

INSTITUTO HOLOS DE EDUCAÇÃO S/S LTDA

FACULDADE HOLÍSTICA – FAHOL

**REGULAMENTO DE TECNOLOGIA DE INFORMAÇÃO E
COMUNICAÇÃO - TIC**

**CURITIBA
2020**

ELABORAÇÃO DO REGULAMENTO DE TECNOLOGIA DE INFORMAÇÃO E COMUNICAÇÃO - TIC

COMISSÃO ORGANIZADORA:

Direção Geral: Lurdes Guimarães da Silva

Direção Acadêmica: Denise Godoi Ribeiro Sanches

Coordenação da CPA: Edilson da Costa

Secretaria Geral: Selvino Muraro

PROFESSORES COLABORADORES:

Cleverson França Silveira

Marcos Junitsi Uda

Scheila Patrícia da Cruz Fogaça Cândido

SUMÁRIO

CAPÍTULO I	4
DA NATUREZA E FINALIDADE.....	4
CAPÍTULO II	4
DOS OBJETIVOS	4
CAPÍTULO III	5
DOS RECURSOS E COMPOSIÇÃO	5
CAPÍTULO IV	5
DOS PROCEDIMENTOS GERAIS	5
CAPÍTULO V	6
DAS COMPETÊNCIAS E RESPONSABILIDADES DA IES	6
CAPÍTULO VI	8
DA AUTORIZAÇÃO	8
CAPÍTULO VII	9
DAS RESPONSABILIDADES DOS USUÁRIOS	9
CAPÍTULO VIII	10
DO ACESSO À REDE DE COMUNICAÇÃO DE DADOS	10
CAPÍTULO IX	10
DO USO DA INTERNET	10
CAPÍTULO X	11
DAS PROIBIÇÕES	11
CAPÍTULO XI	13
DAS PENALIDADES	13
CAPÍTULO XII	14
DO CONTROLE DO PARQUE DE INFORMÁTICA E ARMAZENAMENTO	14
CAPÍTULO XIII	14
DAS DISPOSIÇÕES GERAIS E TRANSITÓRIAS	14
GLOSSÁRIO	16

A Faculdade Holística – FaHol dispõe normas de organização e funcionamento para TIC: Tecnologia da Informação e Comunicação.

CAPÍTULO I

DA NATUREZA E FINALIDADE

Art. 1º TIC (Tecnologia da Informação e Comunicação) é um conjunto de recursos tecnológicos integrados entre si, que proporcionam, por meio das funções de *hardware*, *software* e telecomunicações, a automação e comunicação dos processos, da pesquisa, ensino, extensão e de gestão.

Art. 2º É uma ferramenta que dá base ao sucesso do Ensino a Distância (EAD) e possibilita o acesso aos conteúdos de forma rápida, num ambiente de aprendizagem interativo e inovador. A EaD é voltada à aprendizagem, está vinculada a vários princípios educacionais, entre os quais o de aprendizagem aberta, aprendizagem ao longo de toda vida ou educação permanente.

CAPÍTULO II

DOS OBJETIVOS

Art. 3º São objetivos:

I – Desenvolver um ambiente com possibilidade técnica de entrelaçar a cultura, a prática social, os saberes, a prática pedagógica, a ciência, expressando-se por diferentes linguagens, na tentativa de produzir novos sentidos e, em consequência, uma nova paisagem;

II – Usar recursos tecnológicos para facilitar o processo ensino-aprendizagem, bem como favorecer, por meio de Ambientes Virtuais de Aprendizagem (AVA), a troca de informações e experiências entre alunos e professores e/ou tutores.

