Norma Complementar Nº01 (NC01)

USO DOS RECURSOS COMPUTACIONAIS

1 – CAMPO DE APLICAÇÃO

Esta norma se aplica no âmbito do IFB, devendo os Campi adotá-la ou criar norma própria, desde que não seja divergente do que aqui se estabelece.

2 – OBJETIVO

Estabelecer critérios e procedimentos para o uso dos recursos computacionais disponíveis aos usuários da rede do IFB, assim como o controle, administração e requisitos mínimos desses recursos.

Essa norma visa proteger o IFB e os servidores de danos ou responsabilização civil, administrativo ou criminal devido à utilização incorreta dos recursos computacionais.

3 – CONCEITUAÇÃO

Gerenciamento Remoto: Nome atribuído ao acesso realizado a um computador por outro, dentro da mesma rede ou a partir de redes diferentes.
Ataque: Evento que pode comprometer a segurança de um sistema ou uma rede. Um ataque pode ter ou não sucesso. Um ataque com sucesso caracteriza uma invasão. Um ataque também pode ser caracterizado por uma ação que tenha um efeito negativo, Ex: DoS.
Auditoria: Processo de análise de causas e efeitos de incidentes, análise de logs, etc.
Conta De Rede: Identificação pessoal do usuário que permite acesso à rede local.
Controle De Acesso: Processo que determina o acesso ou não de um indivíduo às áreas ou objetos específicos, identificando e registrando esses acessos.
Cracking: Tentativas de obter acesso não autorizado, tais como tentativas de fraudar autenticação de usuário ou segurança de qualquer servidor, rede ou conta de rede.
Firewall: É o nome dado ao dispositivo de uma rede de computadores que tem por objetivo aplicar uma política de segurança a um determinado ponto de controle da rede. Sua função consiste em regular o tráfego de dados entre redes distintas e impedir a transmissão e/ou recepção de acessos nocivos ou não autorizados de uma rede para outra.
DoS: *Denial of Service* - é um ataque que consiste na tentativa de tornar os recursos de um sistema indisponíveis para os seus utilizadores.
Invasão: Um ataque bem sucedido.
Logoff: É o processo de encerramento da sessão de trabalho pelo usuário.

Login: É o processo pelo qual o acesso a um sistema informatizado é controlado através da identificação e autenticação do utilizador, por meio de credenciais fornecidas por esse mesmo utilizador. Essas credenciais são normalmente constituídas por um nome de utilizador (do inglês username) e uma palavra-chave ou senha (do inglês password) - ocasionalmente, dependendo de sistemas menos complexos, apenas pedida a senha.
DTIC: Diretoria de Tecnologia da Informação e Comunicação.
Recursos Computacionais: São os equipamentos, as instalações ou bancos de dados direta ou indiretamente administrados, mantidos ou operados pela Área de TI tais como: Computadores e terminais de qualquer espécie, incluidos seus equipamentos acessórios; Impressoras ;Redes de computadores e de transmissão de dados ;"Arrays" de discos, de fitas, e equipamentos afins; Bancos de dados ou documentos residentes em disco, fita ou outros meios ;Leitoras de códigos de barra, "scanners", equipamentos digitalizadores e afins; Manuais técnicos; Salas de computadores ;Serviços e informações disponibilizados via a arquitetura de informática da instituição ;Softwares adquiridos ou desenvolvidos ;
Data Center :é um ambiente projetado para abrigar servidores e outros componentes como sistemas de armazenamento de dados (*storages*) e ativos de rede (*switches*, roteadores)
Ativos De Rede:são os equipamentos básicos que fazem sua rede funcionar. São os switches, hubs, roteadores, access points, dentre outros.
BIOS: um acrônimo Basic Input/Output System e também conhecido como System **BIOS**, ROM **BIOS** ou PC **BIOS**) é um tipo de chip e usado para realizar a inicialização do hardware durante o processo de inicialização em computadores .
MODEM: vem da junção das palavras modulador e demodulador. É um dispositivo eletrônico que modula um sinal digital numa onda analógica.
Rede Corporativa: Conjunto de redes e sistemas (responsáveis pelo processamento de informações) dentro de uma corporação.
IP: significa Internet Protocol e é um número que seu computador (ou roteador) recebe quando se conecta à Internet. É através desse número que seu computador é identificado e pode enviar e receber dados.
Vírus: São códigos ou programas que infectam outros programas e se multiplicam, na maioria das vezes podem causar danos aos sistemas infectados.
Wireless: Rede sem fio.

