NORMA DE SEGURANÇA PARA A UNIFAPNET

1. Objetivo

As Normas de Segurança para a UNIFAPnet 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 Universidade, a saber:

- Estabelecer procedimentos para a instalação e manutenção de ferramentas, hardware e software, visando a segurança dos sistemas computacionais e de comunicação da UNIFAP interligados à UNIFAPnet;
- Orientar, por meio de suas diretrizes, todas as ações de segurança das Unidades de Ensino e Pesquisa, Departamento de Informática 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 incidentes de segurança.

2. Abrangência

Esta norma tem abrangência para toda Universidade, em relação às instalações, equipamentos, informação e pessoal relacionados à UNIFAPnet.

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

- Segurança física dos dispositivos de rede da UNIFAPnet e da infra-estrutura;
- Segurança lógica dos equipamentos de rede da UNIFAPnet;
- 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 e Aterramento

Recomenda-se que as edificações onde se encontram instalações de processamento, estejam protegidas por um sistema contra descargas atmosféricas (pára-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 devem estar em conformidade com a norma NBR-5419-2000;
- A função do pára-raios é proteger edificações e pessoas, não abrangendo necessariamente equipamentos eletro-eletrônicos.
- 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 no-break em equipamentos que suportam atividades críticas e para todos os componentes do backbone UNIFAPnet.
- O uso de grupo-gerador em instalações estratégicas e áreas do núcleo e de distribuição da rede UNIFAPnet é fortemente recomendado.
- Para outros equipamentos em áreas sujeitas a corte do fornecimento de energia

freqüentemente, o seu uso deve ser estudado, sendo uma boa alternativa a aquisição de no-break com maior autonomia.

- Tanto para o no-break 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.

4. 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.

4.1. 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;
- Restrições de acesso baseadas no status do funcionário e horas de operação;

4.2. Segurança do acesso à instalação:

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

- 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.

5. 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;
- A instalação, manutenção e atualização de equipamentos no backbone da UNIFAPnet é de responsabilidade única e exclusiva do Departamento de Informática.

5.1. Segurança de equipamentos instalados fora da UNIFAPnet

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

6. Manutenção de equipamentos

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

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

- 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.

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 Unidade ou Universidade:

- 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 eletro-eletrônica ou papel, deve ficar sempre guardada em locais apropriados e de acesso restrito, especialmente fora dos horários de trabalho normal.

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;
- Novo funcionário da Universidade 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 UNIFAP, 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 Departamento de Informática;
- Funcionários demitidos pela Universidade terão suas contas canceladas no ato da demissão;
- O Setor de Pessoal da Unidade ao qual esteja vinculado um funcionário demitido ou

afastado deve comunicar o responsável de segurança da Unidade para as providências.

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.

- Cabe a Unidade implantar regras de proteção nos seus roteadores e/ou firewall para proteger as redes de uma forma restritiva (método de exceção);
- Para os roteadores do backbone UNIFAPnet, os filtros e regras deverão ser obrigatórios e estudados para cada caso;
- 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 pelo Departamento de Informática;
- 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 Universidade ou da função;
- 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;
- Os equipamentos devem ter habilitados somente os protocolos necessários;

7.3. 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 à recepção, ou outro 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 de UNIFAPnet;

- 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;

7.4. 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;

7.5. Segurança para notebooks e dispositivos móveis

- 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;

8. Segurança Administrativa

Os usuários devem atender às seguintes diretivas básicas:

- A utilização dos recursos de rede da Universidade 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 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.