



**UNIVERSIDADE FEDERAL DO ESPÍRITO SANTO**  
**CENTRO UNIVERSITÁRIO NORTE DO ESPÍRITO SANTO**  
Conselho Departamental

**RESOLUÇÃO Nº 022/2011**

Estabelece a Política de Segurança da Informação e Comunicação (POSIC) do Centro Universitário do Norte do Espírito Santo (CEUNES)

O CONSELHO DEPARTAMENTAL DO CENTRO UNIVERSITÁRIO DO NORTE DO ESPÍRITO SANTO, DA UNIVERSIDADE FEDERAL DO ESPÍRITO SANTO, no uso de suas obrigações legais e estatutárias;

Considerando o Decreto nº 3505, de 13 de junho de 2000, que institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal;

Considerando o Regimento e o Estatuto da Universidade Federal do Espírito Santo;

Considerando o que consta do protocolado Nº 23068.759622/2010-49;

Considerando a Decisão Nº 207/2010 do Conselho Departamental do Centro Universitário do Norte do Espírito Santo, da Universidade Federal do Espírito Santo;

Considerando, ainda, a aprovação na Plenária, por unanimidade, na Décima Quinta Sessão Ordinária, realizada no dia 24 de agosto de 2011.

**RESOLVE:**

**Capítulo I – Objetivos**

**Artigo 1º** - Esta Resolução estabelece as Normas e Procedimentos para o uso dos recursos de TIC (Tecnologia da Informação e Comunicação) do CEUNES (Centro Universitário Norte do Espírito Santo).

Parágrafo Único. Esta Resolução não é exaustiva em todas as suas Normas de Uso e Políticas de Segurança, ficando de responsabilidade da Comissão Permanente de Gestão da Política de Segurança da Informação e Comunicação do CEUNES propor complementações a alterações, sob demanda de novos cenários. A complementação desta Resolução sempre deverá ser submetida ao Conselho Departamental do CEUNES para a sua devida aprovação.

*[Assinatura manuscrita]*





**UNIVERSIDADE FEDERAL DO ESPÍRITO SANTO**  
**CENTRO UNIVERSITÁRIO NORTE DO ESPÍRITO SANTO**  
Conselho Departamental

**Artigo 2º** - É política do CEUNES prover para a sua comunidade o acesso a fontes de informação locais, nacionais e internacionais, promovendo um ambiente de produção, uso e compartilhamento do conhecimento e de comprometimento com a liberdade acadêmica.

§ 1º - As fontes de informações devem ser utilizadas pelos membros da comunidade dentro do respeito e da ética de acordo com as regulamentações estabelecidas pelo CEUNES.

§ 2º - Os Recursos de TIC devem ser utilizados de maneira responsável, consistente com objetivos educacionais, de pesquisa e administração do CEUNES.

§ 3º - Todas as utilizações que não estiverem de acordo com estes objetivos são consideradas inapropriadas e podem colocar em risco os demais acessos aos serviços.

### Capítulo II - Definições

**Artigo 3º** - Nesta Resolução, considera-se:

I. Recursos de TIC são todos os equipamentos, instalações e recursos de informação direta ou indiretamente administrados, mantidos ou operados pelos setores administrativos e departamentos do CEUNES, tais como:

- a) equipamentos de informática de qualquer espécie;
- b) impressoras;
- c) equipamentos de redes e de telecomunicações de qualquer espécie;
- d) laboratórios de informática de qualquer espécie;
- e) recursos de informação que incluem todas as informações eletrônicas, serviço de correio eletrônico, mensagens eletrônicas, dados corporativos, documentos, programas ou software que são armazenados, executados ou transmitidos através da infraestrutura computacional do CEUNES.

II. Usuário é qualquer pessoa, física ou jurídica, com vínculo oficial com o CEUNES ou em condição autorizada que utiliza, de qualquer forma, algum Recurso de TIC deste Centro.

III. Dados corporativos da Universidade incluem, mas não estão restritos às informações sobre:

- a) recursos humanos;
- b) recursos financeiros;
- c) equipamentos de qualquer natureza;
- d) alunos;
- e) cursos e disciplinas;
- f) políticas, procedimentos e manuais;
- g) páginas Web.





**UNIVERSIDADE FEDERAL DO ESPÍRITO SANTO**  
**CENTRO UNIVERSITÁRIO NORTE DO ESPÍRITO SANTO**  
**Conselho Departamental**

IV. Comissão Permanente de Gestão da Política de Segurança da Informação e Comunicação: grupo de pessoas com a responsabilidade de assessorar a implementação das ações de segurança da informação e comunicações.

V. Administradores: grupo de pessoas com a responsabilidade de receber, analisar e responder a notificações e atividades relacionadas à incidentes de segurança em computadores.

VI. Gestor da Política de Segurança da Informação e Comunicação: é o responsável pelas ações de segurança da informação.

VII. Política de Segurança da Informação e Comunicações (POSIC): documento aprovado pelo Conselho Departamental do CEUNES, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação e comunicações.