4 – DIRETRIZES GERAIS:

a) Recursos Computacionais em Geral

I. Os usuários devem ter acesso unicamente àqueles recursos computacionais que forem indispensáveis à realização de suas atividades no IFB;

II. A utilização dos recursos de tecnologia, com finalidade pessoal, é permitida, desde que não viole as Normas Institucionais, a Política de Segurança da Informação - POSIC, as Normas Complementares e o Código de Ética da Instituição;

III. Os usuários são responsáveis pelos recursos computacionais por eles utilizados, devendo preservar a sua integridade e continuidade;

IV. Os ambientes onde se encontram instalados ou guardados os recursos computacionais devem permanecer protegidos mesmo na ausência dos usuários;

V. É vedado aos usuários do IFB utilizar a identificação e/ou senha de outro usuário para acessar ou utilizar um recurso computacional;

VI. É vedado aos usuários fazer uso de exploração de falhas de configuração, falhas de segurança ou tentar obter conhecimento de senhas especiais para alterar um recurso computacional;

VII. Tendo em vista a preservação do ambiente computacional do IFB, é vedado aos usuários o fornecimento de informações a terceiros sobre características, funcionalidades e configurações dos recursos de tecnologia da informação disponíveis, ressalvada a possibilidade de disponibilização de tais informações pela DTIC, quando o desempenho de atividades institucionais assim exigir;

VIII. Os equipamentos disponíveis aos servidores são de propriedade da Instituição, cabendo a cada um utilizá-los e manuseá-los corretamente para as atividades de interesse do IFB, bem como cumprir as recomendações constantes nos procedimentos operacionais fornecidos pelas áreas responsáveis. Dessa forma, esta norma faz conhecer que:

a. É proibido todo procedimento de manutenção física ou lógica, instalação, desinstalação, configuração ou modificação, sem o conhecimento prévio e o acompanhamento de um técnico de TI, ou de quem esta norma determinar;

b. Os computadores devem ter versões do software antivírus instalado, ativado e atualizado permanentemente;

c. O usuário, em caso de suspeita de vírus ou problemas na funcionalidade, deverá acionar o departamento técnico responsável, mediante abertura de chamada técnico;

d. A transferência e/ou a divulgação de qualquer software, programa ou instruções de computador para terceiros, por qualquer meio de transporte (físico ou lógico), somente poderá ser realizada com a devida autorização da Instituição, de acordo com o nível de classificação da informação, após identificação e justificativa do solicitante;

e. Arquivos pessoais e/ou não pertinentes à atividade da Instituição (fotos, músicas, vídeos, etc.) não deverão ser copiados, movidos e armazenados nos computadores da Instituição. Caso identificada a existência desses arquivos, eles serão excluídos definitivamente sem comunicação prévia ao usuário;

f. Documentos imprescindíveis para as atividades dos servidores da Instituição deverão ser salvos em pastas compartilhadas de cada setor. Tais arquivos, se gravados apenas localmente nos computadores (por exemplo, no drive C:), não terão garantia de backup e poderão ser perdidos caso ocorra uma falha no computador, sendo, portanto, de responsabilidade do próprio usuário;

g. Os servidores do IFB e/ou detentores de contas de rede privilegiadas não devem executar nenhum tipo de comando ou programa que venha sobrecarregar os serviços existentes na rede corporativa sem a prévia solicitação e a autorização da área de TI;

