



**MINISTÉRIO DA EDUCAÇÃO
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
CENTRO FEDERAL DE EDUCAÇÃO TECNOLÓGICA DE RORAIMA
GERÊNCIA DE TECNOLOGIA DA INFORMAÇÃO**

**POLÍTICA DE SEGURANÇA DA ESTRUTURA DE INFORMÁTICA DO CENTRO FEDERAL DE
EDUCAÇÃO TECNOLÓGICA DE RORAIMA (CEFET-RR)**

A Política de Segurança da estrutura de informática abrange itens relacionados à segurança da informação relacionada à utilização da mesma e serão contemplados os seguintes aspectos: política de utilização da rede, administração de contas, senhas, e-mail, acesso a Internet, uso das estações de trabalho, utilização de impressoras.

1. POLÍTICA DE UTILIZAÇÃO DA REDE

Esse tópico visa definir as normas de utilização da rede que abrange o *login*, manutenção de arquivos no servidor e tentativas não autorizadas de acesso. Estes itens estarão sendo abordados para todos os usuários dos sistemas e da rede de computadores do CEFET-RR.

1.1. Regras Gerais

- a) Não são permitidas tentativas de obter acesso não autorizado, tais como tentativas de fraudar autenticação de usuário ou segurança de qualquer servidor de rede (equipamento), rede ou conta. Isso inclui acesso aos dados não disponíveis para o usuário, conectar-se a servidor de rede (equipamento) ou conta cujo acesso não seja expressamente autorizado ao usuário ou colocar à prova a segurança de outras redes.
- b) Não são permitidas tentativas de interferir nos serviços de qualquer outro usuário, servidor de rede (equipamento), ou rede. Isso inclui ataques, tentativas de provocar congestionamento em redes, tentativas deliberadas de sobrecarregar ou de "quebrar" (invadir) um servidor de rede (equipamento).
- c) Antes de ausentar-se do seu local de trabalho, o usuário deverá fechar todos os programas em uso, evitando, desta maneira, o acesso por pessoas não autorizadas. Se possível efetuar o *logout/logoff* da rede ou bloqueio do computador através de senha.
- d) O usuário deve fazer manutenção no diretório pessoal, evitando acúmulo de arquivos desnecessários.
- e) Material de natureza pornográfica e racista não pode ser exposto, armazenado, distribuído, editado ou gravado através do uso dos recursos computacionais da rede.
- f) Jogos ou qualquer tipo de software/aplicativo não pode ser gravado ou instalado no diretório pessoal do usuário, no computador local e em qualquer outro diretório da rede. Podem ser utilizados apenas os softwares previamente instalados no computador.
- 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. As áreas de armazenamento de arquivos são designadas conforme se segue:
 - I. Diretório Pessoal (XX:) - Arquivos Pessoais de responsabilidade do usuário dono deste diretório;
 - II. Diretórios Departamentais (ZZ:) - Arquivos do departamento em que trabalha;

- III. Diretório Público (PP:) - Arquivos temporários ou de compartilhamento geral, para todos os usuários.
- h) A pasta PÚBLICA ou similar, não deverá ser utilizada para armazenamento de arquivos que contenham assuntos sigilosos, confidenciais ou de natureza sensível. Devem ser armazenadas apenas informações comuns a todos.
 - i) Haverá limpeza semestral dos arquivos armazenados na pasta PÚBLICA ou similar, para que não haja acúmulo desnecessário de arquivos.
 - j) É proibida a instalação ou remoção de softwares que não forem devidamente acompanhadas pela Gerência de Tecnologia da Informação (GTI), e que não tenha sido feita através de solicitação escrita.
 - k) Não são permitidas alterações das configurações de rede e inicialização das máquinas, bem como modificações que possam trazer algum comprometimento do equipamento, sem a devida autorização da GTI.
 - l) Quanto à utilização de equipamentos de informática particulares, computadores, impressoras, entre outros, o CEFET-RR não fornecerá acessórios, software ou suporte técnico para computadores particulares, incluindo assistência para recuperar perda de dados, decorrentes de falha humana, ou pelo mau funcionamento do equipamento ou do software.
 - m) O acesso a sistemas deve ser controlado pela identificação do usuário e pelas senhas designadas para usuários autorizados. Senhas compartilhadas devem ser excepcionais e autorizadas pela GTI.