### **Capítulo III – Da Composição da Comissão**

**Artigo 4º** - Integram a Comissão Permanente de Gestão da Política de Segurança da Informação e Comunicação:

- a) 4 (quatro) docentes do CEUNES;
- b) 2 (dois) representantes do setor de TIC do CEUNES;
- c) 1 (um) servidor TAE do CEUNES;

§1º – Todos os membros serão escolhidos pelo Conselho Departamental do CEUNES e terão mandatos de 2 (dois) anos, sendo permitida 1 (uma) recondução.

§2º – O presidente da comissão será eleito entre seus pares.

§3º – O presidente da Comissão será o Gestor da Política de Segurança da Informação e Comunicação do CEUNES.

### **Capítulo IV – Do acesso aos dados, informações e Recursos de TIC**

**Artigo 5º** - Os usuários dos Recursos de TIC do CEUNES têm direito de acesso a todos os registros que lhes dizem respeito.

**Artigo 6º** - O acesso e a utilização de informações relativas à vida acadêmica ou funcional de outrem, por qualquer membro da Universidade, dependem de:

- I. Expressa autorização do titular do direito;
- II. Ato administrativo motivado em razão de objetivos acadêmicos ou funcionais, devidamente justificados.

**Artigo 7º** - Arquivos computacionais são de uso privativo e confidencial de seu autor ou proprietário, sendo igualmente confidencial todo o tráfego na rede.





**UNIVERSIDADE FEDERAL DO ESPÍRITO SANTO**  
**CENTRO UNIVERSITÁRIO NORTE DO ESPÍRITO SANTO**  
**Conselho Departamental**

Parágrafo Único - Os administradores dos sistemas computacionais poderão ter acesso aos arquivos em casos de necessidade de manutenção ou falha de segurança.

**Artigo 8º** - Constituem responsabilidades dos usuários, relativamente ao uso dos Recursos de TIC deste centro:

- I. Respeitar todas as políticas e procedimentos de uso dos Recursos de TIC.
- II. Utilizar qualquer Recurso de TIC deste centro somente após assinar o Termo de Responsabilidade, no qual declara conhecer as políticas e normas em vigor e se compromete a cumpri-las.
- III. Exibir a comprovação de vínculo com a Universidade ou autorização especial ao pessoal responsável, sempre que solicitado, durante a utilização dos recursos de TIC.
- IV. Respeitar a integridade e os limites de sua autorização de acesso ou conta.
- V. Garantir a segurança de suas contas e de suas senhas. A conta e a respectiva senha são atribuídas a um único usuário e não devem ser compartilhadas com mais pessoas sem a autorização expressa e por escrito da chefia imediata.
- VI. Informar imediatamente ao setor de TIC deste centro qualquer suspeita ou tentativa de violação desta Política de Segurança.
- VII. Não permitir ou colaborar com o acesso aos Recursos de TIC por parte de pessoas não autorizadas, sob pena de ser corresponsabilizado pelos eventuais problemas que esses acessos vierem a causar.
- VIII. Respeitar a integridade dos Recursos de TIC deste Centro.
- IX. Respeitar os direitos de propriedade intelectual, de acordo com a regulamentação pertinente, em particular a Lei de direitos autorais de software (Lei nº 9610 de 19 de fevereiro de 1998).
- X. Respeitar todas as obrigações contratuais e as limitações definidas nos contratos de software e outras licenças no uso dos Recursos de TIC.
- XI. Comunicar, através de email ou memorando, o setor de TIC deste centro qualquer evidência de violação das normas em vigor, não podendo acobertar, esconder ou ajudar a esconder violações de terceiros, de qualquer natureza.

**Artigo 9º** - No que concerne ao uso dos Recursos de TIC compartilhados, é vedado aos usuários:

- I. utilizar a identificação de outro usuário;
- II. enviar mensagens sem identificação do remetente;
- III. degradar o desempenho do sistema ou interferir no trabalho dos demais usuários;
- IV. fazer uso de falhas de configuração, falhas de segurança ou conhecimento de senhas especiais para alterar os Recursos de TIC;





**UNIVERSIDADE FEDERAL DO ESPÍRITO SANTO**  
**CENTRO UNIVERSITÁRIO NORTE DO ESPÍRITO SANTO**  
Conselho Departamental

V. fazer uso de meio eletrônico para enviar mensagens ofensivas, preconceituosas ou caluniosas.

VI. fazer-se passar por outra pessoa, ou esconder sua identidade, na utilização dos Recursos de TIC do CEUNES, com exceção dos casos em que o acesso anônimo é explicitamente permitido.

**Capítulo IV – Das senhas e contas individuais**

**Artigo 10** - Senhas são confidenciais, pessoais e intransferíveis. É de responsabilidade do usuário mantê-las como tal, observando os mecanismos de segurança e integridade.

**Artigo 11** - Ao manter e usar uma conta em sistema computacional do CEUNES, o usuário responsabiliza-se pela sua senha de acesso, obrigando-se a não revelá-la a terceiros, sejam pessoas vinculadas ao CEUNES ou não.

§1º - Excepcionalmente, a senha poderá ser repassada desde que seja assinado um termo de responsabilidade.

§2º - Caso a senha seja repassada sem adoção da medida prevista no parágrafo 1º, o titular da senha responderá pelo mau uso do sistema em qualquer circunstância, não podendo transferir responsabilidade a terceiros.