h. No uso dos computadores, equipamentos e recursos de informática, algumas regras devem ser atendidas:

i. Todos os computadores da Instituição deverão ter senha de BIOS para restringir o acesso de servidores não autorizados. Tais senhas serão definidas pela área de TI que terá acesso a elas para manutenção dos equipamentos;

ii. Os servidores devem informar ao departamento técnico qualquer identificação de dispositivo estranho conectado ao seu computador;

iii. É vedada à equipe de TI. e de seus prestadores de serviço, a manutenção de equipamentos pessoais dos servidores ou de terceiros. Caso isso ocorra, o responsável e/ou empresa serão advertidos;

iv. É vedado o uso de modens para impedir a invasão/evasão de informações, programas, vírus. Em alguns casos especiais, conforme situação específica, será considerada a possibilidade de uso para planos de contingência mediante a autorização dos gestores das áreas e/ou da alta gestão do IFB;

v. É expressamente proibido o consumo de alimentos, bebidas ou fumo na mesa de trabalho e próximo aos equipamentos;

vi. Todos os recursos tecnológicos adquiridos pela Instituição devem ter imediatamente suas senhas padrões (default) alteradas;

vii. Não é permitido o uso da rede corporativa por notebooks de terceiros e/ou particulares, sem a prévia autorização da área de TI;

viii. Os equipamentos deverão manter preservados, de modo seguro, os registros de eventos, constando a identificação do usuário, datas e horários de acesso.

b) Estações de Trabalho

I. Estações de trabalho devem ser utilizadas para execução de atividades de interesse do IFB;

II. Cada estação de trabalho tem códigos internos que permitem que ela seja identificada na rede. Isso significa que tudo que venha a ser executado em uma determinada estação, acarretará em responsabilidade daquele usuário que está com suas credenciais (*login/senha*) na máquina. Por isso, é de fundamental importância que o usuário, ao sair da frente de sua estação de trabalho, tenha certeza que efetuou *logoff* ou travou o console. Portanto, o usuário, sempre que se ausentar da estação de trabalho deverá bloqueá-la para impedir o acesso não autorizado;

III. É vedado ao usuário abrir as estações de trabalho ou modificar a configuração do hardware;

IV. O usuário deve informar imediatamente à área de TI, quando identificada violação da integridade do equipamento por ele utilizado;

V. A configuração do ambiente operacional da estação de trabalho somente poderá ser alterada por técnico autorizado pela área de TI;

VI. O usuário deve ligar/desligar de forma adequada e segura o equipamento;

VII. As atualizações de segurança ocorrerão automaticamente mediante procedimentos realizados pela área de TI;

VIII. Caso o usuário identifique a necessidade de alguma atualização deverá comunicar à área de TI;

IX. Todas as estações de trabalho deverão possuir o programa de antivírus homologado pela DTIC;

X. O antivírus deve estar atualizado e com a autoproteção ativa na estação de trabalho;

XI. O usuário deve obrigatoriamente executar o antivírus nos dispositivos removíveis antes de sua abertura quando inseridos na estação de trabalho;

XII. O usuário não deve cancelar o processo de verificação de vírus quando este for iniciado automaticamente na sua estação de trabalho;

XIII. Não é permitida a conexão de equipamentos particulares, portáteis ou não, à rede corporativa do IFB, exceto em casos de comprovada necessidade, situações nas quais deverá ser assegurada a devida adoção de padrões de segurança compatíveis com o disposto nessa norma, devendo a equipamento ser objeto de verificação de conformidade pela área de TI;

XIV. Arquivos salvos na unidade de disco local não terão garantia de recuperação;

XV. As credenciais de administrador do equipamento deverão ficar sob a guarda e responsabilidade da área de TI, restando ao usuário, ao qual se destina o equipamento, utilizá-lo mediante credenciais de usuário padrão. Ressalva-se o caso de usuários da área técnica, devidamente autorizados pela DTIC, que por força de suas funções e conhecimento técnico, reservam-se o direito de efetuar suas próprias instalações, bem como, a guarda e o uso oportuno das credenciais de administrador.

