

NORMATIZAÇÃO PARA UTILIZAÇÃO DE CORREIO ELETRÔNICO EM ORGANIZAÇÕES

JOCÊNIO MARQUIOS EPAMINONDAS, M.SC.

*Laboratório de Ensino a Distância do Programa de Pós-Graduação em Engenharia de Produção,
Universidade Federal de Santa Catarina, Campus Universitário, Trindade,
Caixa Postal: 5090 - CEP: 88040-970 - Florianópolis - SC - Brasil
E-mail: marquios@yahoo.com*

JOSÉ LUCAS PEDREIRA BUENO, M.SC.

*Laboratório de Ensino a Distância do Programa de Pós-Graduação em Engenharia de Produção,
Universidade Federal de Santa Catarina, Campus Universitário, Trindade,
Caixa Postal: 5090 - CEP: 88040-970 - Florianópolis - SC - Brasil
E-mail: lucas@led.br*

ÉDIS MAFRA LAPOLLI, DRA.

*Laboratório de Ensino a Distância do Programa de Pós-Graduação em Engenharia de Produção,
Universidade Federal de Santa Catarina, Campus Universitário, Trindade,
Caixa Postal: 5090 - CEP: 88040-970 - Florianópolis - SC - Brasil
E-mail: oriente@led.br*

Resumo:

O correio eletrônico, mesmo sendo o primeiro mecanismo de comunicação da Internet, ainda hoje causa diversos transtornos a seus usuários particulares ou organizacionais, devido ao não estabelecimento de uma normatização, tanto moral quanto técnica, para seus usuários cumprirem. Este trabalho tem como objetivo caracterizar o mecanismo de comunicação da Internet, correio eletrônico, abordando questões de segurança e das informações e propondo a implementação de uma metodologia para normatização do correio eletrônico em organizações, a qual orientará sobre quais tipos de mensagens devem ser enviados via rede institucional.

Palavras-chave:

Correio Eletrônico - E-mail, Internet, Segurança de Dados

1 Considerações Iniciais

As organizações passam por sérios problemas com relação ao uso de correio eletrônico: invasão da rede corporativa de computadores, recebimentos de arquivos contaminados com vírus, tipos de mensagens que trafegam na rede etc.

A falta de normatização de procedimentos agrava ainda mais esta situação, pois os administradores de redes criam suas próprias regras e geralmente não as tem documentado, além de não orientarem seus usuários de tais processos implementados. A responsabilidade por normatizar procedimentos acaba dependendo do bom senso de cada um.

As mensagens enviadas através do correio eletrônico podem ser interceptadas e lidas por outras pessoas. Por este motivo, não é aconselhável que se envie mensagens confidenciais, uma vez que o envio de mensagens via correio eletrônico não é totalmente seguro.

Não há garantia de privacidade no uso do correio eletrônico. O ideal é imaginar a mensagem enviada por este meio como um cartão postal, destinado a alguém, mas que pode ser lido no meio do caminho. Uma mensagem de e-mail fica armazenada no computador de quem a enviou, onde pode ser lida por programas de recuperação de dados mesmo que apagada. A mensagem, uma vez enviada, passa por uma série de provedores, numa rota que depende do seu destino, e fica armazenada no servidor até que o destinatário se conecte à rede e baixe a mensagem. Nesse servidor pode facilmente ser lida pelos administradores. Isso não significa que os provedores leiam as mensagens, significa apenas que isso é tecnicamente possível, uma vez que o administrador da rede tenha poder para isso. É importante lembrar também que é muito fácil falsificar o remetente de uma mensagem eletrônica, no que se chama *fake mail*, e que o texto pode ser facilmente editado.

Diante disto, propõe-se a implementação de uma metodologia para normatização de correio eletrônico em organizações, a qual orientará sobre quais tipos de mensagens devem ser enviados via rede.

2 Correio Eletrônico

O correio eletrônico foi a primeira aplicação desenvolvida para a Internet, pois facilitava a comunicação entre os membros da comunidade acadêmica que estava experimentando a Internet. Antes, os documentos desta comunidade eram distribuídos via correio tradicional, conseqüentemente, pouco ágil (DE MORAES, 1997).

É um dos recursos mais utilizados pelos usuários da Internet. Através do correio eletrônico pode-se enviar textos, gráficos e arquivos multimídia.