**Artigo 12** - São recomendações para as senhas individuais:

- I. Devem ser trocadas imediatamente após o primeiro uso;
- II. Devem ser trocadas periodicamente, num prazo não superior a 3(três) meses;
- III. Devem conter no mínimo seis caracteres.
- IV. Os usuários devem trocar suas senhas imediatamente após suspeitarem que foram violadas;
- V. Não repetir as 4 (quatro) últimas senhas utilizadas.

**Artigo 13** – O bloqueio das senhas ocorrerá nas seguintes situações:

- I. Após a 5ª tentativa de autenticação sem sucesso;
- II. Inatividade por mais de 90 (noventa) dias.

Parágrafo Único – O usuário que tiver sua senha bloqueada por qualquer motivo deverá solicitar formalmente ao setor de TIC do CEUNES o desbloqueio da sua senha.

**Artigo 14** - As chefias imediatas dos servidores e órgãos de recursos humanos, ao programar ou efetivar transferências ou desligamentos de servidores, deverão informar os fatos ao setor de TIC do CEUNES para que sejam providenciadas as reconfigurações ou remoção das contas e senhas individuais destes servidores.





**UNIVERSIDADE FEDERAL DO ESPÍRITO SANTO**  
**CENTRO UNIVERSITÁRIO NORTE DO ESPÍRITO SANTO**  
Conselho Departamental

**Capítulo V – Dos computadores**

**Artigo 15** - Os usuários dos computadores, conectados ou não à rede da Universidade, devem seguir normas de forma a minimizar os problemas com relação à perda de informação e comprometimento das atividades acadêmicas, científicas e administrativas da Universidade.

**Artigo 16** - Os usuários são responsáveis por todas as atividades nos computadores que estiverem utilizando. Portanto, devem agir de acordo com as regras e observar as seguintes normas:

- I. Sempre utilizar a sua identificação de usuário e senha para acesso aos computadores da Universidade;
- II. Responsabilizar-se pelo equipamento (hardware), mantendo-o nas suas perfeitas condições de uso, na forma como lhe foi entregue, independente do recebimento do termo de responsabilidade;
- III. Responsabilizar-se pelo software (sistema operacional, utilitários, aplicativos e arquivos) criado e/ou instalado nos computadores da Universidade;
- IV. Somente instalar software livre ou software licenciado pela Universidade, desde que esta instalação não prejudique o desempenho do equipamento ou da rede, e não comprometa a imagem da Universidade;
- V. Não remover os equipamentos dos locais onde foram instalados, exceto sob autorização da chefia imediata.
- VI. Manter o registro no serviço de patrimônio de todos os equipamentos de TI sob sua responsabilidade, sendo também sua responsabilidade informar qualquer alteração relativa à transferência desse patrimônio;

**Artigo 17** - É responsabilidade dos usuários dos computadores da Universidade:

- I. Fazer *backup* (cópia de segurança) dos seus arquivos pessoais instalados nos computadores sob a sua responsabilidade;
- II. Conhecer e respeitar o manual de boas práticas divulgado pelo setor de TIC do CEUNES.

**Artigo 18** - O usuário que obtiver a senha de administrador deverá manter o computador dentro dos padrões e procedimentos estabelecidos pelo setor de TIC deste centro.

§1º - Em eventual ocorrência de danos ao computador e à rede da Universidade devido ao mau uso da permissão de administrador (por exemplo através da





**UNIVERSIDADE FEDERAL DO ESPÍRITO SANTO**  
**CENTRO UNIVERSITÁRIO NORTE DO ESPÍRITO SANTO**  
**Conselho Departamental**

disseminação de vírus ou software mal intencionado), o usuário torna-se responsável por todas as consequências deste ato.

§2º - O setor de TIC não se responsabiliza pela recuperação de dados destes usuários em casos de reinstalação e configuração destes computadores.

§3º - É vedado o fornecimento destas senhas de administrador aos usuários dos computadores que armazenam dados corporativos do Centro, tais como Chefias, Coordenações, Secretarias e Direção.

**Capítulo VI – Da Rede de Computadores do CEUNES.**

**Artigo 19** – É vedado aos usuários da Rede de Computadores do CEUNES:

I. Interceptar ou tentar interceptar a transmissão de dados através da rede, exceto quando autorizado por escrito pela chefia imediata, com prévio conhecimento do setor de TIC.

II. Desenvolver, manter, usar ou divulgar meios que possibilitem a violação da segurança da rede da Universidade.

III. Adicionar equipamentos (hub, repetidor, switch, ponto de acesso sem fio, roteador, computador, estações de trabalho, modem, placas de rede, impressoras, dentre outros) na rede da Universidade sem prévio conhecimento e autorização da chefia do setor.

IV. Interferir no trabalho de outros usuários, provocando, por exemplo, congestionamento da rede, disseminação de vírus, tentar ou apropriar-se dos Recursos de TIC de outros usuários ou setores.

**Capítulo VII – Do nome ceunes.ufes.br**

**Artigo 20** - Nomes de domínios são formados por um conjunto de caracteres que mapeiam um ou mais endereços de rede IP. Estes nomes são usados para identificar sítios na Web e direcionar endereços de e-mail além de outras aplicações na Internet.

