CURSO TÉCNICO EM OPERAÇÕES COMERCIAIS

05

INFORMÁTICA I

Política de segurança digital

Raimundo Nonato Camelo Parente

Governo Federal
Ministério da Educação

Projeto Gráfico
Secretaria de Educação a Distância – SEDIS

EQUIPE SEDIS | UNIVERSIDADE FEDERAL DO RIO GRANDE DO NORTE – UFRN

Coordenadora da Produção dos Materias
Marta Maria Castanho Almeida Pernambuco

Coordenador de Edição
Ary Sergio Braga Olinisky

Coordenadora de Revisão
Giovana Paiva de Oliveira

Design Gráfico
Ivana Lima

Diagramação
Ivana Lima
José Antônio Bezerra Júnior
Mariana Araújo de Brito
Vitor Gomes Pimentel

Arte e ilustração
Adauto Harley
Carolina Costa
Heinkel Huguenin

Revisão Tipográfica
Adriana Rodrigues Gomes

Design Instrucional
Janio Gustavo Barbosa
Luciane Almeida Mascarenhas de Andrade
Jeremias Alves A. Silva
Margareth Pereira Dias

Revisão de Linguagem
Maria Aparecida da S. Fernandes Trindade

Revisão das Normas da ABNT
Verônica Pinheiro da Silva

Adaptação para o Módulo Matemático
Joacy Guilherme de Almeida Ferreira Filho

Revisão Técnica
Rosilene Alves de Paiva

Você verá por aqui...

Quando falamos em política de segurança digital nas empresas, estamos nos referindo às ações para proteger seus dados sigilosos. Porém o foco maior será sempre a proteção das informações que podem fazer a diferença competitiva dentro do mercado que está cada dia mais disputado.

Nesta aula, iremos debater sobre uma política de segurança digital começando com os princípios que regem uma política de segurança, as ameaças existentes, os controles, as ferramentas e as rotinas nas empresas.

Objetivo

- Compreender a importância de uma política de segurança digital.
- Entender os princípios e ameaças a uma política de segurança digital.
- Conhecer os controles para uma política de segurança digital.
- Classificar as informações dentro de um sistema de informação.
- Elaborar rotinas de backup para uma pequena empresa.

Para começo de conversa...

Atualmente, a tecnologia da informação oferece uma base de sustentação imprescindível aos negócios de quaisquer empresas ou governos. Uma falha ou o uso impróprio e malicioso das informações, principal ativo de uma empresa, pode trazer conseqüências negativas irreparáveis.

A necessidade de um programa corporativo de segurança da informação não é mais uma necessidade para uma empresa, faz parte do planejamento estratégico e considero essencial e até decisivo para o sucesso ou insucesso da empresa. Conscientizar a todos na empresa não é tarefa fácil, pois trata-se de um bem intangível cuja importância só é notada quando o caos está instalado. É imprescindível o comprometimento dos dirigentes maiores da empresa para que a implantação de qualquer política de segurança digital tenha êxito.

Praticando... **1**

Leia a notícia *Piratas concentram foco no roubo de informações* <http://www.cert.br/docs/reportagens/2006/2006-01-07.html> e reflita: as empresas precisam ser melhores preparadas contra estes crimes? Tem que formalizar princípios para reger uma política de segurança digital? Os funcionários necessitam ser treinados para desempenhar suas funções nas empresas com segurança digital? Os dirigentes das empresas têm que se comprometer e apoiar uma política de segurança digital?

Princípio da política de segurança digital

Para manter uma estrutura de segurança digital nas empresas, alguns princípios têm que ficar registrados para que todos absorvam uma cultura de trabalho digital. A equipe de informática deve treinar a todos e manter uma campanha ativa e permanente. Qualquer falha tem que ser vista como gravíssima, pois colocam em risco as informações estratégicas da organização.

Os princípios de uma política de segurança digital são:

Integridade: é a condição na qual a informação ou os recursos da informação são protegidos contra modificações não autorizadas. Evitar que pessoas não autorizadas modifiquem informações e, também, evitar modificações acidentais.

Confidencialidade: faz referência à propriedade que certas informações têm que não podem ser disponibilizadas ou divulgadas sem autorização prévia do seu dono. Evitar que informações confidenciais sejam disponibilizadas sem critério comprometendo as estratégias da empresa.