III - Disciplinar a administração e o uso dos recursos de Tecnologia da Informação (TI), para proteger os dados e as informações da instituição e à privacidade dos usuários;

IV - Servir à pesquisa, o desenvolvimento tecnológico, às atividades administrativas da IES e atender os usuários para atingirem as suas metas;

V – Promover desenvolver debates, fóruns, trabalhos em grupo, de maneira a incentivar o uso das TIC, tornando a aprendizagem mais significativa;

CAPÍTULO III

DOS RECURSOS E COMPOSIÇÃO

Art. 4º Os recursos computacionais de TI, desenvolvidos, adquiridos, recebidos em doação e/ou mantidos pela Instituição, disponibilizados às áreas acadêmicas e/ou administrativas da FaHol, são constituídos por:

- I - Equipamentos de informática de qualquer espécie;
- II - Equipamentos de redes e de telecomunicações de qualquer espécie;
- III - Ativos de TI, contendo as informações eletrônicas, serviço de correio eletrônico, dados corporativos, documentos administrativos, programas de computadores adquiridos de terceiros ou desenvolvidos pelo TI e arquivos que sejam armazenados no servidor da IES;
- IV - Material de Consumo: CDs, formulários, papéis, cartuchos e toners para impressoras, etc.

Art. 5º Faz parte da TIC:

- I – Área administrativa que se constitui por todos os órgãos administrativos com exceção dos ambientes de ensino, pesquisa e extensão;
- II – Administrador de Sistemas e da rede, que pode ser um técnico com a função de gerenciar esta, e, os recursos do TIC do campus e, o que a ela está conectada;
- III - Usuário é a pessoa que utiliza os recursos de TIC da IES.

CAPÍTULO IV

DOS PROCEDIMENTOS GERAIS

Art. 6º São procedimentos gerais para o uso de recursos:

- I - Todos os recursos de TI são disponibilizados como ferramentas de apoio às atividades de ensino, pesquisa e extensão e para uso exclusivo no desenvolvimento dos trabalhos e tarefas vinculadas à IES;
- II – O termo de licença de uso de *software* corporativo ou específico das áreas e

suas mídias devem ser guardados;

III - A comunicação oficial eletrônica deve ser realizada por e-mail institucional;

IV - As informações produzidas, armazenadas e controladas pelos sistemas corporativos são de propriedade da IES, sendo proibido o seu repasse e/ou disponibilização, sem a autorização da autoridade competente, ressalvado os casos previstos em lei;

V – Os computadores deverão dispor de *software* de segurança composto por antivírus, *anti-spyware*, *firewall* ou outros, especificados e definidos, sendo atualizados e ativados automaticamente na inicialização dos sistemas;

VI - A garantia na integridade de dados e de informações deve ser assegurada mediante a execução de programas de computadores que atendam as normas e padrões de segurança estabelecidos pela IES;

VII – É passível de responsabilização, sem prejuízo às outras ações penais, a utilização de meios para burlar as normas definidas pela política de segurança da informação e de recursos de TI estabelecidas pela IES;

VIII - Todas as informações e registros de acessos (*logs*) contidos nos recursos e disponibilizados pela IES podem ser utilizados por meio de autorização do responsável.

CAPÍTULO V

DAS COMPETÊNCIAS E RESPONSABILIDADES

Art. 7º Compete à IES:

I - A gestão e a supervisão do sistema de informação e dos recursos computacionais de processamento, armazenamento e de transmissão de dados da FaHol;

II – Instalar na área administrativa, nos equipamentos para os usuários, os programas de computador necessários ao desenvolvimento de suas atividades, considerando o sistema operacional e programas específicos;

III – Usar ferramentas para acompanhar o parque de informática da área administrativa, de uso acadêmico e da pesquisa, ensino e extensão, mantendo a legalidade das licenças de *software* e atualizações de *hardware*;

IV – Liberar, monitorar, gerenciar e auditar o acesso dos aplicativos, sistemas, serviços, ativos de TI, violação, quebra de senhas nos recursos de TI existentes;

