Universidade Católica de Brasília

Pró-Reitoria de Pós-Graduação e Pesquisa

Coordenação de Pós-Graduação em Latu Sensu em Informática

MBA em Gestão de Sistemas de Informação

Segurança da Informação em uma Universidade

Anderson Nilson Borges

Fernanda dos Santos Valadares

Rônia Marra

Professor: Ly Freitas

Brasil, DF – Brasil

Julho de 2002

Segurança da Informação em uma Universidade

Anderson Nilson Borges

Fernanda dos Santos Valadares

Rônia Marra

Resumo

A informação é hoje considerada como um dos maiores patrimônios de uma organização, seja ela pública ou privada. Sendo ela um bem de grande valor, necessita consequentemente ser protegido adequadamente. A segurança da informação protege a informação de um grande número de ameaças, inclusive fisicamente, onde o objetivo é garantir a continuidade dos negócios, minimizar riscos e danos e maximizar o retornos dos investimentos e preparar a organização para se lançar em novas oportunidades.

Palavras-chave

Segurança da informação, ameaças, continuidade dos negócios, minimizar riscos e danos.

Security of the Information in a University

Summary

The information today is considered as one of the biggest patrimonies of an organization, either public or private it. Being it a good of great value, consequently needs to be protected adequately. The security of the information protects the information of a great number of threats, also physically, where the objective is to guarantee the continuity of the businesses, to minimize risks and damages and to maximize the returns of the investments and to prepare the organization to launch itself in new chances.

Keywords

Security of the information, threats, continuity of the businesses, to minimize risks and damages.

1. Apresentação da Universidade

Será abordado a seguir, a segurança da informação da Universidade do Centro Oeste (fictícia), que possui 20 cursos de graduação e com 12.000 alunos.matriculados por semestre. Possui 1.200 funcionários, sendo 800 destes docentes, mais 150 funcionários terceirizados para os serviços de limpeza e vigilância e um fluxo diário aproximado a 15.000 pessoas, valor maior que muitos municípios brasileiros. O parque de informática conta com 1.800 computadores ligados em rede distribuídos em laboratórios, salas de aula, salas de professores e áreas administrativas. Todo este complexo é administrado pelo Centro de Tecnologia da Informação, que está organizado em áreas de atuação de desenvolvimento de sistemas, administração de redes, banco de dados, help-desk e operação dos servidores. Para uma melhoria na gestão dos recursos, a rede de computadores foi dividida em duas redes isoladas, sendo uma destinada para a área acadêmica, dedicada a alunos e professores, e outra para a área administrativa, para as atividades de controle interno da instituição.

2. Segurança

2.1 Redes de Computadores

Visando a segurança e privacidade das redes, administrativa e acadêmica, a UCO, vem se moldando a regras de seguranças em todo seu campus, em especial aos acessos aos computadores interligados. Com esse intuito, foram criadas alguma rotinas distintas como a seguir:

Na rede acadêmica, onde estão os laboratórios utilizados em diversas disciplinas de todos os cursos, inclusive alguns voltados ao uso de trabalhos e pesquisas dos alunos, o acesso só é permitido com a apresentação da carteira de estudante da Universidade. Esse controle é feito por monitores que sempre trabalham em pares nos turnos da manhã, tarde e noite. O acesso à internet é permanente, mas restritos a determinados sites, como os de conteúdo pornográfico. Também há a restrição de uso de salas de bate-papo conhecidas como “chat”, instalação de aplicativos, assim como downloads. Nos laboratórios destinados a aplicação de aula, a internet fica indisponível, exceto quando necessário solicitado pelo professor.

Na rede administrativa, onde estão os computadores destinados a aplicações comerciais, como os sistemas de Contabilidade, Patrimônio, Acadêmico, sendo este de controle de registro de notas, freqüência, histórico, etc. Somente funcionários e professores autorizados, possuem acesso a esta rede. Estes usuários são segmentados por perfil de acesso, onde alguns sistemas e funcionalidades são liberados mediante autorização do gestor da informação. Este gestor é o responsável pelo conteúdo da informação armazenada nas bases de dados da instituição. Portanto somente o gestor do Sistema é autorizado a permitir o uso do sistema a qualquer usuário, ou seja, possui a autoridade de incluir e excluir o acesso de usuários do sistema sob sua responsabilidade.

2.2 Gerência de Recursos

Os usuários não são administradores dos computadores que utilizam, portanto qualquer configuração ou instalação de aplicativos, deve ser solicitada à equipe de Help-Desk, que possuem o perfil de administradores de todas as máquinas, permitindo assim realizar os serviços de atendimentos a esses chamados.