Disponibilidade: característica da informação que se relaciona diretamente à possibilidade de acesso por parte daqueles que dela necessitam para o desempenho de suas atividades. Todo sistema de informática tem que estar pronto para uso no momento em que a empresa precisar. Sistema parado é perda de tempo no trabalho e de produtividade, podendo gerar aumento de custos e perda de cliente e fornecedor.

Legalidade: estado legal da informação, em conformidade com os preceitos da legislação em vigor. Mesmo as informações sendo armazenadas no modo digital, existem normas legais a ser seguidas no seu formato e no tempo de armazenamento das informações. A empresa receber multa por não seguir as normas dos agentes fiscalizadores é imperdoável.

Ameaças à política de segurança

A empresa tem que ficar atenta às ameaças existentes no ambiente organizacional (interno e externo à empresa). Essas ameaças podem comprometer toda a política de segurança e levar o caos ao sistema de informação da empresa. As ameaças estão implícitas nos princípios vistos no tópico anterior, são eles:

Integridade: Ameaças de Ambiente (fogo, enchente, tempestade, etc.), erros humanos, fraudes e erro de processamento.

Indisponibilidade: Falhas em sistemas ou nos diversos ambientes computacionais.

Divulgação da Informação: Divulgação premeditada de informações e divulgação acidental de informações.

Alterações não Autorizadas: Alteração premeditada e alteração acidental.

Procedimentos de controle para o sistema de informação são necessários e devem ser planejados por profissionais qualificados na área de segurança digital. As empresas não podem prescindir dos controles necessários e no próximo tópico vamos debater esses controles.

Controles na política de segurança digital

A empresa precisa ter no seu planejamento estratégico de informática além dos princípios a ser seguidos no que se refere à segurança da informação como também os

controles essenciais a serem perseguidos. No planejamento tático de segurança digital, é preciso detalhar que tipo de controle vai ser implementado. Os tipos de controles usuais são: Controles de Instalações, Controles de Procedimentos e Controles dos sistemas de Informação.

Controles de instalações

São métodos que protegem as instalações físicas que guardam recursos de computação e seu conteúdo contra a perda ou destruição. É a segurança colocada na parte física para assegurar que o sistema não pare e não autorize modificações indesejadas. Os principais controles nesta categoria são:

Criptografia – Criptografia (kriptós = escondido, oculto; grápho = grafia) é a arte ou ciência de escrever em cifra ou em códigos, de forma a permitir que somente o destinatário a decifre e compreenda. É colocar a informação em formato que só possa ser lida no seu destinatário correto e, caso seja interceptada por estanhos, não consiga ser visualizada.

Criptografia

Leia os seguintes sítios para ter mais informações sobre o assunto: <http://pt.wikipedia.org/wiki/Criptografia>. <http://cartilha.cert.br/conceitos/sec8.html>.

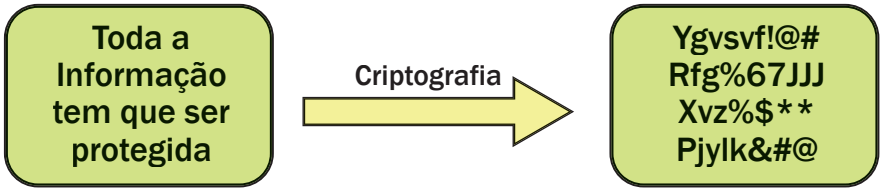

Figura 1 – Criptografia de um documento

Dispositivos para controle de acesso – A primeira barreira que se deve colocar em um sistema de informação é o controle de acesso. Os controles **biométricos** através de algumas características únicas da pessoa como impressão digital ou a córnea do olho são os mais utilizados e não permitem que sejam burlados. Controlar o acesso ao sistema de informação da empresa é fundamental, já que é o começo de qualquer sistema de segurança digital.

Biométricos

Para conhecer mais sobre biometria e segurança leia em: <http://elisagomes.info/redes/biometria.html>.

Figura 2 – Dispositivo de impressão digital com conector USB

Fonte: <http://www.testech.com.br/View.asp?codigo=36&cod_secao=24>. **Acesso em:** 20 jan. 2009.

