsabilidade de proteger a segurança e a integridade das informações e dos equipamentos de informática.

## 1.1 A Instituição

A FACELI é uma Instituição de ensino superior, de estudo, pesquisa e extensão, em todos ramos do saber e da divulgação científica técnica e cultural, pública, sem fins lucrativos, mantida pela FUNDAÇÃO FACELI, com limite territorial de atuação circunscrito ao município de Linhares, Estado do Espírito Santo, credenciada pela Resolução CEE Nº 1343/2006 de 20 de setembro de 2006, publicado no diário Oficial em 27 de setembro de 2006.

## 1.2 Compromisso com a Política de Segurança da Informação

Todas as normas estabelecidas neste documento serão seguidas por todos os servidores públicos, alunos, parceiros e prestadores de serviços. Ao receber essa cópia da PSI, o (a) Sr. (a) compromete-se a respeitar todos os tópicos aqui abordados e passa a ter conhecimento de que seus e-mails, chat interno e históricos de navegação na internet/intranet podem estar sendo monitorados. A equipe da

tecnologia da informação (TI) encontra-se a total disposição para esclarecimentos de dúvidas e suporte técnico.

## 2. OBJETIVO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Definir responsabilidades e orientar a conduta dos usuários de TI, visando a continuidade dos negócios através da confidencialidade, da integridade e da disponibilidade das informações da FACELI.

**É Dever de todos dentro da FACELI:**

*Considerar a informação como sendo um bem da organização, um dos recursos críticos para a realização do negócio, que possui grande valor para a FACELI e deve sempre ser tratada profissionalmente.*

## 3. VIOLAÇÕES E SANÇÕES

É considerado violação as regras desta política de segurança, não se limitando às mesmas, qualquer ato que:

- Exponha a Instituição a uma perda monetária efetiva ou potencial por meio do comprometimento da segurança dos dados e/ou de informações ou ainda da perda de equipamento.
- Envolva a revelação de dados confidenciais, direitos autorais, negociações ou patentes.
- Envolva tentativas de acesso ou uso não autorizado a dados e sistemas da instituição.
- Envolva o uso de dados para propósitos ilícitos, que venham a incluir a violação de qualquer lei, regulamento ou qualquer outro dispositivo governamental.

A violação à política, às normas ou aos procedimentos de segurança da informação ou a não aderência à política de segurança da informação da FACELI são consideradas faltas graves, podendo ser aplicadas penalidades previstas em lei.

No Código Penal estão listados os seguintes atos ilícitos com suas devidas penalidades, não se limitando às mesmas:

**DECRETO-LEI Nº 2.848, DE 7 DE DEZEMBRO DE 1940**

- **Divulgação de segredo**

Art. 153. § 1º-A. Divulgar, sem justa causa, informações sigilosas ou reservadas, assim definidas em lei, contidas ou não nos sistemas de informações ou banco de dados da Administração Pública: (Incluído pela Lei nº 9.983, de 2000)
Pena – detenção, de 1 (um) a 4 (quatro) anos, e multa.

- **Violação do segredo profissional**

Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita: (Incluído pela Lei nº 12.737, de 2012)
Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.

- **Inserção de dados falsos em sistema de informações**

Art. 313-A. Inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou bancos de dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano: (Incluído pela Lei nº 9.983, de 2000)
Pena – reclusão, de 2 (dois) a 12 (doze) anos, e multa.

- **Modificação ou alteração não autorizada de sistema de informações**

Art. 313-B. Modificar ou alterar, o funcionário, sistema de informações ou programa de informática sem autorização ou solicitação de autoridade competente: (Incluído pela Lei nº 9.983, de 2000)
Pena – detenção, de 3 (três) meses a 2 (dois) anos, e multa

O Código de Ética do Servidor Público determina que é vedado ao servidor público (Art. XV, Decreto Nº 1.171, de 22/06/1994**)**:

- Fazer uso de informações privilegiadas obtidas no âmbito interno de seu serviço, em benefício próprio, de parentes, de amigos ou de terceiros;

## 4. CLASSIFICAÇÃO DA INFORMAÇÃO

É de responsabilidade do Gerente/Supervisor de cada área estabelecer critérios relativos ao nível de confidencialidade da informação (relatórios e/ou mídias) gerada por sua área de acordo com a tabela abaixo:

- **Pública**
- **Interna**
- **Confidencial**
- **Restrita**

**Conceitos:**

- **Informação Pública:** É toda informação que pode ser acessada por usuários da organização, clientes, fornecedores, prestadores de serviços e público em geral.