A troca de mensagens é realizada através do protocolo SMTP (Protocolo de Transporte de Simple Postagem) que é o protocolo para o envio de mensagens e-mail, que especifica o conteúdo e o formato de tais mensagens, bem como a seqüência correta das mensagens trocadas. O SMTP é conhecido como o “servidor de mensagens de saída”, ou seja, cuida das mensagens enviadas por uma estação cliente conectada ao servidor (GASPARINI, 1999).

Carvalho (1997) diz que: “O funcionamento do correio eletrônico é baseado no paradigma ”*store-and-forward*” (armazenar e enviar)”, ou seja, os usuários envolvidos na transferência de uma mensagem não interagem diretamente entre si, e sim com programas servidores encarregados de executar e gerenciar essa transferência.

Os sistemas de correios eletrônicos utilizam como arquitetura básica o Cliente-Servidor, em que há módulos de programa distintos para, de um lado, receber e executar os pedidos de informação (o módulo servidor) e, do outro lado, para capturar os pedidos do usuário e apresentar os resultados da execução desses pedidos (o módulo cliente) (SOARES, 1995).

A escolha de softwares para a rede local de correio eletrônico deve ser cuidadosamente adequada às necessidades da empresa. O avanço da funcionalidade dos softwares de correio eletrônico (licenças de calendário, planejamento, opções de personalização de mensagens, dentre outros) é constantemente atualizado por seus fornecedores.

Para que o e-mail funcione bem em uma organização é importante ter uma equipe especialista para tal. Geralmente esta equipe é formada por: analista de suporte, administradores de rede, pessoas especialistas aptas a esclarecerem as dúvidas de usuários e configurar estações de trabalho.

3 Segurança da Informação

A possibilidade de funcionar em rede e assegurar a prestação de serviços de forma rápida e descentralizada é um privilégio que a era da informação concede às organizações. O grau de eficiência dessas organizações depende de sua capacidade de processar informação e de uma estrutura capaz de assimilar um modo de funcionamento mais flexível e interativo.

As transações comerciais via Internet permitem o acesso direto a um mercado global. Atributos como tamanho físico e uma enorme população de usuários finais tornam a Internet o maior mercado que existe. Características como velocidade e baixo custo a tornam um dos meios mais interessantes para a realização de transformações comerciais. Além de ser o maior mercado, a Internet é o maior provedor de informações. Os usuários podem se conectar a bibliotecas, agências, instituições, empresas, serviços de *news* ou a outros usuários para trocar informações. A única exigência é conhecer o endereço na Internet que pode ser facilmente obtido através dos inúmeros índices e dispositivos de pesquisa. Na Internet é possível ter acesso gratuito a um vasto volume de informações.

A segurança nos sistemas e redes é construída com diversas técnicas: criptografia, controle de acesso etc. e de políticas de utilizações adequadas.

Para que as empresas possam ser competitivas, é imperativo que elas possam contar com um trabalho de profissionais especializados e qualificados que saibam como alinhar segurança à tecnologia da informação (BERNTEIN, 1997).

A seguir são descritos os agentes envolvidos em segurança da informação (FONTE, 2000):

- Gestor da Informação: O indivíduo responsável para fazer decisões em nome da organização no que diz respeito ao uso, à identificação, à classificação, e à proteção de um recurso específico da informação.
- Custodiante: Agente responsável pelo processamento, organização e guarda da informação.
- Usuário: Alguma pessoa que interaja diretamente com o sistema computadorizado. Um usuário autorizado com poderes de adicionar ou atualizar a informação. Em alguns ambientes, o usuário pode ser o proprietário da informação.

De acordo com Gil (1994), todas as informações críticas segundo o seu grau de criticidade e teor podem ser classificadas em:

- Informações Confidenciais: devem ser disseminadas somente para empregados nomeados.
- Informações Corporativas: devem ser disseminadas somente dentro da empresa.
- Informações Públicas: devem ser disseminadas dentro e fora da empresa.

É importante que a organização tenha especialistas na área de segurança da informação, utilizando produtos, que ofereçam serviços com uma abrangência muito ampla, permitindo apontar problemas e brechas na segurança dos sistemas de informação (CHESWICK, 1994).

