FACULDADE PAULISTA
DE COMUNICAÇÃO

Infraestrutura Tecnológica

2020

Infraestrutura Tecnológica

Sumário

Inventário de Recursos de Tecnologia

1. Setores Acadêmicos
   1.1. Laboratório de Informática

13 computadores modelo SONY com Processador Pentiun(R) Dual Core CPU E5400 - 2.7GHz com frequência de clock de 2.93GHz, HD 300GB, 2GB SDRAM-DDR3, Monitor AOC, unidade DVD/RW – SATA, com acesso à Internet em banda larga. **Softwares instalados:** Windows 7; BR Office; DosVox; Arduino; 7zip; DEV C++; Adobe Photoshop CS6; Kurupira; Webfilter Free, Scratch 2 e 3; VLC player e Teamviewer.

8 iMac 27 polegadas, resolução de 5120 x 2880 e suporte para um bilhão de cores 500 nits de brilho, processador Intel Core i5 de dois núcleos e 2,3 GHz (Turbo Boost até 3,6 GHz), DDR4 de 8 GB com 2133 MHz, Disco rígido de 500 GB (5400 rpm), placa gráfica Intel Iris Plus Graphics 640, câmera de vídeo e áudio integrados. Acesso à Internet em banda larga. **Softwares instalados:** Davinci Resolve, Gimp, Inkscape

   1.2. Laboratórios de Rádio

Estúdio de Rádio (2º andar)

- **1 computador** com Processador Intel Core I5 - 4.7GHz HD SSD 120GB, 8GB SDRAM-DDR3, Monitor Ultra Wide LG LED 25 polegadas;
- **Mesa De Som Yamaha MG 32 14FX** - Mixer Analógico com 32 canais de entrada: 24 mono (mic/linha), 4 canais estéreo (linha), 24 pré-amplificadores de microfone com phantom power, Insert I/O nos canais mono 2 Processadores de Efeitos SPX com 16 presets cada, 14 Barramentos de saída (4 estéreo + 6 auxiliares + Saída Máster ST) 6 auxiliares (4 pré/pós-fader, 2 pós fader para efeito) 3 bandas de equalização (semi-paramétrico nos médios), etrada para Talkback, LPF chaveado em todas as saídas mono;
- **1 Mesa de Som Novik Neo NVK-800P USB**, 2 canais estéreo, efeitos Delay / Reverb internos, MP3 Player com controles individuais e de exibição, 3 bandas Equalizador por canal, 7 bandas Equalizador gráfico para a saída mestre para monitorar através de fones de ouvido com função PFL, 4 canais com Phantom Power + 48V e pré-amplificador de microfone, 2 canais estéreo balanceados, DSP com efeitos internos Delay / Reverb, Controle de fader dual do master estéreo L + R;
- **4 Microfones** Studio GT649-Lorben com Pop Filter anti puff;

- **1 fone de ouvido** AKG K414P, resposta de frequência: 13Hz 27kHz Impedância: 32 Ohms Sensibilidade: 125dB SPL/V

Ilha de Edição do Estúdio de Rádio (2º andar)

- **1 computador** com Processador Intel Core I5 - 4.7GHz HD SSD 120GB, 8GB SDRAM-DDR3, Monitor Ultra Wide LG LED 25 polegadas;
- **1 fone de ouvido** AKG K414P, resposta de frequência: 13Hz 27kHz Impedância: 32 Ohms Sensibilidade: 125dB SPL/V

1.3. Laboratórios de TV e Imagem

Estúdio TV e Imagem (2º andar)

- **1 computador** com Processador Intel Core I5 - 4.7GHz HD SSD 120GB, 8GB SDRAM-DDR3, Monitor Ultra Wide LG LED 25 polegadas;
- **1 Switcher ATEM mini**, 4 Entradas de Vídeo, 2 saídas, entrada para 2 miniconectores estéreo tipo jack de 3,5 mm, 4 entradas de vídeo HDMI tipo A, HD de 10 bits alternável, 2 canais de áudio embutido, ressincronização das entradas de vídeo Em todas as 4 entradas HDMI, Conversor de taxa de quadro e formato, saída USB-C 2.0.
- **1 Grua Maxi MX3:** tripé com doly, 2 lanças de 1,5 metros, Girocam para câmeras emonitor de 7 polegadas

Estúdio de áudio e Ilha de áudio (2º andar)

- **1 computador** com Processador Intel Core I7 Turbo Bboost 3770 – 3,9GHz, 16GB SDRAM-DDR3, HD SSD 240 GB SATA, placa de vídeo GTX 1660 6 GB, monitor Sansung Ultra HD 28 polegadas 4K;
- **1 Mesa de Som** Novik Neo NVK-800P USB, 2 canais estéreo, efeitos Delay / Reverb internos, MP3 Player com controles individuais e de exibição, 3 bandas Equalizador por canal, 7 bandas Equalizador gráfico para a saída mestre para monitorar através de fones de ouvido com função PFL, 4 canais com Phantom Power + 48V e pré-amplificador de microfone, 2 canais estéreo balanceados, DSP com efeitos internos Delay / Reverb, Controle de fader dual do master estéreo L + R.
- **2 Microfones** Studio GT649-Lorben com Pop Filter anti puff;
- **1 fone de ouvido** AKG K414P, resposta de frequência: 13Hz 27kHz Impedância: 32 Ohms Sensibilidade: 125dB SPL/V

Estúdio de Comunicação Avançado (ECA) (andar térreo): **3 câmeras** de alta definição Pan/Tilt/Zoom (PTZ), modelo EVI-HD1

Ilha de Edição do Estúdio de Comunicação Avançado

- **3 computadores** com Processador Intel Core I7 Turbo Bboost 3770 – 3,9GHz, 16GB SDRAM-DDR3, HD SSD 240 GB SATA, placa de vídeo GTX 1660 6 GB;
- **1 monitor** Sansung 28 polegadas;
- **5 monitores** Philips 42 polegadas;
- **1 mesa de corte** Sony AG-MX70 de 8 canais;
- **1 Mesa de Corte** Panasonic Av-hs400a com 06 entradas SDI e 04 entradas de vídeo composto;
- **1 mesa de som Yamaha** – Digital Mixing Console 01V 16 canais;
- **2 Blackmagic Design Atem** 1 M/e Production Studio 4k: 10 x 6G-SDI & 1 x HDMI Inputs (SD/HD/4K), Tri-Sync/Blackburst Ref. Sync Input, 10 x Built-In Frame Synchronizers, Multiview Monitoring in HD, Program Outputs in SD/HD/4K HD, 4 x Keyers Total: 3 x Luma, 1 x Chroma, 12 x Channel Audio Mixer;
- **1 Compix Chanel Brander**: HD-SDI / SD-SDI - 1 canal

1.4. Audiovisual

- **2 Datashows** EPSON 3 LCD HDMI: 2700 lumens em cores, 2700 ANSI lumens em branco, Resolução XGA, HDMI, Wireless;
- **4 câmeras CANON** EOS T7: 11 funções personalizadas com 33 definições ajustáveis com a câmera, Cena Automática Inteligente e Estilo de Imagem Automático, compatível com a linha completa de lentes EF/EF-S e flashes Speedlite da Canon, gravação simultânea em RAW + JPEG, Live View Mode, correção da iluminação periférica, Impressão direta compatível com impressoras que possuem Pict Bridge, taxas de proporção pré-definidas: 4: 3, 1: 1 16: 9 ou 3: 2, compatível com USB 2.0 Hi-Speed;
- **2 microfones de lapela** BY-M1 tipo Condensador Omni-direcional, faixa de freqüência: 65Hz-18 kHz, Sensibilidade: -30dB +/-3dB/0dB = 1 V/Pa, 1 kHz, Conector de 3.5mm (1/8) e 4-pole plug ouro;
- **5 Rádios Comunicador** HT Profissional UHF VHF Baofeng BF-UV82, potência de Saída: 8W, fonte da Base: 0.25A, tensão operacional: DC 7.4V, consumo no Stand by: 380mA, Frequência: VHF 136-174MHz / UHF 400-520MHz, impedância da Antena: 50 Ohm (Dual Band).

1.5. Biblioteca

- 1 computador modelo CCE com processador Pentiun® Dual Core CPU E5400 – 2.7GHz com frequência de clock de 2.93GHz, HD 300GB, 2GB SDRAM-

DDR3, Monitor AOC, unidade DVD/RW – SATA, com acesso à Internet em banda larga;

- 10 iPads para consulta dos alunos.

1.6. Salas de aula (7º andar)

- **Sala 71:** 1 Datashow EPSON 3 LCD HDMI: 2700 lumens em cores, 2700 ANSI lumens em branco, Resolução XGA, HDMI, Wireless;
- **Sala 73:** 1 Datashow EPSON 3 LCD HDMI: 2700 lumens em cores, 2700 ANSI lumens em branco, Resolução XGA, HDMI, Wireless;
- **Sala 74:** 1 Datashow EPSON 3 LCD HDMI: 2700 lumens em cores, 2700 ANSI lumens em branco, Resolução XGA, HDMI, Wireless;
- **Sala 76:** 1 Datashow EPSON 3 LCD HDMI: 2700 lumens em cores, 2700 ANSI lumens em branco, Resolução XGA, HDMI, Wireless.

1.7. Salas de aula (11º andar)

- **Sala 111:** 1 Datashow EPSON 3 LCD HDMI: 2700 lumens em cores, 2700 ANSI lumens em branco, Resolução XGA, HDMI, Wireless;
- **Sala 112:** 1 Datashow EPSON 3 LCD HDMI: 2700 lumens em cores, 2700 ANSI lumens em branco, Resolução XGA, HDMI, Wireless;
- **Sala 113:** 1 Datashow EPSON 3 LCD HDMI: 2700 lumens em cores, 2700 ANSI lumens em branco, Resolução XGA, HDMI, Wireless;
- **Sala 114:** 1 Datashow EPSON 3 LCD HDMI: 2700 lumens em cores, 2700 ANSI lumens em branco, Resolução XGA, HDMI, Wireless;

1.8. Pacote Office 365

A Faculdade Paulista de Comunicação possui uma parceria com a Microsoft, oferecendo a seus estudantes e docentes, acesso gratuito à solução completa do Office 365, que inclui o Office Online (Word, PowerPoint, Excel e OneNote), 1 TB de armazenamento no OneDrive, o Yammer e sites do SharePoint.

O estudante e colaboradores da FPAC, podem utilizar a ferramenta em até cinco dispositivos, como smartphones e tablets. Dessa forma, é possível o acesso aos programas em qualquer lugar e a qualquer momento, por meio da computação em nuvem, facilitando seus estudos e aumentando sua produtividade. O Licenciamento inclui os seguintes programas e serviços:

- Azure Active Directory Basic para EDU
- School Data Sync (Plano 1)
- Stream for Office 365
- Microsoft Teams
- Microsoft StaffHub

- Flow para Office 365
- PowerApps para o Office 365
- Azure Rights Management
- Microsoft Forms (Plano 2)
- Microsoft Planner
- Sway
- Gerenciamento de Dispositivo Móvel do Office 365
- Yammer for Academic
- Office Online Educacional
- Skype for Business Online (Plano 2)
- Sharepoint Plano 1 para EDU
- Exchange Online (Plano 1)
- OneDrive (1TB de armazenamento)

2. Setores Administrativos

2.1. Atendimento ao aluno

- **2 computadores** modelo CCE com processador Pentiun(R) Dual Core CPU E5400 - 2.7GHz com frequência de clock de 2.93GHz, HD 300GB, 2GB SDRAM-DDR3, Monitor AOC, unidade DVD/RW – SATA, com acesso à Internet em banda larga. **Softwares instalados:** Windows 10; BR Office; Pacote Office 365.
- **2 impressoras** HP LaserJet Pro MFP M426fdw

2.2. Secretaria

- **2 computadores** modelo CCE com processador Pentiun(R) Dual Core CPU E5400 - 2.7GHz com frequência de clock de 2.93GHz, HD 300GB, 2GB SDRAM-DDR3, Monitor AOC, unidade DVD/RW – SATA, com acesso à Internet em banda larga. **Softwares instalados:** Windows 10; BR Office; Pacote Office 365.
- **2 impressoras** HP LaserJet Pro MFP M426fdw.

2.3. Painel de Divulgação/Mídia Eletrônica

- **3 Televisores** Sansung 29 polegadas

2.4. Sistema de Comunicação / Telefonia

O sistema de Telefonia da Faculdade Paulista de Comunicação está baseado em Nuvem, através da Jive Communications, com plataforma redundante de entrega pelos centros de dados localizados em São Paulo e no exterior: Atlanta, Chicago, Dallas, Londres, Los Angeles, Nova York, Seattle, dentre outros,

garantindo escalabilidade e confiabilidade na disponibilidade e manutenção dos serviços.

Intranet

A área de intranet encontra-se integrada ao Portal Institucional, gerido pelo sistema Foxxnet. O objetivo básico da rede de comunicação interna é a disponibilização de informações corporativas com o intuito de integrar os colaboradores, facilitar os processos comunicacionais e informativos e conceituar a Instituição junto a este público. Esse meio online de comunicação com os colaboradores disponibiliza informações acadêmicas, sistema de solicitações de trabalhos, entre outros dados necessários ao desenvolvimento do trabalho interno. Além de informação e notícias, essa área do Portal também disponibiliza manuais e regimentos com procedimentos burocráticos e administrativos específico de cada setor, destinados a normatizar os fluxos internos.

Outros setores importantes do Portal são o “Portal do Aluno” e a “Extranet”, onde estão disponíveis acesso a dados, ferramentas e serviços como acervo da biblioteca, link para matrícula, sua confirmação ou alterações, consulta ao horário de aulas, controle de presença, notas, requerimentos diversos, avisos gerais sobre os cursos e sobre a Faculdade, acesso a ferramentas e serviços de apoio, como a Biblioteca, outras informações sobre a vida acadêmica.

O Portal institucional fornece ainda, acesso a outros sites específicos de cursos de graduação, eventos e congressos, setores institucionais. Esses sites são desenvolvidos com o objetivo de informar, orientar e integrar o estudante e seus planejamentos seguem as mesmas premissas da política de comunicação da FPAC, tais como o atendimento as legislações educacionais, compromisso com a função social da Instituição, qualidade estética, estímulo à vida universitária integrada e construtiva, valorização da formação acadêmica ética e humanística, informações e orientações objetivas e funcionais.

Políticas de Contingência e Redundância

Para garantir a segurança dos dados, acesso ininterrupto às informações acadêmicas (24 x 7), bem como aos materiais de cursos presenciais e a distância, por intermédio da Plataforma Moodle, a Faculdade Paulista de Comunicação dispõe de dois servidores de hospedagem Enterprise SG-64**,** exclusivos para essa finalidade, com as seguintes características:

- Processador: Intel Xeon E5-1650v3 - 6 c / 12 t - 3.5 GHz / 3.8 GHz
- Memória: 64GB DDR4 ECC 2133MHz
- Disco: 2x2 TB
- Largura de banda: 1 Gbps

Ambos localizados nos datacenters da OVH, a segunda maior operadora de datacenters do mundo, garantindo segurança e alta disponibilidade, acima de 99,95% conforme SLA (*Service Level Agreement)*.

Serviços disponíveis nos servidores:

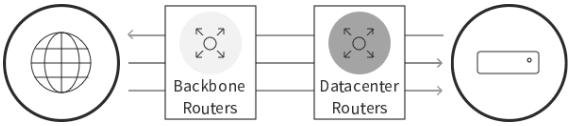
- 500 GB de espaço de backup;
- Área de configuração do cliente;
- API;
- Acesso root ao servidor;
- Acesso KVM/IPMI;
- Anti-DDoS;

Backup Storage

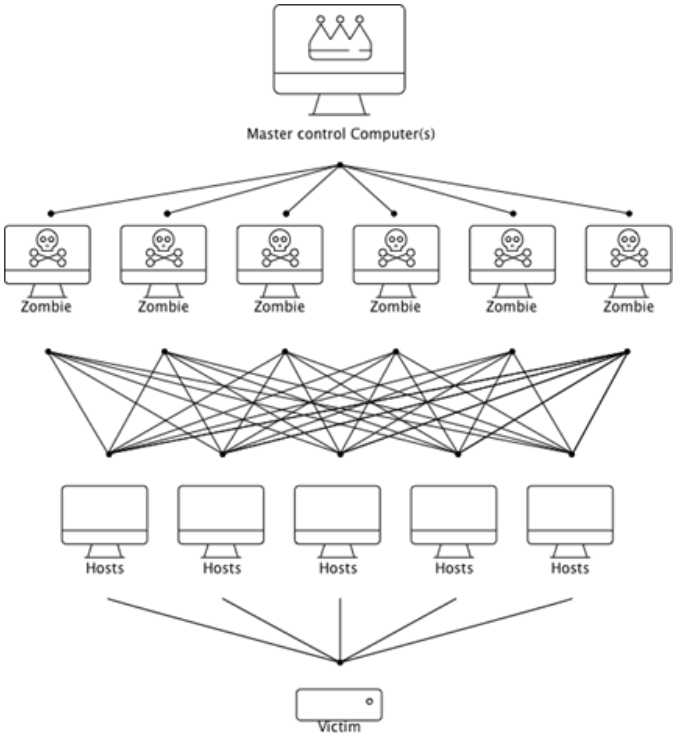
Para garantir a preservação da informação de forma confiável, a Faculdade Paulista de Comunicação possui uma infraestrutura de Backup com espaço de armazenamento de 500GB por servidor, realizado diariamente pelo processo incremental e semanalmente pelo processo integral no próprio Data Center. Para uma segurança adicional também é realizado um espelhamento em servidor local (localizado no Campus Lapa do Grupo Educacional Campos Salles) contando com o equipamento IBM Series Server, Intel Xeon E2, 8GB DDR4 2133MHz, 1TB.