**Artigo 21** - A criação de nomes de domínios em "ceunes.ufes.br" será permitida somente nos seguintes casos:

I. Para os Departamentos, com o seguinte padrão de nomenclatura: [nome].ceunes.ufes.br.

II. Para eventos, convênios, projetos, grupos de pesquisa ou serviços institucionais que necessitam de visibilidade em função de seus objetivos, com o seguinte padrão de nomenclatura: [nome].ceunes.ufes.br.





**UNIVERSIDADE FEDERAL DO ESPÍRITO SANTO**  
**CENTRO UNIVERSITÁRIO NORTE DO ESPÍRITO SANTO**  
Conselho Departamental

**Artigo 22** - Para a criação de domínios de mensagens eletrônicas em "ceunes.ufes.br" fica definida a utilização das mesmas regras expostas no item acima, ou seja: [usuário]@[nome].ceunes.ufes.br.

**Capítulo VIII - Da gestão de software**

**Artigo 23** - O programa de computador ou software é propriedade intelectual, protegida por Lei federal nº 9.609, de 19 de fevereiro de 1998, que dispõe sobre a proteção da propriedade intelectual de programa de computador, e pela Lei federal nº 9.610, de 19 de fevereiro de 1998, que trata dos direitos autorais.

Parágrafo Único - A política de uso de software proprietário do CEUNES estabelece, fundamentada na Lei de Direitos Autorais e na Lei de Software, que nenhum membro de sua comunidade se envolva em qualquer atividade que viole leis federais, estaduais ou locais relacionadas à direitos de propriedade intelectual referentes a licenças de software ou qualquer outra política relacionada a software de computador ou conteúdos em formato digital.

**Artigo 24** - Copiar software para distribuição para outros usuários ou computadores, caso tal hipótese não seja contemplada na sua licença, é ilegal e viola as leis de software e de direitos autorais.

**Artigo 25** - Fica estabelecido que para utilizar qualquer software ou hardware de propriedade ou licenciado pelo CEUNES, os usuários:

- I. Devem concordar com todos os termos do acordo de licença de software;
- II. Devem estar cientes que todos os software são protegidos por direitos autorais, a menos que explicitamente rotulados como software livre ou de domínio público;
- III. Não podem copiar software para qualquer propósito com exceção daqueles permitidos no acordo de licença de utilização;
- IV. Não podem tornar o software disponível para outras pessoas usarem ou copiarem, se tal procedimento estiver em desacordo com os termos da licença de software e/ou procedimentos adotados pelo CEUNES;
- V. Não podem aceitar software não licenciado de terceiros;
- VI. Não podem instalar, nem permitir ou induzir outros a instalarem, cópias ilegais de software, ou software sem as devidas licenças, em qualquer recurso computacional de propriedade ou operado pelo CEUNES.

**Artigo 26** - Toda aquisição de equipamento computacional deve incluir necessariamente a aquisição de licenças do software básico mínimo apropriado para o seu uso funcionamento.





**UNIVERSIDADE FEDERAL DO ESPÍRITO SANTO**  
**CENTRO UNIVERSITÁRIO NORTE DO ESPÍRITO SANTO**  
Conselho Departamental

**Capítulo IX – Da Gestão de Software Corporativo.**

**Artigo 27** - É política deste Centro manter os dados corporativos integrados e íntegros através de todos os seus setores, permitindo que os seus administradores acessem as informações que necessitam, dentro de um ambiente controlado.

**Artigo 28** - A Universidade deverá prover meios de backup de forma a assegurar a integridade e segurança dos dados corporativos, sob custódia dos usuários de setores tais como direção, chefias de departamentos e setor, coordenações e suas respectivas secretarias.

**Artigo 29** - São responsabilidades dos usuários de dados corporativos:

- I. Acessar os dados conforme as suas atribuições;
- II. Garantir que os mecanismos de proteção física dos dados estão instalados e operando de forma satisfatória;
- III. Não divulgar dados sem a permissão da chefia do setor responsável pela custódia destes dados.

**Artigo 30** - A Universidade é proprietária de todos os seus dados corporativos e detém os direitos autorais de todas as políticas, manuais e compilações destes dados.

**Capítulo X – Do Correio Eletrônico.**

**Artigo 31** - Mensagens eletrônicas são consideradas de uso privativo e confidencial na forma permitida em lei.

**Artigo 32** - As mensagens eletrônicas somente serão acessadas com a permissão do remetente ou destinatário da mensagem ou dono, salvo por ordem judicial.

§1º - Havendo uma sindicância interna, por força de acusações de má conduta de algum usuário, mensagens podem ser copiadas pelos administradores para impedir a destruição ou perda de informações.

§2º - Compete aos Administradores analisar os conteúdos e emitir parecer técnico, caso seja obtida uma autorização legal para tal.

§3º - Compete aos Administradores rastrear o trajeto de mensagens eletrônicas consideradas ofensivas ou abusivas pela Instituição, afim de determinar o ponto de origem da qual foi enviada.

§4º - Os pedidos de rastreamento devem ser encaminhados à Comissão Permanente de Gestão da Política de Segurança da Informação e Comunicação, pela chefia do





**UNIVERSIDADE FEDERAL DO ESPÍRITO SANTO**  
**CENTRO UNIVERSITÁRIO NORTE DO ESPÍRITO SANTO**  
Conselho Departamental

setor, ao qual se encontra vinculado o destinatário da mensagem ofensiva ou abusiva.