2.3 Usuários e Senhas

As senhas de acesso à rede, devem ser únicas e individuais, seguindo critérios de qualidade. A responsabilidade da senha é do usuário proprietário da mesma. Por padrão a senha deverá conter no mínimo 8 caracteres alfanuméricos e expirada a cada 15 dias. Seguindo critérios de qualidade, as senhas deverão ser criadas evitando:

- o uso do próprio login;
- nomes como “senha”, “pass” ou “password”;
- o uso de qualquer nome do usuário, assim como de filhos, pais, esposa/marido, etc,
- placa do carro, data de nascimento, telefone, CPF;
- nomes comuns encontrados na língua portuguesa ou inglesa.

É recomendado é a utilização de letras combinadas entre maiúscula e minúscula, com caracteres não apenas alfabéticos (números e sinais) e de fácil memorização, evitando o registro escrito. Também deve ser de fácil digitação, evitando ter de olhar para o teclado. Após 45 dias sem a utilização do login de acesso, há o bloqueio do mesmo, sendo este liberado novamente através da solicitação feita pelo responsável da área do usuário bloqueado.

No caso do perfil de acesso, há dois administradores “master” que possuem a autorização de criação de grupos de acesso, assim como a atribuição de criarem o administrador (gestor) deste grupo. A inclusão de um usuário a um grupo de acesso deve atender ao princípio de menor privilégio. Todo pedido de acesso deve ser documentado, com a justificativa de acesso.

Outro ponto a ser observado é de que o gestor deve estar atento para que haja segregação de função, ou seja, não deve haver um único usuário com acesso a todas as informações de um processo, como por exemplo, um funcionário com acesso à geração de pagamentos e liberação do mesmo.

2.4 Controle de Acesso

Da mesma forma que existe um controle de acesso de todos os usuários, também é importante que se mantenha trilhas de auditorias, ou seja, qualquer registro de atualização no banco de dados, fica registrado em “log”, a operação realizada, o usuário que efetuou a operação, data e hora, computador cliente, conteúdo alterado.

No caso do sistema Acadêmico, este acesso é feito através do perfil de usuário, com permissões para grupos específicos, como o grupo professores, que permite somente o lançamento de notas e freqüência e conteúdo ministrado em aula.

2.5 Classificação da Informação

As informações devem ser classificadas quanto aos princípios da disponibilidade, integridade e confidencialidade pelo seu gestor.

No caso de confidencialidade, algumas informações como Notas, Freqüência, Disciplinas, Pré-requisitos, dentre outros; são classificados como pública, onde sua divulgação não implica perda ou dano para a instituição. Outras informações como dados pessoais do aluno, inadimplência, histórico, dentre outras, são consideradas como restritas. Existe ainda informações classificadas como confidenciais, onde o seu acesso

é restrito a um grupo interno da instituição, onde são consideradas informações estratégicas.

3. Perigos e ameaças

3.1 Catástrofes

Incêndio

Alagamento

Explosão

Desabamento

Impacto

Terremotos

Guerras

3.2 Problemas ambientais

Variações térmicas

Umidade

Poeira

Radiações

Ruído

Vapores e gases corrosivos

Fumaça

Magnetismo

Trepidação

3.3 Supressão de serviços

Falha de energia elétrica

Queda nas comunicações

Pane nos equipamentos

Pane na rede

Problemas nos sistemas operacionais

Problemas nos sistemas corporativos

Parada de sistema

Paralisações e greves

Piquetes

Invasões

Hacker

Alcoolismo e drogas

Disputas exacerbadas

3.4 Ação criminosa

Furtos e roubos

Fraudes

Sabotagem

Atentados

Seqüestros

Espionagem industrial

Cracker

3.5 Incidentes variados

Erros de usuários

Erros em backups

Uso inadequado dos sistemas

Manipulação errada de arquivos

Treinamento insuficiente

Ausência/demissão de funcionário

Estresse/sobrecarga de trabalho

Equipe de limpeza

3.6 Ameaças Possíveis

Vírus – pequenos programas projetados para se replicarem e se espalharem de um computador a outro, atacando programas ou o setor de boot de um disco rígido.

Worms – programas que se propagam de um computador a outro em uma rede, sem necessariamente modificar programas nas máquinas de destino.

Cavalo de Tróia – programa que parece ter uma função mas que, na realidade, executa outras funções.

Todas as ameaças possíveis descritas acima são potencialmente percebidas nos laboratórios onde os alunos possuem acesso através da unidade de disco flexível (disquete) e e-mail. Portanto há um maior controle sobre as atualizações de antivírus e monitoramento do firewall para evitar este tipo de ameaça.