Proteção Anti-DDoS

Para garantir a segurança máxima das suas infraestruturas, o conjunto dos servidores dedicados, utilizados pela Faculdade, incluem uma proteção anti-DDoS, assegurando a continuidade dos serviços e suas aplicações em caso de ataque. Com o aumento significativo do volume de dados na web, os ataques distribuídos de negação de serviço (DDoS) são cada vez mais frequentes.



Um ataque DDoS visa tornar um servidor, serviço ou infraestrutura indisponível. O ataque pode assumir várias formas: uma sobrecarga da largura de banda do servidor para o tornar indisponível ou um esgotamento dos recursos de sistema da máquina, impedindo-a de responder ao tráfego legítimo.



No momento de um ataque DDoS, é enviada uma série de pedidos ao mesmo tempo a partir de vários pontos da web. A intensidade deste “fogo cruzado” torna o serviço instável, e, no pior dos casos, indisponível.

Para combater esses ataques distribuídos de negação de serviço em específico, a OVH (Data Center utilizado pelo Grupo Educacional Campos Salles) criou o anti-DDoS. Em todos os serviços, são disponibilizados uma solução de migração baseada numa tecnologia única que combina três técnicas para:

- analisar todos os pacotes de forma rápida e em tempo real;
- desviar o tráfego de entrada do seu servidor;
- separar os elementos não legítimos dos restantes, para deixar passar o tráfego legítimo.

Load Balancer

O Load Balancer da OVH permite distribuir a carga das ligações aos seus serviços pelos diferentes datacenters da OVH. A capacidade da sua infraestrutura é ajustada ao volume

de tráfego. Resultado: tolerância às falhas, tempos de resposta otimizados e zero downtime.

Certificação SSL

Os sites da Faculdade contam com a certificação SSL (Secure Sockets Layer) para troca de informações sigilosas via Internet, emitida por DST Root CA X3 com validade até 30 de setembro de 2021 às 11:01:15

Estes recursos atendem as necessidades institucionais de maneira excelente, o plano de expansão da IES, o contrato firmado com empresas de alto nível garantindo condições de funcionamento de excelência para nossa comunidade acadêmica assim como seu pleno desenvolvimento educacional.

Infraestrutura de Execução e Suporte ao EaD

A equipe de TI da FPAC e o EaD atende de forma excelente nossa comunidade acadêmica. A equipe de TI presta atendimento a todas as equipes vinculadas ao EaD, incluindo demandas acadêmicas e administrativas. Também é responsável pelo gerenciamento do sistema operacional acadêmico.

As atividades realizadas a distância são propostas, acompanhadas e avaliadas por meio da Plataforma Moodle (Modular Object Oriented Distance LEarning) um dos mais conceituados sistemas de gerenciamento para cursos a distância, dispondo de um conjunto de ferramentas que podem ser selecionadas pela equipe de curso, de acordo os objetivos pedagógicos pretendidos, tais como: fóruns de discussão, chat, questionário, glossário, entre outras.

Disponibilidade e segurança dos serviços

Para garantir segurança aos usuários do EaD e alta disponibilidade, acima de 99,95% e (24 x 7), a Plataforma Moodle encontra-se hospedada em dois servidores distintos na OVH Datacenter, dispondo dos seguintes serviços: a) backup storage; b) proteção Anti-DDoS; c) load balancer e; d) certificação SSL, todos descritos no item 5.14.

É importante ressaltar que todos os sistemas estão hospedados em servidores já mencionados, garantindo segurança nos dados (nosso contrato com a empresa algar prevê o plano de contingência, redundância e expansão). Além disso, a equipe de TI trabalha com servidores de testes para o desenvolvimento e validação dos sistemas. Após a validação, as codificações dos projetos são enviadas para o repositório de projetos e, a seguir, são disponibilizadas no servidor de produção.

Políticas de Rede

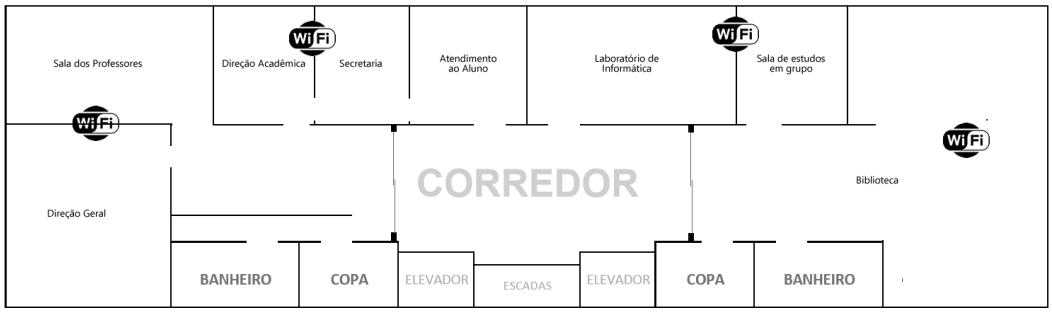
A Faculdade Paulista de Comunicação utiliza um grande número de ativos, essenciais para toda a comunidade Acadêmica. Assim, os recursos computacionais e de rede da FPAC e a informação através desses recursos precisam ser protegidos, como qualquer outro ativo importante para a Faculdade. Com relação à segurança da informação, implementamos Políticas que se caracterizam pela tentativa de manter a confidencialidade, a integridade e a disponibilidade da mesma, independentemente de onde ela esteja, residente em memória de máquinas e dispositivos, armazenada em disco ou em trânsito, salvaguardando a exatidão e completeza da mesma, dos métodos de processamento e garantindo que usuários obtenham acesso à informação e aos ativos correspondentes sempre que necessário e de acordo com a permissão atribuída a cada um.

Integram as Políticas de Segurança as seguintes normas:

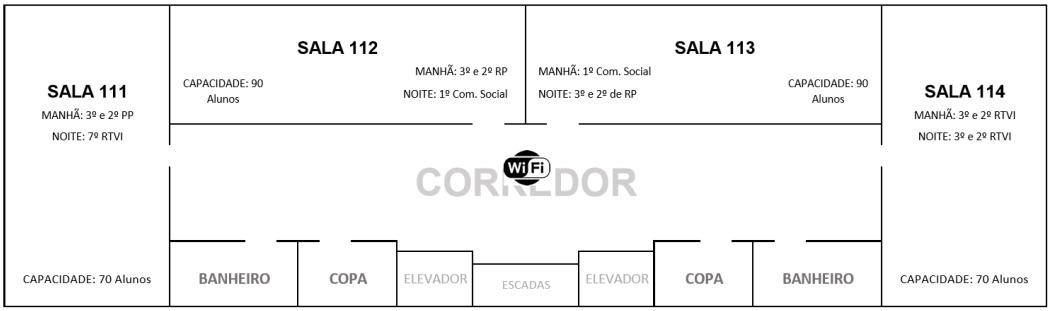
- PS-01 - Norma de Segurança (anexo I)
- PS-02 - Norma de Utilização da Rede (Anexo II)
- PS-03 - Norma para Serviços e Servidores WWW (Anexo III)
- PS-04 - Norma para Implantação e Utilização de Redes Móveis (Anexo IV)

Mapa de Pontos WiFi

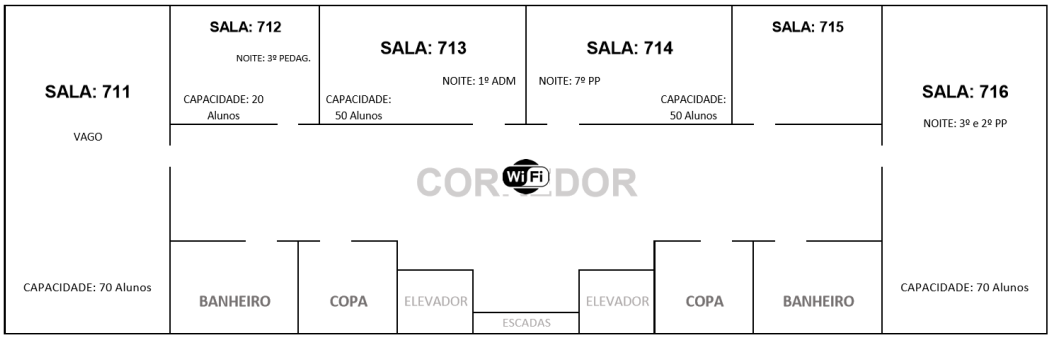
12º ANDAR



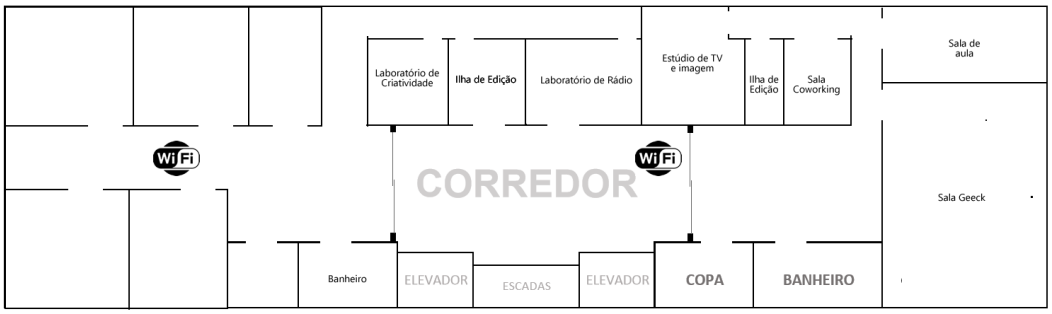
11º ANDAR



7º ANDAR



2º ANDAR



Regulamento e Normas de TI

Objetivo

Estabelecer os procedimentos para utilização correta dos recursos computacionais de propriedade da FPAC e colocados à disposição de seus colaboradores para o bom desempenho de suas atividades profissionais.

Abrangência

Esta norma compreende desde a utilização de equipamentos de informática, uso correto do e-mail, internet, intranet, extranet, até o acompanhamento e monitoramento de conteúdo e arquivos, previamente autorizados.

Responsáveis

Diretor de Tecnologia da Informação (TI).

Conceito

1. Recursos computacionais

São os equipamentos, as instalações ou banco de dados administrados, mantidos e operados pelo Departamento de Tecnologia da Informação (TI), tais como:

- Computadores e terminais de qualquer espécie, incluindo periféricos e acessórios;
- Impressoras;
- Cabeamento lógico, telefônico e elétrico que compõe as redes de computadores e de transmissão de dados;
- Softwares adquiridos ou desenvolvidos;
- Banco de dados ou documentos residentes em disco, fitas ou outros meios;
- Salas de computadores, laboratórios, escritórios e mobiliários.
- Equipamentos analógicos, como no-breaks, estabilizadores e filtros de linha.

Os Recursos computacionais da FPAC têm por finalidade oferecer condições adequadas e tecnologia avançada a seus colaboradores, buscando alcançar os objetivos da organização.

2. Usuário

Qualquer pessoa, autorizada, que utiliza, de alguma forma, algum recurso computacional da FPAC.

3. Atribuições

O Departamento de Tecnologia da Informação (TI) é responsável pela gestão dos Sistemas de Informação e dos recursos computacionais de processamento e de transmissão de dados da FPAC.

Para garantir a adequada utilização dos recursos computacionais da FPAC, fica autorizado aplicar penalidades aos que violarem a legislação em vigor e as dispostas nesta política.

Os usuários detêm as seguintes responsabilidades referentes ao uso dos recursos computacionais da FPAC:

- Não usar os recursos computacionais disponíveis para fins comerciais, pessoais ou quaisquer outros, senão para aqueles que sejam diretamente relacionados com as atividades e interesses da função e da FPAC;
- Não utilizar os recursos computacionais da associação, fora dela, exceto os equipamentos portáteis utilizados para este fim;
- Para utilizar qualquer recurso computacional da FPAC, o usuário deve antes obter uma autorização por escrito e assinar o termo de compromisso e o aditivo ao contrato de trabalho, no qual declara conhecer as normas em vigor e se compromete a cumpri-las;
- Toda conta de acesso (login) é de responsabilidade e de uso exclusivo de seu titular, não podendo este permitir ou colaborar com o acesso aos recursos computacionais da FPAC por parte de pessoas não autorizadas. Os usuários são responsáveis por qualquer atividade desenvolvida através de suas contas de acesso na FPAC e pelos eventuais custos dela decorrentes.

4. Política de utilização dos recursos computacionais

4.1. Utilização dos Equipamentos

É absolutamente proibido efetuar ou permitir qualquer manutenção de qualquer dos recursos computacionais da FPAC, sem autorização do Departamento de Tecnologia da Informação (TI).

Ao averiguar qualquer problema de mau funcionamento de qualquer equipamento da FPAC, os usuários dos recursos computacionais deverão comunicar o Departamento de Tecnologia da Informação (TI), pelos canais e procedimentos corretos, para solicitarem o devido reparo.

É absolutamente vedada a abertura de computadores para qualquer tipo de reparo, verificação, limpeza ou qualquer outra situação. Pessoal técnico terceirizado só poderá ter acesso aos recursos computacionais da FPAC devidamente autorizados pelo Departamento de Tecnologia da Informação (TI).

Não é permitida a alteração das configurações de rede e inicialização das máquinas, bem como, modificações que possam trazer algum problema no desempenho.

Não é permitido o manuseio, troca, substituição ou mudança de local de conjuntos completos de equipamentos ou de seus acessórios, por qualquer que seja o motivo, sem a anuência do Departamento de Tecnologia da Informação (TI).

É vedado o acesso e manuseio dos equipamentos e instalações computacionais, ao usuário que portar alimentos e/ou bebidas, devendo esses permanecer em locais apropriados. Qualquer acidente, que coloque em risco a integridade dos recursos computacionais da FPAC será considerado atitude irresponsável e cabível de sanções trabalhistas.

4.2. Utilização de e-mail

É vedada a utilização de e-mail organizacional, em lojas virtuais, listas de discussões, ou qualquer outra utilização de internet, em ambiente fora da FPAC.

É proibida a distribuição voluntária ou despercebida de mensagens não desejadas, como circulares, correntes, pirâmides ou outros esquemas que possam prejudicar o trabalho de terceiros, causar excessivo tráfego na rede ou sobrecarregar os sistemas operacionais.

É proibido o uso do spam, sendo considerado o envio simultâneo de mensagens eletrônicas não solicitadas, de conteúdo similar para mais de 20 caixas postais.

Não fazer uso dos recursos para finalidades políticas, tais como o uso do correio eletrônico para circular propagandas de candidatos políticos ou denegrir a imagem de outros.

Não visualizar, armazenar, transferir ou enviar materiais pornográficos, eróticos, indecentes, ofensivos, que incentivem a violência, uso de drogas, discriminação de raça, credo etc.

4.3. Utilização da Internet

É proibida a divulgação de informações confidenciais da FPAC 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.

Sendo do interesse da associação que os seus colaboradores estejam bem informados, o uso de sites de notícias ou de serviços de notícias é aceitável, desde que o seu uso não comprometa o uso de banda da rede, nem perturbe o bom andamento dos trabalhos.

Poderá ser utilizada a Internet para atividades não relacionadas com a atividade fim durante o horário de almoço, ou fora do expediente, desde que dentro das regras de uso definidas nesta política.

Não utilizar a Internet para acessar salas de bate-papo (chat) e sites de lazer que se contraponham às regras de uso definidas nesta política.

A instalação ou utilização de qualquer tipo de jogos é proibido, inclusive jogos locais do Windows.

Não é permitida a instalação ou utilização de qualquer tipo de programa que toque, armazene ou baixe músicas ou vídeos.

Não será permitida a utilização de serviços de streaming, tais como rádios on-line e afins.

4.4. Utilização de dados e programas

Somente utilizar software e materiais protegidos por direitos autorais, de acordo com a lei. - Nunca instalar software sem o controle de procedência e dos direitos autorais e somente com a autorização por escrito do Departamento de Tecnologia da Informação (TI).

Sem uma autorização específica do Departamento de Tecnologia da Informação (TI) da FPAC, os usuários não podem remover dos recursos computacionais de nenhum documento de propriedade da entidade ou por ela administrado.

Os usuários não devem, deliberadamente, efetuar ou tentar qualquer tipo de acesso não autorizado a dados dos recursos computacionais da FPAC, ou tentar sua alteração, como por exemplo, ler mensagens pessoais de terceiros ou acessar arquivos confidenciais.

Os recursos computacionais da FPAC não podem ser utilizados para constranger, assediar ou ameaçar qualquer pessoa. Esses recursos não podem ser usados para alterar ou destruir recursos computacionais de outras empresas/Instituições. Se a partir de uma conta, um usuário estiver, de qualquer maneira, interferindo no trabalho de outro, este deve comunicar o fato ao responsável pelo equipamento onde está a conta, o qual, a seu critério, e sem prejuízo de outras sanções, poderá determinar a imediata suspensão temporária da conta de onde parte interferência, comunicando o caso ao Departamento de Tecnologia da Informação (TI).