Redundante

↗ Mais informações, leiam: <http://pt.wikipedia.org/wiki/Firewall>. <http://cartilha.cert.br/prevencao/sec4.html>.

Sistemas tolerantes a falhas – É um sistema preparado para continuar funcionando caso haja alguma falha de hardware ou software. Existem vários níveis de tolerância, como por exemplo, usar dois discos rígidos em paralelo, dos quais o segundo armazena uma cópia exata dos dados contidos no primeiro. Caso o disco rígido principal falhe, a controladora mudará imediatamente para o segundo, permitindo que tudo continue funcionando como se nada tivesse acontecido. Um nível mais alto seria usar dois ou mais servidores completos no mesmo sistema, pois caso o primeiro falhasse, o segundo assumiria imediatamente. Um nível mais baixo seria fazer uma simples cópia de segurança dos dados importantes em uma mídia removível e guardar em local seguro para evitar perda de dados ou mesmo usar um no-break para se prevenir de falhas na corrente elétrica. Usar também mais de um provedor de Internet para ter mais garantia de não ficar sem a linha de comunicação. O ideal é que o nosso sistema seja o mais **redundante** possível na energia elétrica, na linha de comunicação, na guarda dos dados, etc.

Firewall

↗ Um exemplo de redundância veja no sítio <http://www.edumar.com.br/datacenter.htm>.

Firewalls – **Firewall** é uma barreira de proteção, que controla o tráfego de dados entre seu computador ou a rede local onde seu computador está ligado e a Internet. Seu objetivo é permitir somente a transmissão e a recepção de dados autorizados. Existem Firewalls baseados na combinação de hardware e software e Firewalls baseados somente em software (recomendado ao uso doméstico).

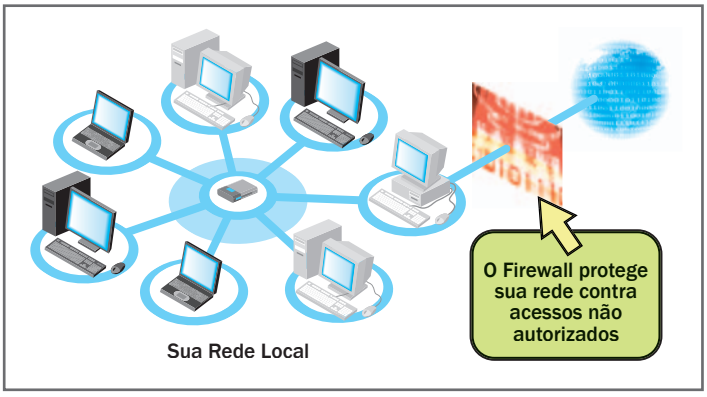

Figura 3 – Firewall protegendo uma rede local

Fonte: <http://www.oficinadanet.com.br/artigo/596/seguranca_na_internet_e_possivel>. **Acesso em:** 20 jan. 2009.

Praticando... **2**

Um sistema de tolerância a falha é viável para pequenas empresas? Mostre com um caso hipotético, imaginando uma empresa com rede local e seus dirigentes desejando nunca ficar fora do ar.

Controles de Procedimentos

São métodos que especificam como os serviços de informação da organização devem ser operados para a segurança máxima. A padronização dentro da empresa no gerenciamento da informação digital facilita o controle e a recuperação do sistema de informação em caso de desastre.

Controles da computação pelo usuário final – Cada usuário final tem o controle sobre as entradas de dados do seu serviço. Sua permissão na rede de computadores é total, mas limitado ao que o usuário necessita para exercer seu trabalho.

Padrão de procedimentos e documentação – Devem-se ter padrões de qualidade e classificações para documentação quanto ao acesso.

Requisitos para desenvolvimento de sistemas – Os projetos para desenvolvimentos de sistemas devem ser orientados segundo a visão dos usuários. Devem ser elaborados para compreender a real necessidade dos usuários e suas expectativas, dimensionando a sua abrangência e só depois pensar na solução técnica que devem levar em conta desde o começo a preocupação com a segurança e a tolerância a erros.