4. Segurança Física

Com um contingente de 15.000 pessoas/dia circulando pelas dependências do campus universitário, são necessárias algumas medidas de controle de acesso. As áreas administrativas são acessadas fisicamente através de cartões magnéticos que autenticam

sua validade para aquele setor. Da mesma forma, algumas áreas acadêmicas, como as salas dos professores, exigem a autenticação através deste cartão de identificação. A sala dos servidores também possui a liberação de acesso através do cartão de identificação, porém muito limitado em número de pessoas, pois somente o pessoal técnico envolvido com estas plataformas, como operadores ou técnicos de hardware e software, podem ter acesso a esta instalação. Além desta restrição de acesso, existem equipes de segurança em todo o campus universitário e um monitoramento centralizado através de câmeras de vídeo instaladas pelo campus, registrando imagens 24 horas por dia. Como foi exposto anteriormente, para utilização de laboratórios por alunos é obrigatória apresentação da carteirinha da universidade e estar regularmente matriculado na instituição.

Só é permitida a movimentação de equipamentos com número de patrimônio, e com a autorização do responsável pelo bem. As exceções referem-se a equipamentos que trazidos por alunos ou por empresas que realizarão apresentação ou treinamento interno, contratado pela UCO, que deverão ser registrados na pelo setor de segurança e impedidas de acessar a rede

Qualquer consultoria terceirizada só poderá ter acesso a ambientes com informação classificada (financeiro, TI), com o acompanhamento de um funcionário e devidamente identificado

Todos os projetos para novas instalações devem ser revisados pelo Comitê de Segurança e todos os funcionários devem estar devidamente identificados no campus.

5. Segurança de dados

5.1 Backup

Todos os dias e de log, realizado de 01:00hs ate 05:00hs, ata diária do setor de operação sobre quaisquer eventos ocorridos durante o processo.

5.2 Contingência

- Maquinas espelhos
- Backups armazenados em outra instalação
- Obrigatória apresentação de Plano de Contingência para quaisquer alterações

6. Gestão de Segurança

Há um comitê de segurança e uma administração de segurança responsáveis por revisões periódicas na política de segurança e sanções em caso de violação da mesma.

6.1 Comitê de Segurança

A composição desta comissão de segurança deverá ser interdisciplinar, mas de preferência, categorizada por funções como:

- Coordenador de Segurança: com a atribuição de coordenador e tomada de decisão sobre a gestão de segurança;
- Consultores de Segurança/Contingência: com o perfil pesquisador em tendências tecnológicas futuras;

- Auditor de Segurança: com conhecimento de auditoria de segurança em TI;
- Gerente de Risco: com perfil de análise de riscos.

Como atribuição deste comitê, a divulgação da política de segurança através de treinamento, de capacitação e conscientização, porém seu principal objetivo é manter a integridade, confidencialidade, disponibilidade e auditoria de dados, verificando e analisando todos os riscos e contingências a serem adotados.

6.2 Integridade, confidencialidade, disponibilidade e auditoria de dados

Com relação à integridade dos dados, podemos entender como evitar que dados sejam apagados, ou alterados sem a permissão do gestor da informação. Para uma universidade é dentre os critérios de segurança o mais importante.

A confidencialidade ou privacidade, visa a proteger as informações contra acesso de qualquer pessoa não autorizada pelo gestor da informação. Este objetivo envolve medidas como controle de acesso e criptografia. Dentro da universidade há um administrador de controle de acesso e as conexões são efetuadas através de criptografia entre os usuários e o banco de dados.

Quanto à disponibilidade, é a garantia do funcionamento do serviço de informática, sob demanda, sempre que necessário aos usuários autorizados. As medidas relacionadas a esse objetivo podem ser duplicação de equipamentos/sistemas e backup. Um bom exemplo de ataque contra disponibilidade é a sobrecarga provocada por usuários ao enviar enormes quantidades de solicitação de conexão com o intuito de provocar "crash" nos sistemas. A universidade dispõe de redundância nos servidores críticos (banco de dados, intranet, aplicações, etc), instalados em outro local permitindo a continuidade do serviço. Por isso são efetuados backups diários.

A auditoria objetiva proteger os sistemas contra erros e atos cometidos por usuários autorizados. Também para identificar autores e ações, são utilizadas trilhas de auditorias e logs, que registram o que foi executado no sistema, por quem e quando.

Todos os sistemas críticos da Universidade possuem registros de logs informando a ação executada e o conteúdo modificado.