Os usuários não podem violar ou tentar violar os sistemas de segurança dos recursos computacionais da FPAC, como quebrar ou tentar adivinhar identificação ou senhas de terceiros, interferir em fechaduras automáticas ou sistemas de alarme.

Os usuários não podem interceptar ou tentar interceptar transmissão de dados não destinados ao seu próprio acesso, seja monitorando barramentos de dados, seja através da rede, exceto quando autorizados explicitamente pela diretoria da FPAC.

Os usuários são responsáveis pela segurança de suas contas de acesso e de suas senhas. A conta e a respectiva senha são atribuídas a um único usuário e não devem ser compartilhadas com mais pessoas sem a autorização expressa do Departamento de Tecnologia da Informação (TI) da FPAC. Os usuários devem relatar imediatamente ao Departamento de Tecnologia da Informação (TI) da FPAC, qualquer suspeita de tentativa de violação de segurança.

Os usuários, a menos que tenham uma autorização específica do Departamento de Tecnologia da Informação (TI) para este fim, não podem tentar, permitir ou causar qualquer alteração ou destruição de ambientes operacionais, dados ou procedimentos de processamento ou comunicações da FPAC, de sua propriedade ou de qualquer outra pessoa ou instituição. Essas alterações incluem, mas não se limitam à alteração de dados, reconfiguração de chaves de controle ou parâmetros.

Material sexualmente explícito (em especial pedofilia), racista, político, religioso, ou quaisquer tipos de discriminação, não podem ser expostos, armazenados, distribuídos, editados ou gravados através do uso dos recursos computacionais e de comunicação da FPAC. Se qualquer um dos colaboradores tomar conhecimento da prática de algum dos atos ilícitos, aqui já elencados, deverá informar o fato ao Departamento de Tecnologia da Informação (TI), para que sejam tomadas as devidas providências junto às autoridades competentes.

Os usuários devem respeitar os direitos autorais de propriedade intelectual, em particular a lei de direitos autorais de software.

Não é permitida a cópia ou instalação de programas licenciados para FPAC em equipamentos de terceiros.

Nos recursos computacionais da FPAC, será garantido o maior grau possível de confidencialidade no tratamento dos dados dos usuários, de acordo com as tecnologias disponíveis, entretanto, os colaboradores do Departamento de Tecnologia da Informação (TI) da FPAC, poderão acessar arquivos de dados pessoais ou corporativos nos sistemas, sempre que isso for necessário para backups ou diagnóstico de problemas nos sistemas, inclusive nos casos de suspeita de violação de regras.

5. Controle da política de utilização dos recursos computacionais

Para garantir o cumprimento das normas mencionadas acima a FPAC se reserva no direito de:

- Implantar softwares e sistemas que podem monitorar e gravar o uso da Internet através da rede e das estações de trabalho da entidade;
- Inspecionar qualquer arquivo armazenado na rede, esteja no disco local da estação ou nas áreas privadas da rede, visando assegurar o rígido cumprimento desta política. Todo e qualquer uso dos recursos computacionais da FPAC devem estar de acordo com todas as obrigações contratuais da associação, inclusive com as limitações definidas nos contratos de software e outras licenças.

O uso de qualquer recurso computacional da FPAC está sujeito às leis federais, estaduais, municipais, às regulamentações da associação e às normas para uso da internet recomendadas pelo comitê gestor da internet Brasil.

Os usuários devem comunicar ao Departamento de Tecnologia da Informação (TI) da FPAC, qualquer evidência de violação das normas em vigor, não podendo acobertar, esconder ou ajudar a esconder violações de terceiros.

6. Das punições

Para garantir a adequada utilização dos recursos computacionais da FPAC, fica autorizado aplicar penalidades aos que violarem a legislação em vigor e as dispostas nesta política.

As penalidades a serem aplicadas por infração às normas indicadas no “caput” são: a aplicação de advertências que variam de 1 (uma) no mínimo, e de 3 (três) no máximo, dependendo da gravidade da infração e de justa causa, nos termos do artigo 482 alíneas “b” e “h” da consolidação da Legislação Trabalhista.

Sempre que julgar necessário para a preservação da integridade dos recursos computacionais da FPAC, dos serviços aos usuários ou dos dados, o Departamento de Tecnologia da Informação (TI) da FPAC poderá suspender temporariamente qualquer conta, seja ou não o responsável pela conta de alguma violação.

O usuário suspeito de violação dessas normas será notificado da acusação e terá a oportunidade de se pronunciar antes de qualquer decisão a ser tomada pela FPAC.

Com esta norma, a FPAC não renuncia a nenhuma pendência que possa ter quanto à propriedade ou controle de quaisquer software e hardware e dos dados criados ou armazenados em seus sistemas ou transmitidos através de sua rede.

Licenças – Softwares para uso nos Laboratórios

A Faculdade Paulista de Comunicação prioriza a adoção de Softwares Open Souce para realização de atividades em seus Laboratórios, como instrumento de inclusão social, vez que possibilita a seus alunos a adoção dos mesmos sistemas em seus próprios dispositivos. Mas é notório que não é possível garantir uma formação adequada a seus alunos sem a ambientação e treinamento nas principais Suítes do mercado, tais como os produtos Microsoft e Adobe. Neste sentido, os laboratórios contam com as assinaturas das soluções em Nuvem das referidas suítes:

Adobe Creative Cloud	Office 365
- Photoshop - Ilustrator - Acrobat DC - InDesign - XD - Lightroom - Premier Pro - Premier Rush - After Efects - Bridge - Lightroom Classic - Dimension - Dreamweaver - Animate - Character Animator - Audition - Media Encoder - inCopy - Prelude - Fuse CC - Muse CC	- Azure Active Directory Basic para EDU - School Data Sync (Plano 1) - Stream for Office 365 - Microsoft Teams - Microsoft StaffHub - Flow para Office 365 - PowerApps para o Office 365 - Azure Rights Management - Microsoft Forms (Plano 2) - Microsoft Planner - Sway - Gerenciamento de Dispositivo Móvel do Office 365 - Yammer for Academic - Office Online Educacional - Skype for Business Online (Plano 2) - Sharepoint Plano 1 para EDU - Exchange Online (Plano 1) - OneDrive (1TB de armazenamento)

O monitoramento de Licenças é realizado através de ferramenta Open Source SpiceWorks:

SOFTWARE	Produzido por
Microsoft SQL Server VSS Writer	Microsoft Corporation
Microsoft Windows SDK for Visual Studio 2008 .NET Framework Tools	Microsoft
Microsoft Windows SDK for Visual Studio 2008 Headers and Libraries	Microsoft Corporation
Microsoft Windows SDK for Visual Studio 2008 Tools	Microsoft Corporation
Microsoft .NET Framework 4.6.1	Microsoft Corporation
Microsoft Windows SDK for Visual Studio 2008 SDK Reference Assemblies and IntelliSense	Microsoft Corporation
Microsoft Windows SDK for Visual Studio 2008 Win32 Tools	Microsoft Corporation
Microsoft Visual C++ 2010 x64 Redistributable - 10.0.30319	Microsoft Corporation
Google Chrome	Google Inc.
Microsoft Document Explorer 2008	Microsoft Corporation

Microsoft Visual Studio 2008 Professional Edition - ENU	Microsoft Corporation
Mozilla Maintenance Service	Mozilla
Visual Studio Tools for the Office system 3.0 Runtime	Microsoft Corporation
Microsoft Visual Studio Web Authoring Component	Microsoft Corporation
WinPcap 4.1.2-Spiceworks	CACE Technologies
Microsoft Visual C++ 2013 Redistributable (x64) - 12.0.30501	Microsoft Corporation
Agent Shell	Spiceworks
Microsoft Visual C++ 2013 x86 Minimum Runtime - 12.0.21005	Microsoft Corporation
Microsoft SQL Server Compact 3.5 for Devices ENU	Microsoft Corporation
Microsoft .NET Compact Framework 3.5	Microsoft Corporation
Microsoft SQL Server Compact 3.5 Design Tools ENU	Microsoft Corporation
Microsoft Visual Studio 2005 Tools for Office Runtime	Microsoft Corporation
Google Update Helper	Google Inc.
Windows Mobile 5.0 SDK R2 for Pocket PC	Microsoft Corporation
Microsoft Office Visual Web Developer 2007	Microsoft Corporation
Microsoft Office Visual Web Developer MUI (English) 2007	Microsoft Corporation
Microsoft Office Shared MUI (English) 2007	Microsoft Corporation
Microsoft Office Shared Setup Metadata MUI (English) 2007	Microsoft Corporation
Security Update for Microsoft .NET Framework 4.6.1 (KB3122661)	Microsoft Corporation
Security Update for Microsoft .NET Framework 4.6.1 (KB3127233)	Microsoft Corporation
Security Update for Microsoft .NET Framework 4.6.1 (KB3136000)	Microsoft Corporation
Security Update for Microsoft .NET Framework 4.6.1 (KB3136000v2)	Microsoft Corporation
Security Update for Microsoft .NET Framework 4.6.1 (KB3142037)	Microsoft Corporation
Security Update for Microsoft .NET Framework 4.6.1 (KB3143693)	Microsoft Corporation
Security Update for Microsoft .NET Framework 4.6.1 (KB3164025)	Microsoft Corporation
Update for Microsoft .NET Framework 4.6.1 (KB4014511)	Microsoft Corporation
Update for Microsoft .NET Framework 4.6.1 (KB4014553)	Microsoft Corporation
Windows Mobile 5.0 SDK R2 for Smartphone	Microsoft Corporation
Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.17	Microsoft Corporation
Microsoft SQL Server Database Publishing Wizard 1.2	Microsoft Corporation
Adobe Refresh Manager	Adobe Systems Incorporated
Adobe Acrobat Reader DC	Adobe Systems Incorporated
Microsoft SQL Server Compact 3.5 ENU	Microsoft Corporation
Microsoft Visual C++ 2013 Redistributable (x86) - 12.0.21005	Microsoft Corporation
Microsoft .NET Compact Framework 2.0 SP2	Microsoft Corporation
Microsoft Visual C++ 2010 x86 Redistributable - 10.0.40219	Microsoft Corporation
Microsoft Visual C++ 2013 x86 Additional Runtime - 12.0.21005	Microsoft Corporation

VC Runtimes MSI	Microsoft
Microsoft Visual C++ 2008 Redistributable - x86 9.0.21022	Microsoft Corporation
CCleaner	Piriform
Intel(R) Network Connections Drivers	Intel
Microsoft Visual C++ 2010 x64 Redistributable - 10.0.40219	Microsoft Corporation
Intel® Trusted Connect Service Client	Intel Corporation
Spiceworks Desktop	Spiceworks, Inc.
Intel(R) USB 3.0 eXtensible Host Controller Driver	Intel Corporation
Intel(R) Management Engine Components	Intel Corporation
Intel(R) Processor Graphics	Intel Corporation
Intel(R) SDK for OpenCL - CPU Only Runtime Package	Intel Corporation
Java Auto Updater	Oracle Corporation
AVG AntiVirus FREE	AVG Technologies
Microsoft Visual C++ 2012 Redistributable (x86) - 11.0.61030	Microsoft Corporation
Office 16 Click-to-Run Extensibility Component	Microsoft Corporation
Office 16 Click-to-Run Localization Component	Microsoft Corporation
Microsoft Visual C++ 2012 x86 Additional Runtime - 11.0.61030	Microsoft Corporation
Microsoft Visual C++ 2012 x86 Minimum Runtime - 11.0.61030	Microsoft Corporation
Realtek High Definition Audio Driver	Realtek Semiconductor Corp.
Office 16 Click-to-Run Extensibility Component 64-bit Registration	Microsoft Corporation
Office 16 Click-to-Run Licensing Component	Microsoft Corporation
Microsoft Silverlight	Microsoft Corporation
Nmap 5.61-Spiceworks	
TeamViewer 13	TeamViewer
Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.6161	Microsoft Corporation
Microsoft Visual C++ 2008 Redistributable - x64 9.0.30729.6161	Microsoft Corporation
Microsoft Visual C++ 2008 Redistributable - x64 9.0.30729.17	Microsoft Corporation
Microsoft Visual C++ 2013 x64 Additional Runtime - 12.0.21005	Microsoft Corporation
Microsoft Visual C++ 2013 x64 Minimum Runtime - 12.0.21005	Microsoft Corporation
Microsoft Visual C++ 2005 Redistributable (x64)	Microsoft Corporation
Audacity 2.2.2	Audacity Team
Dev-C++	Bloodshed Software
Microsoft Visual C++ 2005 Redistributable	Microsoft Corporation
Realtek Ethernet Controller Driver	Realtek
Microsoft Visual C++ 2013 Redistributable (x86) - 12.0.30501	Microsoft Corporation
Foxit Reader	Foxit Software Inc.

Java 8 Update 131	Oracle Corporation
MiniTerm	Terminal window application for PPP
FaceTime	
Dashboard	1.8, Copyright 2006-2014 Apple Inc.
Automator	
App Store	
Terminal	
Grapher	
Console	
QuickTime Player	10.4, Copyright 2009-2014 Apple Inc. All Rights Reserved.
Photo Booth	
Mission Control	1.2, Copyright 2007-2014 Apple Inc.
Mail	
Launchpad	1.0, Copyright 2010-2014 Apple Inc.
Time Machine	1.3, Copyright 2007-2014 Apple Inc.
Google Chrome	
Keynote	
Numbers	
Adobe Flash Player Install Manager	
Siri	1.0, Copyright 2016 Apple Inc.
OneDrive	
Creative Cloud Uninstaller	
Creative Cloud Installer	
Creative Cloud Desktop App	
Adobe Application Updater	
Creative Cloud	
adobe_licutil	
AASIapp	
Spotify	
CCXProcess	
adobe_lichelper	
ACCFinderBundleLoader	
Core Sync	

Uninstaller	4.3.0.256
Install	
Adobe Application Manager	Adobe Application Manager 10.0.0.49, Copyright 2009-2015 Adobe Systems Incorporated. All rights reserved.
AAMLauncherUtil	Adobe Application Manager 10.0.0.49, Copyright 2013-2015 Adobe Systems Incorporated. All rights reserved.
LogTransport2	Copyright 2008-10 Adobe Systems Incorporated. All rights reserved.
AAM Updates Notifier	Adobe Application Manager Updates Notifier 9.0.0.281, 2009-2015 Adobe Systems Incorporated and its licensors. All rights reserved.
Setup	5.0.65.0, " 2005-2012 Adobe Systems Incorporated and its licensors. All rights reserved."
Evernote	
Install Spotify	
VLC media player	VideoLAN
Microsoft Office Enterprise 2007	Microsoft Corporation
Microsoft Office Proof (English) 2007	Microsoft Corporation
Microsoft Office Proof (French) 2007	Microsoft Corporation
Microsoft Office Office 64-bit Components 2007	Microsoft Corporation
Arduino	Arduino LLC
Dropbox	Dropbox, Inc.
Dropbox Update Helper	Dropbox, Inc.
Intel® Active Management Technology	Intel Corporation
Microsoft Security Essentials	Microsoft Corporation
Microsoft Security Client	Microsoft Corporation
Mediatek RT2870 Wireless LAN Card	MediatekWiFi
Microsoft Office Proof (Spanish) 2007	Microsoft Corporation
Microsoft Office Proofing (English) 2007	Microsoft Corporation
Microsoft Office Proof (English) 2010	Microsoft Corporation
Microsoft Office Proof (Spanish) 2010	Microsoft Corporation
Microsoft Office File Validation Add-In	Microsoft Corporation
Intel(R) Graphics Media Accelerator Driver	Intel Corporation
Microsoft SQL Server Native Client	Microsoft Corporation

Microsoft SQL Server 2005	Microsoft Corporation
Microsoft SQL Server Setup Support Files (English)	Microsoft Corporation
Update for Microsoft Office Outlook 2007 (KB2687404) 32-Bit Edition	Microsoft
Microsoft Office Professional Plus 2007	Microsoft Corporation
Rapport	Trusteer
Intel(R) Rapid Storage Technology	Intel Corporation
Lenovo Mouse Suite	Lenovo
Microsoft .NET Framework 4.5.2	Microsoft Corporation
Intel(R) Control Center	Intel Corporation
AAM Registration Notifier	Adobe Application Manager Registration Notifier 3.0.64.0, Copyright 2009-2011 Adobe Systems Incorporated. All rights reserved.
Scan To	HP
Microsoft Office Professional Plus 2010	Microsoft Corporation
MarketResearch	Hewlett-Packard
PDFCreator	pdfforge GmbH
Microsoft Office Office 32-bit Components 2010	Microsoft Corporation
Backup and Sync from Google	Google, Inc.
Microsoft Visual C++ 2015 x64 Minimum Runtime - 14.0.23026	Microsoft Corporation
Oracle VM VirtualBox 5.2.8	Oracle Corporation
Cisco PEAP Module	Cisco Systems, Inc.
Cisco EAP-FAST Module	Cisco Systems, Inc.
REALTEK Wireless LAN Driver and Utility	REALTEK Semiconductor Corp.
Cisco LEAP Module	Cisco Systems, Inc.
Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729	Microsoft Corporation
Microsoft Visual C++ 2015 x64 Additional Runtime - 14.0.23026	Microsoft Corporation
Adobe AIR	Adobe Systems Incorporated
Microsoft Visual C++ 2015 Redistributable (x64) - 14.0.23026	Microsoft Corporation
Microsoft .NET Framework 4.5	Microsoft Corporation
XAMPP	Bitnami
64 Bit HP CIO Components Installer	HP Inc.
Java 8 Update 161 (64-bit)	Oracle Corporation
WinRAR 5.50 (64-bit)	win.rar GmbH
Skype	
Web Gallery	
Export Flash Animation	