- V – Definir normas, aplicação, regulamentação, concessão de acessos, mecanismos de segurança, para o adequado funcionamento dos recursos de TI;
- VI – Monitorar o tráfego e controle de utilização dos recursos de rede e serviços disponibilizados aos usuários;
- VII - Instalar e desinstalar *software*, agentes de gerenciamento e monitoramento de acordo com a legislação vigente, excetuando-se os de uso acadêmico e de pesquisa;
- VIII - Monitorar suspeitas ou riscos à segurança aos ativos de TI, como a infecção por vírus, vazamento de informações, engenharia social nociva, ou outra forma existente que venha a ser desenvolvida;
- IX - Usar sistema de segurança, ou qualquer mecanismo que julgar mais adequado, para a realização de auditoria e controle dos recursos de TI da IES;
- X - Manter licenças e/ou mídias de softwares originais adquiridos pela FaHol e fazer cópias para a IES, mas não permitir que sejam copiados por terceiros ou instalados em computadores não autorizados;
- XI - Manter e disponibilizar informações cadastrais atualizadas de Professores e usuários autorizados, ratificando o conhecimento e a concordância deste e de outras normativas;
- XII - Manter a confidencialidade e integridade das informações sob sua responsabilidade dos dados de usuários e códigos de acesso a recursos de TIC;
- XIII – Realizar a manutenção preventiva e corretiva do parque de equipamentos;
- XIV - Manter a rede local em funcionamento e garantir a segurança de recursos de TIC;
- XV - Manter, na Unidade, um registro das ocorrências de violação dos regulamentos;
- XVI - Comunicar imediatamente à Direção Geral, qualquer dano ou extravio de material de consumo e mobiliário diretamente ligado à informática;
- XVII - Dar ciência e divulgar este regulamento a todos os usuários;
- XVIII - Respeitar e seguir os procedimentos padronizados para a administração de recursos de TIC definidos pelos órgãos superiores da IES;
- XIX - Providenciar mecanismos para controle, extinção ou bloqueio de conta;
- XX – Acompanhar e participar das mudanças de *layout* que possam interferir na estrutura física e/ou lógica da rede de computadores;

XXI - responsáveis pela administração dos recursos de TIC possuem autorização para usando sistemas de auditoria e segurança ou qualquer mecanismo que julgarem mais adequados para a realização de auditoria e controle, informando seus superiores. No entanto, todos os privilégios individuais e direitos de privacidade dos usuários deverão ser preservados, sendo que os mesmos deverão ser notificados das decisões tomadas;

XXII – Definir prioridades em função de regras internas de atendimento por nível de serviços, estabelecidas pela Equipe de TI.

Art. 8º As mudanças na rede de dados institucionais da IES só poderão ser efetuadas pela Equipe de TI, incluindo:

- a) mudança de endereços de rede;
- b) instalação e reconfiguração de roteadores, *switches* ou outros equipamentos de comunicação;
- c) alteração de configurações das estações de trabalho;
- d) disponibilização e alteração de servidores;
- e) inclusão ou configuração de equipamentos de acesso remoto e similares.

CAPÍTULO VI DA AUTORIZAÇÃO

Art. 9º Para atividades de ensino, pesquisa, extensão, administração e outras atividades de interesse da FaHol, que estiverem de acordo com os seus regulamentos.

Art. 10 Serão autorizados: funcionários, docentes e técnico-administrativos ativos e discentes em situação regular junto às Unidades.

Art. 11 A Inatividade do acesso à conta ocorre quando o tempo máximo não for justificado em 6 (seis) meses.

CAPÍTULO VII DAS RESPONSABILIDADES DOS USUÁRIOS

Art. 12 São responsabilidades do usuário:

I - Reconhecer e honrar a propriedade intelectual e os direitos autorais, de acordo com a legislação vigente;

II – Utilizar os recursos com sensatez não criando ações que prejudiquem ou bloqueiam outras pessoas a terem acesso aos recursos;