Não é (são) permitido (s, a, as):

a) Tentativas de obter acesso não autorizado, tais como tentativas de fraudar autenticação de usuário ou segurança de qualquer servidor, rede ou conta (também conhecido 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;

b) Tentativas de interferir nos serviços de qualquer outro usuário, servidor ou rede. Isso inclui ataques do tipo "negativa de acesso", provocar congestionamento em redes, tentativas deliberadas de sobrecarregar um servidor e tentativas de "quebrar" (invadir) um servidor;

c) O uso de qualquer tipo de programa ou comando designado a interferir nas sessões de usuários;

d) A falta de manutenção no diretório pessoal, causando o acúmulo de arquivos inúteis;

e) Material de natureza pornográfica, racista, terrorista e afins. Material deste cunho não pode ser exposto, armazenado, distribuído, editado ou gravado por meio do uso dos recursos computacionais da Instituição;

f) Criar e/ou remover arquivos fora da área alocada ao usuário e/ou que venham a comprometer o desempenho e funcionamento dos sistemas;

g) A instalação ou remoção de softwares que não forem devidamente acompanhadas pela área de TI, por meio de solicitação escrita;

h) A violação e/ou retirada de lacres dos computadores em qualquer hipótese. Caso seja necessária a abertura do equipamento e o seu respectivo reparo, este deverá ocorrer pelo suporte técnico de TI, representada pela Central de Manutenção;
i) A alteração das configurações de rede e inicialização das máquinas bem como modificações que possam trazer algum problema futuro;
j) A conexão de equipamentos que não fazem parte da rede Corporativa do IFB, sem a prévia autorização da área de TI;
k) A conexão de laboratórios da rede acadêmica nos ativos da rede Corporativa, visando ao uso do link para acesso à internet;
l) O uso de configuração manual dos endereços IP´s das estações de trabalho;
m) Acesso aos racks de ativos de rede, sem acompanhamento do responsável da área de TI, sendo considerado tal ato como violação de ambiente;
n) A ligação dos computadores novos e em casos de movimentação, sem o acompanhamento do suporte técnico local, de forma a evitar danos nos componentes ou no equipamento. Caso o usuário proceda com a instalação e seja constatada a queima do equipamento por imperícia ou negligência, os custos do reparo serão de responsabilidade deste, no caso de servidor do IFB. Em caso de terceiros, na forma da lei.

c) Equipamentos Portáteis

Esse item estabelece critérios de manuseio, prevenção e responsabilidade sobre o uso de dispositivos móveis e deverá ser aplicada a todos os servidores que utilizem tais equipamentos. Assim:

I. A Instituição, na qualidade de proprietária dos equipamentos fornecidos, reserva-se o direito de inspecioná-los, a qualquer tempo, caso seja necessária realizar uma manutenção de segurança;
II. Os equipamentos portáteis devem respeitar as mesmas regras estabelecidas para estações de trabalho;
III. Equipamentos portáteis de propriedade do IFB devem ser guardados em local seguro, com controle de acesso e garantia quanto à sua integridade;
IV. O usuário, ao solicitar o empréstimo de equipamentos portáteis do IFB, deve assinar o Termo de Empréstimo de Equipamento;
V. Somente técnicos autorizados pela área de TI devem configurar os equipamentos portáteis para acesso à rede do IFB;
VI. O usuário deve evitar armazenar informações confidenciais em equipamentos portáteis;
VII. Todo servidor deverá realizar periodicamente, cópia de segurança (*backup*) dos dados de seu dispositivo móvel. Deverá, também, guardar estes *backups* em ambiente diferente, longe de seu dispositivo móvel, ou seja, não carregá-los / armazená-los juntos num mesmo lugar;