Plano de Recuperação de Desastres – Na verdade não se trata de recuperar-se de um desastre e sim se trata de prevenir-se dos desastres que podem prejudicar as informações de seu negócio. Um bom plano de ação abrange: tecnologia atualizada, melhor treinamento para os membros da Informática, levantamento dos riscos e auditorias, checagem das prioridades para sua rede local e aplicações, preparação de um inventário atualizado e da documentação do plano, bem como implementação de tolerância às falhas e duplicação dos serviços essenciais, suporte com qualidade

de seus fornecedores de serviço. O plano de recuperação de desastre, também, adiciona um peso considerável no plano para Internet, Voz e Dados, pois a segurança é fundamental para qualidade de tráfego da rede. Não esquecer as rotinas de cópias dos arquivos importantes.

Controles dos Sistemas de Informação

São métodos e dispositivos que procuram garantir a precisão, validade e propriedade das atividades dos sistemas de informação. É ter o controle do processamento digital desde a entrada dos dados até a saída da informação, tendo o cuidado com o armazenamento.

Controles de Entrada – É ter formatos-padrão para evitar erro de digitação e entradas indevidas de dados. Os softwares de entrada de dados devem testar os dados antes de aceitá-los como válidos.

Controles de Processamento – Pontos de Verificação de Software e Hardware. Nunca deve ter dentro da empresa uso de softwares ou hardwares não homologados ou autorizados.

Controles de Saída – Para se ter controle das informações que saem, é necessário registrar os acessos e usos na rede. Então, todo o passo que você fizer dentro da rede, como excluir arquivo, imprimir documentos, enviar dados, etc., deve ser registrado em um arquivo para ser auditado, quando for detectado vazamento de informação para chegar aos culpados.

Controles de Armazenamento – O funcionário, para trabalhar, precisa pesquisar informações em banco de dados e algumas vezes alterar dados. Essa alteração tem que ser restrita a um número mínimo de pessoa para que o controle de acesso e/ou adulteração da informação seja fácil de rastrear.

Outros controles

Outros controles importantes e que não podem faltar nos computadores da empresa são: Software de detecção de vírus, software de controle de acesso lógico (só aceita o acesso ao computador quem for autorizado), classificação de informações (será visto no próximo tópico), política de backup (será vista mais adiante), definição dos agentes envolvidos em segurança da informação dentro das Empresas.

Praticando... **3**

Procure saber quais os controles existentes no pólo para que os computadores não parem e as aulas não sofram por descontinuidade. Analise o controle e ofereça sugestão para melhorar.

Classificação de Informações

Para organizar o seu sistema de arquivos, a empresa precisa classificar as informações em três categorias: informações confidenciais, informações corporativas e informações públicas. Sem essa classificação bem definida, o sistema pode permitir indevidamente vazamento de informações confidenciais. As informações são classificadas com os seguintes critérios:

Informações Confidenciais: devem ser disseminadas somente para empregados nomeados. Geralmente as informações confidenciais são utilizadas para tomar decisões estratégicas e se restringem a um grupo pequeno dentro da empresa, que são os diretores, e algumas informações chegam aos gerentes e outras até o supervisor.

Informações Corporativas: devem ser disseminadas somente dentro da Empresa. São informações que devem ser passadas para todos os funcionários e não interessa ao público externo da empresa. São informações de produção, vendas, motivacionais e de mercado. São utilizadas para manter as equipes dentro da empresa informadas e motivadas.

Informações Públicas: podem ser disseminadas dentro e fora da Empresa. São informações institucionais de divulgação da empresa e promocionais dos produtos e serviços oferecidos como propaganda.

Política de Backup

Backup é uma cópia de segurança dos arquivos de um computador, ou em outras palavras, podemos dizer que é uma segunda via dos arquivos para usar em caso de desastre. Sabemos que gerar dados é um processo natural em qualquer empresa, manter sua integridade é fundamental. Porém, manter a integridade dos dados pode ser um dos maiores desafios da área de tecnologia da informação de uma empresa, principalmente porque soluções de controles, como visto no tópico "Controles na política de segurança digital", principalmente a redundância, não conseguem garantir a integridade do dado em alguns casos de erros humanos, sabotagens ou mesmo desastres de proporções não previstas. Em muitos destes casos, somente um backup pode resolver a situação.