III - Integridade e confiabilidade das informações usadas pelo usuário:

a) estar ciente do potencial e das consequências da manipulação de informações, principalmente as eletrônicas e as informações armazenadas, exigindo cuidado, entendimento e verificação da integridade das informações;

b) não confiar em informações sem antes verificar diretamente ao possível remetente da mensagem, do arquivo ou de qualquer tipo de dado;

c) O usuário responderá pela segurança e integridade das informações da FaHol armazenadas nos recursos de TIC sob sua responsabilidade;

d) O acesso do *login* do usuário permite, usar *softwares* homologados pela FaHol, executar cópias de segurança e controlar o acesso aos recursos sob seu uso, sendo de responsabilidade do usuário qualquer dispositivo ou programa que não pertença à FaHol e que venha a ser conectado, por meio físico ou virtual, às estações de trabalho, rede, sites ou outras plataformas virtuais;

IV - Responsável pelo uso de sua conta de acesso aos recursos de TIC, senha e outros tipos de autorização, estes, são de uso particular e intransferível, sendo ilícito **acesso** compartilhado, salvo em situações especiais que a FaHol julgar necessárias e dentro de prazos curtos e pré-determinados;

V – A senha é de uso obrigatório e o usuário é responsável pelo zelo, confidencialidade e manutenção de sua senha, podendo responder por ações indevidas que vierem ser efetuadas, por outrem, a partir de sua conta de acesso;

VI – Ao deixar de ser membro da IES (como funcionário, colaborador ou estudante), o acesso aos recursos de TIC será cancelado;

VII – O contato do estudante após seu cancelamento de acesso aos recursos de TIC poderá ser realizado pela opção “Egresso” ou “Fale Conosco” na página da IES;

VIII - Os dispositivos do serviço de correio e de acessos aos recursos de TIC precisam de autorização dos administradores de rede e obedecer aos procedimentos estabelecidos pela IES;

IX - É de responsabilidade do usuário todo e qualquer recurso de TI disponibilizado para o desempenho de suas atividades profissionais ou acadêmicas.

CAPITULO VIII

DO ACESSO À REDE DE COMUNICAÇÃO DE DADOS

Art. 13 O acesso e comunicação:

I - O acesso a rede de comunicação dos dados deve ser usado para o desempenho das atividades condizentes ao vínculo do usuário com a instituição, o uso inadequado é passível de auditoria;

II - O acesso e a utilização dos serviços disponibilizados pela Equipe de TI serão efetuados mediante *login* (usuário e senha) de uso pessoal;

III - A criação de *login* para os usuários é de responsabilidade da secretaria;

IV - A conexão e/ou utilização de equipamentos de TI para acesso à rede de comunicação de dados ou qualquer outra solução que estabeleça conexão com a rede local e com outras, deverá ser autorizada pela Equipe de TI;

V - O acesso remoto à rede interna da IES deverá ser solicitado pela chefia imediata e Direção Geral e disponibilizado pela Equipe de TI.

CAPITULO IX

DO USO DA INTERNET

Art. 14 O acesso à internet:

I – Deve ser usado na execução das atividades desenvolvidas na IES, para outras finalidades deverão ser aprovadas pela IES;

II – Deve ser realizado por meio de navegadores recomendados pela Equipe de TI;

III - A FaHol reserva-se o direito de bloquear o acesso a arquivos e páginas que exponham a rede a riscos de segurança ou que comprometam o desempenho dos equipamentos de informática;

IV - É permitido o uso das redes sociais, ferramentas de comunicação instantânea,

porém não priorizado, podendo ser bloqueado a pedido da IES conforme critério da equipe de TI;

V – O uso da Internet em salas de aula e laboratórios acadêmicos deverá seguir as regras estabelecidas, em consonância com o presente Regulamento.

CAPÍTULO X DAS PROIBIÇÕES

Art. 15 São condutas inadequadas consideradas infrações de natureza **LEVE**:

I - Comunicação indesejada: entrar em contato várias vezes com uma ou mais pessoas para perturbar, enviando mensagens (quando não existe uma proposta de comunicação ou quando o receptor expressa o desejo de finalizar a comunicação);

II - Exercer atividades particulares ou em benefício de organizações que não tenham relação com a IES;

III - Causar danos acidentais aos equipamentos seja por manipulação de líquidos, alimentos ou por qualquer outra forma que caracterize imprudência, imperícia ou negligência. A aplicação da punição LEVE não exime o culpado da reparação material do equipamento danificado;