1.2. Regras para servidores

- a) É obrigatório armazenar os arquivos inerentes à Instituição no servidor de arquivos (equipamento) para garantir a cópia de segurança dos mesmos.
- b) É proibida a abertura de computadores para qualquer tipo de reparo, seja isto feito em departamentos ou laboratórios de informática, caso seja necessário o reparo deverá ocorrer pela GTI.
- c) Quanto à utilização de equipamentos de informática particulares o servidor deverá comunicar o responsável de seu departamento.
- d) Quando um servidor é transferido entre departamentos, o responsável que transferiu deve certificar-se de que todos os direitos de acesso aos sistemas e outros controles de segurança ainda serão necessários na sua nova função e informar a GTI qualquer modificação necessária.
- e) Quando ocorrer o afastamento ou exoneração do servidor, o responsável deve informar a GTI para providenciar a desativação dos acessos do usuário à qualquer recurso da rede. Deve-se verificar a necessidade de troca de senhas de contas de uso comum ao departamento, evitando o acesso às informações.

1.3. Regras para alunos

- a) É deletado semestralmente o conteúdo das contas de usuário alunos. Portanto o aluno que desejar manter suas informações deve providenciar a cópia dos arquivos sempre ao final do semestre.
- b) Quanto à utilização de equipamentos de informática particulares o aluno deverá comunicar a Coordenação do Curso.

1.4. Regras para Alunos Bolsistas ou Estagiários

- a) O acesso as informações é feito através da conta criada pela GTI mediante solicitação do Coordenador responsável. Se não existir necessidade o aluno bolsista ou estagiário pode não ter conta de acesso a rede de computadores.
- b) O acesso a diretórios ou compartilhamentos dos departamentos deve ser fornecido somente em caso de necessidade de acesso.

2. POLÍTICA DE ADMINISTRAÇÃO DE CONTAS

Este tópico visa definir as normas de administração das contas que abrange: criação, manutenção e desativação da conta.

2.1. Regras Gerais

2.1.1. Desativação da conta:

É reservado o direito de desativar uma conta de usuário, por parte da GTI, caso verifique-se a ocorrência de algum dos critérios abaixo especificados:

- Incidentes suspeitos de quebra de segurança nas contas dos usuários;
- Reincidência na quebra de senhas por programas utilizados pela GTI.

2.2. Regras para Servidores

Todo servidor do CEFET-RR poderá ter uma conta para acesso aos recursos da rede de computadores. Os acessos a demais sistemas devem ser informados pelo responsável da área no momento da solicitação da conta do usuário. Para solicitação da conta para novos servidores os responsáveis devem proceder da maneira explicada abaixo:

2.2.1. Criação de contas:

Todo servidor pode obter uma conta de acesso a rede de computadores, para isto:

- O responsável do departamento a que o servidor pertence deverá fazer uma solicitação da criação da conta. Esta solicitação deve ser feita através de e-mail para a GTI;
- Deve-se informar o número da matrícula do servidor, assim como os acessos que serão necessários para este usuário.

2.2.2. Manutenção da conta:

- a) Cada servidor que tiver sua conta criada terá um espaço no servidor para gravar seus arquivos pessoais;
- b) A manutenção dos arquivos na conta pessoal é de responsabilidade do usuário, sendo que o mesmo deve evitar acúmulo de arquivos desnecessários e sempre que possível verificar o que pode ser eliminado;
- c) As contas podem ser monitoradas pela GTI com o objetivo de verificar possíveis irregularidades no armazenamento ou manutenção dos arquivos nos diretórios pessoais.

2.3. Regras para Alunos

Todo aluno do CEFET-RR poderá ter uma conta para acesso aos recursos da rede de computadores. Todos os usuários têm um limite de armazenamento de arquivos em seu diretório

pessoal, qualquer necessidade de um espaço maior para armazenamento dos arquivos nos diretórios pessoais deve ser informada pelo professor a GTI.