- **Informação Interna:** É toda informação que só pode ser acessada por funcionários da organização. São informações que possuem um grau de confidencialidade que pode comprometer a imagem da organização.

- **Informação Confidencial:** É toda informação que pode ser acessada por usuários da organização e por parceiros da organização. A divulgação não autorizada dessa informação pode causar impacto (financeiro, de imagem ou operacional) ao negócio da organização ou ao negócio do parceiro.

- **Informação Restrita:** É toda informação que pode ser acessada somente por usuários da organização explicitamente indicado pelo nome ou por área a que pertence. A divulgação não autorizada dessa informação pode causar sérios danos ao negócio e/ou comprometer a estratégia de negócio da organização.

Todo Gerente/Supervisor deve orientar seus subordinados a não circularem informações e/ou mídias consideradas confidenciais e/ou restritas, como também não deixar relatórios nas impressoras, e mídias em locais de fácil acesso, tendo sempre em mente o conceito “mesa limpa”, ou seja, ao terminar o trabalho não deixar nenhum relatório e/ou mídia confidencial e/ou restrito sobre suas mesas.

## 5. RESPONSABILIDADES

Os recursos de informática e as informações disponibilizadas são fornecidos com o objetivo de garantir o desempenho e continuidade das atividades da FACELI, portanto todos os usuários devem manter-se responsáveis e condizentes com as normas dessa PSI.

### 5.1 Dos Usuários

a) Respeitar esta Política de Segurança da Informação;
b) Responder pela guarda e proteção dos recursos computacionais colocados à sua disposição para o trabalho;
c) Responder pelo uso exclusivo e intransferível de suas senhas de acesso;
d) Ativar suas senhas de proteção para Correio Eletrônico e Sistema Operacional, sob orientação do Gestor de Liberações da área de TI;
e) Buscar conhecimento necessário para a correta utilização dos recursos de hardware e software;
f) Relatar prontamente à área de TI qualquer fato ou ameaça à segurança dos recursos, como quebra da segurança, fragilidade, mau funcionamento, presença de vírus, etc.;

g) Assegurar que as informações e dados de propriedade da FACELI não sejam disponibilizados a terceiros, a não ser com autorização por escrito do responsável hierárquico;
h) Relatar para o seu responsável hierárquico e à Gerência de TI, o surgimento da necessidade de um novo software para suas atividades;
i) Responder pelo prejuízo ou dano que vier a provocar a FACELI ou a terceiros, em decorrência da não obediência as diretrizes e normas aqui referidas;
j) Não se fazer passar por outra pessoa ou dissimular sua identidade quando utilizar os recursos computacionais.

## 5.1 Dos Responsáveis Hierárquicos

a) Apoiar e zelar pelo cumprimento desta PSI, servindo como modelo de conduta para os colaboradores sob a sua gestão;
b) Atribuir na fase de contratação e de formalização dos contratos individuais de trabalho CLT, prestação de serviços ou de parceria, a responsabilidade do cumprimento da PSI;
c) Autorizar o acesso e definir o perfil do usuário junto ao gestor de liberações da área de TI;
d) Autorizar as mudanças no perfil do usuário junto ao gestor de liberações da área de TI;
e) Educar os usuários sobre os princípios e procedimentos de Segurança da Informação;
f) Notificar imediatamente ao gestor de liberações da área de TI quaisquer vulnerabilidades e ameaças a quebra de segurança;
g) Assegurar treinamento para o uso correto dos recursos computacionais e sistemas de informação;
h) Advertir formalmente o usuário e aplicar sanções cabíveis quando este violar os princípios ou procedimentos de segurança, relatando imediatamente o fato ao gestor de liberações da área de TI;
i) Obter aprovação técnica do gestor de liberações da área de TI antes de solicitar a compra de hardware, software ou serviços de informática;

j) Adaptar as normas, os processos, procedimentos e sistemas sob sua responsabilidade para atender a esta PSI.