Contact Sheets	
Make Calendar	
Analyze Documents	
7-Zip 18.05	Igor Pavlov
Adobe Acrobat Reader DC - Português	Adobe Systems Incorporated
64 Bit HP CIO Components Installer	Hewlett-Packard
hppLaserJetService	Hewlett-Packard
HP Product FWUpdater	Hewlett-Packard Company
HPLJDXPHelper	HP
HPLJUTCore	HP
HP Update	Hewlett-Packard
Avast Free Antivirus	AVAST Software
Microsoft Visual C++ 2015 x86 Additional Runtime - 14.0.24123	Microsoft Corporation
Microsoft Visual C++ 2015 x86 Minimum Runtime - 14.0.24123	Microsoft Corporation
Microsoft Visual C++ 2015 Redistributable (x86) - 14.0.24123	Microsoft Corporation
LogMeIn	LogMeIn, Inc.
LogMeIn Client	LogMeIn, Inc.
hpStatusAlerts	HP Development Company, L.P.
HP Unified IO	HP
HPDXP	HP
LJDXPHelperUI	HP
Adobe Flash Player 29 NPAPI	Adobe Systems Incorporated
32 Bit HP CIO Components Installer	Hewlett-Packard
Microsoft Visual C++ 2010 x86 Redistributable - 10.0.30319	Microsoft Corporation
Update for Microsoft .NET Framework 4.6.1 (KB3210136)	Microsoft Corporation
Update for Microsoft .NET Framework 4.6.1 (KB4040973)	Microsoft Corporation
Adobe Flash Player 28 NPAPI	Adobe Systems Incorporated
OKI Network Extension	Okidata
ScannerDriver	Oki Data Corporation
OKI ActKey	Oki Data Corporation
ActKey	Oki Data Corporation
Java 8 Update 121	Oracle Corporation
Java 8 Update 111	Oracle Corporation
EPSON Scan	Seiko Epson Corporation
Visual Studio 2012 x86 Redistributables	AVG Technologies CZ, s.r.o.
I.R.I.S. OCR	HP

Microsoft Office Access MUI (Portuguese (Brazil)) 2007	Microsoft Corporation
HP Customer Experience Enhancements	Hewlett-Packard
Java 8 Update 101	Oracle Corporation
Intel(R) Network Connections 16.8.45.1	Intel
Service Pack 2 for Microsoft Office 2010 (KB2687455) 64-Bit Edition	Microsoft
OpenOffice 4.1.5	Apache Software Foundation
HP Support Solutions Framework	HP
VC90_CRT_x64	Intel Corporation
VC_CRT_x64	Intel Corporation
HP Google Drive Plugin	HP
HP Dropbox Plugin	HP
GemPcCCID	Gemalto
Samsung Printer Live Update	Samsung Electronics Co., Ltd.
Wondershare Helper Compact 2.5.2	Wondershare
Python Launcher	Python Software Foundation
EaseUS Todo Backup Free 10.6	CHENGDU YIWO Tech Development Co., Ltd
Proteção de Terminal Trusteer	Trusteer
Samsung Universal Scan Driver	Samsung Electronics Co., Ltd.
Adobe Flash Player 28 PPAPI	Adobe Systems Incorporated
hpStatusAlerts	Hewlett Packard
Foxit Cloud	Foxit Software Inc.
Mouse Suite	
Security Update for Microsoft Office 2010 (KB2289078)	Microsoft
Security Update for Microsoft InfoPath 2010 (KB2553322) 32-Bit Edition	Microsoft
Security Update for Microsoft Word 2010 (KB2345000)	Microsoft
Security Update for Microsoft Office 2010 (KB2598243) 32-Bit Edition	Microsoft
Security Update for Microsoft Office 2010 (KB2553371) 32-Bit Edition	Microsoft
Microsoft SQL Server 2005 Tools Express Edition	Microsoft Corporation
IRPF2018	Receita Federal do Brasil
Aplicativo Ita 	Banco Ita
Security Update for Microsoft .NET Framework 4.5.2 (KB2972107)	Microsoft Corporation
Security Update for Microsoft .NET Framework 4.5.2 (KB3023224)	Microsoft Corporation
Security Update for Microsoft .NET Framework 4.5.2 (KB3074230)	Microsoft Corporation
Security Update for Microsoft .NET Framework 4.5.2 (KB3074550)	Microsoft Corporation
Security Update for Microsoft .NET Framework 4.5.2 (KB3097996)	Microsoft Corporation
Security Update for Microsoft .NET Framework 4.5.2 (KB3098781)	Microsoft Corporation

Security Update for Microsoft .NET Framework 4.5.2 (KB3122656)	Microsoft Corporation
Security Update for Microsoft .NET Framework 4.5.2 (KB3127229)	Microsoft Corporation
Security Update for Microsoft .NET Framework 4.5.2 (KB3135996)	Microsoft Corporation
Security Update for Microsoft .NET Framework 4.5.2 (KB3142033)	Microsoft Corporation
LAV Filters 0.67	Hendrik Leppkes
Intel(R) Network Connections 15.2.89.2	Intel
Reimage Repair	Reimage
Security Update for Microsoft .NET Framework 4.5.2 (KB2972216)	Microsoft Corporation
Microsoft Office Visio Professional 2007	Microsoft Corporation
Microsoft Visual J# 2.0 Redistributable Package	Microsoft Corporation
Pages	
PDF Expert	
Microsoft .NET Framework 4.6.1 (PTB)	Microsoft Corporation
Microsoft .NET Framework 4.5.2 (PTB)	Microsoft Corporation
Microsoft SQL Server Management Studio Express	Microsoft Corporation
Security Update for Microsoft Visual Studio 2005 Professional Edition - ENU (KB2251481)	Microsoft Corporation
Security Update for Microsoft Visual Studio 2005 Professional Edition - ENU (KB2538218)	Microsoft Corporation
Security Update for Microsoft Visual Studio 2005 Professional Edition - ENU (KB2548826)	Microsoft Corporation
Hotfix for Microsoft Visual Studio 2005 Professional Edition - ENU (KB2938803)	Microsoft Corporation
Microsoft Visual Studio 2005 Professional Edition - ENU Service Pack 1 (KB926601)	Microsoft Corporation
Update for Microsoft Visual Studio 2005 Professional Edition - ENU (KB932232)	Microsoft Corporation
Security Update for Microsoft Visual Studio 2005 Professional Edition - ENU (KB937061)	Microsoft Corporation
Security Update for Microsoft Visual Studio 2005 Professional Edition - ENU (KB973673)	Microsoft Corporation
Microsoft Document Explorer 2005	Microsoft Corporation
Microsoft Visual Studio 2005 Professional Edition - ENU	Microsoft Corporation
Microsoft SQL Server 2005 Mobile [ENU] Developer Tools	Microsoft Corporation
Microsoft .NET Compact Framework 1.0 SP3 Developer	Microsoft Corporation
Microsoft Device Emulator version 1.0 - ENU	Microsoft Corporation
Avast Secure Browser	AVAST Software
Giesecke & Devrient GmbH StarSign CUT	Giesecke & Devrient GmbH
Componente de Seguran&#65533;a Bradesco	Banco Bradesco S.A.
Dropbox	

Uninstall Product	5.0.65.0, " 2005-2012 Adobe Systems Incorporated and its licensors. All rights reserved."
Atom	
Scratch 2 Offline Editor	Massachusetts Institute of Technology
IRPF2017	Receita Federal do Brasil
Microsoft .NET Framework 4.5.2 (Portugu&#65533;s do Brasil)	Microsoft Corporation
Microsoft SQL Server 2005 Express Edition (SQLEXPRESS)	Microsoft Corporation
hpStatusAlertsM425	Hewlett-Packard
HP LaserJet 400 MFP M425	Hewlett-Packard
hppM425LaserJetService	Hewlett-Packard
HP LJ400 M425 HP Scan	Hewlett-Packard Co.
Web Signer	Softplan Sistemas
Microsoft Office Shared 64-bit MUI (Portuguese (Brazil)) 2007	Microsoft Corporation
Avira Antivirus	Avira Operations GmbH & Co. KG
Microsoft Office Excel MUI (Portuguese (Brazil)) 2007	Microsoft Corporation
Microsoft Office PowerPoint MUI (Portuguese (Brazil)) 2007	Microsoft Corporation
Microsoft Office Publisher MUI (Portuguese (Brazil)) 2007	Microsoft Corporation
Microsoft Office Outlook MUI (Portuguese (Brazil)) 2007	Microsoft Corporation
Microsoft Office Word MUI (Portuguese (Brazil)) 2007	Microsoft Corporation
Microsoft Office Proof (Portuguese (Brazil)) 2007	Microsoft Corporation
Microsoft Office Proofing (Portuguese (Brazil)) 2007	Microsoft Corporation
Microsoft Office InfoPath MUI (Portuguese (Brazil)) 2007	Microsoft Corporation
Microsoft Office Shared MUI (Portuguese (Brazil)) 2007	Microsoft Corporation
Microsoft Office OneNote MUI (Portuguese (Brazil)) 2007	Microsoft Corporation
Microsoft Office Groove MUI (Portuguese (Brazil)) 2007	Microsoft Corporation
Avira	Avira Operations GmbH & Co. KG
DriverToolkit version 8.5.0.0	Megaify Software
Security Update for Microsoft .NET Framework 4.5 (KB2737083)	Microsoft Corporation
Security Update for Microsoft .NET Framework 4.5 (KB2742613)	Microsoft Corporation
Security Update for Microsoft .NET Framework 4.5 (KB2840642v2)	Microsoft Corporation
Security Update for Microsoft .NET Framework 4.5 (KB2861208)	Microsoft Corporation
Security Update for Microsoft .NET Framework 4.5 (KB2894854v2)	Microsoft Corporation
Security Update for Microsoft .NET Framework 4.5 (KB2898864)	Microsoft Corporation
Security Update for Microsoft .NET Framework 4.5 (KB2901118)	Microsoft Corporation
Security Update for Microsoft .NET Framework 4.5 (KB2972107)	Microsoft Corporation
Security Update for Microsoft .NET Framework 4.5 (KB3035490)	Microsoft Corporation

Microsoft .NET Framework 4.7.2	Microsoft Corporation
Inkscape 0.92.3	Inkscape Project
HP LaserJet Pro MFP M426f-M427f Fax Driver	Hewlett-Packard Co.
HP LaserJet Pro MFP M426f-M427f Fax	Hewlett-Packard Co.
HP LaserJet Pro MFP M426f-M427f Common Files	Hewlett-Packard Co.
HPLJUTM426f_427f	HP
hpStatusAlertsM426f_M427f	Hewlett-Packard
hppM41426427LaserJetService	Hewlett-Packard
HP LJ M426fM427f Scan HP Scan	Hewlett-Packard Co.
HP LaserJet Pro MFP M426f-M427f HP Device Toolbox	Hewlett-Packard Co.
HP LaserJet Pro MFP M426f-M427f Digital Filing	Hewlett-Packard Co.
HP LaserJet Pro MFP M426f-M427f	Hewlett-Packard
HPLJProMFPM426fM427f	Hewlett-Packard
HP LaserJet Pro MFP M426f-M427f Scan Shortcuts	Hewlett-Packard Co.
RStudio	RStudio
Security Update for Microsoft .NET Framework 4.5.2 (KB2978128)	Microsoft Corporation
Brother Printer Driver	Brother Industries Ltd.
Brother Port Driver	Brother Industries Ltd.
Brother Scanner Driver	Brother Industries Ltd.
K-Lite Codec Pack 11.8.5 Basic	KLCP
HPSSupply	Hewlett Packard Development Company L.P.
MrvlUsgTracking	Marvell
Microsoft Office Proof (Portuguese (Brazil)) 2010	Microsoft Corporation
hppM1130M1210SeriesLaserJetService	Hewlett-Packard
IrfanView 4.44 (32-bit)	Irfan Skiljan
HP LaserJet Professional M1130-M1210 MFP Series	
HP LaserJet Professional M1210 MFP Series Fax Installer	HP
MySQL Tools for 5.0	MySQL AB, Sun Microsystems, Inc.
ControlCenter4 CSDK	Brother Insutries Ltd.
HowToGuide	Brother Industries Ltd.
NetworkRepairTool	Brother Insutries Ltd.
UsbRepairTool	Brother Insutries Ltd.
ScannerUtilityInstaller	Brother
StatusMonitor	Brother Insutries Ltd.
BrLogRx	Brother Industries Ltd.
BrLauncher	Brother Industries Ltd.

BrSupportTools	Brother Industries Ltd.
WinRAR 5.11 (64-bit)	win.rar GmbH
MySQLWorkbench	
Termius	
Receitanet	Serpro - Servi&#65533;o Federal de Processamento de Dados
MyEpson Portal	SEIKO EPSON Corporation
Microsoft Virtual PC 2007	Microsoft Corporation
Security Update for Microsoft .NET Framework 4.5.2 (KB3037581)	Microsoft Corporation
Microsoft Office Excel MUI (Portuguese (Brazil)) 2010	Microsoft Corporation
Microsoft Office PowerPoint MUI (Portuguese (Brazil)) 2010	Microsoft Corporation
Microsoft Office Publisher MUI (Portuguese (Brazil)) 2010	Microsoft Corporation
Microsoft Office Outlook MUI (Portuguese (Brazil)) 2010	Microsoft Corporation
Microsoft Office Word MUI (Portuguese (Brazil)) 2010	Microsoft Corporation
Microsoft Office Proofing (Portuguese (Brazil)) 2010	Microsoft Corporation
Microsoft Office Shared MUI (Portuguese (Brazil)) 2010	Microsoft Corporation
Microsoft Office OneNote MUI (Portuguese (Brazil)) 2010	Microsoft Corporation
WhatsApp	
PC-CCID	Gemalto
Microsoft Office Visio MUI (English) 2007	Microsoft Corporation
Update for Microsoft Office Visio 2007 Help (KB963666)	Microsoft
Calendario	
aTube Catcher vers&#65533;o 3.8	DsNET Corp
IRPF2015 - Declara&#65533;&#65533;o de Ajuste Anual, Final de Esp&#65533;lio e Sa&#65533;da Definitiva do Pa&#65533;s	Receita Federal do Brasil
IRPF2016 - Declara&#65533;&#65533;o de Ajuste Anual, Final de Esp&#65533;lio e Sa&#65533;da Definitiva do Pa&#65533;s	Receita Federal do Brasil
Microsoft Office Access MUI (Portuguese (Brazil)) 2010	Microsoft Corporation
Microsoft Office InfoPath MUI (Portuguese (Brazil)) 2010	Microsoft Corporation
Microsoft Office Groove MUI (Portuguese (Brazil)) 2010	Microsoft Corporation
HP Softpaq SP57135	
MemoryBooster	
ControlCenter4	Brother Industries, Ltd.
HP LaserJet Toolbox	Hewlett-Packard
HP LaserJet Professional M1210 MFP Series Toolbox	Hewlett-Packard
hppusgM1130M1210Series	Hewlett-Packard
Microsoft .NET Framework 4.5 PTB Language Pack	Microsoft Corporation

Pacote de Idiomas do Microsoft .NET Framework 4.5 - Portugu&#65533;s (Brasil)	Microsoft Corporation
Arquivo do WinRAR	
MIT App Inventor Tools 2.3.0	Massachusetts Institute of Technology
Editor de Scripts	
Fotos	
Notas	
Mapas	
CopySpider 1.3.2	CopySpider Software
WampServer 2.5	Herv&#65533; Leclerc (HeL)
Microsoft Office Project Professional 2007	Microsoft Corporation
Microsoft Office Shared 32-bit MUI (Portuguese (Brazil)) 2010	Microsoft Corporation
PremiumScanEventHandler	Copyright (c) 2013 Hewlett-Packard Development Company, L.P.
HP Scan	Copyright 2010-2013, Hewlett-Packard Development Company, L.P.
Atualiza&#65533;&#65533;o do produto Microsoft Office Excel 2007 Help (KB963678)	Microsoft
Atualiza&#65533;&#65533;o do produto Microsoft Office Powerpoint 2007 Help (KB963669)	Microsoft
Atualiza&#65533;&#65533;o do produto Microsoft Office Outlook 2007 Help (KB963677)	Microsoft
Atualiza&#65533;&#65533;o do produto Microsoft Office Word 2007 Help (KB963665)	Microsoft
Microsoft .NET Framework 4.6.1 (Portugu&#65533;s do Brasil)	Microsoft Corporation
SafeNet Authentication Client 8.1 SP2	SafeNet, Inc.
Crystal Reports Basic for Visual Studio 2008	Business Objects
Hotfix for Microsoft Visual Studio 2008 Professional Edition - ENU (KB971091)	Microsoft Corporation
Update for Microsoft Visual Studio 2008 Professional Edition - ENU (KB972221)	Microsoft Corporation
Hotfix for Microsoft Visual Studio 2008 Professional Edition - ENU (KB973674)	Microsoft Corporation
Editor de Texto	
Utilitario do VoiceOver	
Assistente de Migracao	
Acesso as Chaves	
Utilitario de Disco	
Utilitario ColorSync	
Preferencias do Sistema	
Anotacoes	
Lembretes	

