Segurança da Informação
O usuário faz a diferença

Professor: Danilo Giacobo
E-mail: danilogiacobo@gmail.com
Página Pessoal: www.danilogiacobo.eti.br

Segurança da Informação
Definição

Segurança de informação é o conjunto de orientações, normas, procedimentos, políticas e demais ações que tem por objetivo proteger o recurso informação, possibilitando que o negócio da organização seja realizado e a sua missão seja alcançada.

Segurança da Informação
Introdução

O tema segurança da informação tem se tornado cada vez mais conhecido na medida em que:

- **as organizações possuem informações processadas e armazenadas no ambiente computacional;**
- **as organizações dependem do ambiente computacional para realizarem seus negócios; e**
- **o acesso à informação no ambiente computacional está disponível a todos os colaboradores da organização.**

Segurança da Informação
Introdução

A informação, independente de seu formato, é um ativo importante da organização. Por isso, os ambientes e os equipamentos utilizados para seu processamento, seu armazenamento e sua transmissão devem ser protegidos.

A informação tem valor para a organização.

Sem informação, a organização não realiza seu negócio.

Para que a proteção da informação seja eficaz no dia-a-dia da organização, os conceitos e regulamentos de segurança devem ser compreendidos e seguidos por todos os usuários.

Segurança da Informação

Um bem chamado informação - Para refletir

- Você tem cópia de seus documentos pessoais e de família?
- A fita de vídeo com momentos da família está bem guardada para evitar o mofo e a umidade?
- Você consegue construir informação a partir dos dados que você recebe por Internet, TV, jornais e outras mídias? Qual a maior dificuldade para que isso aconteça?
- Os prestadores de serviços na sua vida pessoal são escolhidos considerando critérios de valor que você defende e acredita?
- Você conhece o posicionamento de sua organização em relação aos funcionários e prestadores de serviço no que diz respeito à proteção da informação?
- A organização orienta você periodicamente sobre ações para a proteção da informação?
- O executivo de maior nível hierárquico da empresa está comprometido com a segurança da informação?

Segurança da Informação
Um bem chamado informação - Caso real

“Computador faz empresa aérea vender passagens a US$ 1,86”

“Charlotte, EUA – A US Airways se transformou na empresa área de menor tarifa de todos os tempos, vendendo passagem de ida e volta entre algumas cidades americanas a US$ 1,86 (cerca de R$ 5), mais impostos, enquanto durou um problema em seu sistema de informática. Em média, o preço final da viagem de ida e volta ficou em US$ 40 (R$ 104). A ‘oferta’ durou duas horas. Depois de descobrir o problema, a US Airways tratou de corrigi-lo. Um porta-voz da companhia disse que a empresa não sabe quantas pessoas compraram os bilhetes superbaratos. ‘Obviamente, se vendemos bilhetes a esse preço, iremos honrá-lo’, afirmou o porta-voz Chuck Allen.”

Fonte: www.estadao.com.br

Data: 18/04/2005

Segurança da Informação
Proteger a informação

Proteger a informação significa garantir:

- **Disponibilidade**
- **Integridade**
- **Confidencialidade**
- **Legalidade**
- **Auditabilidade**
- **Não repúdio de autoria**

Segurança da Informação
Famosas frases ouvidas no dia-a-dia

- **Não consigo achar aquele relatório que elaborei no ano passado!**
- **Mas esta não é a última versão da planilha! Perdemos a versão atual?**
- **Como foi que você soube disso?**
- **Achei várias folhas do relatório da audiência no lixo!**
- **Mas eu pensei que não fosse pirataria!**
- **Quem alterou esse contrato?**
- **Olha o que eu encontrei junto da impressora: a ata da reunião de diretoria. Vai ter corte de pessoal até o final do mês.**
- **Eu não mandei essa mensagem de correio eletrônico!**
- **Eu não fiz essa compra pela internet!**
- **Como aquele jornalista soube disso?**

Segurança da Informação

A segurança da informação na organização - Para refletir

- Existe uma política de segurança da informação na sua organização?
- Você conhece essa política de segurança da informação?
- Você conhece suas responsabilidades em relação à informação?

- A informação está sempre disponível para você realizar suas atividades profissionais na organização?
- Como é garantido, na sua organização, que cada usuário não possa negar que realizou determinado acesso e ação sobre uma informação?
- Você acha que a política de segurança da informação de sua organização foi divulgada adequadamente? Você consegue localizá-la?
- Seus subordinados conhecem a política de segurança da informação?
- Você já leu, pela segunda vez, a política de segurança da informação?