VIII. O suporte técnico aos dispositivos móveis de propriedade IFB e aos seus usuários deverá seguir o mesmo fluxo de suporte contratado pela Instituição;
IX. Todo servidor deverá utilizar senhas de bloqueio automático para seu dispositivo móvel, quando couber;
X. Não será permitida, em nenhuma hipótese, a alteração da configuração dos sistemas operacionais dos equipamentos, em especial os referentes à segurança e à geração de *logs*, sem a devida comunicação e a autorização da área responsável e sem a condução, auxílio ou presença de um técnico da área de TI;
XI. O servidor deverá responsabilizar-se por quaisquer programas e/ou aplicativos que não tenham sido instalados ou autorizados pela área de TI;
XII. A reprodução não autorizada dos softwares instalados nos dispositivos móveis constituirá uso indevido do equipamento e infração legal aos direitos autorais do fabricante;
XIII. É responsabilidade do servidor, no caso de furto, roubo ou extravio de um dispositivo móvel fornecido pela Instituição, notificar, imediatamente, seu gestor direto e, este, a área de TI;
XIV. O servidor deverá estar ciente de que assumirá todos os riscos e/ou danos causados à Instituição e/ou a terceiros, de forma direta ou indireta, no momento presente ou no futuro, oriundos da má utilização dos dispositivos móveis que estão sob sua responsabilidade.

d) Equipamentos Servidores

I. Todo equipamento servidor deve estar instalado em salas apropriadas e construídas para este fim;
II. Somente os técnicos autorizados da área de TI deverão ter acesso aos equipamentos servidores;
III. Todos os equipamentos servidores devem utilizar os sistemas operacionais atualizados;
IV. A atualização dos equipamentos servidores deverá ser realizada pelos técnicos autorizados pela área de TI;
V. O controle de acesso aos equipamentos servidores deverá ser realizado por técnicos autorizados pela área de TI em parceria com a área responsável pela segurança das instalações físicas do IFB.

e) Equipamento Servidor de Arquivos

I. Nos servidores de arquivos devem ser gravados:
i. Documentos relacionados ao trabalho cotidiano e à produção jurídica e administrativa local, que demande compartilhamento ou resguardo institucional;
ii. Pastas particulares de correio eletrônico, exclusivamente das contas de rede corporativas da unidade.
II. As permissões de acesso deverão ser concedidas em nível de grupos;
III. Só será permitido o acesso a qualquer pasta ou arquivo no servidor mediante autorização formal ao responsável do setor;

IV. Material de natureza pornográfica, racista, terrorista e afins. Material deste cunho não pode ser exposto, armazenado, distribuído, editado ou gravado por meio do uso dos recursos computacionais da Instituição;
V. Não é permitido criar ou remover arquivos fora da área alocada ao usuário ou que venham a comprometer o desempenho e funcionamento dos sistemas;
VI. É vedada a gravação de dados e informações de natureza particular;
VII. É vedada a gravação de arquivos de vídeo, foto, executáveis, musica, sem autorização formal ao responsável do setor, visando a otimização do espaço em disco.
VIII. É obrigatório armazenar os arquivos inerentes ao serviço de cada setor em suas respectivas pastas para garantir o backup dos mesmos;
IX. Deverão ser gravados no servidor apenas documentos de interesse da Instituição, devido ao limite de espaço em disco determinado para cada setor.
X. Documentos de interesse dos departamentos deverão ser criados ou compartilhados na estrutura departamental;
XI. O compartilhamento deve ser restrito aos diretórios necessários, nunca compartilhando o diretório raiz.
XII. Caso haja desacordo com o disposto nos artigos antecedentes, a área de TI poderá, após notificar o responsável e resguardar as evidências necessárias, excluir ou isolar arquivos, revogar acessos ou requisitar o equipamento, relatando o fato imediatamente à autoridade responsável pela apuração da infração.