Mensagens	
Dicionario	
Contatos	
HP LaserJet 400 MFP M425 HP Device Toolbox	Hewlett-Packard Co.
Sublime Text	
K-Lite Mega Codec Pack 6.2.0	
VC80CRTRedist - 8.0.50727.4053	DivX, Inc
Avira Phantom VPN	Avira Operations GmbH & Co. KG
Microsoft Office Project MUI (English) 2007	Microsoft Corporation
CutePDF Writer 2.7	
Dr. Cleaner	
FileZilla	FileZilla Client 3.25.1, Copyright (C) 2004-2016 Tim Kosse, Website: https://filezilla-project.org
Teams Machine-Wide Installer	Microsoft Corporation
Security Update for Microsoft Office 2010 (KB2598039) 32-Bit Edition	Microsoft
Security Update for Microsoft PowerPoint 2010 (KB2553185) 32-Bit Edition	Microsoft
AVG 2016	AVG Technologies
HP Softpaq SP67118	
MPC-HC 1.7.10	MPC-HC Team
Inkscape	0.92.2, Copyright 2003-2017 Inkscape Developers
SafeSign	A.E.T. Europe B.V.
WinRAR 4.11 (32-bit)	win.rar GmbH
Avira System Speedup	Avira Operations GmbH & Co. KG
Avira Software Updater	Avira Operations GmbH & Co. KG
Microsoft Windows SDK for Visual Studio 2008 Express Tools for Win32	Microsoft Corporation
Microsoft Windows SDK for Visual Studio 2008 Express Tools for .NET Framework	Microsoft
Microsoft Office 365 ProPlus - pt-br	Microsoft Corporation
Kurupira Update vers&#65533;o 1.3.4	
Kurupira WebFilter FREE	Kurupira.NET
Security Update for Microsoft Visual Basic for Applications 6.5 (KB2688865)	
PDFill FREE PDF Editor Basic	PlotSoft LLC
iZip Unarchiver	
Sicalc Auto Atendimento	Receita Federal do Brasil
adobe_licensing_helper	

EasyFind	4.9.3 2001-2014 Christian Grunenberg, DEVONtechnologies.
PDFill PDF Editor Professional	PlotSoft LLC
Update for Microsoft .NET Framework 4.7.2 (KB4087364)	Microsoft Corporation
Microsoft Visual Basic 2008 Express Edition - ENU	Microsoft Corporation
Java 8 Update 181 (64-bit)	Oracle Corporation
CertiInstaller 1.1.0.2	Certisign
SafeNet iKey Driver v4.1.1.5	SafeNet, Inc.
Web Signer for Internet Explorer	Softplan Sistemas
Avira Privacy Pal	Avira Operations GmbH & Co. KG
Curso PER_DCOMP	
Carn�-Le�o 2018	Receita Federal do Brasil
IRPF2013 - Declara��o de Ajuste Anual, Final de Esp�lio e Sa�da Definitiva do Pa�s	Receita Federal do Brasil
IRPF2014 - Declara��o de Ajuste Anual, Final de Esp�lio e Sa�da Definitiva do Pa�s	Receita Federal do Brasil
Componente de Seguran�a Bradesco	Bradesco (Departamento de Seguranca Corporativa)
Microsoft .NET Framework 4.7.2 (PTB)	Microsoft Corporation
Microsoft .NET Framework 4.7.2 (Portugu�s (Brasil))	Microsoft Corporation
Assistente de Instala��o Certisign	CERTISIGN
Wondershare Recoverit(Build 7.0.4.7)	Wondershare Software Co.,Ltd.
SRS Premium Sound for HP Thin Speakers	SRS Labs, Inc.
HP Softpaq SP49161	
Captura de Imagem	
Update for Microsoft Office Project 2007 Help (KB963668)	Microsoft
Samsung SCX-6x55 Series	Samsung Electronics CO.,LTD
Adobe Flash Player 31 NPAPI	Adobe Systems Incorporated
Security Update for Microsoft Office 2010 (KB2553353) 32-Bit Edition	Microsoft
Stencyl	Stencyl, LLC
AVG Update Helper	AVG Technologies
NTFS for Mac	
OKI Universal Scanner	Oki Data Corporation
Itau	
L&H TTS3000 Portugu�s (Brasil)	
IRPF2017	
IRPF2018	

Max Impress&#65533;o 1.0	Maxprint
Microsoft MSDN 2005 Express Edition - ENU	Microsoft Corporation
Folha Phoenix 12.23.2.40175	Contmatic
HP Alerts	HP Alerts, Copyright 2010-2017 HP Development Company, L.P.
HP Email Alerts	HP Email Alerts, Copyright 2011-2017 HP Development Company, L.P.
Cont&#65533;bil Phoenix 12.12.21.40349	Contmatic
MSDN Library for Microsoft Visual Studio 2008 Express Editions	Microsoft Corporation
Printer Driver Installer	3.3, Copyright 1991-2008 by MindVision Software. All rights reserved.
Mbrola Tools 3.5	FPMs TCTS Lab
HP LaserJet M1120 MFP Series	
hppusgM1120	Hewlett-Packard
Java(TM) SE Development Kit 6 Update 7	Sun Microsystems, Inc.
Calculadora	10.14, Copyright 2001-2018, Apple Inc.
Bolsa	
Casa	
Jive View	
S4A version 1.6	Citilab (Cornell&#65533;)
XP Codec Pack	XP Codec Pack team
CP-Pro Mais	NovaProlink
WinRAR 5.61 (64-bit)	win.rar GmbH
RAR Extractor and Expander	
Pre-Visualizacao	10.1, Copyright 2002-2018 Apple Inc.
Monitor de Atividade	10.14, Copyright 2000-2018 Apple Inc.
Livros	
Xadrez	3.16, Copyright 2003-2017 Apple Inc.
Catalogo de Fontes	9.0, Copyright 20032018 Apple Inc.
Utilitario AirPort	6.3.9, Copyright 2001 -2018 Apple Inc.
Configuracao de Audio e MIDI	3.3, Copyright 2002-2017 Apple, Inc.

Assistente do Boot Camp	Boot Camp Assistant 6.1.0, Copyright 2018 Apple Inc. All rights reserved
Medidor de Cor Digital	5.13, Copyright 2001-2018 Apple Inc. All Rights Reserved.
Informacoes do Sistema	
Captura de Tela	
Gravador	
Java 8 Update 191	Oracle Corporation
Java 8 Update 191 (64-bit)	Oracle Corporation
Lexmark S300-S400 Series	Lexmark International, Inc.
Samsung OCR Software	HP Printing Korea Co., Ltd.
Mozilla Firefox 33.1 (x86 pt-BR)	Mozilla
TeamViewer 14	TeamViewer
JivoSite	
Arquivo do WinRAR	win.rar GmbH
Windows Mobile 6 Professional SDK	Microsoft Corporation
OCLC Dewey Cutter Program	
MSDN Library for Visual Studio 2008 - ENU	Microsoft
LibreOffice 6.1.3.2	The Document Foundation
Mozilla Firefox 63.0.1 (x86 pt-BR)	Mozilla
Ferramentas do Visual Studio 2005 para Office Second Edition Runtime	Microsoft Corporation
StarUML 5.0.2.1570	Plastic Software, Inc.
LegacyScanEventHandler	Legacy Scan Event Handler 5.37.1, Copyright 2014-2017 HP Development Company, L.P.
HP Event Status	HP Event Status 5.37.1, Copyright 2013-2017 HP Development Company, L.P.
Avira Safe Shopping	Avira Operations GmbH & Co. KG
iTunes	iTunes 12.9.2.5, 20002018 Apple Inc. All rights reserved.
PDF24 Creator 8.7.0	PDF24.org
Warsaw 2.7.0.135 64 bits	GAS Tecnologia
Adobe Flash Player 32 ActiveX	Adobe Systems Incorporated
SafeSign IC Standard Windows 64-bits	A.E.T. Europe B.V.
FileZilla 2	FileZilla Client 3.30.0, Copyright (C) 2004-2018 Tim Kosse, Website: https://filezilla-project.org

GoToMeeting	GoToMeeting v8.38.1.11282, Copyright 2018 LogMeIn, Inc.
Update for Microsoft .NET Framework 4.7.2 (KB4470640)	Microsoft Corporation
Safari	12.0.3, Copyright 2003-2018 Apple Inc.
IP Scanner Pro	IP Scanner Pro 3.70
Update for Microsoft .NET Framework 4.7.2 (KB4480055)	Microsoft Corporation
Java 8 Update 201 (64-bit)	Oracle Corporation
Avast Secure Browser	Autores do Avast Secure Browser
Java DB 10.3.1.4	Sun Microsystems, Inc
CopySpider 1.3.9	CopySpider Software
AdobeIPCBroker	5.5.0.66 Copyright 2017, Adobe Systems Incorporated. All rights reserved.
Microsoft Visual Basic 2005 Express Edition - ENU	Microsoft Corporation
Warsaw 2.8.0.61 64 bits	GAS Tecnologia
AVG Secure Browser	Autores do AVG Secure Browser
Viper FTP Lite	Viper FTP Lite 5.2.1, Copyright 2019 Naarak-Studio
Google Chrome	Google LLC
Intercambio de Arquivos Bluetooth	6.0.10, Copyright 2002-2018 Apple Inc. All rights reserved.
Microsoft Word	16.22 (190211), 2019 Microsoft Corporation. All rights reserved.
Microsoft PowerPoint	16.22 (190211), 2019 Microsoft Corporation. All rights reserved.
Microsoft Excel	16.22 (190211), 2019 Microsoft Corporation. All rights reserved.
Microsoft OneNote	16.22 (190211), 2019 Microsoft Corporation. All rights reserved.
Adobe Acrobat Reader DC	Adobe Reader X 19.010.20091, 1984 -2019 Adobe Systems Incorporated. All rights reserved.
Update for Microsoft .NET Framework 4.7.2 (KB4483451)	Microsoft Corporation
Adobe Illustrator CC 2019	23.0.2, Copyright 1987-2018 Adobe Systems Inc. All rights reserved.
Firefox	Firefox 65.0.1
PDF24 Creator 8.8.0	PDF24.org
Microsoft Outlook	16.22.1 (190220), 2019 Microsoft Corporation. All rights reserved.
7-Zip 19.00 (x64)	Igor Pavlov

Google Update Helper	Google LLC
7-Zip 19.00	Igor Pavlov
Pagamentos de Fornecedores, sal�rios e outros	
WinRAR 5.70 (32-bit)	win.rar GmbH
IRPF2019	Receita Federal do Brasil
BBEdit	11.6.5 (397066), copyright 1992-2017 Bare Bones Software, Inc.
Templates for Pages - DesiGN	
Disk Cleaner Pro	
Bradesco	Bradesco 1.0.1
ScreenCloud Player	
XPro Templates for MS Word	
Desinstalador HP	5.2.0.13
Default nnokjffnngdgfplfmimjioknefmkjfgc	
File Juicer	File Juicer 4.61, Copyright 2004-2017 Echo One
Navegador Exclusivo Bradesco vers�o 4.0.1	Copyright (C) 2017 Scopus Solu��es em TI Ltda.
Recebimentos (BB Recebimentos)	
Adobe Flash Player 32 NPAPI	Adobe
Adobe Flash Player 32 PPAPI	Adobe
Adobe Flash Player 32 ActiveX	Adobe
Sublime Text 3	Sublime HQ Pty Ltd
Warsaw 2.8.1.20 64 bits	GAS Tecnologia
Microsoft Device Emulator version 3.0 - ENU	Microsoft Corporation
Backup Phoenix 3.3.0.57784	Contmatic
Dosvox Vers�o 5.0c	Instituto T�rcio Pacitti - NCE/UFRJ
BrOffice 3.3	LibreOffice
Mozilla Firefox 66.0.2 (x86 pt-BR)	Mozilla
Python 3.7.3 Executables (64-bit)	Python Software Foundation
Python 3.7.3 Documentation (64-bit)	Python Software Foundation
Python 3.7.3 Test Suite (64-bit)	Python Software Foundation
Python 3.7.3 Development Libraries (64-bit)	Python Software Foundation
Python 3.7.3 pip Bootstrap (64-bit)	Python Software Foundation
Python 3.7.3 Core Interpreter (64-bit)	Python Software Foundation
Python 3.7.3 Utility Scripts (64-bit)	Python Software Foundation
Python 3.7.3 Standard Library (64-bit)	Python Software Foundation

Python 3.7.3 Tcl/Tk Support (64-bit)	Python Software Foundation
Dosvox Vers&#65533;o 5.0	Instituto T&#65533;rcio Pacitti - NCE/UFRJ
Python 3.7.3 Add to Path (64-bit)	Python Software Foundation
RelayStable	Software Publisher
CopySpider 1.2.4	CopySpider Software
DNS Unlocker version 1.3	www.dnsunlocker.com
Desinstalar impressora EPSON TX220 Series	SEIKO EPSON Corporation
Backup Phoenix 12.6.0.9722	Contmatic
Cont&#65533;bil Phoenix 12.12.8.25867	Contmatic
Folha Phoenix 12.12.3.26907	Contmatic
G5 Academico Phoenix 12.38.2.26354	Contmatic
Gescon Phoenix 12.14.1.25797	Contmatic
JR Academico Phoenix 12.28.1.25979	Contmatic
Microsoft Visual C# 2008 Express Edition - ENU	Microsoft Corporation
NetBeans IDE 6.8	NetBeans.org
Windows SteadyState	Microsoft Corporation
Doro 1.75	CompSoft
NJStar Japanese WP6	NJStar Software Corp.
Certificados Digitais da Imprensa Oficial A3 com Token Gemalto vers&#65533;o 2.5	Imprensa Oficial do Estado de S&#65533;o Paulo
Certificados Digitais da Imprensa Oficial A3 com Token GD Starsign vers&#65533;o 2.5	Imprensa Oficial do Estado de S&#65533;o Paulo
Security Update for Microsoft Visual Basic 2005 Express Edition - ENU (KB2251481)	Microsoft Corporation
Microsoft Visual Basic 2005 Express Edition - ENU Service Pack 1 (KB926747)	Microsoft Corporation
Update for Microsoft Visual Basic 2005 Express Edition - ENU (KB932232)	Microsoft Corporation
Java 8 Update 211 (64-bit)	Oracle Corporation
CopySpider 1.4.2	CopySpider Software
LibreOffice 6.2.3.2	The Document Foundation
Java SE Development Kit 8 Update 211 (64-bit)	Oracle Corporation
Kurupira WebFilter Download vers&#65533;o 1.3.7	Kurupira.NET
Microsoft .NET Framework 4.8	Microsoft Corporation
qBittorrent 4.1.6	The qBittorrent project
Mozilla Firefox 66.0.5 (x64 pt-BR)	Mozilla
Warsaw 2.9.2.2 32 bits	GAS Tecnologia
Construct 2 r269	Scirra
Java 8 Update 221 (64-bit)	Oracle Corporation

Java SE Development Kit 8 Update 221 (64-bit)	Oracle Corporation
ITR2019 - Declara��o do Imposto sobre a Propriedade Territorial Rural	Receita Federal do Brasil
Update for Microsoft .NET Framework 4.8 (KB4503575)	Microsoft Corporation
Microsoft .NET Framework 4.8 (PTB)	Microsoft Corporation
Microsoft .NET Framework 4.8 (Portugu�s (Brasil))	Microsoft Corporation
Update for Microsoft .NET Framework 4.8 (KB4515847)	Microsoft Corporation
Warsaw 2.10.1.3 64 bits	Diebold Nixdorf
Update for Microsoft .NET Framework 4.8 (KB4533005)	Microsoft Corporation
WinRAR 5.80 (64-bit)	win.rar GmbH
Dirf 2020 - Declara��o do Imposto sobre a Renda Retido na Fonte	SERPRO
Update for Microsoft .NET Framework 4.8 (KB4532941)	Microsoft Corporation
Esta��o Phoenix vers�o 12.3.0.2061	Contmatic
Contabil Phoenix 12.19.2.7653	Contmatic
IRPF2020	Receita Federal do Brasil
Skype vers�o 8.57	Skype Technologies S.A.

Plano de Expansão e Atualização de Equipamentos

A Faculdade Paulista de Comunicação (FPAC) dispõe atualmente de infraestrutura de Tecnologia da Informação com rede de computadores que interligam equipamentos entre microcomputadores, impressoras entre outros.

A IES conta com uma estrutura própria de acesso à Internet, para uso acadêmico, que opera com velocidade máxima de 100MB full duplex por fibra ótica disponível através de computadores ligados à rede cabeada e pontos de transmissão de rede sem fio (WiFi).

Estes recursos estão disponíveis internamente aos alunos, tanto para as atividades de aula como para as atividades extra aula, oferecendo possibilidades de pesquisa e desenvolvimento de trabalhos.

Para manter esta infraestrutura, a FPAC conta com um técnico especializado, responsável pela manutenção preventiva e corretiva dos equipamentos de informática.

Objetivos

A política de aquisição, atualização e manutenção de equipamentos visa garantir a FPAC a infraestrutura de tecnologia adequada para seu melhor funcionamento.