Estratégia Básica de um Backup

Duas perguntas cruciais que se faz são: com que freqüência deve ser feito o backup? E quantas cópias de backup fazer?

A freqüência tem o seguinte critério: a empresa deve fazer cópias incrementais diariamente, ou seja, cópia dos arquivos que foram criados ou modificados desde o último Backup. E, no final da semana, fazer cópias completas de todos os arquivos, quer ele tenha sido alterado ou não. Os softwares de backup gerenciam a freqüência do modo que for configurado.

A quantidade de cópias depende do gerenciamento que a empresa planejou para sua segurança digital. O mais comum é estabelecer a quantidade de cópias incrementais, que são diárias, em número de 1 (uma). E as cópias completas, que são semanais, em número de 2 (duas).

Organizações das pastas e arquivos

Para facilitar o gerenciamento do backup se faz necessária uma boa organização das pastas e dos arquivos. Uma maneira de organizar seria, por exemplo, separado por: aplicativos, projeto, clientes, fornecedores, etc. O que não pode é deixar que cada usuário na empresa estabeleça o seu padrão. As pastas padronizadas nas empresas facilitam configurar o software de backup para que arquivos importantes não fiquem fora dos backup's realizados na empresa.

Praticando... **4**

Antes do próximo tópico veja um produto oferecido por vários sítios na Internet, que é o backup virtual para proteção de seus arquivos. A vantagem maior é ter uma empresa especializada cuidando dos seus dados. Nos sítios: <http://atendimento.ig.com.br/ig_bkp/> e

<http://site.locaweb.com.br/assinaturas/discovirtual.asp>.

Analise tamanho do espaço cedido, velocidade e preço. Anote as vantagens oferecidas. Guarde as informações para comparar com os dispositivos e rotinas de armazenamento da empresa para confrontar as soluções.

Dispositivos de armazenamento

Dispositivo de armazenamento é um dispositivo capaz de gravar informação (armazenar dados). Dispositivos de Armazenamento mantêm os dados, mesmo quando o computador é desligado. O material físico que armazena dos dados é chamado de mídia de armazenamento. Ex.: A superfície de um DVD-R é uma mídia de armazenamento. O hardware que escreve os dados ou lê os dados de uma mídia de armazenamento é chamado de dispositivo de armazenamento. Ex.: O leitor de DVD é um dispositivo de armazenamento. As principais tecnologias de armazenamento são: por meios ópticos Ex.: CDs, DVDs, etc.; por meios magnéticos Ex.: HD's, Fitas DAT, etc.; por meios de circuitos integrados de memória – chip. Ex.: cartão de memória, pen drive, etc.

A escolha do melhor dispositivo de armazenamento é realizada confrontando quantidade de dados a ser armazenado dentro da empresa com a capacidade de armazenamento da mídia. Outros fatores a considerar são maturidade da tecnologia, velocidade de gravação e o custo/benefício da escolha.

Praticando... **5**

Procure na Web as características dos principais dispositivos de armazenamento de backup. Identifique capacidade, conexão com o computador, se é interno (ficará fixo no computador) ou externo (será móvel), velocidade de transmissão de dados e preço. Procure saber as mídias mais utilizadas, dentre as quais devem estar: CD±R, DVD±R, disco rígido (HD), pen drive, Fita date ou Fita DAT, cartão de memória SD, microdrive e a novíssima tecnologia Blu-Ray.

Segurança externa do Backup

Gravar os arquivos em backup é a primeira fase do processo. Uma segunda fase, mas também igualmente importante, é armazenar em local protegido de umidade, mofo e incêndio. Se o dado é de vital importância, deve-se ter mais de uma cópia em locais diferentes. Manter rótulo nos Backup facilita a identificação na hora em que precisar restaurar alguns arquivos. Importante também é colocar em local de acesso restrito, onde somente os funcionários responsáveis pelo backup possam entrar. Com essas ações, a segurança externa fecha a política que deve pensar na segurança da informação como um todo, não havendo margem para o acaso.

Backup

↗ Mais informações sobre Backup, leiam <http://pt.wikipedia.org/wiki/Backup> e <http://www.infowester.com/colbackup.php>.