**Artigo 33** - Os serviços de correio eletrônico são oferecidos como um recurso profissional para apoiar alunos, docentes e funcionários no cumprimento de seus objetivos nas áreas de educação, pesquisa, comunicação e serviços.

§1º - O uso pessoal é permitido e não priorizado, desde que não provoque efeitos negativos para qualquer outro usuário, não viole o sistema de mensagens, não interfira nas suas atividades ou viole qualquer outra lei ou norma vigente.

§2º - Cada usuário é responsável por utilizar os serviços de correio eletrônico de maneira profissional, ética e legal.

§3º - Material obtido de forma fraudulenta, racista, profana, obscena, intimidadora, difamatória, ilegal, ofensiva, abusiva ou inapropriada não pode ser enviado via correio eletrônico ou através de qualquer outra forma de comunicação eletrônica.

§4º - O CEUNES, de forma geral, não pode, e não tem por objetivo, ser o árbitro do conteúdo de mensagens eletrônicas.

**Artigo 34** - Os usuários de mensagens eletrônicas não devem dar a impressão que estão representando, dando opiniões ou fazendo declarações em nome do CEUNES a menos que autorizado, implícita ou explicitamente através de suas funções.

**Artigo 35** - Os usuários do correio eletrônico não devem falsificar sua identidade ou o seu nome de usuário ou alterar a origem da mensagem;

**Artigo 36** - A inconveniência e possível ameaça contida em mensagens indesejáveis, provenientes de fontes comerciais ou não, pode levar os Administradores a bloquear a recepção de mensagens provenientes de alguns domínios ou remetentes específicos.

**Artigo 37** - Os serviços de correio eletrônico podem ser utilizados para propósitos pessoais desde que, além do que está exposto neste Capítulo, tal uso:

I. Não interfira direta ou indiretamente nas operações dos recursos computacionais e serviços de correio eletrônico do CEUNES;

II. Não incorra em gastos adicionais para o CEUNES;

III. Não interfira nas suas obrigações internas e externas no CEUNES;

IV. Não interfira na produtividade das atividades funcionais do CEUNES.

V. Não tenha propósitos comerciais, exceto à serviço autorizado ou institucional.

**Artigo 38** - É vedada a utilização do serviço Correio Eletrônico no CEUNES nas seguintes situações:







**UNIVERSIDADE FEDERAL DO ESPÍRITO SANTO**  
**CENTRO UNIVERSITÁRIO NORTE DO ESPÍRITO SANTO**  
**Conselho Departamental**

- I. Envio de mensagens não autorizadas divulgando informações sigilosas e/ou de propriedade exclusiva do CEUNES;
- II. Acesso à caixa postal eletrônica (e-mail) de outro usuário;
- III. Envio de correntes e/ou spam;
- IV. Envio intencional de mensagens contendo vírus ou qualquer outras formas de rotinas de programação de computador que sejam danosas ao bom funcionamento dos recursos de TIC do CEUNES;
- V. Uso do serviço de correio eletrônico de forma a afetar negativamente a imagem do CEUNES.

**Capítulo XI – Do Sítio Web e Intranet**

**Artigo 39** - O Portal do CEUNES é um repositório de informações sobre o centro, disponibilizadas para a comunidade universitária e para o público em geral. O Portal foi projetado para promover a publicação periódica de estudos, trabalhos, eventos e informações institucionais de forma geral. Também tem a finalidade de servir como veículo de apresentação da comunidade universitária e seus recursos.

**Artigo 40** - O CEUNES reconhece o escopo e a importância da tecnologia Web na disseminação das informações internas e externas e está comprometido com o desenvolvimento e com o suporte ao conteúdo de qualidade através dos servidores Web.

**Artigo 41** - O CEUNES reconhece a importância e a utilidade de publicações eletrônicas através da Internet, principalmente as páginas pessoais, que podem prover informações relevantes sobre o papel de cada indivíduo dentro da Universidade.

§1º - Considerando que as páginas pessoais são documentos públicos disponíveis para qualquer pessoa em qualquer lugar, torna-se necessário o estabelecimento de critérios para a elaboração das mesmas, visto que, mesmo sendo de caráter pessoal, as informações colocadas nos servidores Web da CEUNES podem influir na formação de sua imagem e reputação frente à comunidade.

§2º - Dado o elevado número de páginas pessoais e a dinâmica inerente à criação e publicação destas páginas, o CEUNES considera inviável a revisão das informações publicadas eletronicamente por seus membros - professores, funcionários e alunos - e descarta esta prática.

§3º - Os autores de páginas pessoais assumem toda a responsabilidade pelo conteúdo de suas páginas e devem estar cientes das responsabilidades e consequências inerentes a estas publicações, prevalecendo a assinatura colhida por ocasião da abertura da conta.





**UNIVERSIDADE FEDERAL DO ESPÍRITO SANTO**  
**CENTRO UNIVERSITÁRIO NORTE DO ESPÍRITO SANTO**  
**Conselho Departamental**

**Artigo 42** - Este Capítulo estabelece as seguintes regras básicas para as páginas pessoais residentes em servidores da CEUNES:

I. Páginas pessoais devem ser elaboradas considerando as portarias, normas e regulamentos do CEUNES, regulamentações externas e a legislação vigente.