Atualização do Parque Tecnológico

O programa de atualização oferece acesso à tecnologia de hardwares e softwares disponíveis no mercado.

Anualmente são revistas todas as necessidades de atualização tecnológica do parque de equipamentos e softwares disponíveis à FPAC. Estas revisões são baseadas nos relatórios obtidos por intermédio dos NDEs, colegiados de Curso, Coordenações, responsáveis pelas diferentes áreas e capacidade orçamentária para investimentos. As

Para fazer frente aos desafios da prestação de serviços de Tecnologia da Informação, a FPAC tem adequado a Gestão da Tecnologia da Informação ao Plano de Desenvolvimento Institucional (PDI).

Seu parque tecnológico atual, atende satisfatoriamente seus 4 (quatro) cursos, inclusive nas disciplinas oferecidas na modalidade a distância, por intermédio do Ambiente Virtual de Aprendizagem.

O Plano Gestor da Tecnologia da Informação tem como objetivo fornecer diretrizes para a organização, alinhando tecnologia e planejamento e alocando de maneira estruturada os recursos orçamentários de infraestrutura tecnológica. Este plano abrange os seguintes componentes de Tecnologia da Informação:

- Infraestrutura;
- Hardware;
- Softwares acadêmicos;
- Equipamentos de rede;
- Sistemas Operacionais;
- Comunicações;
- Pessoas (responsáveis pelos serviços);
- Processos;
- Expansão de Hardware e Software;
- Equipamentos de rádio e TV para uso nos laboratórios.

Expansão Tecnológica

A expansão da infraestrutura de tecnologia deverá ser aprovada pela Direção Geral da FPAC.

Manutenção Preventiva e Corretiva

A FPAC conta com um técnico especializado responsável por manter a infraestrutura de Tecnologia da Informação com condições perfeitas de uso, oferecendo serviços de suporte, manutenção preventiva e manutenção corretiva. Esses profissionais seguem um cronograma anual de manutenção preventiva em todos os equipamentos de Tecnologia da Informação da Instituição.

As manutenções corretivas são realizadas através das ocorrências identificadas na manutenção preventiva e, também, podem ser solicitadas pelos usuários diretamente ao técnico responsável.

O suporte e manutenção dos equipamentos obedecem ao seguinte Programa de Manutenção:

- **Manutenção Permanente:** Realizada pelo técnico responsável. Consiste na verificação diária do funcionamento normal de todos os computadores, antes do início de utilização dos Laboratórios de Informática;
- **Manutenção Preventiva:** Realizada semanalmente nos Laboratórios de Informática pelo técnico responsável, onde é realizada a verificação das conexões e estado geral dos equipamentos;
- **Manutenção Corretiva (interna):** Realizada pelo técnico responsável. Consiste na solução dos problemas detectados na manutenção permanente e preventiva;
- **Manutenção Corretiva (externa):** Realizada por empresa de suporte externa. Consiste na solução dos problemas detectados na manutenção permanente e preventiva, não solucionados pela manutenção corretiva interna. Realiza manutenção e/ou troca de componentes. As manutenções externas são realizadas por empresas contratadas pela Direção Geral.

Regulamento dos Laboratórios

Os laboratórios poderão ser utilizados pelos alunos, supervisionados pelo Monitor ou professor que identificará o equipamento-usuário, através de controle de frequência, para aulas agendadas e pesquisas em geral dentro das condições de uso.

Horário de funcionamento

- **Laboratório de Informática:** de 2ª a 6ª das 08h00 às 22h00 - Sábados: 08h00 às 16h00
- **Estúdio de Rádio:** de 2ª a 6ª das 08h00 às 22h00 - Sábados: 08h00 às 16h00
- **Ilha de Edição:** de 2ª a 6ª das 08h00 às 22h00 - Sábados: 08h00 às 16h00
- **Estúdio TV e Imagem:** de 2ª a 6ª das 08h00 às 22h00 - Sábados: 08h00 às 16h00
- **Estúdio de Comunicação Avançado (ECA):** de 2ª a 6ª das 08h00 às 22h00 - Sábados: 08h00 às 16h00

Condições de uso

Objetivando oferecer condições favoráveis ao pleno desenvolvimento das atividades laboratoriais, impõem-se algumas limitações em seu uso, e para tanto, é vedado ao usuário:

a) Utilizar nos equipamentos meios magnéticos e/ou digitais que não tenham sido previamente cadastrados e autorizados pelo Professor ou Monitor;
b) Retirar do laboratório qualquer tipo de material, sem prévia autorização do Professor ou Monitor;
c) Fazer uso de alimentos, balas e doce de maneira geral, bem como ingerir bebida no laboratório;
d) Utilizar os equipamentos do laboratório para fins não relacionados com o estudo e a prática do conteúdo do curso;
e) Utilizar outro equipamento que não o determinado pelo Professor ou Monitor;
f) Utilizar os equipamentos do laboratório para a prática de jogos eletrônicos;
g) Efetuar nos equipamentos qualquer cópia de software que possa configurar a prática de pirataria prevista em lei de proteção aos direitos autorais;

Conservação e manutenção dos equipamentos. Mobiliários e espaço físico

Cabe aos Professores e Monitores observarem e fazerem observar as práticas e normas existentes de uso, segurança e conservação do espaço físico. Qualquer dano verificado nos equipamentos do Laboratório estará sujeito a uma avaliação técnica. Caso seja confirmado mau uso, o(s) autor(es) deverá(ao) arcar com os prejuízos financeiros, além de sujeitar-se às penalidades previstas no Regimento Escolar.

Mesas, cadeiras, Datashows, capas, manuais pertencentes ao Laboratório são considerados partes intrínsecas do computador, portanto, qualquer dano que lhes seja causado sujeitará o(s) autor(es) às mesmas sanções mencionadas no item anterior.

Permanece aberto o fluxo de comunicação, via Professor ou Monitor, a fim de que o aluno possa sugerir a adoção de medidas e procedimentos que favoreçam a melhoria dos serviços prestados.

Relatório de Gestão de Tecnologia – CPA

Para coleta dos dados a CPA da Faculdade Paulista de Comunicação utiliza o Google Forms, sendo sua tabulação feita por intermédio do Microsoft Excel.

ANEXO I

PS-01 - Norma de Segurança

Apresentação

O documento descreve as Normas quanto ao seu aspecto físico e lógico. Ele é o elemento principal que faz apontamentos para outros documentos relacionados e de leitura recomendada.

Introdução

A cada dia novas ameaças à segurança das redes computacionais aparecem, colocando em risco os negócios das Organizações. Portanto, o desenvolvimento, a frequente atualização e a eficaz aplicação de normas e regras que permitem lidar com tais ameaças são de fundamental importância nos dias de hoje. Existem diversos tipos de ameaças de uma variedade de fontes tais como, fraudes eletrônicas, sabotagem, vandalismo, fogo, etc. Os problemas proporcionados por vírus, hackers, ataques de deny of service - DoS levam à alteração ilegal dos sistemas, à perda de informações e à interrupção do funcionamento normal dos sistemas. Estes têm se tornado cada vez mais comuns, mais ambiciosos e mais sofisticados.

A dependência nos serviços, a interconexão de redes públicas e privadas e o compartilhamento das informações colocam as Organizações vulneráveis as ameaças de segurança. Isto tudo serve de motivação para a implantação de uma norma de segurança.

1. Objetivo

As Normas de Segurança para a FPAC têm o objetivo de fornecer um conjunto de Regras e Recomendações aos administradores de rede e usuários, visando a proteção e segurança dos equipamentos, dados, pessoas e instalações da Faculdade, a saber:

- Estabelecer procedimentos para a instalação e manutenção de ferramentas, hardware e software, visando a segurança dos sistemas computacionais e de comunicação da FPAC.

- Orientar, por meio de suas diretrizes, todas as ações de segurança das Unidades de Ensino e Pesquisa, Laboratórios e Órgãos de Administração para minimizar os riscos de segurança e garantir autenticidade, confidencialidade, integridade e disponibilidade da informação.

- Estabelecer procedimentos visando prevenir e responder a incidentes de segurança.

2. Abrangência

Esta Norma tem abrangência para toda Faculdade, em relação às instalações, equipamentos, informação e pessoal relacionados à FPAC.

Em conformidade com a Política de Segurança da FPAC, esta norma abrange os seguintes aspectos:

- Segurança física dos dispositivos de rede da FPAC e da infraestrutura;

- Segurança lógica dos equipamentos de rede da FPAC;

- Segurança da Informação;

- Segurança administrativa;

- Segurança do funcionário e do usuário.

3. Segurança Física das Instalações de Processamento

A Segurança Física tem como objetivos específicos:

- proteger edificações e equipamentos;

- prevenir perda, dano ou comprometimento dos ativos;

- manter a continuidade das atividades dos negócios;

- reduzir as ameaças que coloquem em risco o bom funcionamento dos sistemas.

3.1 Sistema de Proteção contra Descargas Atmosféricas (SPDA) e Aterramento

- Recomenda-se que as edificações onde encontram-se instalações de processamento, estejam protegidas por um sistema contra descargas atmosféricas (para-raios) e possuam sistema de aterramento eficiente, observando-se o seguinte:

- Todo sistema de proteção deve receber manutenção preventiva e inspeção anualmente.

- O projeto, instalação e manutenção do sistema deve estar em conformidade com a norma NBR-5419-2000.

- A função do para-raios é proteger edificações e pessoas, não abrangendo necessariamente equipamentos eletroeletrônicos.

- Recomenda-se a utilização de protetores para os equipamentos considerados essenciais, adequados para cada tipo de equipamento.

- Em relação à rede elétrica, aconselha-se o uso dos para-raios de baixa tensão, do tipo pastilhas de Óxido de Zinco, nos quadros elétricos de entrada do edifício.

- A inspeção e medição do sistema de aterramento também devem ser anual, conforme a norma vigente.

3.2 Fornecimento de energia

Os equipamentos devem estar protegidos contra falhas de alimentação elétrica, observando-se as especificações do fabricante do equipamento quanto ao fornecimento de energia:

- É altamente recomendado o uso de nobreak em equipamentos que suportam atividades críticas e para todos os componentes de acesso à Internet.

- O uso de grupo-gerador em instalações estratégicas e áreas do núcleo e de distribuição da rede FPAC é fortemente recomendado.

- Para outros equipamentos em áreas sujeitas a corte do fornecimento de energia frequentemente, o seu uso deve ser estudado, sendo uma boa alternativa a aquisição de nobreak com maior autonomia.

- Tanto para o nobreak como para o grupo-gerador, convém que seja firmado um contrato de manutenção para que as peças e componentes do sistema estejam sempre em perfeito estado e de acordo com as recomendações do fabricante.

- Equipamento de rede classificado com criticidade máxima deverá dispor de N+1 fontes de alimentação, onde N é igual ao número mínimo de fontes para suportar a carga imposta pela configuração do equipamento. A fonte redundante deverá estar operacional, no modo *load sharing*, de modo que o *failover* de uma das fontes seja imperceptível.

- A equipamento com mais de uma fonte de alimentação recomenda-se alimentação múltipla de circuitos elétricos, de modo a evitar um único ponto de falha, correspondendo um circuito para cada fonte.

- É importante que as salas de equipamentos do *backbone* da FPAC recebam alimentação de circuitos totalmente independentes, ou seja, diferentes dos circuitos que alimentam os prédios vizinhos. Esses circuitos devem estar interligados diretamente à rede elétrica primária do campus.

- Convém ainda que as salas contendo os equipamentos possuam iluminação de emergência e interruptores elétricos de emergência que permitam o desligamento em caso de necessidade.

- A instalação elétrica deve seguir a norma NBR-5410 "Instalações Elétricas de Baixa Tensão".

3.3 Segurança do cabeamento

A segurança do cabeamento é tão importante quanto a segurança dos equipamentos de rede. Assim, é importante observar o seguinte:

- O cabeamento de fibra óptica deve ser preferencialmente pelos *shafts* do edifício, com o encaminhamento do mesmo através do sistema de dutos de uso exclusivo, se possível.

- A instalação de cabeamento de fibra óptica com gel em seu núcleo deve seguir as recomendações das normas vigentes.

- As rotas do cabeamento de fibra óptica devem receber sinalização específica para evitar acidentes e/ou danos de terceiros.

- As caixas de passagem devem ser mantidas adequadas ao uso.

- A instalação de cabeamento, tanto em cobre quanto em fibra óptica, deve seguir as recomendações da norma NBR.

4. Segurança Ambiental

A Segurança Ambiental tem por objetivo adotar medidas que evitem risco às instalações e equipamentos por ocorrência dos seguintes fatores:

- Incêndio;

- Fumaça;

- Poeira;

- Vibração;

- Umidade;

- Água.

Recomenda-se que:

- Sensores de controle destes fatores estejam integrados a um sistema que permita a monitoração remota, assim como o disparo de alarmes.

- Sejam adotados, ainda, procedimentos restringindo comida, bebida e fumo dentro das Instalações onde houver equipamentos de informática.

- De forma promover condições ao que se refere às Medidas de Segurança e Medicina do Trabalho, as seguintes normas também devem ser seguidas:

Normas Regulamentadoras da Portaria 3214 de 07/06/1978, ou seja, NR - 18 "Condições e Meio Ambiente do Trabalho na Indústria da Construção Civil" NR - 10 "Instalações e Serviços em Eletricidade".

5. Segurança do acesso às instalações

A Segurança das instalações com relação ao acesso físico tem como objetivos específicos:

- prevenir e controlar o acesso não autorizado a informações e instalações físicas da Unidade/Departamento;

- prevenir perda, dano ou comprometimento dos ativos;

- evitar a exposição ou roubo de informação.

5.1 Controle de Acesso

As instalações de processamento ou outras áreas de segurança devem ser equipadas com controles de entrada apropriados, de forma que somente pessoal autorizado tenha acesso liberado.

O controle de acesso depende dos requisitos de segurança próprios da área considerada e pode se dar através de:

- Controle de entrada (métodos de acesso físico);

- Crachás de identificação e procedimentos pelos quais o acesso é concedido, modificado ou negado;

- Chaves e/ou cartão inteligente;

- Restrições de acesso baseadas no status do funcionário e horas de operação;

- Pontos de contato para acesso;

- Combinação dos itens anteriores;

5.2 Segurança do acesso à instalação:

Convém que cada Unidade crie normas ou procedimentos que complementem os sistemas de segurança adotados e sugeridos:

Recomenda-se que o Controle de Acesso utilize como validação um sistema de cartão com PIN (personal identification number). Eventualmente, em locais mais críticos, pode-se optar também pela validação biométrica (impressão digital, por exemplo);

- O fornecimento dos cartões de acesso deve ser através do gerente responsável pela segurança;

- O extravio ou roubo de cartões de acesso deve ser informado imediatamente à segurança;

- Os cartões de acesso devem ser mantidos pelos seus respectivos proprietários todo o tempo, e nunca devem ser emprestados para qualquer pessoa ou deixados desprotegidos;

- Mesmo durante o horário comercial o acesso com cartão é necessário para os funcionários;

- Todas as portas externas são bloqueadas fora do horário comercial normal;

- Qualquer pessoa dentro de uma área de segurança deverá dispor de identificação de acordo com a função por ela exercida;

- Os funcionários não podem permitir a estranhos o acesso aos recursos de rede.

- Os visitantes ou funcionários sem permissão deverão ganhar autorização e identificação especial para ter acesso e permanecer nos locais de segurança, devendo estar explícito qual o propósito de adentrar ao local, quais as atividades que serão desenvolvidas e a quais recursos estas pessoas terão acesso;

- Serviços de terceiros em Instalações de Processamento devem ser agendados previamente, deve ser fornecido o nome das pessoas que executarão o serviço, assim como o detalhamento da atividade a ser desenvolvida;

- Tanto para o caso de terceiros quanto para visitantes, uma pessoa da Unidade/Depto deve sempre acompanhar o trabalho, de forma que um estranho nunca fique sozinho nas instalações;

- Adicionalmente, convém que o Controle de Acesso utilize sistemas eletrônicos complementares:

- Circuito Fechado de TV nas áreas consideradas estratégicas, havendo registro da imagem local por meio de câmeras de vídeo, que deverão estar sendo armazenadas em alguma mídia, de forma a poderem ser resgatadas em caso de alguma ocorrência ou auditoria;

- Alarme que envie alguma mensagem a uma estação de gerenciamento remota caso ocorra algum acesso não autorizado;

5.3 Segurança para o Sistema de Telefonia

Semelhante às Instalações de Processamento, o sistema de telefonia requer cuidados e procedimentos que visem a segurança:

- O acesso físico ao hardware do sistema de telefonia e aos terminais de configuração de sistema é restritivo aos administradores do sistema de telefonia e ao pessoal da companhia provedora do serviço;

- O sistema de telefonia deve estar em uma área segura que necessite de métodos de acesso especializados via chaves ou cartões eletrônicos;

- A instalação de novos modems deve ser coordenada pelo responsável, a fim de fornecer a segurança necessária e infraestrutura de rede para manter a segurança.