6.3 Sistema principal

Como qualquer organização, uma universidade possui um foco de atuação, o negócio que é a prestação de serviço educacional. Portanto seu sistema crítico, ou seu maior ativo de informação, é o sistema acadêmico que visa o registro da vida acadêmica de todos os alunos matriculados, como também manter as informações de egressos da universidade. O sistema acadêmico é composto de diversos módulos que contém internamente diversas funcionalidades que controlam os processos. Podemos relacionar alguns destes controles como o registro de notas de avaliação, freqüência dos alunos, professores, histórico de disciplinas, currículo dos cursos. cadastro de professores e disciplinas/turmas, instalações como salas de aula e laboratórios, mensalidades, bolsas de estudo, controle de ingresso como vestibular e transferências, dentre outros.

Para que todos os critérios de segurança sejam observados, existem algumas regras de negócio que devem ser seguidas, como:

- Todo aluno confirmado no processo de matrícula, não pode ser excluído do cadastro, mesmo que não freqüente nenhuma aula;
- Qualquer tipo de acesso ao sistema Acadêmico deverá ser registrado em arquivo de “Log”;

- Nenhum funcionário que seja aluno na instituição poderá trabalhar na Secretaria Acadêmica, Gráfica ou Centro de Tecnologia da Informação.

Além de toda a observância destes critérios que podem afetar o desempenho da instituição, devemos observar também as exigências de informações solicitadas por órgão fiscalizadores externos, principalmente os governamentais que são o Ministério da Educação e Cultura – MEC e o Instituto Nacional de Estudos e Pesquisas Educacionais – INEP.

7. Política de Segurança da Informação

Para que a segurança da informação seja implementada é necessário uma definição de política de segurança da informação, através de uma diretriz de segurança de informação, normas de segurança da informação e procedimentos de segurança..

As diretrizes são como uma “Constituição” da política de segurança, onde todos e não havendo exceção, deverão se submeter e cumprir o que determina as regras contidas neste documento. Deve ser clara para o entendimento de todos, sem o uso de termos técnicos e abrangente de forma a atingir a todo o assunto referente a segurança da informação. Um exemplo de uma diretriz contida neste documento pode ser:

- Toda e qualquer informação gerada, adquirida e processada pela Universidade é considerada de sua propriedade, devendo ser utilizada exclusivamente para os interesses da instituição .

As normas são o “como” solucionar a segurança defina nas diretrizes. Dependem da estrutura da organização e da tecnologia empregada pela mesma. Um exemplo de norma:

- Os logins e suas respectivas senhas de acesso à rede, devem ser únicas e individuais, com permissões determinadas pelo gestor responsável da informação, mediante solicitação do responsável da lotação do usuário.

Os procedimentos são as rotinas operacionais que definem utilização e manutenção dos recursos de informática. Este documento deve conter as informações sobre quem é o responsável pela condução da operação, o que deve ser feito, em que local, quando deverá ser realizado, de que maneira, o quê fazer no caso de contingência e a quem procurar nesta situação. Um exemplo específico para um procedimento:

- Quem é o responsável: administrador;
- O que deve ser feito: executar o backup;
- Em que local: no banco de dados de produção;
- Quando deverá ser realizado: todos os dias às 23 horas;
- De que maneira: seguir as instruções contidas no manual de backup do Oracle;
- O quê fazer no caso de contingência: anotar a mensagem de erro apresentada no console;
- Quem procurar: Sr. Fulano de Tal (DBA) no telefone 333-3333.

8. Conclusão

A Universidade possui vários segmentos que são considerados como ativos: alunos, professores, sistemas de informação. Devido ao alto volume e grande relevância da informação, a segurança se torna indispensável para a manutenção e crescimento da instituição. O ponto mais sensível da Universidade é o Sistema Acadêmico, pois armazena e recupera informações das quais dependem a sobrevivência da universidade, como dados dos alunos, notas, históricos; portanto toda recurso em segurança aplicado neste ativo deve ser observado como investimento obrigatório e de enorme retorno.

Outra questão a ser observada é a preocupação com a segurança física, por se tratar de uma empresa de grande porte e extensa área construída. A Universidade entende a necessidade de monitoramento de toda a área como o passo inicial de um plano efetivo de segurança.

9. Bibliografia

DIAS, Cláudia. Segurança e Auditoria da Tecnologia da Informação. 1 ed. Rio de Janeiro: Axcel Books do Brasil 2000
GIL, Antonio de Loreiro. Segurança em Informática. 2 ed. São Paulo: Atlas, 1998
Janeiro: Editora Ciência Moderna Ltda, 2000
www.sans.org
www.jseg.net
www.cnasi.com.br
www.modulo.com.br