f) Ativos de Rede

I. As portas dos *switches* somente devem estar ativas se utilizadas e inventariadas;
II. Os *switches* e *access points* devem possuir controle de acesso;
III. Todo roteador utilizado na rede do IFB deve prover, no mínimo, o uso de ACLs (*Access lists*) e o filtro de pacotes;
IV. Todo ativo de rede deve estar em local seguro. Os *switches* departamentais devem estar instalados em racks devidamente fechados e seguros;
V. Os ativos de rede só podem ser instalados na rede do IFB após a sua adequação aos padrões de segurança definidos pela área de TI;
VI. Os ativos de rede somente devem ser liberados para uso após a efetiva homologação, realizada em ambiente apropriado, distinto do ambiente de produção, e devidamente documentado;
VII. As intervenções no ambiente de rede somente serão permitidas mediante supervisão pelos técnicos autorizados pela área de TI;
VIII. Não são permitidas tentativas de obter acesso não autorizado, tais como tentativas de fraudar autenticação de usuário ou segurança de qualquer servidor, rede ou conta;
IX. Profissionais técnicos no exercício de suas funções, não devem utilizar a rede de dados do IFB para testes, devendo, para isto, a área de TI prover segmento de rede independente;

X. A DTIC reserva o direito de realizar investigação forense computacional em quaisquer dos equipamentos que integrem a sua rede local.

g) Rede Sem Fio Corporativa

I. Não é permitido o uso da rede sem fio (Wireless) por notebooks de terceiros e/ou particulares, sem a prévia autorização da área de TI e /ou da chefia superior do servidor;
II. A utilização da rede sem fio para acesso à rede do IFB somente será efetuada com autenticação utilizando mecanismos de protocolo seguro;
III. Qualquer equipamento que utilize a rede sem fio do IFB deve respeitar as regras estabelecidas para Estações de Trabalho e dispositivos portáteis, inclusive, quando justificados, os equipamentos particulares;
IV. Somente os técnicos autorizados pela área de TI devem estabelecer os procedimentos e configurações de segurança de rede sem fio;
V. A área de TI deve verificar a adequação das Estações de Trabalho e instruir os usuários sobre os procedimentos para acesso à rede sem fio de acordo com os requisitos estabelecidos.

h) Impressoras

I. Somente os usuários previamente autorizados poderão ter acesso aos recursos de impressão;
II. A configuração da impressora na estação de trabalho do usuário somente deverá ser realizada pelos técnicos autorizados pela área de TI ou a partir do consentimento formal destes;
III. Os usuários não devem deixar informações críticas, sigilosas ou sensíveis da Instituição em equipamentos de impressão, de tal forma que pessoas não autorizadas possam obter acesso a elas;
IV. Não é permitido deixar impressões erradas na mesa das impressoras, na mesa das pessoas próximas, visando à privacidade e à confidencialidade das informações. Deve-se seguir política de descarte no caso de se garantir o sigilo das informações;
V. Toda troca de cartuchos, toner ou fita de qualquer impressora, deve ser feita por pessoa capacitada ou terceirizado da empresa que fornece a impressora (casos de impressoras alugadas), evitando, dessa forma, danos aos equipamentos;
VI. Todo cartucho ou toner deve ser devolvido no ato da troca deste, objetivando com isso a possibilidade de recarga e evitar o extravio de cartuchos da Instituição para uso de terceiros;
VII. Não são permitidas impressões de material que não seja para uso da Instituição, tanto em impressoras locadas ou da própria Instituição.

i) Utilização de Software

A seguir, são definidas as normas de utilização de softwares disponíveis e licenciados pela Instituição, visando a evitar o uso de software ilegal, de tal forma que não comprometa o IFB no que diz respeito a direitos autorais e licenças.