## 6. INSTALAÇÕES DE PROGRAMAS

É terminantemente proibido a instalação de programas ilegais (PIRATAS) na FACELI. Os usuários não podem, em hipótese alguma, instalar este tipo de "software" (programa) nos equipamentos da Instituição.
Periodicamente, o Setor de Informática fará verificações nos dados dos servidores e/ou nos computadores dos usuários, visando garantir a correta aplicação desta diretriz.
Toda instalação de software deve ser solicitada com antecedência de até 72h ao TI e através de memorando ou E-mail.

## 7. CADASTRAMENTO DE NOVOS USUÁRIOS

Quando da necessidade de cadastramento de um novo usuário para utilização da "rede", sistemas ou equipamentos de informática da FACELI, o setor de origem do novo usuário deverá comunicar esta necessidade ao setor de Informática, por meio de memorando ou e-mail, informando a que tipo de rotinas e programas o novo usuário terá direito de acesso e quais serão restritos. A Informática fará o cadastramento e informará ao novo usuário qual será a sua primeira senha, a qual deverá, obrigatoriamente, ser alterada a cada 45 (quarenta e cinco) dias.
Por segurança, a Informática recomenda que as senhas tenham sempre um mínimo de 6 (seis) caracteres Alfanuméricos.

## 8. UTILIZAÇÃO DA REDE

Esse tópico visa definir as normas de utilização da rede que engloba desde o *"logon/login"*, manutenção de arquivos no servidor e tentativas não autorizadas de acesso.

a) Não é permitido tentativas de obter acesso não autorizado, tais como tentativas de fraudar autenticação de usuário ou segurança de qualquer servidor, rede ou conta (pratica conhecida como "*cracking*"). Isso inclui acesso aos dados não disponíveis para o usuário, conectar-se ao servidor ou conta cujo acesso não seja expressamente autorizado ao usuário ou colocar à prova a segurança de outras redes, **crime previsto por lei: 12.737 de 30 novembro de 2012**;

b) Não é permitido tentativas de interferir nos serviços de qualquer outro usuário, servidor ou rede. Isso inclui ataques do tipo "negativa de acesso" (pratica conhecida como DDOS ou DOS – *Distributed Denial of Service* ou *Denial of Service*) como, provocar congestionamento em redes, tentativas deliberadas de sobrecarregar um servidor e tentativas de burlar (invadir) um servidor, **crime previsto por lei: 12.737 de 30 novembro de 2012**;

c) Não é permitido o uso de qualquer tipo de programa ou comando designado a interferir com sessão de usuários;

d) Antes de ausentar-se do seu local de trabalho, o usuário deverá fechar todos os programas acessados, evitando, desta maneira, o acesso por pessoas não autorizadas e se possível efetuar o "*logout/logoff*" da rede ou bloqueio do desktop através de senha;

e) É de total responsabilidade do usuário a manutenção no diretório seu pessoal, evitando acúmulo de arquivos inúteis;

f) Material de natureza pornográfica e preconceituosa não pode ser exposto, armazenado, distribuído, editado ou gravado através do uso dos recursos computacionais da rede. Preconceito é crime previsto em **LEI nº 7.716, de 5 de janeiro de 1989;**

g) Não é permitido criar e/ou remover arquivos fora da área alocada ao usuário e/ou que venham a comprometer o desempenho e funcionamento dos sistemas

nas áreas de armazenamento de arquivos que são designados conforme abaixo:

| Local | Descrição |
|---|---|
| Diretório (Z:) em Meu computador | Arquivos do departamento em que trabalha. |
| Meus Documentos e Desktop | Arquivos pessoais e sem importância para a Instituição |

h) Cada usuário tem um espaço de 5GB para armazenamento de dados institucionais na rede. Ultrapassando este limite a equipe de TI irá comunicar que seja deletado alguns arquivos para liberar espaço no servidor;
i) Jogos ou qualquer tipo de software/aplicativo não poderão ser gravados ou instalados no diretório pessoal do usuário, no computador local ou em qualquer outro diretório da rede. Podem ser utilizados apenas os softwares previamente instalados no computador;
j) Pastas públicas ou similares não deverão ser utilizadas para guardar arquivos de assuntos sigilosos ou confidenciais. Devem ser armazenadas apenas informações comuns a todos.

## 8.1 Regras para os Servidores

a) É obrigatório armazenar os arquivos inerentes à Instituição no servidor de arquivos para garantir a cópia de segurança dos mesmos. (Diretório (Z:) em Meu computador)
b) É proibida a abertura do computador para qualquer tipo de reparo, seja em departamentos ou laboratório de informática. Caso seja necessário, o reparo será feito pelo TI;
c) Quando ocorrer o afastamento ou exoneração do servidor, o responsável deve informar o TI para providenciar a desativação dos acessos do usuário a qualquer recurso da rede.