Na prática, defina grupo de arquivos que farão parte do **Backup** e estabeleça uma rotina a ser seguida na empresa. Motive os funcionários e os servidores terceirizados a cumprirem as políticas de segurança e a se envolverem com a proteção do ativo da empresa, sensibilizando-os através de palestras, treinamentos, campanhas internas, cartilhas, folders, cartazes, etc.

Praticando... **6**

Procure no pólo como é feito a guarda do backup das aulas e atividades no Moodle, dos registros dos alunos, das tarefas enviadas aos professores. Analise os locais de guarda, faça crítica e sugestões.

Exercícios

Com base nas informações aqui passadas nos textos e nos sítios indicados, responda às seguintes questões:

01. O que é Spam?

02. Leia o seguinte texto:

Os firewalls são os responsáveis pela segurança das bordas das redes, permitindo a entrada de pacotes apenas por áreas definidas, monitoradas e auditadas por suas regras. Podemos comparar os firewalls com as paredes, piso e teto que protegem uma agência bancária. As portas de entrada continuam abertas ao público, porém são facilmente controladas, monitoradas e filmadas. Da mesma forma que os assaltos ocorrem durante o expediente bancário e pela porta da frente, já que a mesma está aberta ao público, os ataques às redes ocorrem pelos acessos abertos no firewall: portas de acesso aos servidores Web, servidores de correio eletrônico, servidores de arquivos e demais "portas" abertas no nosso firewall. Da mesma forma que as paredes são necessárias em uma agência bancária, os firewalls são necessários na definição e proteção das bordas das redes. Sabemos, porém, que as novas técnicas de ataques utilizam as portas públicas para explorar as vulnerabilidades das aplicações.

Fonte: <http://www.tdec.com.br/Produtos/Seguranca/Firewalls.htm>. **Acesso em:** 20 jan. 2009.

Agora responda: O firewall é realmente importante? Por quê?

03. Usar o Blu-Ray para armazenamento de dados de alta densidade já pode ser usado nas empresas para backup. Justifique.

04. O que é uma política de backup?

Leituras complementares

ANTISPAM.BR. Disponível em: <http://www.antispam.br/>. Acesso em: 20 jan. 2009.

CERT.BR. Disponível em: <http://www.cert.br/>. Acesso em: 20 jan. 2009.

_____. **Práticas de Segurança para Administradores de Redes Internet**. 2003. Disponível em: <http://www.cert.br/docs/seg-adm-redes/seg-adm-redes.html>. Acesso em: 20 jan. 2009.

A leitura a fontes variadas de informação é importante para consolidar conhecimento e, na era da informação virtual, temos a facilidade de ter em casa ou no trabalho, ou em qualquer lugar que tenha um computador e um ponto de entrada para Internet, informação disponível vinte e quatro horas, de qualidade e gratuita. Recomendo os sítios seguintes.

Resumo

Nesta aula, tivemos uma visão geral de uma política de segurança digital. Foi mostrado que a implementação de políticas de segurança da informação disciplina o uso adequado e responsável das informações e ativos de uma empresa. O que ficou também de nossa discussão é que a Política de Segurança deve fornecer as diretrizes para o estabelecimento de normas e procedimentos que garantam a segurança da informação, bem como determinem as responsabilidades dentro de uma empresa.

Anotações

Auto-avaliação

Com o conhecimento adquirido na aula de hoje, você já pode identificar, em uma empresa, aspectos de sua política de segurança digital. Imagine uma pequena empresa com uma rede local de dez computadores. Faça uma política de segurança digital, deixando identificados os princípios que regem a sua política; atentar para ameaça ambiental, listar os controles necessários com a justificativa, classificar as informações a serem protegidas e finalizar com uma política de backup completa. Ao completar a sua política de segurança, escolha três colegas de curso e por e-mail troque a sua política com as políticas feitas pelos colegas. Confronte as políticas, faça criticas e discuta por e-mail as soluções divergentes e convergentes que tiveram.

Referências

LAUDON Kenneth C.; LAUDON Jane P. **Sistemas de informação gerenciais**. 7. ed. São Paulo: Ed. Pearson Prentice Hall, 2007. Capítulo 7.

SCUDERE, Leonardo. **Risco digital**. São Paulo: Ed. Campus, 2007.

Anotações

Anotações

Ministério
da Educação