II. O conteúdo das páginas deve refletir o papel de seu autor, os interesses e os padrões correntes no CEUNES e não deve constituir material questionável sob os aspectos legais, éticos e morais.

III. É proibida a inclusão e a criação de referências a:

- a) material com conteúdo comercial de caráter publicitário;
- b) empresas ou entidades externas com objetivos comerciais;
- c) material calunioso ou difamatório;
- d) material que infrinja a legislação sobre direitos autorais;
- e) material ofensivo ou que faça uso de linguagem ofensiva;
- f) material que incite a qualquer tipo de discriminação;
- g) material que incite à violência;
- h) material pornográfico de qualquer natureza;
- i) imagens ou dados que possam ser considerados abusivos, profanos, incômodos;
- j) ameaçadores ou sexualmente ofensivos a uma pessoa comum, considerados os padrões éticos e morais correntes na comunidade.

IV. Os autores devem assumir explicitamente toda a responsabilidade pela informação contida em suas páginas pessoais.

Parágrafo único - Eventuais ocorrências não previstas neste documento serão analisadas pelos órgãos competentes do CEUNES.

### **Capítulo XII – Do acesso à Internet.**

**Artigo 43** - O CEUNES deverá possuir mecanismos de autenticação, que determinam a titularidade de todos os acessos à Internet feitos por seus usuários.

**Artigo 44** - O usuário é responsável por todas as atividades realizadas por intermédio de sua conta de usuário e senhas de acesso.

**Artigo 45** - Os usuários poderão fazer download de arquivos da Internet que sejam necessários ao desempenho de suas atividades desde que seja observado os termos de licença de uso e registro, quando necessário.

**Artigo 46** – Os usuários devem observar as seguintes recomendações:

I. Utilizar a Internet de forma adequada e diligente;





**UNIVERSIDADE FEDERAL DO ESPÍRITO SANTO**  
**CENTRO UNIVERSITÁRIO NORTE DO ESPÍRITO SANTO**  
**Conselho Departamental**

II. Utilizar a Internet observando a conformidade com a lei, a moral, os bons costumes aceitos e a ordem pública;

**Artigo 47** – É vetado aos usuários dos computadores e da rede do CEUNES:

I. Utilizar a Internet com objetivos ou meios para a prática de atos ilícitos, proibidos pela lei ou pela presente Norma, lesivos aos direitos e interesses da Universidade ou de terceiros.

II. Utilizar a Internet com objetivo de danificar, inutilizar, sobrecarregar ou deteriorar os Recursos de TIC e dados de qualquer tipo, de uso corporativo, pessoal ou de terceiros.

III. Utilizar software de compartilhamento de arquivos do tipo Peer-to-Peer (P2P), tais como Kazaa, E-mule, BitTorrent e afins;

Parágrafo único - A utilização destes software para fins de pesquisa será permitida mediante projeto específico, registrado e aprovado nos departamentos e conselhos superiores deste centro. O setor de TIC deste centro poderá ser consultado e deverá ser informado destes projetos.

IV. Acesso a sites de Proxy com o objetivo de burlar os mecanismos de segurança existentes;

V. Acesso a sites de pornografia, pedofilia e outros contrários à lei. O acesso à esses sites é terminantemente proibido, ainda que os mesmos não estejam sendo bloqueados no sistema de segurança do CEUNES.

**Artigo 48** - O CEUNES se reserva ao direito de monitorar automaticamente todo o tráfego efetuado através das suas redes de comunicação, incluindo o acesso à Internet e o uso do Correio Eletrônico, afim de evitar qualquer violação, ou suspeita de violação, dessas normas e preservar a integridade e segurança dos Recursos de TIC do centro.

**Artigo 49** - A não observância de qualquer item acima implicará nas sanções previstas nesta norma.

**Capítulo XIII – Dos Laboratórios.**

**Artigo 50** - É dever dos usuários e coordenadores dos laboratórios deste centro seguirem as normas estabelecidas nesta Política de Segurança da Informação.

**Artigo 51** - Os Laboratórios deverão possuir um Coordenador, que será responsável por estabelecer os softwares e serviços que poderão instalados e utilizados em suas dependências e as normas de utilização dos recursos de TIC do laboratório.





UNIVERSIDADE FEDERAL DO ESPÍRITO SANTO  
CENTRO UNIVERSITÁRIO NORTE DO ESPÍRITO SANTO  
Conselho Departamental

Parágrafo único – Os Laboratórios de Informática poderão ter normas de acesso mais restritivas, incluindo bloqueio e restrições de acesso.

**Capítulo XIV – Do acesso externo à Intranet.**

**Artigo 52** - Por serviços de acesso remoto entende-se qualquer serviço disponibilizado para o acesso aos serviços da rede local do CEUNES a partir de um computador remoto, englobando desde o software cliente usuário, o qual faz conexão com os computadores da Universidade, até os servidores de VPN, SSH, FTP e assemelhados.