### 8.2 Regras para os Alunos

a) Conteúdos salvos na conta de usuário "aluno" podem ser deletados sem aviso prévio por qualquer usuário ou mesmo pelo TI. Portanto o aluno deve ter uma cópia de segurança de seus arquivos.

## 09. POLÍTICA DE SENHAS

A política de senhas é um controle de segurança para evitar possíveis ataques ou acessos não autorizados. Mediante isto é preciso ter conhecimento dos seguintes tópicos:

a) Os cuidados para a manutenção da segurança dos recursos, tais como sigilo da senha, troca periódica da senha e o monitoramento da conta, evitando a utilização indevida é de responsabilidade do usuário;
b) As senhas são sigilosas, individuais e intransferíveis, não podendo ser divulgadas em nenhuma hipótese;
c) Tudo que for executado com a senha de um usuário, tanto de rede ou de qualquer sistema, será de sua inteira responsabilidade.

## 10. UTILIZAÇÃO DE E-MAIL

Esse tópico visa definir as normas de utilização de e-mail que engloba desde o envio, recebimento e gerenciamento das contas de e-mail.

a) É proibido o assédio ou perturbação de outrem, seja através de linguagens utilizadas, frequência ou tamanho das mensagens;
b) É proibido o envio de e-mail a qualquer pessoa que não o deseje receber. Se o destinatário solicitar a interrupção de envio e-mails, o usuário deve acatar tal solicitação não lhe enviar qualquer e-mail;

c) É proibido o envio de grandes quantidades de mensagem de e-mail (“Lixo Eletrônico” ou “*spam*”) que, de acordo com a capacidade técnica da Rede, seja prejudicial ou gere reclamações de outros usuários. Isso inclui qualquer tipo de mala direta, como, por exemplo, publicidade, comercial ou não, anúncios e informativos, ou propaganda política;

**d) Não é permitido o uso do e-mail institucional para a realização de cadastros pessoais;**

e) Não é permitido má utilização da linguagem em resposta aos e-mails comerciais, tais abreviações de palavras (Ex.: “vc” ao invés de “você”);

f) É obrigatório a manutenção da caixa de e-mail, evitando acumulo de e-mails e arquivos inúteis;

g) É obrigatória a utilização de assinatura nos e-mails com o seguinte formato:


**Nome do Funcionário**
Função:
E-mail:
Fone:
www.faceli.edu.br

## 11. UTILIZAÇÃO DE ACESSO A INTERNET

Esse tópico visa definir as normas de utilização da internet que engloba desde a navegação a sites, downloads e uploads de arquivos.

a) É proibido utilizar os recursos da instituição para fazer o download ou distribuição de software ou dados não legalizados;

b) É proibido a divulgação de informações confidencias da instituição em rede social, fórum, grupo de discussão, lista ou bate-papo, não importando se a divulgação foi deliberada ou inadvertida, sendo possível sofrer as penalidades previstas nas políticas e procedimentos internos e/ou na forma da lei;

c) Os usuários não deverão tentar burlar, nem subverter as medidas de segurança dos recursos de rede da instituição ou de qualquer outro sistema conectado ou acessível pela Internet;

d) Não é permitido usar a Internet para enviar material ofensivo ou de assédio para outros usuários;
e) Não é permitido visitar sites da Internet que contenha material obsceno e/ou pornográfico;
f) A conexão à Internet na instituição não deve ser usada para objetivos comerciais nem políticos;
g) Poderá ser utilizada a Internet para atividades não relacionadas a negócios durante o horário de almoço, ou fora do expediente, desde que dentro das regras de uso definidas nesta política;
h) Os funcionários com acesso à Internet podem baixar programas ligados diretamente às atividades da instituição e devem providenciar o que for necessário para regularizar a licença e o registro desses programas;
i) Funcionários com acesso à Internet não podem efetuar upload de qualquer software licenciado à instituição ou de dados de propriedade da instituição ou de seus gestores, sem expressa autorização da diretoria responsável ou pelos dados;
j) O Acesso a redes sociais só poderá ser feito mediante a autorização do seu responsável imediato.
k) Os recursos de internet não deverão ser utilizados para ouvir música, como sites de músicas, rádios e vídeos.
l) É de inteira responsabilidade do usuário os danos sofridos pela Faceli em virtude de acesso a sites maliciosos, downloads, abertura de anexos de e-mails, etc. Que podem infectar o computador do usuário e a rede da Instituição.