2.3.1. Criação de contas:

- a) A criação da conta do aluno é feita através do envio das informações de matrícula dos alunos pela Coordenação do Curso. A cada semestre as informações das contas dos alunos são apagadas e uma nova senha é gerada;
- b) A senha do aluno é criada pela GTI no momento da criação da conta, esta senha poderá ser alterada quando o usuário utilizar sua conta.

2.3.2. Administração de contas:

- a) O CEFET-RR não se responsabiliza por documentos, programas e relatórios dentro das contas pessoais dos alunos. Os alunos deverão salvar seus arquivos periodicamente para, no caso de falhas, reverem seus dados;
- b) Não é feita cópia de segurança dos arquivos pessoais de alunos;
- c) As contas podem ser monitoradas pela GTI com o objetivo de verificar possíveis irregularidades no armazenamento ou manutenção dos arquivos nos diretórios pessoais.

2.4. Regra para Alunos Bolsistas ou Estagiários

- a) A criação de conta para acesso a rede de computadores do CEFET-RR para alunos bolsistas ou estagiários dependerá da necessidade de utilização, se existir necessidade o procedimento será o mesmo utilizado para criação de contas para servidores, o coordenador da área responsável deve informar a GTI as informações para criação da conta.

3. POLÍTICA DE SENHAS

3.1. Regras Gerais

As responsabilidades do usuário incluem, principalmente, os cuidados para a manutenção da segurança dos recursos, tais como sigilo da senha e o monitoramento de sua conta, evitando sua utilização indevida. As senhas são sigilosas, individuais e intransferíveis, não podendo ser divulgadas em nenhuma hipótese.

Tudo que for executado com a sua senha de usuário da rede ou de outro sistema será de inteira responsabilidade do usuário.

4. POLÍTICA DE 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. As mensagens podem estar sujeitas a demora e serviços potencialmente não confiáveis.

4.1. Regras Gerais

- a) O e-mail deve ser utilizado de forma consciente, evitando qualquer tipo de perturbação a outras pessoas, seja através da linguagem utilizada, frequência ou tamanho das mensagens.
- b) O envio de e-mail deve ser efetuado somente para pessoas que desejam recebê-los, se for solicitada a interrupção do envio deve ser acatada e o envio não devesse acontecer.

- c) É proibido o envio de grande quantidade de mensagens de e-mail (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) É proibido reenviar ou de qualquer forma propagar mensagens em cadeia independentemente da vontade do destinatário de receber tais mensagens.
- e) É proibido o envio de e-mail mal-intencionado ou sobrecarregar um usuário, site ou servidor de email (equipamento) com e-mail muito extenso ou numerosas partes de e-mail.
- f) Caso o CEFET-RR julgue necessário haverá bloqueios:
 - 1. De e-mail com arquivos anexos que comprometa o uso de banda ou perturbe o bom andamento dos trabalhos;
 - 2. De e-mail para destinatários ou domínios que comprometa o uso de banda ou perturbe o bom andamento dos trabalhos.
- g) É proibido forjar qualquer das informações do cabeçalho do remetente.
- h) É obrigatória a manutenção da caixa de e-mail, evitando acúmulo de e-mails e arquivos inúteis.
- i) A cota máxima de e-mails armazenados não deve ultrapassar os 25 MegaBytes.
- j) É orientado não executar ou abrir arquivos anexados enviados por emissores desconhecidos ou suspeitos.
- k) É orientado não abrir arquivos anexados com as extensões **.bat**, **.exe**, **.src**, **.lnk** e **.com** se não tiver certeza absoluta que solicitou este e-mail.
- l) Desconfie de todo o e-mail com assuntos estranhos e/ou em inglês. Alguns dos vírus mais terríveis dos últimos anos tinham assuntos como: ILOVEYOU, Branca de neve pornô, etc;
- m) Evite anexos muito grandes.