Segurança da Informação

A segurança da informação na organização - Caso real

“Assalto cinematográfico: levados R$ 4 milhões”

“Um túnel com 100 metros de extensão desembocava no único ponto vulnerável da empresa Transbank: o banheiro, onde não havia câmeras ou sensores para registrar movimentos suspeitos. Foi por ali que a quadrilha entrou. Armados, os homens dominaram uns 75 funcionários e levaram pelo menos R$ 4 milhões. A polícia diz que o valor pode chegar a R$ 10 milhões.

Após entrarem eles quebraram as câmeras, renderam seguranças e exigiram que os funcionários pusessem o dinheiro nos malotes. Os bandidos fugiram pelo túnel. A ação não durou mais que 15 minutos. Não houve feridos. (...)”

Fonte: Jornal O Estado de São Paulo, por José Luís Dacauaziliquá

Data: 13/10/2004

Segurança da Informação
Termo de Compromisso

A informação utilizada pela organização é um bem valioso e precisa ser protegido e gerenciado.

Normalmente, um termo de compromisso registra sua responsabilidade em relação a:

- **Manter sigilo das informações da organização às quais você terá acesso;**
- **Seguir as normas de segurança da informação; e**
- **Seguir o padrão ético da organização.**

Segurança da Informação
Termo de Compromisso - Para refletir

- Você já assinou o termo de compromisso (ou equivalente) na organização em que trabalha ou presta serviços?
- Você lembra o que esse termo explicita? Quais são suas principais responsabilidades? Existem penalidades caso você não as cumpra?
- A existência do termo de compromisso causa algum mal-estar a você, a seus colegas ou subordinados? Por quê?
- Você acha importante a existência de um termo de compromisso?
- Na sua organização, o termo de compromisso é assinado por todos os funcionários, incluindo o presidente? E os prestadores de serviço?
- Você tem uma cópia do termo de compromisso e de confidencialidade que assinou?

Segurança da Informação
Termo de Compromisso - Caso real

“Unicamp: sistema de votação do Senado é vulnerável”

“Brasília - O presidente do Senado, Jader Barbalho (PMDB-PA), disse que lamentavelmente o sistema de votação secreta do Senado é vulnerável. ‘Há possibilidade de, inclusive, adulterar os votos dos senadores’, afirmou Jader. O senador acrescentou ainda que os técnicos da Unicamp que fizeram a perícia no sistema de votações concluíram que é possível a identificação dos votos dos parlamentares. Diante desse quadro, o presidente anunciou que, até a modificação do sistema para aumentar o nível de segurança das votações, não haverá votação secreta utilizando-se o painel eletrônico. As votações secretas, segundo ele, serão realizadas com a utilização de urnas ficando o painel eletrônico reservado apenas para as votações nominais. (...)”

Fonte: www.estadao.com.br

Data: 27/03/2001

Segurança da Informação
Autenticação de Usuário

Dicas importantes ao escolher uma senha:

- ✓ **Não utilize datas de nascimento, nomes de pessoas, nomes de times ou outras informações que estejam ligadas a você ou à organização;**
- ✓ **Não utilize sequencia óbvia de caracteres;**
- ✓ **Utilize as de tamanho mínimo de seis posições;**
- ✓ **Construa-a utilizando letras, números e caracteres especiais;**
- ✓ **Utilize a primeira letra de cada palavra que forma uma frase; ou**
- ✓ **Defina uma frase que faça sentido para você.**

Ao utilizar senhas, escolha uma sequencia de caracteres fácil de ser lembrada por você e difícil de ser adivinhada por outra pessoa.

Segurança da Informação

Autenticação de Usuário - Para refletir

- Como você se autentica no ambiente computacional? Por meio de senha?
- Você acredita que as senhas que utiliza são difíceis de serem adivinhadas?
- Você utiliza a mesma senha em todos os ambientes computacionais que acessa?
- Como você sabe se alguém utilizou sua identificação, sua senha e assumiu sua identidade no ambiente computacional?
- Como você encara o fato de ter de decorar várias senhas?
- Você consegue decorar todas as senhas que utiliza? Se isso for uma dificuldade, como supera esse problema?
- Acredita que somente você conheça a sua senha na organização?

Segurança da Informação
Autenticação de Usuário - Caso real

“A delegacia do centro só tinha um problema: era falsa”

“Na Delegacia do Cidadão que funcionava há dois anos e meio, tudo era de mentira. Delegados e escrivães faziam BOs e negociavam suspensão de denúncias, mas a única coisa verdadeira era o pagamento do serviço.