IV – Realizar campanhas políticas externas ou propaganda de qualquer espécie;

Art. 16 São condutas inadequadas e consideradas infrações de natureza **MÉDIA**:

I – Instalar, alterar ou remover *software* ou alterar a configuração de *hardware* e de *software* da estação de trabalho sem autorização da equipe TI;

II - Copiar, alterar ou remover arquivos de terceiros sem autorização explícita, com exceção dos casos especiais protegidos por lei;

III - Utilizar programas do tipo *peer-to-peer* (P2P), de compartilhamento de arquivos, não será permitida na IES.

Art. 17 São condutas inadequadas e consideradas infrações de natureza **GRAVE**:

I – Importunar, difamar, caluniar ou molestar pessoas e outros. São indícios de importunos: perturbar, amedrontar, ameaçar ou ofender pessoas usando linguagem, imagem, ou qualquer outro mecanismo e/ou material para fazer ameaças que comprometam a integridade física ou moral do receptor ou de sua família;

- II - Indisponibilizar ou sobrecarregar recursos de TIC de forma intencional;
- III - Identificar-se como outra pessoa ou esconder sua identidade;
- IV - Receber benefícios para si ou para terceiros, de qualquer ordem ou espécie, por intermédio da utilização dos recursos de TI da IES;
- V – Usar como para fins particulares ou de recreação serviços que sobrecarreguem as redes de computadores, como: escuta de rádio, páginas de animação, telefone via Internet, jogos, salas de bate papo (chat), downloads, acesso a sites de conteúdos impróprios sexuais, etc.

Art. 18 São condutas inadequadas e consideradas infrações de natureza **GRAVÍSSIMA:**

- I - Copiar, alterar, distribuir ou remover recursos computacionais, sistemas, documentos ou informações de propriedade da IES ou por ela administrados, que sejam de acesso restrito;
- II - Prejudicar ou causar danos às atividades de ensino, pesquisa, extensão ou administrativas;
- III - Apoderar-se dos conteúdos privados da FaHol e de outros;
- IV - Violar direitos e questões relacionadas à propriedade intelectual, propriedade industrial, licenças de uso em que a IES for parte;
- V - Interferir ou tentar interferir no funcionamento de equipamentos ou serviços de terceiros, externos à IES;
- VI – Monitoramento não autorizado de mensagens eletrônicas ou de qualquer transmissão de dados;
- VII - Destruir, alterar, desmontar, desconfigurar, impedir o acesso de direito ou interferir na integridade dos recursos computacionais que causem prejuízos à IES;
- VIII - Invadir a privacidade de pessoas ou entidades vinculadas à IES, considerando os autores, criadores, usuários ou responsáveis pelos recursos computacionais;
- IX - Violar ou tentar violar os sistemas de segurança dos recursos computacionais da IES e quebrar ou tentar quebrar a identificação ou senhas;
- X - Criar ou propagar vírus, danificar serviços e arquivos;
- XI - Utilizar direitos especiais de acesso já extintos com o término do período de ocupação de cargo ou função.

Art. 19 Qualquer violação ou suspeita dos artigos 14, 15, 16 e 17, deverá ser comunicada imediatamente ao responsável da área onde o fato tenha ocorrido, a não comunicação configura conivência com o ato, respondendo pelo mesmo.

CAPÍTULO XI DAS PENALIDADES

Art. 20 As penalidades a serem aplicadas por infração à presente Ordem Interna são redução ou eliminação, temporárias ou permanentes, aos Recursos Computacionais da IES. São penalidades:

I - **Penalidade Leve:** quando a violação das normas descritas referente ao Artigo 14 resultará na revisão temporária de privilégios de acesso ao recurso que originou a infração, por, no mínimo, 7 dias e, no máximo, 3 meses, ou outras penalidades que a comissão julgar pertinentes;