## 12. UTILIZAÇÃO E INSTALAÇÃO DE IMPRESSORAS

Esse tópico visa definir as normas de utilização de impressoras disponíveis na rede interna.

a) Ao imprimir verifique na impressora se o que foi solicitado já está impresso. Impressões “sem dono” provocam o acúmulo de papel e gastos desnecessários para a FACELI;

b) Não é permitido utilizar a impressora para imprimir arquivos pessoais sem autorização prévia;
c) Utilizar sempre rascunhos para imprimir documentos não oficiais;
d) Caso a impressão resulte em erro e o papel poder ser reaproveitado, recoloque-o na bandeja da impressora;
e) Caso a impressão der errado e o papel servir para rascunho, leve para seu setor;
f) Caso a impressão der errado e o papel não servir para mais nada, jogue no lixo;
g) Não é permitido a instalação de impressora sem autorização expressa do responsável pelo setor.
h) A instalação de impressoras deverá ser solicitada ao TI através de abertura de chamado pelo responsável do setor.

A FACELI se reserva a remover ou mudar impressoras de lugares sem aviso prévio.

## 13. VÍRUS E CÓDIGOS MALICIOSOS.

a) Mantenha seu antivírus atualizado. Provavelmente nossa equipe técnica irá se encarregar disso, mas caso não tenha sido feito ou você perceba que a atualização não está funcional, entre em contato com a mesma para que a situação possa ser corrigida;
b) Não traga Pen drives ou CDs de fora da FACELI. Caso isso seja extremamente necessário, solicite ao TI uma verificação de segurança ou se precisar utilizar com frequência, solicite a instalação de um software de proteção. É de responsabilidade do usuário a prevenção de seus dados;
c) É proibido de qualquer forma introduzir vírus e outros tipos de códigos maliciosos nos ativos ou na rede da instituição;
d) Reporte atitudes suspeitas em seu sistema a equipe técnica, para que possíveis vírus possam ser identificados no menor espaço de tempo possível;
e) Suspeite de softwares onde "você clica e não aconteça nada".

## 14. POLÍTICA DE ADMINISTRAÇÃO DE CONTAS

Esta Política define normas de administração de contas abrangendo: criação, manutenção e desativação da conta.

### 14.1 Servidores

Desde que seja necessário, todo servidor poderá ter uma conta de acesso à rede de computadores. Demais acessos devem ser informados pelo responsável do setor no momento da solicitação da conta de usuário. Para manutenção ou solicitação de novas contas o responsável deve proceder da seguinte forma:

#### 14.1.1 Criação de Contas

a) O responsável pelo setor a que o servidor pertencerá deverá fazer a solicitação da conta para o TI, preferencialmente por e-mail ou abertura de chamado.
b) Deve-se informar o nome completo do servidor, setor em que irá trabalhar, os níveis de acessos aos diretórios de rede do setor, os níveis de acessos ao sistema utilizado no setor.

#### 14.1.2 Manutenção da Conta

a) Cada servidor que tiver sua conta criada terá um espaço no servidor para gravar seus arquivos importantes para a instituição;
b) O servidor não deverá armazenar em sua pasta de rede arquivos pessoais que não sejam de interesse da FACELI.
c) A manutenção dos arquivos na conta pessoal é de responsabilidade do usuário, sendo que o mesmo deve evitar acumulo de arquivos desnecessários e sempre que possível verificar o que pode ser eliminado;
d) As contas podem ser monitoradas pelo TI com o objetivo de verificar possíveis irregularidades no armazenamento ou manutenção dos arquivos nos diretórios pessoais.

### 14.2 Alunos

a) Os alunos não possuem o direito de criar uma conta pessoal;
b) Os alunos que desejarem utilizar algum computador da Instituição poderão ter o acesso através da conta de usuário “aluno” com a senha padrão “123456”, que é destinada a este grupo de usuários.