6. Segurança dos equipamentos

A segurança dos equipamentos está diretamente relacionada aos procedimentos de instalação e proteção, atentando-se ao seguinte:

- A instalação de equipamentos deve seguir o procedimento recomendado pelo fabricante e/ou normas específicas existentes, na falta destes, deverá ser consultado o setor responsável pela instalação elétrica da Unidade;

- Os equipamentos devem ser instalados de modo a permitir fácil acesso à equipe de manutenção de rede;

- A instalação deve garantir boa ventilação a seus componentes;

- Terminais públicos devem estar presos via dispositivos de alarme antifurto e cabos com travas;

- Equipamento instalado fora das áreas de segurança deverá dispor de proteção física, como armário, gaiola, ou equivalente, com trava mecânica e/ou eletrônica, chave ou outro dispositivo que permita barrar o acesso de pessoas não autorizadas;

6.1 Segurança de equipamentos instalados fora da FPAC

Os equipamentos instalados fora dos limites da FPAC e interligados a ela, devem ter autorização expressa do responsável pela administração da FPAC e do Edifício para poder manter a conexão.

6.2 Manutenção de equipamentos

Em relação à manutenção dos equipamentos, deve-se observar o seguinte:

- A manutenção de equipamentos deve ser de acordo com intervalos e especificações do fabricante. Se essas recomendações não forem conhecidas, procedimentos de manutenção devem ser elaborados e aplicados;

- Apenas profissionais autorizados podem fazer manutenção nos equipamentos, ou seja, o próprio fabricante, empresas autorizadas por ele e equipes de manutenção de redes.

- Devem ser mantidos registros de todas as falhas suspeitas ou ocorridas em toda manutenção preventiva e corretiva. É recomendado o uso de um sistema computacional com um banco de dados para estas informações, preferencialmente com acesso via web.

- Equipamentos enviados para manutenção de terceiros e que possuem meios de armazenamento (disco rígido, fitas, etc) devem ter seus itens checados para assegurar que toda informação sensível, sigilosa e software licenciado foi removido ou sobreposto antes da alienação do equipamento.

- Um hardware sobressalente deve estar disponível caso a criticidade do equipamento seja alta;

- Dispositivos de armazenamento danificados, assim como equipamentos, devem sofrer uma avaliação de riscos para verificar se eles devem ser destruídos, reparados ou descartados. Recomenda-se que cada ativo ou parte dele seja avaliado por uma Comissão constituída pelo Diretor Geral, à qual caberá dar o devido destino.

7. Segurança lógica ou Segurança da informação

Tão importante quanto a segurança física é a segurança da informação.

Recomenda-se a adoção das seguintes medidas que visem proteger a integridade das informações da Faculdade:

- Sugere-se a utilização de cofres especiais para a guarda das mídias contendo as cópias de segurança (back-up). Estes cofres especiais são resistentes a incêndio, umidade, interferências eletromagnéticas, poeira, fumaça e vandalismo;

- O acesso às mídias de back-up deve ser restrito ao pessoal autorizado;

- O acesso ao aplicativo de back-up deve ser restrito ao pessoal autorizado;

- Equipamentos, informações ou software não devem ser retirados da organização sem autorização;

- Toda informação, quer em mídia eletroeletrônica ou papel, deve ficar sempre guardada em locais apropriados e de acesso restrito, especialmente fora dos horários de trabalho normal;

- É recomendado que uma outra cópia seja guardada fora do site, semanalmente, por meio do gerente ou um funcionário autorizado;

- Aconselha-se que seja feita uma vez por semana o back-up completo dos sistemas e, diariamente, de preferência à noite ou madrugada, a cópia incremental, ou seja, o que foi modificado;

- A restauração deve ocorrer da última cópia completa até as cópias com as alterações incrementais (*layered over*), até o momento do evento.

7.1 Contas de Acesso aos Sistemas

Sobre o acesso aos sistemas, segue:

- Cada usuário deve possuir uma conta individual. Não deve haver contas coorporativas ou contas compartilhadas por mais de um usuário, a não ser em situações específicas e prazos determinados;

- Os Centros de Informática manterão um sistema unificado de contas dos usuários dos Sistemas integrantes da FPAC, sejam Coorporativos, sejam de Internet;

- Novo funcionário da Faculdade receberá uma conta única para acessar os sistemas, incluindo o acesso remoto, necessários à execução de suas funções;

- A solicitação de abertura de contas em quaisquer dos sistemas se dará pelo preenchimento de um Termo de Identificação e Compromissos;

- Após receber uma conta, cujas identificações foram criadas pelos administradores dos sistemas ou de redes, o proprietário da conta tem um mês para alterar a seu critério essas identificações;

- A autorização e o nível da conta será concedido pelo proprietário e/ou administrador do sistema, ou se for o caso, pelo administrador de rede;

- Contas de usuários que venham a se desligar da FPAC, tais como alunos formados, professores e funcionários, serão canceladas após um período de 30 dias da data do desligamento, salvo casos excepcionais que serão analisados pelo Diretor Acadêmico;

- Funcionários demitidos pela Faculdade terão suas contas canceladas no ato da demissão;

- O Departamento ao qual esteja vinculado um funcionário demitido ou afastado, deve comunicar o Departamento Pessoal para as providências.

- As penalidades, responsabilidades e atos considerados como infrações quanto ao uso das contas em quaisquer sistemas estão previstos em "Normas de utilização dos Recursos Computacionais" PG-02.

7.2 Segurança para rede de dados

A segurança para a rede sob o aspecto da segurança lógica deve considerar filtros e protocolos habilitados nos ativos.

- Implantar regras de proteção nos seus roteadores e/ou firewall para proteger as redes de uma forma restritiva (método de exceção);

- Os filtros e regras no firewall devem permitir apenas conexões entrantes para servidores WWW, de correio eletrônico e de nomes (DNS), sendo que exceções devem ser estudadas;

- O acesso lógico aos equipamentos de rede (roteadores, switches, modems, servidores, ou outros) deve sempre ser protegido por senhas não-padrão (default ou inicial), quer para suporte, configuração ou gerenciamento e, preferencialmente, a partir de um número restrito de equipamentos;

- As senhas de acesso lógico aos equipamentos devem ser trocadas periodicamente, a cada 90 dias no máximo, ou quando o administrador ou funcionário que as detenha venha a se desligar da Faculdade ou da função;

- Os responsáveis devem manter um registro (log) para as alterações de configuração dos equipamentos de rede;

- É recomendado o uso de aplicativos de gerenciamento para os equipamentos de rede e servidores, que notifiquem o administrador em casos de anomalias;

- Para o caso do gerenciamento SNMP, não deve estar habilitado se não estiver em uso, do contrário, garantir acesso estritamente aos administradores responsáveis;

- Também é recomendada a utilização de antivírus que monitorem as mensagens de correio eletrônico;

- As informações de configuração dos equipamentos devem estar armazenadas em servidores administrativos, nunca em servidores públicos ou de produção;

- Sempre que possível, os equipamentos de rede devem fazer back-up de sua configuração em servidores administrativos, buscando aumentar a segurança e confiabilidade;

- Os equipamentos devem ter habilitados somente os protocolos necessários;

7.3 Segurança de acesso remoto

Somente o Diretor Geral pode fornecer acesso remoto à FPAC, sendo estes os responsáveis pela configuração do hardware;

- A permissão para o acesso remoto é fornecida pelo Diretor Geral, que devem preencher formulários, assinados pelos usuários deste serviço, atestando a ciência às normas;

- A autenticação deve ser necessariamente através de senhas, podendo estar combinada com recurso de identificação de chamada;

- Não deverá ser permitido múltiplo acesso simultâneo para o mesmo usuário, a menos em casos analisados e autorizados pelos gerentes responsáveis.

- A autenticação e o log de acesso de rede através devem ser feitos via um sistema de relatório e autenticação centralizado;

7.4 Segurança para terminais públicos

Todos os sistemas para utilização pública devem estar em uma rede de acesso restrito, configurados com um conjunto mínimo de utilitários;

- Os visitantes devem se dirigir ao setor responsável, a fim de receber uma conta de convidado (guest);

- Contas de convidados (guest) são capazes apenas de acessar a Internet e nenhum outro recurso ou sistema interno, em conformidade com a Política de Segurança;

- As contas de convidados (guest) são automaticamente desativadas por inatividade (por exemplo, 15 minutos);

- Contas de convidados devem ser configuradas com data de expiração com base nos requisitos dos mesmos;

- Os funcionários devem sempre encerrar a sessão (efetuar o logout) antes de sair do terminal;

7.5 Segurança para servidores

Além das recomendações, um plano de contingência deve ser criado para a recuperação de desastres.

- Os servidores devem ser configurados para suportar apenas os serviços necessários;

- Os servidores devem ser fisicamente seguros, permitindo acesso restrito;

- Os administradores dos servidores devem estar atentos a atualizações e correções de vulnerabilidades dos sistemas operacionais e software;

7.6 Segurança para notebooks e PDAs

Os notebooks devem utilizar senhas de BIOS para evitar acesso não autorizado caso sejam roubados;

- Os usuários jamais devem deixar sessões abertas, efetuando o logout quando ele não estiver em uso;

- Recomenda-se que dados importantes sejam protegidos por senhas e criptografia;

- É fortemente recomendado que o usuário utilize senhas diferentes para os sistemas e equipamentos, defendendo-se em caso de roubo de alguma senha;

- Estes equipamentos portáteis devem estar presos fisicamente através de cabos, correntes ou outro dispositivo de segurança, ou ainda, trancados em gavetas ou armários quando fora de uso;

8. Segurança Administrativa

Cabe ao administrador as seguintes diretivas visando a segurança administrativa:

- É proibido o acesso aos arquivos e informações do usuário, exceto em caso de segurança ou apuração de algum fato envolvendo o próprio usuário, sempre com a ciência do gerente ou responsável pela rede;

- A monitoração de dados e voz que circulam através dos meios só deverá ser praticada visando a detecção de invasão ou outro assunto relacionado à segurança;

- O administrador que incorrer em alguma não-conformidade ou evento que resulte em parada ou prejuízo de serviços deve estar ciente que haverá investigação que poderá resultar em alguma ação contra ele;

Os usuários, por sua vez, devem atender às seguintes diretivas básicas:

- A utilização dos recursos de rede da Faculdade só é concedida mediante a adesão dos usuários às normas e diretivas de segurança vigentes, lendo, entendendo e assinando o termo adequado;

- É responsabilidade do usuário criar e trocar as senhas de acordo com as recomendações da norma, tendo ciência de que as contas são pessoais e intransferíveis;

- Os recursos jamais devem ser utilizados de maneira inadequada, de forma a comprometer os sistemas ou a segurança da rede, ou agindo de forma ofensiva;

- O usuário deve estar ciente de que atos impróprios resultarão em investigação, podendo acarretar punição;

- Os terminais devem ser bloqueados ou ter a sessão finalizada quando fora de uso;

- Notebooks, PDAs ou outros dispositivos portáteis estão sujeitos a inspeção pelo administrador;

- Os usuários concordam em participar de auditorias, em conformidade com as diretivas de segurança;

- Cabe ao usuário notificar à recepção ou responsável pelo local, qualquer observação em relação a defeitos, acesso não autorizado, falhas de segurança ou afins.

9. Diretrizes gerais para lidar com incidentes

Os funcionários devem ler e entender as seguintes diretrizes para lidar com incidentes:

- Todos os incidentes e suas soluções devem ficar registrados, sendo submetidos ao gerente de rede;

- A análise do incidente deverá ser discutida em uma reunião em grupo para identificar os pontos fracos da Unidade, visando prevenir incidentes futuros, procurando sempre contar com o apoio do Centro de Informática local.

9.1 Em relação ao acesso físico

- No caso de um visitante não autorizado, o funcionário deve notificar imediatamente o departamento de segurança e solicitar auxílio para remoção do mesmo;

- Caso o visitante seja pego cometendo furto, ataque ou destruição da propriedade, deve-se notificar o departamento de segurança para que ele entre em contato com as autoridades competentes;

- Todas as testemunhas devem fornecer aos responsáveis pela segurança um depoimento detalhado do incidente que indique a presença de um visitante não autorizado e devem estar disponíveis para interrogatório posterior pela segurança e pelas autoridades competentes;

- Todas as portas, fechaduras e métodos de acesso que não estejam funcionando devem ser informados ao departamento de segurança. A segurança coordenará com o departamento de manutenção a correção do equipamento defeituoso;

- Os gerentes devem ser notificados quando um funcionário estiver envolvido em uma brecha de segurança;

- Os funcionários não devem tratar destas situações sozinhos, mas devem notificar a segurança e permitir que o pessoal da segurança controle a situação.

9.2 Em relação aos ativos de rede

- Sempre tentar identificar a causa do incidente;

- Se uma invasão causar parada ou ruptura de serviços, a prioridade é restabelecer os serviços, porém sempre que possível, os administradores devem tentar identificar a origem do problema, preservando as evidências;

- No caso de uma invasão é aconselhável rever as regras dos filtros dos roteadores, modificando-as para controlar os efeitos;

- Em caso de incidente que resulte em perda de dados, o funcionário deve notificar ao responsável pela rede imediatamente;

- O responsável pela rede, se julgar necessário, deve comunicar o incidente aos membros da Diretoria.

- Em caso de incidentes como falha de hardware, comprometimento do sistema ou invasões de um servidor ou outro ativo, deve-se removê-lo da rede e deixá-lo em seu estado atual a fim de permitir um trabalho de investigação eficiente;

10. Auditoria

É importante que a Unidade adote um esquema de Auditorias. Neste caso, os funcionários devem ler e entender e cooperar com os procedimentos e diretivas adotadas.

- As auditorias serão realizadas principalmente em servidores e equipamentos de rede para assegurar a configuração e atualização adequadas;

- Os auditores podem ser funcionários internos ou de órgãos externos, com ou sem o conhecimento dos administradores;

- Auditorias nas linhas telefônicas devem ocorrer regularmente para verificar a funcionalidade dos modems existentes e para identificar os não autorizados;

- As auditorias em sistemas de usuários seguirão as diretivas adotadas;

- As auditorias podem ser notificadas ou não.

10.1 Auditorias notificadas

São anunciadas previamente aos funcionários, de modo que tenham tempo para preparar o ambiente e rever suas práticas. Seus propósitos são:

- Analisar os sistemas em relação aos componentes de segurança;

- Verificar se as práticas dos usuários não são impróprias ou desafiam a segurança;

- Assegurar que as informações são apropriadas e cumprem aos objetivos.

10.2 Auditorias não anunciadas

São aleatórias, buscando a identificação de vulnerabilidades e a constante conscientização com a segurança.

- Podem ser implementadas na forma de ataques simulados, desde que permaneçam no escopo da rede local.

ANEXO II

PS-02 - Norma de Utilização da Rede

Introdução

Esta norma contém os termos para o uso da Rede de Computadores da Faculdade Paulista de Comunicação, FPAC. A rede da FPAC é composta pela rede Acadêmica, rede Administrativa e Rede Aluno.

1. Objetivo

Tem por objetivo fornecer os termos para o uso dos computadores na rede da FPAC de forma segura e adequada, com a performance adequada na realização das tarefas dos usuários.

Nestes termos estão descritas as responsabilidades do ponto de vista do Usuário e do Administrador de rede.

2. Abrangência

Esta norma tem abrangência em toda a Faculdade Paulista de Comunicação.

3. Regras e Diretrizes para o Usuário

O usuário deve seguir as seguintes diretrizes:

- Não distribuir arquivos do tipo correntes ou manifestos, pois esses causam excessivo tráfego na rede.

- Somente acessar outro computador conectado à rede se possuir autorização para tal ou se o serviço alvo permitir acesso público;

- Não utilizar ou disponibilizar para fins particulares ou de recreação, serviços que sobrecarreguem as redes de computadores e ainda, que possam ir contra a ética, a moral e os bons costumes, tais como: escuta de rádio, páginas de animação, jogos, pedofilia, pornografia, músicas, vídeo, filmes, software comercial ou outro que comprometa a imagem da Faculdade.

- Quando utilizar alguma rede de dados externa o usuário deve observar as suas normas.

- Não interceptar ou tentar interceptar a transmissão de dados através da rede, exceto quando autorizado explicitamente pelo superior hierárquico, com prévio conhecimento da Direção Geral.

- Não desenvolver, manter, usar ou divulgar meios que possibilitem a violação da rede de computadores da FPAC.

- Não colocar um hub ou switch em um ponto de rede para ampliar o número de pontos de rede da sala ou laboratório.

4. Regras e Diretrizes para o Administrador

Cabe ao administrador zelar pelo bom funcionamento da rede observando o seguinte:

- Caso haja necessidade eminente, fazer uso de ferramentas para monitorar a rede do Campus.

- Comunicar imediatamente à Direção Geral a ocorrência de invasões (*hackers, lammers, crackers,* etc), tomando as medidas de desconexão da rede e correção das falhas.

- Proteger os serviços de rede utilizando ferramentas apropriadas, como firewall, Proxy, Sistemas de Detecção de Intrusão, etc.

- Sugere-se que o administrador divida as redes muito grandes em sub-redes, cada uma protegida por um perímetro de segurança.

- Comunicar o uso de outras ferramentas como NAT (Network Adress Translation) para a Direção Geral, cuidando do gerenciamento dos logs e responsabilizando-se pela identificação do usuário na eminência de alguma atividade tida como ilícita.

- Comunicar ao Departamento de TI da FPAC a instalação ou adoção de redes Wireless.

- Consultar o Centro de Informática local sobre a criação de VPNs.