É muito importante que a organização tenha segurança sobre os dados que circulam em seus servidores. A realização de backup's dos dados em fitas ou outra mídia de armazenamento removível deverá atender aos seguintes propósitos (JENNINGS, 1997):

- Evitar a perda irreparável de dados;
- Oferecer uma cópia *off-line* dos dados que podem ser recuperados a qualquer instante;
- Fornecer um arquivo de dados que pode ser preservado para fins históricos ou legais.
- Fornecer cópia dos dados corporativos, em servidores situados em outras localidades.

4 Segurança em Correio Eletrônico

Qualquer correspondência pode ser enviada pela Internet. Assim como qualquer pessoa que tenha um bom conhecimento técnico pode interceptá-la.

O correio eletrônico pode ser comparado a uma agência de correios convencional, na qual uma carta vai de um bairro a outro através de ruas e avenidas, existindo pontos de verificação e nestes pontos pode-se facilmente interceptar a carta, lê-la e enviá-la novamente para o seu destino.

Sadler (1996) afirma que “há várias opções e questões básicas, que se pode utilizar para minimizar a chance de os dados confidenciais da empresa serem interceptados e lidos por convidados inesperados e elas incluem”:

- Qual o grau de confidencialidade dos dados que meus usuários estão enviando?

- A criptografia de mensagens e arquivos é uma opção viável?
- Por qual caminho de roteamento as mensagens dos meus usuários estão trafegando antes de serem recebidas pelo receptor pretendido?

5 Normatização para Utilização do Correio Eletrônico

Abaixo são listadas as normas que os usuários dos serviços de correio eletrônico devem seguir:

- Realizar prevenção com software de antivírus de qualquer arquivo recebido através de sua caixa postal;
- Não enviar mensagens de interesse particular através do serviço de correio eletrônico institucional, exceto com autorização prévia;
- Não enviar ou divulgar o seu endereço de correio eletrônico institucional, em listas de discussões, chat, news, sites de compras, dentre outros;
- No envio de mensagens externas (quando autorizado) utilizar os meios corretos para o envio seguro de dados homologados pela organização;
- Zelar pela integridade dos dados organizacionais de sua responsabilidade (memorandos internos, contratos, planilhas gerenciais, dentre outros.);
- Manter o controle e uso exclusivo de suas senhas;
- Não baixar através de correio eletrônico, arquivos anexos oriundos de redes externas;
- Não divulgar através de correio eletrônico corporativo qualquer tipo de software aos usuários, a não ser aqueles homologados pela organização;
- Não enviar através do serviço de correio eletrônico alertas de vírus;
- É proibida qualquer tentativa de teste ou de burla dos dispositivos de segurança adotada pela organização;
- Não divulgar, enviar, transmitir ou de qualquer outra forma disponibilizar qualquer conteúdo que seja ilegal, vexatório, difamatório, evasivo à privacidade, abusivo, ameaçador, prejudicial, vulgar, obsceno, injurioso, preconceituoso ou de qualquer forma censurável através do serviço;
- Não forjar “Headers” ou de qualquer outra forma manipular identificadores com objetivo de disfarçar a origem de qualquer conteúdo transmitido, através do correio organizacional;
- Não divulgar, enviar, transmitir ou de qualquer outra forma disponibilizar qualquer conteúdo, seja em virtude de compromisso legal, contratual ou de confiança (informações internas, exclusivas ou confidenciais);
- Não divulgar, enviar, transmitir ou disponibilizar qualquer tipo de propaganda ou material não autorizado ou solicitado (“junk mail” ou “SPAN”), correntes, esquemas pirâmides ou qualquer outra forma de apelo;
- Não interferir ou interromper, servidores ou redes conectadas ao serviço de correio eletrônico organizacional;
- Não obter ou tentar obter acesso não autorizado a outros sistemas ou redes de computadores conectados ao serviço de correio eletrônico;
- Não desobedecer qualquer regra, procedimento, política ou regulamento de sistemas ou redes conectadas ao serviço de correio eletrônico organizacional;
- Não violar, intencionalmente ou não, qualquer lei ou regulamento aplicado para utilização do correio eletrônico organizacional;
- Não assediar terceiros através de correio eletrônico organizacional;
- Não obter ou armazenar dados pessoais de outros usuários, inclusive informações financeiras;
- Não divulgar informações sobre produtos ou serviços de natureza particular ou de outras empresas;
- Não divulgar material de natureza político-partidária ou sindical.