Uma falsa Delegacia do Cidadão, com falsos delegados e escrivães, que funcionava há pelo menos dois anos e meio no centro de São Paulo e a 100 metros da 1ª Delegacia Seccional (Centro) e do 3º DP (Santa Efigênia), foi fechada na tarde de ontem pela Polícia Civil. (...)”

Fonte: Jornal O Estado de São Paulo
Data: 07/02/2003

Segurança da Informação
Evite o Carona

Caso você se ausente do seu local de trabalho e deixe aberta no computador uma sessão de trabalho, alguém poderá efetuar transações nesse computador como se fosse você. Para evitar esse tipo de problema, você deve:

a) **Suspender sua sessão de trabalho toda vez que necessitar se ausentar do local onde se encontra o computador ou terminal. Na maioria dos sistemas, teclando simultaneamente a sequencia "Ctrl+Alt+Delete" você consegue fechar essa sessão. A partir desse momento, qualquer pessoa (inclusive você) terá de se identificar e se autenticar para ter acesso ao equipamento.**

b) **Programar seu equipamento para que ele entre em estado de proteção de tela, com exigência de senha, sempre que não estiver sendo usado durante um certo período de tempo. 10 minutos é um tempo aceitável.**

Segurança da Informação
Evite o Carona - Para refletir

- Você já programou seu micro para o bloqueio após dez minutos de não uso?
- Você bloqueia a tela quando se ausenta do local de trabalho?
- Você chama a atenção dos seus colegas que deixam a tela aberta quando estão ausentes do local de trabalho?
- Você conhece uma situação de fraude feita por carona?
- Você acha que as pessoas da sua organização estão cientes do risco de carona através de terminal aberto?

Segurança da Informação
Evite o Carona - Caso real

“Prejuízo com roubo de identidade atinge US$ 48 bi”

“Cerca de 27 milhões de norte-americanos foram vítimas de roubo de identidade durante os últimos cinco anos, de acordo com pesquisa divulgada pela Federal Trade Commission (FTC). A agência, no entanto, não sabe dizer quantos desses crimes aconteceram em razão de meios tecnológicos.

Depois de conduzir uma pesquisa por telefone, a FTC estimou que 9,8 milhões de norte-americanos tiveram suas identidades roubadas no ano passado, o que ocasionou um prejuízo de R$ 48 bilhões para empresas e instituições financeiras. Para as vítimas individuais, as perdas são estimadas em US$ 5 bilhões.

A pesquisa ouviu mais de 4 mil pessoas durante março e abril de 2003. ‘É mais alto do que esperávamos’, declarou Howard Beales, diretor de proteção ao consumidor da FTC. (...)”

Fonte: www.csoonline.com.br

Data: 30/09/2004

Segurança da Informação

Importante!

- As orientações e os regulamentos formais sobre a segurança da informação da organização se aplicam a todos os usuários, independentemente do nível hierárquico!
- Toda informação deve ser protegida para que não seja indevidamente alterada, acessada ou destruída!
- Ninguém na organização deve conhecer sua senha.

Segurança da Informação
Gestor da Informação

Cabe ao Gestor da Informação:

- **Garantir que a informação esteja sendo disponibilizada apenas para as pessoas que precisam dela para o desempenho de suas atividades profissionais na organização.**
- **Garantir que cada usuário tenha apenas o tipo de acesso necessário para o desempenho de sua função profissional dentro da organização.**
- **Formalizar o pedido e a liberação da informação. Registrar a ocorrência para que, em qualquer tempo, possa-se saber quem autorizou determinado usuário a ter acesso a uma determinada informação.**

Segurança da Informação
Gestor da Informação - Para refletir

- Cada informação de sua organização possui o respectivo gestor?
- Você conhece os gestores de informação de sua organização?
- Você tem justificativa profissional para as informações que está autorizado a acessar?
- Em caso de auditoria, pode-se identificar quem autorizou o acesso à informação e quando foi feita essa autorização?
- É possível saber quem liberou o acesso de determinada informação para você?
- Quando o gestor da informação está ausente da organização, como acontece a autorização para o acesso a uma determinada informação? O gestor indicou uma segunda pessoa para fazê-lo?

Segurança da Informação
Gestor da Informação - Caso real

“Bandidos pagavam propina para ‘limpar’ ficha”

“A corregedoria da Polícia Civil está investigando um esquema envolvendo policiais do Instituto de Identificação Ricardo Gumbleton Daunt (IIRGD) e funcionários da empresa de Processamento de Dados do Estado de São Paulo, que adulteraram antecedentes criminais em troca de propina.