**Artigo 53** - São requisitos fundamentais para utilização do Serviço de Acesso Remoto:

- I. Ser aluno, devidamente autorizado por um professor responsável, ou servidor ativo deste centro, devidamente autorizado pelo seu superior hierárquico;
- II. Possuir um projeto de ensino, pesquisa ou extensão aprovado nas instâncias superiores deste centro;
- III. Cadastrar nome de usuário e senha junto ao TIC ou coordenador do laboratório que receberá o acesso externo deste usuário;
- IV. Efetuar a configuração da máquina cliente de acesso conforme instruções do TIC, e de acordo com as normas previstas neste documento.

**Artigo 54** - Para utilização dos serviços de acesso remoto do CEUNES é necessário submeter-se às normas gerais estabelecidos nesta política de segurança da informação, bem como nas normas da Universidade.

**Artigo 55** - O Coordenador do projeto ou laboratório que solicitou o acesso remoto torna-se corresponsável por toda ocorrência relacionada ao mal uso do Serviço de Acesso Remoto, em consequência da concessão do acesso.

**Artigo 56** - É vedado aos usuários do Serviço de Acesso Remoto:

- I. Usar a conexão de acesso remoto para fins de compartilhamento de arquivos tipo P2P ("peer-to-peer"), transmissão de e-mails não solicitados ou de propaganda ("spam"), transmissão de softwares mal-intencionados (vírus, "trojans", "worms", "spywares" e assemelhados), acesso a pornografia ou conteúdo considerado ilegal pela legislação vigente, download de softwares ou arquivos sem licença do proprietário (pirata) e ocultação da própria identidade ("Proxy").
- II. Usar a conexão para qualquer outra finalidade não autorizada;





**UNIVERSIDADE FEDERAL DO ESPÍRITO SANTO**  
**CENTRO UNIVERSITÁRIO NORTE DO ESPÍRITO SANTO**  
**Conselho Departamental**

III. Compartilhar o acesso à rede do CEUNES com usuários não autorizados, por qualquer meio, inclusive através de compartilhamento por meio físico, ou através da divulgação de nome de usuário e senha.

### **Capítulo XV – Das Penalidades**

**Artigo 57** - As penalidades a serem aplicadas às condutas elencadas nesta norma, sem prejuízo de outras penas previstas em lei ou em normas da Universidade, são: restrição ou eliminação temporária ou permanente, de privilégios de acesso, tanto aos recursos computacionais, quanto às redes, computadores do CEUNES e outros serviços ou facilidades.

§ 1º - A infração ou tentativa de infração das regras constantes desta norma ou das regras previstas em lei serão apuradas por meio de sindicância administrativa, processo administrativo disciplinar ou processo sumário, nos termos da Lei 8.112/90 e Regimento Geral da UFES, assegurado em todos os casos o contraditório e a ampla defesa.

§ 2º - Sempre que julgar necessário, para a preservação da integridade dos recursos computacionais do CEUNES, dos serviços aos usuários ou dos dados, o Gestor de Segurança da Informação poderá suspender temporariamente qualquer conta, seja o responsável pela conta suspeito de alguma violação, ou não.

§ 3º - Esta Norma se aplica a qualquer membro da comunidade universitária, quer ele esteja dentro do CEUNES ou fora deste, e se refere a todos os recursos computacionais, controlados individualmente ou compartilhados, isolados ou em rede.

### **Capítulo XVI – Das Competências.**

**Artigo 58** – Cabe ao Gestor de Segurança da Informação e Comunicações:

- I. Encaminhar a Política de Segurança da Informação e suas revisões para aprovação no Conselho Departamental do CEUNES;
- II. Informar ao Conselho Departamental do CEUNES dos casos de descumprimento da Política e/ou de suas Normas encaminhados pela Comissão Permanente de Gestão da Política de Segurança da Informação e Comunicação.

**Artigo 59** – Cabe à Comissão Permanente de Gestão da Política de Segurança da Informação e Comunicação:

- I. Propor ajustes, aprimoramentos e modificações desta Política;
- II. Analisar os casos de violação desta Política e das Normas de Segurança da Informação, encaminhando-os ao Gestor de segurança da Informação quando for o caso;





**UNIVERSIDADE FEDERAL DO ESPÍRITO SANTO**  
**CENTRO UNIVERSITÁRIO NORTE DO ESPÍRITO SANTO**  
**Conselho Departamental**

III. Propor projetos e iniciativas relacionados à melhoria da segurança da informação do CEUNES;

IV. Propor o planejamento e a alocação de recursos financeiros, humanos e de tecnologia, no que tange à segurança da informação;

V. Determinar a elaboração de relatórios, levantamentos e análises que dêem suporte à gestão de segurança da informação e à tomada de decisão;

VI. Acompanhar o andamento dos principais projetos e iniciativas relacionados à segurança da informação;

Parágrafo único: a Comissão Permanente de Gestão da Política de Segurança da Informação e Comunicação deverá ser nomeada pela direção do CEUNES em portaria específica para tal finalidade.