II – **Penalidade Média:** quando a violação das normas descritas referente aos itens, o Artigo 15 resultará na revisão temporária de privilégios de acesso ao recurso que originou a infração por, no mínimo, 14 dias e, no máximo, 6 meses, ou outras penalidades que a comissão julgar pertinentes;

III – **Penalidade Grave e/ou Reincidente:** quando a violação das normas descritas referente aos itens Artigo 16 resultará na revisão temporária de privilégios de acesso ao recurso que originou a infração por, no mínimo, 21 dias e, no máximo, 1 (um) ano, ou outras penalidades que a comissão julgar pertinentes;

IV – **Penalidade Gravíssima:** quando a violação das normas descritas referente aos itens Artigo 17 resultará no cancelamento de todos os acessos e poderá ser responder civil e criminal.

V - Todas as demais violações das normas e regulamentos, ainda que não expressamente descritas, serão punidas com revisão temporária de privilégios de acesso aos recursos de TIC na IES, após avaliação da gravidade da infração;

VI - Os incidentes que forem considerados crimes, de acordo com a legislação federal, estadual e municipal, deverão ser denunciados pela Unidade às autoridades competentes. O possível desconhecimento deste regulamento por parte do usuário não o isenta das responsabilidades e das sanções aplicáveis, nem pode minimizar as medidas cabíveis;

VII - Os usuários que receberem penalidades poderão apelar aos Diretores.

CAPITULO XII

DO CONTROLE DO PARQUE DE INFORMÁTICA E ARMAZENAMENTO

Art. 21 Do controle:

- I - As requisições para aquisições de *hardware* e *software* para área administrativa deverão ser homologadas pelo responsável pela TI;
- II - Qualquer alteração/atualização no Parque de Informática, o responsável pela solicitação deverá comunicar por escrito a Direção Geral a respeito da nova configuração do equipamento e solicitar a aprovação;
- III - As áreas interessadas na aquisição de recursos de informática poderão solicitar à Equipe de TI auxílio para especificação.

Art. 22 Do armazenamento de arquivos:

- I - Os arquivos institucionais das áreas administrativas devem ser armazenados nos servidores de dados e, sempre que possível, os arquivos devem ser criptografados;
- II – A IES não autoriza o *backup* de material particular nos discos rígidos locais dos equipamentos de Informática;
- III - Equipe de TI deve manter o *backup* dos dados existentes nos servidores da rede;
- IV – A IES não autoriza o uso ou *download* de *softwares* não vinculados às atividades administrativas e serviços armazenados nos servidores e estações de trabalho;
- V - Informação confidencial de uso institucional, que se encontre armazenada em meio eletrônico, deverá ser protegida contra roubo ou acessos não autorizados, sendo recomendado seu armazenamento em local seguro.

CAPÍTULO XIII

DAS DISPOSIÇÕES GERAIS E TRANSITÓRIAS

Art. 23 Das disposições:

- I – A Equipe de TI, com autorização do Diretor Geral ou Responsável de TI, poderá

suspender temporariamente os acessos por suspeita de violação das normas de segurança ou por uso indevido dos recursos de TI;

II - O uso de qualquer recurso computacional da FaHol está sujeito à legislação vigente, às normas internas do Regimento Geral e, às normas para uso da Internet recomendadas pelo Comitê Gestor da Internet Brasil;

III - As áreas acadêmicas podem definir condições de uso específicas para laboratórios e recursos de TI sob seu controle, ficando sob a responsabilidade do respectivo Departamento Acadêmico ou Coordenação de Curso, Programa de Pós-Graduação qualquer dano que venha ser gerada a instituição;

IV – Os Casos Omissos serão resolvidos pela Diretoria, cabendo recurso ao CONSUP;

V – O uso de acesso privilegiado dos recursos de TIC, só pode ser usado para o exercício de tarefas oficiais, por meio de atos administrativos. As informações obtidas por meio de direitos especiais e privilégios devem ser tratados como privativas e totalmente confidenciais pelos usuários, que responderão por qualquer uso indevido;

VI - Todos os equipamentos conectados à FaHol, bem como os sistemas desenvolvidos, estão sujeitos a normas descritas neste documento;

VI – Baixas Patrimoniais, referentes a equipamentos de TI, só deverão ser realizadas após passar por avaliação e não houver conserto, o responsável da TI deverá encaminhar um documento à Direção Geral, e somente após a aprovação é que o equipamento poderá ser devidamente descartado;

VII – Este Regulamento entrará em vigor após sua deliberação pelo CONSUP e sua publicação.

