UNIVERSIDADE FEDERAL DE ALAGOAS - UFAL

INSTITUTO DE COMPUTAÇÃO - IC/UFAL

COMPILADORES

MEER - COMPILER

UNIVERSIDADE FEDERAL DE ALAGOAS - UFAL

INSTITUTO DE COMPUTAÇÃO - IC/UFAL

COMPILADORES

MEER - COMPILER

Trabalho solicitado pelo professor Dr. **Alcino Dall'Igna Júnior**, para avaliação e composição da primeira parte da nota, feito pelos alunos Vitor Barcelos de Cerqueira e Pedro Mateus Veras, alunos do Instituto de Computação da Universidade Federal de Alagoas.

SUMÁRIO

1. Introdução 4
2. [Diretrizes gerais 5](#_30j0zll)
3. [Câmara de Segurança da Informação 5](#_1fob9te)
4. [Competências da Gerência de TI na Política de Segurança Interna 6](#_3znysh7)
5. [Competências da Gerência Geral na Política de Segurança Interna 6](#_2et92p0)
6. [Direitos e deveres dos usuários 7](#_tyjcwt)
7. Normas quanto ao uso da internet 7
8. [Normas para a utilização do Correio Eletrônico (email) 8](#_3dy6vkm)
9. [Normas para armazenamento de arquivos 9](#_1t3h5sf)
10. [Normas para segurança física e do ambiente 9](#_4d34og8)
11. [Gerenciamento das operações e comunicações 10](#_2s8eyo1)

# Introdução

A informação é o bem mais valioso de uma empresa. Os dados podem estar dispostos em quaisquer tipos de mídia, tais como documentos armazenados em discos físicos, como pen drives, HDs, SSD; por meios digitais, armazenados em servidores e em sistemas operacionais dos computadores; compartilhadas através de conversas por partes da organização etc.

A segurança da informação é obtida através da implementação de medidas que buscam proteger os dados de uma organização, com um conjunto de regras, protocolos e políticas internas que devem ser seguidos à risca pela administração e os diferentes tipos de funcionários que estão presentes na organização. Esses controles devem ser monitorados e analisados, em prol do aperfeiçoamento e melhora da segurança dos dados, para que a organização mantenha os seus dados seguros.

Devido ao crescimento e desenvolvimento exponencial de sistemas de internet, proporcionalmente cresceu também a preocupação com a segurança dos dados e informações que nela se encontram. Logo, faz-se necessário o uso de políticas para o seu uso.

Sabe-se que os sistemas de informação estão dispostos para 100 (cem) funcionários e, além disso, há (5) cinco laboratórios de Ensino com 30 (trinta) computadores cada. Há também 7 (sete) laboratórios de pesquisa, com 10 (dez) computadores cada. Há 20 (vinte) salas de professores, com 2 (dois) computadores em cada sala. Há 7 (sete) salas para a administração, com 1 (um) computador em cada sala. Além disso, há 1 (um) computador em cada sala de aula, junto com 1 (um) datashow, totalizando 20 (vinte) salas de aula. Sabe-se também que os computadores da área administrativa, dos laboratórios, salas de aula e salas de professores estão interligados, através de cabeamento estruturado a um switch de grande porte, que, por sua vez, está interligado a um roteador de saída, que permite acesso a internet e que possui um firewall configurado.

Assim, entende-se que tanto os sistemas de informação quanto às redes de computadores da instituição estão sujeitos, durante os três períodos do dia, a ameaças à segurança da informação, tais como fraudes eletrônicas, sabotagem dos equipamentos, vandalismo, incêndio, roubo dos dados de pesquisa etc. Danos causados por vírus nos sistemas e outras práticas que são bem comuns em ambientes digitais.

Dessa forma, esse documento estabelece as diretrizes para a Segurança da Informação, visando preservar a integridade, a confidencialidade e a disponibilidade dos ativos de informação da instituição, sendo o compromisso com o seu cumprimento de responsabilidade de todos os seus colaboradores, incluindo os professores, recepcionistas, administradores do sistema, estagiários, terceirizados, prestadores de serviço ou quaisquer outros que tenham acesso a qualquer tipo de Tecnologia da Informação e Comunicação presente no ambiente da instituição.