O esquema foi descoberto em escuta telefônica autorizada pelo Departamento de Inquéritos Policiais (Dipo) e Polícia Judiciária – órgão do Judiciário.

Na realidade, a escuta foi o primeiro ato da investigação. Foram gravados diálogos nos quais se negociava a adulteração de antecedentes e os pagamentos. (...)”

Fonte: www.estadao.com.br, por Fabio Diamante e Marcelo Godoy
Data: 03/07/2003

Segurança da Informação
Gestor da Informação - Importante!

Para que o negócio da organização funcione, os usuários autorizados acessarão e utilizarão a informação.

Mas e se um usuário que tem o acesso autorizado quiser cometer alguma ação indevida? Ele vai conseguir? Sim!

Veja algumas medidas que devem ser implementadas:

- **Todas ações de um usuário no ambiente computacional deve ser registradas e guardadas durante um tempo.**
- **Para algumas tarefas críticas, pode-se exigir a autorização de dois usuários.**
- **Para casos como o descrito no último slide, a informação nunca deveria ser apagada, mas retificada, corrigida.**
- **Periodicamente, os acessos autorizados devem ser revistos pelo gestor da informação, para garantir que os usuários devam continuar com esse poder.**

Segurança da Informação
Gestor da Informação - Resumindo

O acesso à informação somente deve ser feito se o usuário estiver previamente autorizado.

Qualquer tentativa de acesso a ambientes não autorizados será considerada pela organização uma violação dos regulamentos de segurança!

A liberação da informação será autorizada pelo gestor da informação que considerará sua confidencialidade e a necessidade de acesso do usuário.

Segurança da Informação
Cópias de Segurança

- **A informação possui uma forte característica: se for destruída e não tiver uma cópia, nunca mais será recuperada.**
- **Cópia de segurança é fundamental para o processo de proteção da informação.**
- **Toda informação deve ser avaliada em relação à sua criticidade e, consequentemente, em relação à necessidade da existência de cópias de segurança.**
- **Uma recomendação importante e fundamental é guardar essas cópias em local seguro e distante o suficiente para que, caso aconteça uma situação de destruição dessa informação (desastre, roubo, ação de má-fé etc.), a cópia de segurança esteja protegida adequadamente.**

Segurança da Informação
Cópias de Segurança - Para refletir

- É possível recuperar uma mensagem do arquivo de correio eletrônico que você removeu há doze meses?
- Você já precisou e conseguiu recuperar informações que estavam em cópias de segurança? A partir de quando você conseguiu recuperar?
- Existem cópias de segurança para os arquivos que você possui no computador de sua casa?
- Você sabe restaurar arquivos provenientes de cópias de segurança para o computador que utiliza?
- Você já perdeu dados que não tinham cópia de segurança? O que aconteceu?
- Você conhece alguém que não possui cópia de segurança de seu computador pessoal? Essa pessoa está ciente do risco que está correndo?

Segurança da Informação
Cópias de Segurança - Caso real

“Fogo destrói laboratório e arrasa muitos anos de pesquisa no Pará”

“Belém - A Reitoria da Universidade do Pará (UFPA) estima em mais de R$ 1 milhão o prejuízo provocado pelo incêndio que destruiu anteontem parte do Centro de Ciências Biológicas. Um provável curto-circuito na velha fiação elétrica do prédio pode ter provocado as chamas, que consumiram décadas de análises e catalogação de espécies, deixando desesperados seus pesquisadores.

‘Foi uma coisa horrível. O prejuízo é inestimável. Pode-se colocar preços em equipamentos, mas não no material de pesquisa’, lamentou o diretor do centro, Ricardo Ishak.

Durante a operação de rescaldo realizada pelos bombeiros, ficou constatada a destruição total dos laboratórios de Citopatologia, Biologia e Ecologia. Nos laboratórios de Zoologia, a destruição foi parcial. No de Ecologia, segundo a coordenadora do projeto Recursos Vivos da Zona Economicamente Exclusiva, Lucinice Belúcio, todas as amostras e informações foram destruídas pelo incêndio. (...)”