4.2. Regras para servidores

- a) Não devem ser enviadas mensagens de correio eletrônico cujo conteúdo seja confidencial ou restrito ao CEFET-RR, não podendo tornar-se público.
- b) Não utilize o e-mail do CEFET-RR para fins pessoais.
- c) É obrigatória a utilização de assinatura nos e-mails, seguindo o seguinte padrão:

*Nome completo ou nome e último sobrenome
Cargo/Função
Telefone/Ramal
Centro Federal de Educação Tecnológica de Roraima
<http://www.cefetrr.edu.br>*

5. POLÍTICA DE ACESSO A INTERNET

Esse tópico visa definir como será o acesso da Internet que engloba desde a navegação a *sites*, *downloads* e *uploads* de arquivos.

A Internet Institucional é uma ferramenta de trabalho e deve ser usada para este fim pelos servidores e alunos do CEFET-RR, não sendo permitido o seu uso para fins recreativos durante o horário de trabalho ou de aula.

5.1 Regras Gerais

- a) Somente navegação de *sites* é permitida. Casos específicos que exijam outros tipos de serviços, como download de arquivos, deverão ser solicitados diretamente à GTI com autorização do responsável pelo departamento a que o usuário pertence.
- b) É proibida a divulgação de informações confidenciais do CEFET-RR em grupos de discussão, listas 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) Caso o CEFET-RR julgue necessário haverá bloqueios de acesso à:
 - 1 - Arquivos que comprometa o uso de banda ou perturbe o bom andamento dos trabalhos;
 - 2 - Domínios que comprometa o uso de banda ou perturbe o bom andamento dos trabalhos.
- d) Obrigatoriedade da utilização do programa Mozilla, Internet Explorer, ou outro software homologado pela GTI, para ser o cliente de navegação.
- e) Não será permitido software de comunicação instantânea, não homologados/autorizados pela GTI.
- f) Não será permitida a utilização de softwares de *peer-to-peer* (P2P), tais como Kazaa, Morpheus e afins.
- g) O acesso a *sites* com conteúdo pornográfico, jogos, bate-papo, apostas, é bloqueado e as tentativas de acesso serão monitoradas.
- h) Não será permitida a utilização de serviços de *streaming*, tais como Rádios On-Line, Usina do Som e afins.
- i) É proibido utilizar os recursos da rede para fazer *download* ou distribuição de software ou dados não legalizados.

5.2 Regras para servidores

- a) Poderá ser utilizada a Internet para atividades não relacionadas com o trabalho durante o horário de almoço, ou fora do expediente, desde que dentro das regras de uso definidas nesta política.
- b) Os servidores com acesso à Internet podem baixar somente programas ligados diretamente às atividades do CEFET-RR e devem providenciar o que for necessário para regularizar a licença e o registro desses programas.
- c) Servidores com acesso à Internet não podem efetuar *upload* de qualquer software licenciado para o CEFET-RR ou de dados de propriedade do CEFET-RR ou de seus fornecedores, sem expressa autorização do responsável pelo software ou pelos dados.
- d) Haverá geração de relatórios dos sites acessados por usuário. Se necessário será publicado o relatório para prestação de contas do usuário referente aos seus acessos.

5.3. Regras para alunos

- a) É proibido a acesso a páginas da Internet que não sejam relacionadas a pesquisas ligadas ao curso a que o aluno está matriculado, ou domínios que não tenham cunho educacional.
- b) Alunos com acesso à Internet não podem efetuar *upload* de qualquer software licenciado para o CEFET-RR ou de dados de propriedade do CEFET-RR ou de seus fornecedores, sem expressa autorização do responsável pelo software ou pelos dados.

- c) Não será permitido software de comunicação instantânea, tais como MSN, Skype, etc.
- d) É proibido utilizar os recursos da rede para fazer download de softwares, vídeos, arquivos de áudio, ou outros tipos que atrapalhem o bom desempenho da rede e o andamento dos trabalhos.

6. POLÍTICA DE USO DAS ESTAÇÕES DE TRABALHO

Cada estação de trabalho possui códigos internos os quais permitem que ela seja identificada na rede. Sendo assim, tudo que for executado na estação de trabalho será de responsabilidade do usuário. Por isso, sempre que sair de frente da estação de trabalho tenha certeza que efetuou o *logoff* ou bloqueou a estação de trabalho.