**Artigo 60 – Cabe aos Administradores:**

I. Prover todas as informações de segurança da informação solicitadas pela Comissão Permanente de Gestão da Política de Segurança da Informação e Comunicação;

II. Prover ampla divulgação da Política e das Normas de Segurança da Informação em todo o Campus do CEUNES;

III. Oferecer orientação e treinamento sobre a Política de Segurança da Informação e suas Normas a todos os servidores e colaboradores do CEUNES;

IV. Propor projetos e iniciativas relacionados ao aperfeiçoamento da segurança da informação do CEUNES, mantendo-se atualizada em relação às melhores práticas existentes no mercado e em relação às tecnologias disponíveis;

V. Estabelecer procedimentos e realizar a gestão dos sistemas de controle de acesso do CEUNES, incluindo os processos de concessão, manutenção, revisão e suspensão de acessos aos usuários;

VI. Analisar os dados relacionados à segurança da informação do CEUNES e apresentar relatórios periódicos sobre tais riscos ao Comitê, acompanhados de proposta de aperfeiçoamento do ambiente de controle do Centro, quando for o caso;

VII. Realizar trabalhos de análise de vulnerabilidade, com o intuito de aferir o nível de segurança dos sistemas de informação e dos demais ambientes em que circulam as informações do CEUNES;

VIII. Realizar testes e averiguações em sistemas e equipamentos, com o intuito de verificar o cumprimento da Política e das Normas de Segurança da Informação;

IX. Estabelecer mecanismo de registro e controle de não-conformidade a esta Política e às Normas de Segurança da Informação, comunicando ao CGSI.

Parágrafo único: a Equipe de Administradores deverá ser composta por membros do setor de TIC deste centro.





**UNIVERSIDADE FEDERAL DO ESPÍRITO SANTO**  
**CENTRO UNIVERSITÁRIO NORTE DO ESPÍRITO SANTO**  
Conselho Departamental

**Capítulo XVII – Referências Legais e Normativas**

- I. Constituição da República Federativa do Brasil de 1988.
- II. Lei nº. 8.112, de 11 de dezembro de 1990. - Dispõe sobre o Regime Jurídico dos Servidores Públicos Civis da União, das Autarquias e das Fundações Públicas Federais.
- III. DECRETO 1.171/94 – Código de Ética dos Servidores Públicos Federais.
- IV. Lei nº. 7.232, de 29 de outubro de 1984. Dispõe sobre a Política Nacional de Informática, e dá outras providências.
- V. Lei nº. 8.248, de 23 de outubro de 1991. Dispõe sobre a capacitação e competitividade do setor de informática e automação, e dá outras providências.
- VI. Lei nº. 9.296, de 24 de julho de 1996. Regulamenta o inciso XII, parte final, do art. 5º da Constituição Federal que dispõe sobre a violação do sigilo de dados e das comunicações telefônicas.
- VII. Lei nº. 9.472, de 16 de julho de 1997. Dispõe sobre a organização dos serviços de telecomunicações, a criação e funcionamento de um órgão regulador e outros aspectos institucionais.
- VIII. Lei nº. 9.507, de 12 de novembro de 1997. Regula o direito de acesso a informações e disciplina o rito processual do habeas data.
- IX. Lei nº. 9.609, de 19 de fevereiro de 1998. Dispõe sobre a proteção de propriedade intelectual de programa de computador, sua comercialização no país, e dá outras providências.
- X. Lei nº. 10.973, de 02 de dezembro de 2004. Dispõe sobre incentivos à inovação e à pesquisa científica e tecnológica no ambiente produtivo e dá outras providências.
- XI. Lei nº. 11.111, de 05 de maio de 2005. Regula o direito à informação e ao acesso aos registros públicos.
- XII. Decreto nº. 2.295, 04 de agosto de 1997. Regulamenta o disposto no art. 24, inciso IX, da Lei nº. 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional. Neste caso o processo deverá ser sigiloso, excetuando-se a publicidade das compras governamentais.
- XIII. Decreto nº. 2.556, de 20 de abril de 1998. Regulamenta o registro previsto no art. 3º da Lei nº. 9.609, de 19 de fevereiro de 1998, que dispõe sobre a propriedade intelectual de programa de computador, sua comercialização no país, e dá outras providências.
- XIV. Decreto nº. 3.505, de 13 de junho de 2000. Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal.
- XV. Decreto nº. 3.996, de 31 de outubro de 2001. Dispõe sobre a prestação de serviços de certificação digital no âmbito da Administração Pública Federal.





**UNIVERSIDADE FEDERAL DO ESPÍRITO SANTO**  
**CENTRO UNIVERSITÁRIO NORTE DO ESPÍRITO SANTO**  
**Conselho Departamental**

XVI. Decreto nº. 4.073, de 03 de janeiro de 2002. Regulamenta a Lei nº. 8.159, de 08 de janeiro de 1991, que dispõe sobre a política nacional de arquivos públicos e privados.

XVII. Decreto nº. 4.829, de 03 de setembro de 2003. Dispõe sobre a criação do Comitê Gestor da Internet no Brasil – CGIbr, sobre o modelo de governança da Internet no Brasil, e dá outras providências.

XVIII. Decreto nº. 5.450, de 31 de maio de 2005. Regulamenta o pregão, na forma eletrônica, para aquisição de bens e serviços comuns, e dá outras providências.

XIX. Resolução nº. 58 do INPI, de 14 de julho de 1998. Estabelece normas e procedimentos relativos ao registro de programas de computador.

Sala das Sessões, 24 de agosto de 2011.

  
**MARCELO SUZART DE ALMEIDA**  
**Presidente**