Curitiba, 28 de junho 2020

GLOSSÁRIO

Para efeito deste regulamento considera-se:

Acesso Remoto: é uma conexão remota de um computador ou de qualquer outro tipo de dispositivo.

Ativos de TI: são informações disponibilizadas e se constituem de todos os conteúdos que são produzidos, contextualizados e compartilhados via computação local por servidores da IES.

Antivírus: programa que permite identificar e eliminar vírus em computadores.

Anti-spyware: é um software de segurança que detecta e remove *adwares* e *spywares*.

Backup: cópia de segurança de dados realizada para salvaguardar arquivos.

Download: transferência de dados de um computador remoto para um computador local.

Engenharia social: Termo referente à manipulação e persuasão de pessoas, para obtenção de informações restritas.

Estação de Trabalho: equipamento utilizado pelo usuário para desenvolver suas tarefas. Pode ser um *notebook*, computador de mesa, etc.

Firewall: é a segurança baseada em *hardware* ou *software* (mais comum) que, a partir de um conjunto de regras ou instruções, analisa o tráfego de rede para determinar quais operações de transmissão ou recepção de dados podem ser executadas.

Hardware: parte física do computador é o conjunto de componentes eletrônico.

HTTP (Hyper-Text Transfer Protocol): protocolo de comunicação padrão da Internet controla o envio de uma página em *HTML* de um servidor para um computador.

Incidente de Segurança da Informação: indicação de eventos, indesejados ou inesperados, que podem ameaçar a segurança da informação.

Login: identificação do usuário perante os sistemas de informação, de caráter pessoal, intransferível.

Logoff: término no uso de um sistema computacional.

Logon: identificação do usuário junto com palavra chave para início do uso de um sistema computacional.

Malware: termo genérico que se refere a todos os tipos de programa que executam

ações maliciosas em um computador. Exemplos de códigos maliciosos são os vírus, *worms*, *bots*, cavalos de tróia, *spywares*, *rootkits*, etc.

Navegadores: Programas de computadores utilizados para acesso a Internet, também conhecido como **browser**.

Peer-to-Peer: arquitetura de sistemas distribuídos, caracterizada pela descentralização das funções na rede, onde cada computador realiza funções de servidor e de cliente. Normalmente utilizado para distribuir arquivos eletrônicos;

Recursos computacionais; são os equipamentos, as instalações ou bancos de dados direta ou indiretamente administrados, mantidos ou operados pela IES.

Rede Corporativa: computadores e outros dispositivos interligados que compartilham informações ou recursos da IES.

Senha de Acesso: palavra chave utilizada para autenticação do usuário fornecendo acesso aos recursos de TI, tem caráter pessoal, intransferível, secreto e que deve ser periodicamente alterada, em conformidade com a norma específica de segurança.

Servidor: computador que fornece serviços ou recursos para outros computadores.

Sistemas Corporativos: todos os sistemas desenvolvidos ou gerenciados pela equipe de desenvolvimento do Departamento de Sistemas de Informação disponibilizados a IES.

Software: conjunto de programas e aplicativos usados em uma estação de trabalho, homologado.

Spam: termo empregado para referir-se aos e-mails não solicitados, que geralmente, mas não necessariamente, são enviados para um grande número de pessoas.

Switch: dispositivo utilizado em redes de computadores para reencaminhar transmissões entre os diversos equipamentos.

Upload: transferência de dados de um computador local para um computador remoto.

Usuário: pessoa autorizada que utiliza algum recurso computacional definido e disponibilizado pela FaHol.