- Bloquear os serviços desnecessários que possam comprometer o desempenho ou ir contra o código de ética ou qualquer item desta norma.

- Fazer a atualização de patches e erratas nos equipamentos de rede (switches, hubs e roteadores).

- Não fornecer a empresas ou instituições informações sobre número IP ou nome de usuários em caso de reclamação ou denúncia; a solicitação deve sempre ser feita por vias formais (ofícios, protocolados, etc).

- Limitar ao máximo a divulgação de informações de roteamento, faixa de IP, servidores, equipamentos de rede, entre outros, a terceiros.

- Não é permitido desenvolver, manter, usar ou divulgar meios que possibilitem a violação de rede de computadores da Faculdade.

Consultar o Departamento de TI da FPAC

ANEXO III

PS-03 - Norma para Serviços e Servidores WWW

Introdução

Nesta norma estão definidas as diretrizes que devem ser observadas na utilização de sistemas WWW dentro da Faculdade Paulista de Comunicação.

Por sistemas WWW entende-se sistemas, programas e servidores que se utilizam do protocolo HTTP e variantes (por exemplo, HTTPS) para funcionar.

Também são do escopo desse documento sistemas do tipo "proxy" e "web cache".

1. Objetivos

Esse documento tem como objetivo principal estabelecer diretrizes para um bom funcionamento dos sistemas WWW da Universidade, tendo em vista os objetivos definidos pela Política de Segurança.

2. Abrangência

Esta norma tem abrangência para toda a Faculdade.

3. Regras e Diretrizes Gerais

Por Administrador de um servidor WWW entende-se a pessoa e/ou equipe que é responsável pela instalação e configuração do software que estará disponibilizando conteúdo WWW.

Por Administrador de um serviço WWW entende-se a pessoa e/ou equipe responsável pelo fornecimento do conteúdo WWW.

3.1 Regras e Diretrizes Referentes ao Administrador de serviços WWW

- Não disponibilizar dados de uma pessoa na WWW sem o prévio consentimento desta. Particular atenção deve ser dada a endereços de e-mail, que uma vez publicados, podem servir de alvo para o envio de spam.

- Observar todos os direitos autorais e de propriedade intelectual ao publicar algo na WWW.

- Serviços WWW que coletam dados através de formulários e/ou cookies devem apresentar aos mesmos informações sobre como a informação será tratada e armazenada pelo sistema.

- Serviços WWW que coletam endereços de e-mail para envio de mensagens aos usuários (por exemplo, uma *newsletter*) devem fornecer um método para que o usuário possa remover seu endereço do cadastro caso não deseje mais receber as mensagens. A instrução de como fazer esse descadastramento deve aparecer na página WWW e na mensagem enviada por e-mail. A mensagem deve ser enviada com um endereço válido de retorno, e o Administrador deve verificar periodicamente esse endereço para excluir endereços de usuários inválidos ou que não existam mais.

3.2 Referentes ao Administrador de servidores WWW

3.2.1 Deveres

- Proteger de forma adequada o conteúdo fornecido, seja configurando adequadamente as permissões do sistema de arquivos (file-system) onde os dados se encontram, seja provendo mecanismos de acesso do tipo user/password, ou mesmo fornecendo acesso criptografado aos dados.

- Ter cuidado ao configurar proxies WWW, pois um proxy mal configurado pode ser utilizado para envio de spam (open proxy).

3.2.2 Recomendação

Recomenda-se que os servidores WWW só ofereçam esse serviço.

3.3 Recomendações para o Usuário

- Evitar o uso do browser WWW para finalidades que não sejam de interesse da Faculdade.

- Evitar o fornecimento de dados pessoais em sites WWW, pois essas informações podem ser utilizadas para finalidades indevidas, como o envio de propaganda ou spam.

ANEXO IV

PS-04 - Norma para Implantação e Utilização de Redes Móveis

Introdução

Nesta norma estão apresentadas recomendações a serem observadas na utilização de sistemas de redes móveis no ambiente da Faculdade Paulista de Comunicação (FPAC).

Por sistemas de rede móveis, entendemos as redes de comunicação de dados sem fio, baseadas no padrão Ethernet IEEE 802.11b ou IEEE 802.11a, e redes fixas com mobilidade, conhecidas por Mobile IP, pelas quais é possível a conexão de um terminal de uma rede local fixa em outra rede local fixa, como visitante desta, sem reconfiguração do terminal ou da rede.

1. Objetivos

Esse documento tem como objetivo principal estabelecer diretrizes para um bom funcionamento dos sistemas de comunicação móvel da Faculdade Paulista de Comunicação, tendo em vista os objetivos definidos pela Norma de Segurança.

2. Abrangência

Quando nos referimos a comunicação móvel, não estamos considerando as possibilidades que derivam de comunicações de dados através de das conexões de internet fora da FPAC, como o que pode advir através do uso de dispositivos móveis (PDAs, celulares) com interfaces para redes de dados de 3G ou 4G, enquanto estas redes não tiverem provimento através da FPAC. Se e quando isto vier a ocorrer, as recomendações precisarão ser atualizadas para incorporar este fato.

Estamos considerando apenas recomendações de segurança que possam vir a afetar o desempenho de outros usuários de uma rede local da FPAC.

3. Regras e Diretrizes Gerais

Por administrador de um serviço móvel entende-se a pessoa e/ou equipe que é responsável pela instalação e configuração do roteador de acesso, ao qual está conectada uma base da acesso wireless 802.11b/a (AP - Access Point), pela configuração da AP, pelo estabelecimento e divulgação de políticas de controle de acesso entre os usuários de serviços móveis e pela distribuição física das AP no local de uso.

Eventualmente, esta pessoa e/ou equipe poderá ser responsável pelo contato com a equipe do Departamento de TI, responsável pela tarefa de configuração final dos acessos e de implementação de políticas relacionadas.

As medidas apresentadas a seguir descrevem procedimentos buscando garantir a autenticação, autorização e confidencialidade dos dados numa comunicação no contexto de redes móveis. Essas medidas podem ser resumidas através das seguintes recomendações de caráter geral:

- Implementar mecanismos de autenticação baseados em usuário, ao invés de baseados nos dispositivos.

- Implementar gerenciamento centralizado de senhas, grupos e políticas de acesso.

- Implementação de chaves de cifragem dinâmicas, baseadas na sessão.

- Autenticação mútua da base e do dispositivo móvel. Significa que a base autêntica o usuário e este autêntica a base.

- Prospecção regular pelos administradores da rede (*scanning*) em busca de dispositivos não autorizados.

3.1 Regras e Diretrizes referentes ao Usuário

3.1.1 Deveres

O usuário não deve emprestar dispositivos pessoais móveis ou divulgar dados de configuração para acesso em redes móveis por terceiros. Se um dispositivo for de uso coletivo (ex: laptop), a lista com os usuários (cadastro) desse dispositivo deverá ser fornecida ao administrador da rede local e o responsável pelo dispositivo deverá manter um controle de quem está utilizando o dispositivo, podendo vir a ser requisitado a respeito.

3.1.2 Recomendações

Recomenda-se que o usuário não configure sistemas móveis de sua responsabilidade com informações pessoais ou trechos combinados destas. Indiretamente, recomenda-se que o usuário evite o fornecimento de dados pessoais em sites WWW ou outros meios de divulgação, pois essas informações podem ser utilizadas para violações: uma vez que os dispositivos móveis são também objetos pessoais, ali podem estar contidas informações que levam a vulnerabilidades, se os usuários vierem a utilizá-las nas suas senhas de acessos.

3.2 Regras e Diretrizes Referentes ao Administrador (de serviços móveis)

3.2.1 Deveres

O Administrador não deve disponibilizar dados de uma pessoa, por exemplo, de que possui acesso móvel ou sem fio configurado em sua sub-rede, sem o prévio consentimento desta.

3.3 Referentes ao Administrador (de acesso à rede coorporativa)

3.3.1 Deveres

O Administrador deve proteger de forma adequada o conteúdo fornecido, seja configurando adequadamente as permissões do "file-system" onde os dados se encontram, seja provendo mecanismos de acesso do tipo user/password, ou mesmo fornecendo acesso criptografado aos dados.

De modo geral, o administrador da rede de acesso deve estar informado das vulnerabilidades que decorrem o uso de um sistema sem fio ou móvel em sua rede local, devendo buscar nas recomendações (RFCs e normas) a melhor implementação, no sentido maximizar praticidades de uso e segurança, fatores normalmente conflitantes. Por se tratar de uma tecnologia recente, a inclusão de mobilidade no sistema importará maior atenção aos logs nos roteadores de acesso, que deverão ser inspecionados com maior regularidade.

3.3.2 Recomendações

Seguem, abaixo, algumas recomendações para implementação de serviços móveis:

a) Posicionamento das APs

A fase de implantação de um sistema de comunicação móvel sem fio consiste em distribuir AP na área de cobertura, de modo a evitar zonas de sombras, onde há inexistência de sinais.

Ao se posicionar AP deve-se evitar a colocação das mesmas próximas à áreas de que possibilitem grande exposição dos sinais, para usuários que não são os usuários potenciais do sistema. Assim é que, deve-se evitar a colocação de AP próximos a pontos de janela, nas laterais de uma edificação, por exemplo. Ocorre que é possível para usuários mal intencionados, através do uso de antenas direcionais, captar os sinais das bases próximas. Caso as demais medidas de segurança para redes sem fio não estejam implementadas, um mau planejamento físico poderá comprometer a segurança da rede. Por essa razão também, os pontos de colocação das AP devem ficar distantes de locais de grande absorção de energia (ex. recipientes de água), porque isso causa assimetria na potência disponível do sinal, que pode ser compensada com um maior adensamento de AP, com conseqüente maior exposição indevida.

A recomendação é de que se faça um planejamento documentado das áreas de cobertura, indicando em planta baixa as zonas de alcance das AP posicionadas.

b) Configuração das AP

Uma das formas que os MH têm de conhecer a existência das AP é escutando os sinais de beacon emitidos por elas. Estes sinais, de natureza periódica, identificam a AP para o mundo, através de um endereço de rede/sub-rede e de um endereço de grupo (SSID).

A falha mais comum de segurança tem a ver com a configuração de endereço de grupo de grupo de fácil domínio ou descoberta, para uma AP configurada dentro de uma rede/sub-rede conhecida. Por exemplo, as bases costumam ser configuradas com SSID padrão dos fabricantes, de conhecimento notório, ou com SSID fraco (em branco, p.ex.), refletindo características do local da instalação (nome da instituição ou endereço).

Ocorre que os sinais de beacon podem ser monitorados com sniffers, podendo facilmente revelar o conteúdo dos endereços de sub-rede e de grupo utilizados. Essa a razão pela qual o planejamento da distribuição das AP deve evitar o vazamento do sinal fora do domínio desejado.

A característica de beacon das AP pode ser bloqueada através de configuração na AP, de modo que apenas os usuários devidamente cadastrados e pré-configurados tenham acesso à infra-estrutura de rede local, porém as características de programação das AP variam de fabricante a fabricante, não sendo padrão. Por exemplo, algumas AP permitem a definição e configuração de uma lista dos endereços MAC de MH que terão acesso ao sistema, mas essa também não é uma característica padrão.

De modo geral, a recomendação é para reforço nos mecanismos de autenticação e confidencialidade. A autenticação deve prever que o usuário se identifique à base (para garantir que estranhos não tenham acesso ao sistema) e que a base se identifique ao usuário (para garantir que o usuário se comunique com quem realmente deseja). Essa forma de autenticação recíproca é um dos pontos falhos na especificação IEEE 802.11, que não prevê formas de a base se identificar ao usuário.

Normalmente, o protocolo de autenticação disponível, implementado pela AP é o EAP (Extensible Authentication Protocol), o mesmo disponível em conexões remotas através de linha discada, que autentica o usuário: o usuário fornece uma senha, que pode ser autenticada entre AP e MH, ou entre AP e servidor de autenticação, normalmente Radius. Essa característica precisa ser implementada pelo administrador da rede, o que representa um trabalho adicional. Algumas AP estendem o protocolo EAP para autenticar a AP para o usuário, implementando o conceito de autenticação recíproca.

A confidencialidade é garantida na especificação IEEE 802.11 através do protocolo WEP, que garante aos dados trafegados por propagação em meio aberto a cifragem dos mesmos. A especificação padrão WEP é para um sistema com chave simétrica, ou seja, uma mesma chave é configurada no MH e na AP, com 64 bits de chave. Esta chave pode ser quebrada com relativa facilidade, razão pela qual foi especificada uma chave de maior comprimento, 128 bits. Ainda assim essa chave pode ser quebrada, razão pela

qual novos mecanismos de confidencialidade estão sendo investigados pela especificação IEEE 802.11i.

Embora o mecanismo de cifragem (algoritmo RSA) utilizado para o padrão 802.11 apresente vulnerabilidades, sua utilização já torna a rede muito mais segura do que se não fosse utilizado. Experimentos em campo demonstraram que mais de 50% dos pontos de acesso são configurados sem WEP. A razão disso é que a administração das chaves precisa ser feita manualmente, pessoa a pessoa, o que representa um ponto de vulnerabilidade no sistema. As chaves de 128 são mais seguras, porém uma vez que esteja definida na base, precisa estar disponível para todos os MH que desejam acessar o sistema. Além disso, só recentemente houve consenso quanto à padronização (Wi-Fi) de como deveria ser implementada. De modo geral, a chave de 64 bits pode ser considerada como padrão mínimo a ser adotado.

Uma outra forma de se conseguir segurança é implementando mecanismos de cifragem e autenticação de usuários na camada de rede (IPSec); esta característica exige mais da rede em desempenho, além de dispositivos mais especializados no acesso (MH e roteadores). Pode ser implementado com chave simétrica, recaindo-se no problema de administração e distribuição de senhas, ou através de chaves assimétricas, o que exige uma estrutura adicional para distribuição das chaves dinamicamente. Tem a vantagem de poder ser utilizado tanto no contexto de wireless IP (Wi-Fi) como no contexto de IP móvel (Móbile IP).

c) redes móveis (Móbile IP)

Um MH pode migrar para outra rede local, sem necessidade de troca de IP e re-configuração de gateway padrão. Para que essa característica seja possível é preciso que no roteador da rede de acesso de origem e destino, determinadas interfaces estejam configuradas para reconhecimento de dispositivos migrantes/visitantes. Supondo que essa característica de configuração esteja disponível nos roteadores, segundo a especificação da RFC 3220, é preciso que os administradores das redes locais estabelecem entendimento sobre as faixas de IP para os quais é permitida migração. Os mecanismos de autenticação disponíveis na RFC 3220 identificam o MH, mas não entram nos detalhes de como o usuário é reconhecido (SPI - security parameter index), portanto, mecanismos de autenticação adicionais devem estar disponíveis (ex. Radius). Os usuários devem ser conhecidos e autenticados preferencialmente através de uma base de dados centralizada; a comunicação posterior entre roteador visitado (FA - foreign agent) e de origem (HA - home agent) irá incluir a autenticação assim definida.

3.4 Resumo das recomendações

Relaciona-se a seguir as recomendações, em ordem decrescente de relevância e/ou facilidade, que podem vir a ser implementadas como proteção da rede local e de seus usuários:

Habilitar WEP. Caso a chave não esteja definida na base, será possível o acesso à rede local pelo dispositivo móvel, sem necessidade de autenticação. É importante que a administração da chave seja implementada e controlada de modo centralizado, e alterada periodicamente.

Mudar o SSID default (pré-configurado) na AP. Repetem-se as razões do item anterior. Não utilizar um SSID que reflita as características da empresa (nome, endereço ou produtos).

Desabilitar broadcast de SSID na AP (se o ponto de acesso implementar essa característica).

Colocar a rede wireless em um subrede separada, de preferência em uma VLAN;

Mudar periodicamente a senha do roteador, ao qual a base wireless está conectada.

Para definição da área de cobertura, posicionar os pontos de acesso mais para o centro do prédio e menos nas proximidades das janelas, onde a energia irradiada poderá ser captada por quem estiver do lado de fora, pelo uso de uma antena direcional.

Escolher APs onde é possível estabelecer uma lista de controle de acesso baseada em endereços MAC dos móbiles. Se isso não for possível, pode-se implementar esse controle através de uma VLAN por MAC address, desde que o switch de acesso implemente essa característica.

Utilizar um nível adicional de autenticação para as associações com os pontos de acesso através de servidores de autenticação (RADIUS). Quando disponível, utilizar equipamentos que de acesso de rede que implementam o padrão 802.1X. Esses dispositivos travam a porta no endereço MAC autenticado, o que impede que uma base clandestina seja instalada na rede local, utilizando um ponto de rede "disponível".

Não utilizar DHCP no roteador, onde a rede wireless está conectada. Preferir alocações estáticas, embora isso dê mais trabalho.

Preferir pontos de acesso que implementem WEP com chaves de 128 bits.

Preferir pontos de acesso com firmware em memória flash, que permitirão a sua atualização com a evolução dos padrões de segurança.

Posicionar a rede wireless em uma DMZ e prover acesso à rede protegida através de túnel (p.ex., com IPSec).

Pesquisar periodicamente a existência de bases clandestinas nas áreas de cobertura de interesse.

Ao alocar as bases na rede corporativa, investigar o quanto um sinal de dentro do prédio pode ser captado pelo lado de fora, pelo uso de uma antena de alto ganho e software de captura apropriado.