6 Considerações Finais

Para realizar a implementação de um modelo piloto no que tange a normatização do serviço de correio eletrônico no âmbito institucional, a organização deverá iniciar primeiramente um trabalho de conscientização dos empregados para ficarem cientes das normas internas a serem implementadas promovendo:

- Seminários de conscientização objetivando esclarecer a importância do uso correto da tecnologia, o âmbito de trabalho e o impacto que o mau uso pode acarretar à organização;
- Apresentação de orientações quanto às formas de envio de uma mensagem eletrônica (netiquetas).
- Divulgação do questionário da pesquisa a todos os usuários do serviço de correio eletrônico corporativo;
- Apresentação de palestras e elaboração de cartilhas que tratem a questão “Monitoramento Eletrônico” na organização;
- Elaboração de palestras sobre a norma de utilização do serviço , no qual são apresentadas as responsabilidades e sanções a que os usuários estão sujeitos;
- Divulgação da norma de utilização de correio eletrônico através da intranet e da administração do serviço;
- Colher assinaturas de ciência da norma de utilização de correio eletrônico, inclusive, o termo de responsabilidade de utilização;
- Disponibilização de conteúdos informativos e da própria norma de utilização em pastas públicas no serviço de correio eletrônico corporativo;

7 Referências Bibliográficas

BERNSTEIN, Terry. **Segurança na Internet**. Rio de Janeiro: Campus, 1997.

BRASIL, Constituição (1988). **Constituição: República Federativa do Brasil**. Brasília: Senado Federal, Centro Gráfico, 1988.

BRASIL, Lei nº 2.572, de 20 de Julho de 2000. Dispõe sobre a prevenção das entidades públicas do Distrito Federal com relação aos procedimentos praticados na área de informática. **Câmara legislativo do Distrito Federal**. Disponível em <<http://www.cl.df.gov.br/legislacao/legisoriginais/leisordinarias/2000/ldf-2000-02572.html>> . Acesso em 21/10/2000.

BRASIL, Lei nº 9.983, de 14 de julho de 2000. Altera o Decreto-Lei nº 2.848, de 07 de dezembro de 1940 – Código Penal e dá outras providências. Publicada no **DOU** de 17.7.2000. Disponível em <http://www.presidencia.gov.br/ccivil_03/Leis/L9983.htm> . Acesso em 29/03/2001.

BRASIL. Decreto - Lei Nº 3.689, De 3 De Outubro De 1941. **Código de Processo Penal**. Acesso em 22/02/2001. Disponível em <http://www.presidencia.gov.br/ccivil_03/Decreto-Lei/Del3688.htm>.

BRASIL. Decreto Lei nº 2.848, de 7 de dezembro de 1940, regulamenta o art. 180 da Constituição Federal. Trata dos crimes contra a pessoa. **Código Penal Brasileiro**.

BRASIL. Lei 4.117/62. **Institui o código Brasileiro de Telecomunicações, estabelecendo preceitos para os serviços de telecomunicações no Território Nacional**.art 53-h. Acesso em 16/03/2001. Disponível em <http://www.presidencia.gov.br/ccivil_03/Leis/L4117.htm>.

BRASIL. Lei 5.250, de 09 de Fevereiro de 1967, art 17 e 21. **Regula a liberdade de manifestação do pensamento e de informação**. Publicada no **DOU** de 10.2.67 E Retificado no **DOU** de 10.3.67. Disponível em: <http://www.planalto.gov.br/ccivil_03/Leis/L5250.htm> . Acesso em 07/01/2001.

BRASIL. Lei 5.988 de 14 de Dezembro de 1973. **Regula os direitos autorais**, Art.4º, V (contrafação a reprografia não autorizada).

BRASIL. Lei 6.538, De 22 De Junho De 1978. Rege sobre os serviços postais. Art. 41º “Violar segredo profissional, indispensável à manutenção do sigilo da correspondência mediante”. Publicada no **DOU** de 23.6.78. Disponível em <http://www.presidencia.gov.br/ccivil_03/Leis/L6538.htm> . Acesso em 13/03/2001.

BRASIL. Lei 8.069/90. **Dispõe sobre o Estatuto da Criança e do Adolescente** e dá outras providências - art 241. Disponível em <http://www.planalto.gov.br/ccivil_03/Leis/Referencia_Legislativa/L8069ref_leg.html> .Acesso em 14/08/2000.