# Diretrizes gerais

* 1. É dever de todos os usuários a garantia do sigilo das informações imprescindíveis à segurança da sociedade e do Estado e a inviolabilidade da intimidade da vida privada, da honra e da imagem das pessoas.
  2. Os usuários internos e externos devem observar que:
     1. O acesso à informação será regulamentado por normas específicas de tratamento da informação. Toda e qualquer informação produzida, adquirida, utilizada ou armazenada pela instituição faz parte de seu patrimônio e deve ser protegida;
     2. Os recursos disponibilizados pela instituição são fornecidos com o único propósito de garantir o desempenho das suas atividades;
     3. As normas para as operações de armazenamento, divulgação, reprodução, recuperação e destruição da informação serão estabelecidas em conformidade com a sua classificação, sem prejuízo de outros cuidados que forem especificados pelo gestor.
  3. Será estabelecido um serviço de gestão de incidentes, que vai receber, filtrar, classificar e responder às solicitações e alertas e fazer análises dos incidentes de segurança, buscando retirar informações que possibilitem o impedimento da ação maliciosa e a identificação de tendências.
  4. Juntamente à gestão de incidentes, também será feito um processo de gestão de riscos a ser aplicado na implementação e operação da Gestão de Segurança da Informação. Os riscos devem ser monitorados e analisados com periodicidade, objetivando averiguar mudanças em critérios de avaliação e aceitação dos riscos, tanto no ambiente, quanto nos ativos de informação e fatores de riscos. Os serviços de gestão de incidentes, gestão de riscos e gestão de segurança da informação são competências da Gerência de TI da instituição.
  5. As informações, os sistemas e métodos idealizados pelos servidores da instituição constituem seu patrimônio intelectual, o que implica que os criadores não possuem direito autoral, exceto em casos regulamentados pela área competente.
  6. Todos os colaboradores, servidores e prestadores de serviço devem assinar o Termo de Responsabilidade e Sigilo, documento oficial que os compromete com a Política de Segurança da Informação da instituição.
  7. Este documento deve ser verificado anualmente, estando a verificação de conformidade da política, acordos, contratos e convênios estabelecidos sob a responsabilidade da Gerência de TI.
  8. Esta política entra em vigor a partir de sua data de publicação.

# Câmara de Segurança da Informação

A Câmara de Segurança da Informação será formada por:

* 1. Gerente de TI - Gerencia e coordena as atividades do Depto. de TI da instituição;
  2. Gerente Geral - Gerencia e coordena as ações do Depto. Administrativo da instituição;
  3. Gerente de Gestão Estratégica de Pessoas.

A Câmara compreende as competências para:

* 1. Avaliar os assuntos relativos a PSI e a elaboração de relatórios periódicos de Segurança;
  2. Assessorar, implementar e promover políticas e ações da segurança da informação;
  3. Propor alterações na PSI;
  4. Propor normas internas relativas à segurança da informação.

# Competências da Gerência de TI na Política de Segurança Interna

Caberá ao Gerente de TI a gestão de segurança da informação da Instituição de Ensino. Compete ao Gerente de TI:

* 1. A solicitação de recursos para a implementação das ações de segurança da informação;
  2. Promover a capacitação por meio de treinamento e seminários para os Recursos Humanos, que são relacionados à segurança da informação;
  3. Coordenar e executar as ações de segurança da instituição;
  4. Implementar a equipe de tratamento e instituir respostas para os incidentes em redes ou computadores;
  5. Recomendar a aplicação das ações corretivas cabíveis nos casos de violação do protocolo de segurança da informação.