### 14.3 Desativação da Conta

É reservado ao TI o direito de desativar uma conta de usuário caso verifique-se a ocorrência de algum dos critérios especificados abaixo:

c) Desligamento do servidor (Comunicado pelo setor responsável pelo servidor desligado).
d) Incidentes suspeitos de quebra de segurança nas contas de usuários.
e) Reincidência na quebra de senhas por utilização de algum tipo de programa.

## 15. POLÍTICA DE UTILIZAÇÃO DE LABORATÓRIOS DE INFORMÁTICA

Este tópico enfatiza algumas regras de utilização dos laboratórios e equipamentos de informática para que possa ser feito o uso correto das instalações evitando qualquer tipo de dano a equipamentos em laboratórios que possam prejudicar a utilização dos mesmos.

### 15.1 Regras Gerais

a) O acesso a laboratórios de informática deve ser controlado.
b) É de responsabilidade do professor/servidor que utilizou o laboratório zelar pela ordem, manutenção e organização do laboratório. Sendo necessário qualquer tipo de manutenção, o TI deve ser informado.

c) Ao entrar no laboratório o professor/servidor responsável deve verificar se os computadores a serem utilizados estão funcionando corretamente. Caso contrário o TI deve ser informado para tomar as providências cabíveis.
d) O professor/servidor que utilizar o Laboratório deverá informar ao TI qualquer irregularidade encontrada antes do início de suas atividades, caso não seja informado, entende-se que o problema foi ocasionado na ultima utilização.
e) Nenhum equipamento pode ser conectado aos sistemas ou rede sem aprovação prévia e, se necessário, sob supervisão.
f) Alimentos, bebidas, fumo são proibidos nos laboratórios.
g) A utilização dos laboratórios deverá ser feita somente mediante reserva, garantindo assim a existência de um registro de utilização dos mesmos.
h) É proibido retirar computadores e componentes de seus devidos lugares.
i) Após a utilização do laboratório, todos os computadores e equipamentos devem ser desligados, incluindo ar condicionado, projetor e filtros de linha.

## 16. POLÍTICA SOCIAL

Como seres humanos, temos a grande vantagem de sermos sociáveis, mas muitas vezes quando discorremos sobre segurança, isso é uma desvantagem. Por isso observe os seguintes tópicos:

a) Não fale sobre a política de segurança da instituição com terceiros ou em locais públicos.
b) Não diga sua senha para ninguém. Nossa equipe técnica jamais irá pedir sua senha.
c) Não digite suas senhas ou usuários em equipamentos que não correspondem à FACELI.
d) Somente aceite ajuda técnica de um membro de nossa equipe técnica previamente apresentado e identificado.
e) Nunca execute procedimentos técnicos cujas instruções tenham chegado por e-mail.

f) Relate a equipe de segurança pedidos externos ou internos que venham a discordar dos tópicos anteriores.

## 17. ATENDIMENTO TÉCNICO

Para estabelecer um ponto único de contato entre o setor de TI e o usuário final, facilitando o acesso aos profissionais de suporte e contribuindo para soluções rápidas e eficazes, é utilizado uma aplicação de *service desk*, distribuído sob licença GPL (Licença Pública Geral GNU), denominado GLPI. Trata-se de um meio único para se gerenciar as requisições e chamadas de serviços.

### 17.1 Solicitação de Atendimento

a) O Colaborador deve solicitar suporte à equipe de TI sempre que ocorrer falha/não funcionamento de equipamentos de informática, sistemas, programas e acesso à rede, através de abertura de chamado no sistema de Help Desk GLPI ou, em casos especiais, ligando para o ramal de suporte de TI;
b) O colaborador através de *login* e senha, fornecidos pelo setor de TI, deve acessar o sistema Help Desk GLPI e solicitar o atendimento de acordo com a área de atendimento disponível;
c) Para solicitação de atendimento o colaborador deve acessar o sistema Help Desk GLPI, realizar *login*, clicar em Criar um chamado e preencher os campos solicitados. Caso necessário, poderá anexar arquivo com print screen exibindo o erro ocorrido ou qualquer outro documento de importância para execução da resolução do chamado. Por fim, clicar em Enviar Mensagem.

### 17.2 Priorização dos atendimentos

a) Os pedidos serão atendidos pela TI seguindo a prioridade dos mesmos, a saber:

• Baixa - baixo impacto nos processos da FACELI, e o usuário pode continuar trabalhando no equipamento.

• Média - médio impacto nos processos da FACELI, e o usuário pode continuar trabalhando no equipamento.