I. No IFB, só será permitida a utilização de softwares homologados pela área de TI, respeitando os direitos autorais e contratuais dos fabricantes, e que sejam necessários para a execução das atividades dos usuários;
II. O registro dos softwares homologados, do número de licenças disponíveis e dos softwares instalados nas estações de trabalho deve ser mantido atualizado pela área de TI;
III. Perante a necessidade de utilização de software não homologado, a chefia imediata deverá solicitar formalmente à área de TI a homologação deste contendo os seguintes itens:
    i. Especificações detalhadas do software solicitado;
    ii. Quantidade de licenças;
    iii. Suporte ao software (necessidade de suporte);
    iv. Justificativa.
IV. O processo de homologação de software deve avaliar, sobretudo, o impacto da utilização deste na segurança da informação do IFB e o suporte para este;
V. A instalação e a utilização de software estão sujeitas ao cumprimento dos seguintes requisitos:
    i. Quantidades de licenças de uso adquiridos;
    ii. Conformidade com a área de atuação do setor interessado;
    iii. Compatibilidade com os softwares utilizados;
    iv. Desempenho do ambiente computacional; e
    v. Impacto entre a necessidade de instalação e a demanda de outros setores.
VI. É vedado:
    i. Efetuar réplicas dos softwares adquiridos pelo IFB, bem como promover esta prática com outros programas;
    ii. Utilizar softwares que, por algum motivo, descaracterizem os propósitos da Instituição ou danifique de alguma forma o ambiente instalado, tais como jogos eletrônicos e outros;
    iii. Remover softwares “padrão” instalados pela área de TI nos computadores;
    iv. Remover, interromper ou qualquer outro meio de parar os programas que fazem inventário, produtividade e controle de acesso aos computadores, sendo tratado como tentativa de burlar as ferramentas de segurança da Instituição;
    v. Instalar outro software de antivírus que não seja o padrão adotado pela Instituição;
    vi. O uso de firewall e/ou outras ferramentas que impossibilitem o gerenciamento remoto, de tal modo que o software de inventário seja impossibilitado de enviar e coletar informações;
    vii. O uso de licenças de Windows, que ficam localizadas nos gabinetes dos computadores, em máquinas de terceiros;
VII. A instalação de software de outras categorias, tais como *freeware* (software gratuito), de domínio público (não protegido por *copyright*) e/ou cópias de demonstração que não sofram ação de direitos autorais, deve ser previamente requerida à área de TI;
VIII. A área de TI poderá remover programa de computador instalado em estação de trabalho que não se enquadre nos critérios estabelecidos nessa norma, a qualquer momento e sem aviso prévio;

IX. Os usuários com credenciais de administrador somente poderão instalar softwares, necessários ao desempenho de suas atribuições excepcionais, mediante prévia e indispensável autorização da área de TI.

j) Manutenção e Configuração

I. Toda solicitação de atendimento para instalação, suporte e configuração dos recursos computacionais deve ser efetuada mediante solicitação formal à área de TI por meio de abertura de chamado técnico;
II. A equipe de atendimento deve estar devidamente identificada para a execução dos serviços de suporte técnico;
III. Nas dependências físicas do IFB somente é permitida a execução dos serviços de suporte técnico nos equipamentos de propriedade da Instituição ou cedidos formalmente, sendo proibida a assistência técnica em equipamentos particulares;
IV. O usuário deve acompanhar o técnico durante a manutenção da sua estação de trabalho;
V. Todo equipamento que tiver a necessidade de ser deslocado para manutenção ou configuração, deverá estar devidamente identificado e embalado;
VI. O usuário deve estar ciente da saída do equipamento de seu local de trabalho caso seja necessária a retirada deste para manutenção;
VII. Todo recurso computacional que sair das dependências físicas do IFB por motivo de manutenção deverá ser registrado pelo responsável do setor e deverá ter os dados institucionais críticos previamente excluídos;
VIII. A saída do equipamento das instalações do IFB deverá ser autorizada pelo chefe imediato do servidor;
IX. O usuário deve manter o número, do registro do chamado ou número do documento de solicitação formal, do pedido de suporte por ele realizado para controle e acompanhamento do respectivo chamado.