Caberá ao Departamento de Tecnologia da Informação:

* 1. Credenciar e descredenciar os logins e senhas dos diferentes tipos de usuários (Gerência, administração, professor, professor pesquisador, professor visitante, alunos, alunos pesquisadores, terceirizados e estagiários) mediante a solicitação do gestor da área e o descredenciamento através de solicitação do gestor de RH;
  2. As definições dos diferentes tipos de usuário ou usuário privilegiado, cujos privilégios sejam compatíveis com as atividades do usuário;
     1. Após a definição do perfil, cabe ao gerente de TI indicar os privilégios que poderão acessar os diferentes níveis das pastas compartilhadas da área, bem como leitura, gravação, inserção dos diferentes tipos de arquivos, acesso, compartilhamento e destruição dos dados.
     2. Os usuários não terão contas com perfil administrador, nem contas com privilégio de administrador local da estação, exceto àqueles cuja atividade funcional necessita.
  3. A instalação de todos os softwares nos equipamentos da instituição;
  4. A desinstalação de quaisquer softwares considerados nocivos à integridade da rede;
  5. A realização de diagnósticos para checagem de segurança por meio dos relatórios emitidos pela gerência de TI;
  6. A instalação de novos equipamentos e substituição de equipamentos defeituosos;
  7. Atualizações dos sistemas internos da instituição;
  8. A instalação, monitoramento e manutenção da rede de computadores da instituição;
  9. Executar as atualizações do plano de segurança da instituição;
  10. Monitorar a integridade dos dados da instituição, por meio de softwares de segurança;
  11. Realizar a chipagem nos equipamentos físicos da instituição para fins de controle interno;
  12. Proteger as instalações de infraestrutura, recursos tecnológicos, sistemas de informação e aplicações da instituição devem ser protegidos contra indisponibilidade, acessos indevidos, alterações, falhas, perdas, roubos, furtos e interrupções não programadas.

# Competências da Gerência Geral na Política de Segurança Interna

Caberá ao Gerente Geral a gestão dos processos administrativos para a Política de Segurança Interna da Instituição de Ensino.

Compete ao Gerente Geral:

* 1. Monitorar os ambientes de trabalho, pesquisa, desenvolvimento e administração da instituição;
     1. Monitorar as atividades de Segurança Física da Instituição, definindo as pessoas que têm acesso às chaves para o acesso de laboratórios de pesquisa, salas de ensino, salas de professores, inventários, acessos restritos aos funcionários.
        1. Solicitar o ID de credenciamento na instituição e documento de identificação comprobatório para o acesso a determinado ambiente. O acesso ao ambiente somente será concedido caso aquela pessoa possua vínculo de atividade privilegiada no sistema.
  2. Chefiar as atividades administrativas da instituição, mediando as autorizações e atualizações de cadastros e descadastros dos funcionários com o Gerente de TI.
  3. Garantir a integridade física da Instituição, tais como os equipamentos eletrônicos de cada ambiente que possua Tecnologias da Informação e Comunicação da Instituição;
  4. Solicitar ao Gerente de TI a implantação de Políticas de Segurança Interna para ambientes que possuam Tecnologias da Informação e Comunicação da Instituição;
  5. Checar as decisões tomadas pelo corpo administrativo, tais como cadastro e recadastro de usuários e gerar relatórios informativos para o Gerente de TI;
  6. Instituir seminários para equipe geral, junto com o Gerente de TI, para o ensino das políticas de Segurança da Informação da Instituição;
  7. Instituir meios físicos de segurança para o acesso aos laboratórios, salas de professores e salas gerais
     1. Solicitar ao Gerente de TI o credenciamento de digitais de acesso de pessoas privilegiadas para o ambiente que necessita de validação por meio de trancas digitais ou senhas.
  8. Solicitar o cadastro do corpo administrativo da instituição ao Gerente de TI
     1. Encaminhar as solicitações de cadastro e descadastro do usuário de um determinado setor administrativo da empresa;
  9. Orientar aos alunos da Instituição sobre a integridade física dos setores que possuem Tecnologias da Informação e Comunicação
     1. Proibir o acesso com alimentos aos laboratórios e salas de aula que possuem equipamentos eletrônicos;
  10. Promover a segurança do fornecimento de energia da instituição;
  11. Promover a segurança dos cabeamentos de rede que estão conectando todos os computadores;
  12. Promover a segurança dos setores que possuem a estrutura física para o funcionamento das Tecnologias da Informação e Comunicação da Instituição e
  13. Checar, junto ao Gerente de TI, se a instituição está dentro dos padrões de segurança.