• Alta - alto impacto nos processos da FACELI, ou o usuário não pode continuar trabalhando no equipamento.

b) Os Técnicos de atendimento definirão a prioridade em função de regras internas de atendimento por nível de Serviço, estabelecidos pela área de TI em conjunto com os superiores de cada área.

### 17.3 Processo de Atendimento

- A abertura de chamados é realizada pelo Cliente, mas pode ser realizada pelo TI;
- Na abertura de um novo chamado o usuário e o TI receberá um aviso (e-mail) informando a existência desse novo chamado;
- O TI faz a análise e responde ao cliente (interação);
- O TI pode durante o atendimento, solicitar o envio de mais informações [Documentação] para melhor compreensão do que foi registrado;
- A cada ação executada pelo TI a situação do chamado é alterada e o cliente receberá um aviso (e-mail) informando a interação do chamado;
- Quando o chamado é atendido o TI faz o encerramento do chamado. O cliente então deverá confirmar se o chamado foi realmente resolvido;
- O cliente também poderá encerrar o chamado a qualquer momento.

### 17.4 Regras e Normas Gerais para um bom atendimento

- Para cada nova demanda deverá ser criado um novo CHAMADO. Jamais utilize um CHAMADO para começar outro;
- Evite escrever textos EXCLUSIVAMENTE EM MAIÚSCULAS ou grifos exagerados. Se bem empregadas, as maiúsculas podem ajudar a destacar,

mas em excesso, a prática é compreendida como se você estivesse gritando, podendo causar irritação ou fazer com que o interlocutor se sinta ofendido;

- Procure ser sempre claro, detalhando a mensagem com propriedade para a melhor compreensão da sua demanda;
- Quando você estiver buscando atendimento, provavelmente é porque precisa de ajuda em algo, então aja como tal. Evite ser arrogante ou inconveniente;
- Lembre-se que dialogar com alguém através do computador, não faz com que você seja imune às regras comuns da nossa sociedade, por exemplo, o respeito para com o próximo. Mesmo que por intermédio de uma máquina, você está conversando com uma pessoa, assim como você. Não diga a essa pessoa o que você não gostaria de ouvir.
- Haja sempre com paciência, entendendo o fato de que os chamados têm diferentes graus de dificuldade, e em alguns casos podem demandar maior tempo para a resolução.

## 17. LEGISLAÇÃO APLICÁVEL

Correlacionam-se com a política, com as diretrizes e com as normas de Segurança da Informação as Leis abaixo relacionadas, mas não se limitando às mesmas:

a) Lei Federal 8159, de 08 de janeiro de 1991 (Dispõe sobre a Política Nacional de Arquivos Públicos e Privados);
b) Lei Federal 9610, de 19 de fevereiro de 1998 (Dispõe sobre o Direito Autoral);
c) Lei Federal 9279, de 14 de maio de 1996 (Dispõe sobre Marcas e Patentes);
d) Lei Federal 3129, de 14 de outubro de 1982 (Regula a Concessão de Patentes aos autores de invenção ou descoberta industrial);
e) Lei Federal 10406, de 10 de janeiro de 2002 (Institui o Código Civil);
f) Decreto-Lei 2848, de 7 de dezembro de 1940 (Institui o Código Penal);
g) Lei Federal 9983, de 14 de julho de 2000 (Altera o Decreto-Lei 2.848, de 7 de dezembro de 1940 - Código Penal e dá outras providencias).

## 18 – EQUIPE DA TECNOLOGIA DA INFORMAÇÃO

### 13.1 - Técnicos

| Nome | E-mail | Celular |
|---|---|---|
| Alécio França | alecio.franca@faceli.edu.br | (27) 99956-8249 |
| Anderson Mendes | anderson.mendes@faceli.edu.br | (27) 99797-7309 |
| Roner Facini | roner.facine@faceli.edu.br | (27) 99963-4384 |
| Stefano Nascimento | stefano.nascimento@faceli.edu.br | (27) 99858-2910 |

### 13.2 – Analista

| Nome | E-mail | Celular |
|---|---|---|
| Jardel Terci | jardel.terci@faceli.edu.br | (27) 99708-6884 |

### 13.2 – Coordenador

| Nome | E-mail | Celular |
|---|---|---|
| Welton Castoldi | welton@faceli.edu.br | (27) 99977-1198 |