k) Inclusão de equipamentos na Rede Corporativa

I. Não é permitida a conexão de dispositivos não autorizados na rede local, principalmente, equipamentos de rede sem fio ou qualquer outra solução que estabeleça conexão simultânea com a rede de dados do IFB e outras redes. Em casos justificados para o uso destes equipamentos, o IFB deve prover segmento de rede independente, de forma a permitir o compartilhamento de sua infraestrutura de TI sem o comprometimento do desempenho e da segurança da rede local;
II. A instalação de novas redes no domínio do IFB deverá ter links próprios. Para tanto, o IFB deverá prover ambiente de segmentação de redes por VLANs de forma a permitir o compartilhamento de sua infraestrutura de TI sem o comprometimento do desempenho e da segurança.

l) Data Center

Para que se garanta a segurança da informação, os aspectos abaixo elencados devem ser respeitados:

I. O acesso físico ao Data Center (DC) somente deverá ser realizado por autorização prévia da área de TI e acompanhada de um técnico responsável. Todo acesso ao Data Center deverá ser registrado (nome, rg\matricula, data e hora);

II. Deverá ser executada ao menos quinzenalmente uma auditoria nos acessos ao Data Center por meio de relatórios;

III. A lista de funções/permissões com direito de acesso ao Data Center deverá ser constantemente atualizada, de acordo com os termos do Procedimento de Controle de Acesso ao Data Center e salva no diretório de rede;

IV. O acesso de visitantes ou terceiros somente poderá ser realizado com acompanhamento de um servidor autorizado, que deverá preencher a solicitação de acesso prevista no Procedimento de Controle de Acesso ao DC, bem como assinar o Termo de Responsabilidade;

V. Caso haja necessidade do acesso não emergencial, a área requisitante deve solicitar autorização com antecedência ao responsável pela administração de liberação de acesso, conforme lista de funções/permissões salva em Procedimento de Controle de Acesso ao DC;

VI. Deverão existir duas cópias de chaves da porta do DC. Uma das cópias ficará de posse do responsável pela área e a outra, de posse do responsável pela Infraestrutrua e Segurança da Informação;

VII. O DC deverá ser mantido limpo e organizado, contendo apenas os equipamentos de TI. Qualquer procedimento que gere lixo ou sujeira nesse ambiente somente poderá ser realizado com a colaboração da equipe de Serviços Gerais;

VIII. Não é permitida a entrada de nenhum tipo de alimento, bebida, produto fumígeno ou inflamável;

IX. A entrada ou retirada de quaisquer equipamentos do DC somente dar-se-á com o preenchimento da solicitação de liberação pelo servidor solicitante e a autorização formal deste instrumento pelo Responsável pela área de TI, de acordo com os termos do Procedimento de Controle e Transferência de Equipamentos;

X. No caso de desligamento de servidores que possuam acesso ao DC, imediatamente deverá ser providenciada a exclusão deste do sistema de autenticação e da lista de servidores autorizados, de acordo com o processo definido no Procedimento de Controle de Acesso ao DC.

5 – AUTOGERENCIAMENTO DO PROCESSO

Consiste no atendimento à Política de Utilização dos Serviços de Tecnologia da Informação definidos nesta Norma Complementar.

6 – DISPOSIÇÕES FINAIS

As dúvidas e os casos omissos na aplicação desta Norma Complementar serão dirimidos pelo Comitê de Gestor de Segurança da Informação ou, em sua ausência, pelo Comitê de Governança Digital.

7 – ANEXOS

Não se aplica.

8 – QUADRO DE REVISÃO

Revisão	Descrição

Elaborado por
Diretoria de Tecnologia da Informação e Comunicações

Aprovado por	Autorizado por