# Direitos e deveres dos usuários

Esta norma busca direcionar as boas práticas para o uso das Tecnologias da Informação e Comunicação para todos os usuários da Instituição.

* 1. É terminantemente proibida a instalação de softwares sem a permissão do Departamento de TI;
  2. É permitida ao usuário a atualização da versão de softwares previamente instalados pelo Departamento de TI;
  3. É de responsabilidade do usuário realizar o correto acionamento e desligamento dos equipamentos de informática aos quais possua acesso (em salas de aula e/ou laboratórios) no período em que estiver nesses espaços;
  4. É terminantemente proibido remanejar e/ou remover quaisquer equipamentos de informática, bem como manipular equipamentos de rede (switches, hubs, fiação, cabeamento de rede, etc) sem aviso prévio e aprovação do Departamento de TI;
  5. Quaisquer solicitações referentes a software e/ou hardware deverão ser encaminhadas pelo para o Departamento de TI através de um documento oficializando a demanda, onde devem estar descrita a necessidade e os objetivos esperados com a aquisição;
  6. É expressamente proibido ao usuário o acesso ou manutenção no interior do gabinete de um computador, assim como troca ou retirada de seus componentes, cabendo a demanda ser solucionada apenas pelo Departamento de TI e/ou servidores devidamente autorizados pelo referido departamento;
  7. Caso o usuário identifique irregularidades, vulnerabilidades e/ou incidentes de segurança que venham impactar os serviços disponibilizados pela instituição, deverá comunicar imediatamente ao Gerente de TI;

1. Normas quanto ao uso da internet

Esta norma pretende estabelecer responsabilidade e requisitos básicos de utilização da internet na instituição de ensino. A internet deve ser usada com o intuito de complementar as atividades relativas ao ensino, pesquisa e extensão, bem como as atividades realizadas por servidores das mais diversas áreas, com o fito de corroborar para o enriquecimento intelectual de seus servidores e como ferramenta para busca de informações para o desenvolvimento de seus trabalhos. Com base nos procedimentos de proteção e integridade dos sistemas de informação, a internet é classificada como conexão de alto risco. Todo o corpo discente, docente e os servidores da instituição devem estar cientes da periculosidade da navegação na internet antes de acessá-la e usufruir de seus recursos. Tendo em vista que o uso da internet é fundamental para as atividades desenvolvidas na instituição e observando-a como ferramenta que possibilita ameaças às informações da instituição, é de extrema importância que seja estabelecido um conjunto de regras para a utilização adequada desse recurso.

* 1. Todos os usuários que utilizarem esse serviço deverão fazê-lo no estrito interesse do órgão, mantendo uma conduta profissional, principalmente quando se diz respeito à utilização de bem público;
  2. O acesso à internet por todos os usuários que estejam sob o domínio da instituição que fazem usufruto de seus equipamentos deve ser feito exclusivamente através da única ligação existente entre a internet e o Conselho, sendo proibido o acesso utilizando provedores privados;
  3. É expressamente proibida a divulgação e/ou compartilhamento indevido de informações sigilosas em listas de transmissão ou bate-papo de qualquer natureza.

# Normas para a utilização do Correio Eletrônico (email)

Este tópico tem a finalidade de estabelecer responsabilidades e requisitos básicos para o uso de serviços de correio eletrônico no ambiente da instituição de ensino. Emails são uma eficiente forma de comunicação, outrossim, também são uma fonte de vulnerabilidade para informações organizacionais. Essa norma é aplicável para todos os usuários que possuam vínculo com a instituição.