6.1. Regras Gerais

- a) Não utilize nenhum tipo de software/hardware sem autorização da GTI.
- b) Não é permitido gravar nas estações de trabalho MP3, filmes, fotos e software com direitos autorais ou qualquer outro tipo que possa ser considerado pirataria.
- c) Mantenha nas estações de trabalho somente o que for supérfluo ou pessoal. Todos os dados relativos ao CEFET-RR devem ser mantidos no servidor de arquivos (equipamento), onde existe sistema de *backup* diário e confiável.
- d) Os arquivos gravados em diretórios temporários das estações de trabalho podem ser acessados por todos os usuários que utilizarem a mesma, portanto não se pode garantir sua integridade e disponibilidade. Poderão ser alterados ou excluídos sem prévio aviso e por qualquer usuário que acessar a estação.

7. POLÍTICA DE USO DE IMPRESSORAS

Esse tópico visa definir as normas de utilização de impressoras disponíveis nos departamentos do CEFET-RR. Esta política é aplicada somente a servidores e alunos bolsistas que utilizam impressoras em seus departamentos, sendo que, nos laboratórios que são utilizados pelos alunos, não existem impressoras instaladas.

7.1. Regras Gerais

- a) Ao mandar imprimir, verifique na impressora se o que foi solicitado já está impresso.
- b) Se a impressão deu errada e o papel pode ser reaproveitado na sua próxima tentativa, recoloque-o na bandeja de impressão. Se o papel servir para rascunho, leve para sua mesa. Se o papel não servir para mais nada, jogue no lixo.
- c) Não é permitido deixar impressões erradas na mesa das impressoras, na mesa das pessoas próximas a ela e tampouco sobre o gaveteiro.
- d) Se a impressora emitir alguma folha em branco, recoloque-a na bandeja.
- e) Se você notar que o papel de alguma das impressoras está no final, faça a gentileza de reabastecê-la. Isso evita que você e outras pessoas tenham seus pedidos de impressão prejudicados e evita acúmulo de trabalhos na fila de impressão.
- f) Utilize a impressora colorida somente para versão final de trabalhos e não para testes ou rascunhos.
- g) É permitido apenas a impressão de material relativo a atividade do usuário.

8. POLÍTICA DE SEGURANÇA FÍSICA

O objetivo desta política é prevenir o acesso não autorizado, dano e interferência às informações e instalações físicas da Instituição. A segurança física dos equipamentos de informática e das informações da Instituição deve ser protegida de possíveis danos. Será abordada a segurança física dos laboratórios de informática, das instalações de TI, dos equipamentos no geral e procedimentos para garantir a segurança.

8.1. Política de controle de acesso

Existem áreas que merecem maior atenção quanto ao controle da entrada de pessoa. Estas áreas são departamentos que contém informações ou equipamentos que devem ser protegidos, como por exemplo: sala de servidores de rede (equipamentos), departamentos financeiro e de recursos humanos, sala de Coordenadores e Diretores, entre outras.

8.1.1. Regras Gerais

- a) Apenas pessoas autorizadas podem acessar as instalações da GTI, sendo que os servidores devem usar crachás de identificação.
- b) Departamentos que tratem com informações confidenciais de alunos, como por exemplo, documentação, informações financeiras e acadêmicas, o acesso deve ser permitido somente para pessoas autorizadas.
- c) A temperatura, umidade e ventilação das instalações que abrigam equipamentos de informática e de comunicações, devem estar de acordo com os padrões técnicos especificados pelos fabricantes dos equipamentos.
- d) Se acontecer a perda de chaves de departamentos ou laboratórios a Coordenação responsável deve ser informada imediatamente para que possa providenciar a troca da fechadura e de outras cópias da chave perdida.