BRASIL. Lei 8.112, de 11 de dezembro de 1990. Dispõe sobre o regime jurídico dos servidores públicos civis da União, das autarquias e das fundações públicas federais. Publicada no **DOU** de 12.12.90 e Republicada em 18.3.98. Disponível em <http://www.planalto.gov.br/ccivil_03/Leis/L8112orig.htm. Acesso em 05/01/2001>.

BRASIL. LEI Nº 5.172, DE 25 DE OUTUBRO DE 1966. Dispõe sobre o **Sistema Tributário Nacional** e institui normas gerais de direito tributário aplicável à União, Estados e Municípios. Disponível em <http://www.presidencia.gov.br/ccivil_03/Leis/L5172.htm> . Acesso em 21/03/2001.

BRASIL. Portaria do MPAS Nº 862, de 23 de Março de 2001. Dispõe sobre o controle de acesso a dados, informações e sistemas informatizados da Previdência e Assistência Social. **MPAS**. Disponível em <<http://www.previdenciasocial.gov.br/inss/links/legislacaoconsultaportariasmpas862de23032001.html>>. Acesso em 26/03/2001.

BRASIL. Projeto de Lei nº 1.713/96. Dispõe sobre o acesso, a responsabilidade e os crimes cometidos nas redes integradas de computadores e dá outras providências. **Câmara dos Deputados**. Disponível em <<http://www.modulo.com.br/linksfaqs/legislacao/lei1713.htm>>, acesso em 30/11/2000.

BRASIL. Recomendação nº 1, de 22 de setembro de 1999. Recomendação para utilização do serviço de Mensageria (correio eletrônico). **Ministério do Planejamento, Orçamento e Gestão**. Disponível em <<http://www.planejamento.gov.br>> . Acesso em 20/01/2001.

CARVALHO, Tereza Cristina Melo de Brito. **Arquiteturas de Redes de Computadores – OSI e TCP/IP**. 2ª Edição. Rev.Ampl. São Paulo: Makron Books. Brisa; Rio de Janeiro: Embratel. Brasília-DF: SGA, 1997.

CHESWICK, W. R; BELLOVIN, S. M. **Firewalls and Internet Security: Repelling the wily hacker**. Addison-Wesley, 1994

DE MORAES, Altair Dias Caldas. **Microsoft Exchange 4 Passo a Passo**. Catapult Inc. Tradução. São Paulo: Makron Books, 1997.

EPAMINONDAS, J. M. **Uma metodologia para normatização de correio eletrônico em organizações**. Florianópolis, 2001. 147f. Dissertação (Mestrado em Engenharia de Produção com Ênfase em Informática)- Programa de Pós Graduação em Engenharia de Produção, UFSC, 2001.

FONTE, Edison. **Política de Segurança da Informação. Modulo Security**. 03/11/2000. Acesso em 30/11/2000. Disponível em <http://www.modulo.com.br/noticias/artigo_entrevista/a-politica.htm>.

GASPARINI, Anteu Fabiano L. **TCP/IP solução para conectividade**. Editoria Érica – 10ª Edição,1999.

GIL, Antonio de Loureiro. **Segurança em Informática**. Editora: Atlas, São Paulo,1994.

ITRI, Maurício P. **Internet 2: A próxima Geração**. Market Books, 1999.

JENNINGS, Roger. **Usando Windows NT Server**. Editora: Campus, 1997.

RNP. O projeto Internet 2. acessado em 08/11/2001. Disponível em <http://www.rnp.br/rnp2/rnp2-Internet2.html>.

RNP1. **Guia do usuário Internet/Brasil**. Atualizado em 15/04/2000. Disponível em <http://www.fapeal.br/rnp/ci/doc/rpu0013b.html>. Acessado em 18/11/2000.

RNP2. **Guia do Empreendedor Internet**. Atualizado em 03/07/1995. Disponível em <http://www.fapeal.br/rnp/ci/doc/rpu0013b.html>. Acessado em 18/11/2000.

SAAD, Eduardo Gabriel. **CLT – Comentada**, 31ª edição. LTR Editora ,1992.

SADLER, Will. **Usando e-mail na Internet**. Editora Campus, 1996.

SOARES, Luiz Fernando Gomes. **Redes de Computadores**. Editora: CAMPUS, 1995.

SPAM. **O que é SPAM?** Acessado em 12/12/2000. Disponível em <http://www.antispam.org.br/oquee.html>.