* 1. Todos os tipos de usuários filiados à instituição (Gerência, administração, professor, professor pesquisador, professor visitante, alunos, alunos pesquisadores, terceirizados e estagiários) terão um email institucional pessoal e intransferível com acesso exclusivo utilizando senha;
  2. Os emails institucionais serão criados preferencialmente no formato [nome.sobrenome@sigladainstituicao.br](mailto:nome.sobrenome@sigladainstituicao.br);
  3. O acesso às mensagens são de exclusividade do usuário dono do endereço eletrônico, sendo garantida a ele a inviolabilidade do conteúdo de suas mensagens eletrônicas, no entanto, todas as mensagens podem ser monitoradas e sujeitas à auditoria;
  4. As auditorias serão solicitadas pela Gerência Geral e realizadas pelo Departamento de TI;
  5. É terminantemente proibido o uso do email para propaganda política, financeira, religiosa ou de qualquer outra natureza;
  6. É terminantemente proibido o uso do email para propagação (envio e/ou recebimento) de material pornográfico, político e/ou financeiro, bem como discursos de ódio racial, religioso, de gênero e quaisquer tipos de material que desrespeitem os direitos humanos; caso haja alguma ocorrência dessa natureza, uma denúncia referente ao caso deverá ser encaminhada para os Recursos Humanos para que sejam tomadas as providências legais cabíveis.
  7. É expressamente proibida a abertura de anexos com as extensões .bat, .exe, .src, .lnk e .com, ou de quaisquer outros formados previamente alertados sem o conhecimento prévio do Departamento de TI.

# Normas para armazenamento de arquivos

* 1. Fica vetado o uso dos computadores da instituição para armazenamento de materiais pessoais de qualquer espécie, devendo o servidor ater-se a utilizar os dispositivos disponibilizados para atividades estritamente profissionais.
  2. Fica proibido o armazenamento de vírus, material ilegal, pornográfico, que viole a privacidade de alguém ou que desrespeite os direitos humanos.
  3. Os servidores devem estar cientes de que todo arquivo armazenado nos computadores e dispositivos da instituição pode ser alvo de auditoria, se a gerência de TI assim julgar necessário.
  4. O funcionário que for pego descumprindo as normas de armazenamento aqui presentes está sujeito às medidas legais cabíveis previstas no termo de responsabilidade e sigilo.

# Normas para segurança física e do ambiente

* 1. A instituição deve garantir os mecanismos de proteção às dependências onde se localizam dados críticos ou sensíveis, de forma a prevenir acesso indevido, interferência ou dano.
  2. Deve ser regulado o acesso de pessoas em áreas de segurança, de forma a garantir que apenas entidades autorizadas possam ingressar aos locais.
  3. Uma vez concedido o acesso, os horários de entrada e saída dos visitantes devem ser registrados, juntamente com a data do ocorrido e as respectivas credenciais.
  4. Desde já é proibido o consumo de comida ou bebida nos laboratórios, áreas de segurança ou próximo a qualquer computador ou componente eletrônico da Instituição.
  5. Para garantir o perfeito funcionamento dos dispositivos das áreas de segurança, fatores como umidade, temperatura, gases e poeira devem ser controlados de forma automática e regular.

# Gerenciamento das operações e comunicações

* 1. A estrutura de Gestão de Segurança da Informação do Departamento de TI, no serviço de suas atribuições, deve:
     1. Estabelecer parâmetros adequados para a disponibilização dos serviços, sistemas e infraestrutura que os suportam, de maneira que atendam aos requisitos mínimos de qualidade e reflitam as necessidades operacionais da instituição.
     2. Descrever procedimentos e responsabilidades operacionais, tais como gestão de mudanças, segregação de funções e separação dos ambientes de produção, desenvolvimento e testes.
     3. Deverá fornecer diretrizes para gerenciamento de serviços terceirizados, cópias de segurança, planejamento e aceitação de sistemas, proteção contra códigos maliciosos, gerenciamento de segurança em redes, manuseio de mídias, troca de informações e monitoramento.
     4. Deve estabelecer critérios e metodologia de segurança que possibilitem o desenvolvimento de sistemas de informação e atividades de manutenção.
     5. Deve criar metodologias que deliberem processos de gestão para tratamento e respostas a incidentes de segurança que estejam em conformidade com a estrutura técnica e normativa do [Ctir.gov](https://www.ctir.gov.br/#%3A~%3Atext%3DO%20CTIR%20Gov%20%C3%A9%20um%2Cem%20%C3%B3rg%C3%A3os%20e%20entidades%20governamentais).