9. POLÍTICA DE UTILIZAÇÃO DE LABORATÓRIOS DE INFORMÁTICA

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

9.1. Regras Gerais

- a) O acesso a laboratórios de informática deve ser controlado, somente sendo permitido o uso dos mesmos com um servidor responsável.
- b) É de responsabilidade do professor/servidor que utilizou o laboratório zelar pela ordem das instalações. Sendo necessário qualquer tipo de manutenção a GTI deve ser informada.
- c) No momento em que entrar no laboratório o professor/servidor responsável deve verificar se todos os computadores estão funcionando corretamente. Após a utilização esta verificação deve ser repetida, e qualquer problema a GTI deve ser informada, para que a solução possa ser providenciada o mais rápido possível.
- d) Os equipamentos devem ser trancados e em segurança quando deixados sem supervisão, não sendo permitida a utilização de laboratórios sem supervisão.
- 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) As chaves de acesso aos laboratórios devem ficar guardadas em locais que o acesso seja controlado, que não seja permitida a entrada de pessoas não autorizadas, evitando que possam ter acesso as chaves.
- h) Se a utilização do laboratório não estiver prevista no horário esta utilização devera ser feita somente mediante a reserva do laboratório, garantindo assim que exista um registro de utilização dos mesmos.

10. VERIFICAÇÃO DA UTILIZAÇÃO DA POLÍTICA

Para garantir as regras mencionadas acima o CEFET-RR se reserva no direito de:

- a) Implantar softwares e sistemas que podem monitorar e gravar todos os usos de Internet através da rede e das estações de trabalho da instituição;
- b) Inspeccionar quaisquer arquivos armazenados na rede estejam estes no disco local da estação ou nas áreas privadas da rede, visando assegurar o rígido cumprimento desta política;
- c) Instalar softwares e hardwares para proteger a rede interna e garantir a integridade dos dados e programas, incluindo *firewalls*, que é a primeira, mas não a única barreira entre a rede interna e a Internet.

11. VIOLAÇÃO DA POLÍTICA, ADVERTÊNCIA E PUNIÇÕES

Ao detectar uma violação da política, a primeira coisa a fazer é determinar a sua razão, ou seja, a violação pode ter ocorrido por negligência, acidente, erro ou por ação previamente determinada, ignorando a política estabelecida. Um processo de investigação deve determinar as circunstâncias da violação, como e porque ela ocorreu.

Nos termos da Política, o CEFET-RR procederá ao bloqueio do acesso ou o cancelamento do usuário caso seja detectado uso em desconformidade com que foi estabelecido ou de forma prejudicial à rede.

É recomendado o treinamento dos usuários em segurança da informação, como forma de conscientização e divulgação da política de segurança a ser seguida por todos. O programa de treinamento em segurança deve fazer parte do programa de integração de novos funcionários e do programa de integração de novos alunos (ao início de cada ano letivo).

11.1. Regras para servidores

- a) Caso seja necessário advertir o servidor, será informado a Gerência de Recursos Humanos para interagir e manter-se informado da situação.
- b) O não cumprimento, pelo servidor, das normas estabelecidas neste documento seja isolada ou acumulativamente, poderá causar, de acordo com a infração cometida, as seguintes punições: Comunicação de Descumprimento, Advertência ou Suspensão.

Comunicação de Descumprimento:

Será encaminhado ao servidor, por e-mail, comunicado informando o descumprimento da norma, com a indicação precisa da violação praticada. Cópia desse comunicado permanecerá arquivada junto a Gerência de Recursos Humanos na respectiva pasta do servidor.

Advertência ou suspensão:

A pena de advertência ou suspensão será aplicada, por escrito, somente nos casos de natureza grave ou na hipótese de reincidência na prática de infrações de menor gravidade.

11.2. Regras para alunos

- a) Caso seja necessário advertir o aluno, será informada a Coordenação do Curso a qual o aluno está matriculado para interagir e manter-se informado da situação.
- b) O não cumprimento pelo aluno das normas estabelecidas neste documento seja isolada ou acumulativamente, poderá causar, de acordo com a infração cometida, as seguintes punições: comunicação de descumprimento, Advertência ou Suspensão.

Comunicação de descumprimento:

Será encaminhado ao aluno, através da Coordenação de Curso, comunicado informando o descumprimento da norma, com a indicação precisa da violação praticada. Cópia desse comunicado permanecerá arquivada junto a CORES na respectiva pasta do aluno.

Advertência ou suspensão:

A pena de advertência ou suspensão será aplicada, por escrito, somente nos casos de natureza grave ou na hipótese de reincidência na prática de infrações de menor gravidade. Antes da aplicação desta punição será realizado o conselho de disciplina, conforme regimento escolar que detalha os direitos e deveres dos alunos.