Fonte: www.estadao.com.br, por Carlos Mendes

Data: 12/09/2003

Segurança da Informação
Cópias de Segurança - Importante

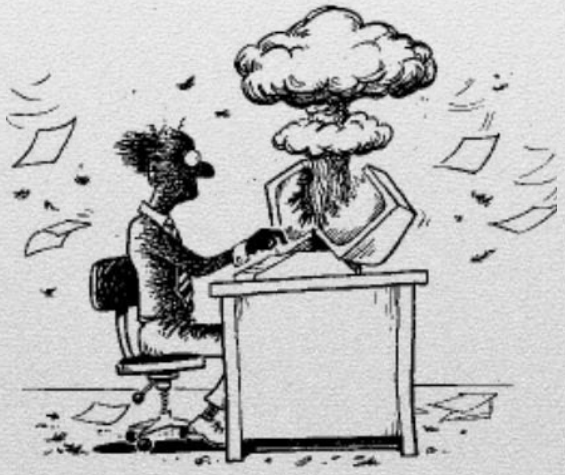
Toda informação crítica para o funcionamento da organização deve possuir, pelo menos, uma cópia de segurança atualizada em local seguro.

Os procedimentos que possibilitam a guarda, a recuperação e o uso da informação devem ser documentados para que a organização continue sua operacionalização mesmo na ausência do usuário responsável pela atividade.

Segurança da Informação
Ações para problemas

Podemos classificar didaticamente as ações que devem ser realizadas na organização com o objetivo de combater os desastres e os problemas.

a) **Ações preventivas**
b) **Ações detectivas ou para detecção**
c) **Ações corretivas**



Segurança da Informação
Ações para problemas - Para refletir

- Você consegue identificar ações preventivas, detectáveis e corretivas na sua organização? E no seu departamento?
- Qual delas você acha que pode ser mais eficaz para a proteção da informação? Você consegue justificar?
- Como você classificaria os procedimentos de realizar cópias de segurança, de fazer treinamento de simulação de incêndios com os funcionários, de contagem de estoque e de barreira física para acesso ao ambiente que possui recursos críticos do ambiente computacional?
- Você adota medidas preventivas na sua vida pessoal?
- Quando você realiza uma viagem de carro, como podemos classificar o seguro do carro, a revisão antes da viagem, o pneu reserva, as garrafas de água e refrigerante para as crianças e a noite bem-dormida de sono?

Segurança da Informação
Ações para problemas - Caso real

“Costureira morta em 2001 ainda recebe aposentadoria”

“Todo mês a Previdência Social deposita na agência Vila Mariana do Banespa, em São Paulo, cerca de R$ 400,00 na conta da contribuinte Belmira Damasco – sua aposentadoria obtida após mais de 30 anos de trabalho como costureira. Ao mesmo tempo manda para a agência Brigadeiro do Banco Itaú outro depósito de meio salário mínimo, pensão que Belmira herdou de seu pai. Os valores conferem, o depósito não atrasa, os extratos chegam regularmente à sua casa, no bairro do Ipiranga. A única coisa estranha nessa história é que Belmira morreu há três anos e meio, aos 89 anos – e sua família não consegue, de modo algum, interromper os pagamentos. (...)”

Fonte: Jornal O Estado de São Paulo, por Gabriel Manzano Filho

Data: 03/04/2005

Segurança da Informação
Ações para problemas - Importante

Toda informação deve ser protegida contra desastres físicos (fogo, calor, inundação etc.) e lógicos (vírus, acesso indevido, erro de programas, alteração incorreta etc.).

Segundo a Universidade de Berkeley, Estados Unidos, 93% da informação produzida hoje no planeta já nasce em formato digital.

Segurança da Informação
Continuidade do Negócio

Toda organização deseja continuar "viva", atuar no segmento escolhido, alcançar seus objetivos e cumprir sua missão.

A organização deve estar preparada para enfrentar situações de contingências e de desastre que tornem indisponíveis recursos que possibilitam seu uso.

Alguns recursos necessários para que uma organização funcione de forma adequada:

- ✓ **Humanos**
- ✓ **Tecnológicos**
- ✓ **Conhecimento de processos**
- ✓ **Ambiente Físico**
- ✓ **Infraestrutura**

Segurança da Informação
Continuidade do Negócio - Para refletir

- Existe, na sua organização, um plano para a recuperação do negócio em caso de situações de desastre ou de contingência?
- Você já participou de um teste ou de uma simulação de situação de desastre?
- Se acontecer um incêndio no seu ambiente de trabalho, você saberá o que fazer? Vai precisar levar alguma coisa?
- Os conceitos de continuidade são válidos para a vida pessoal. Por acaso já considerou sua continuidade profissional ou pessoal caso aconteça um desastre com você?

Segurança da Informação
Continuidade do Negócio - Caso real

“Raio cai 2 vezes em assistente de Mel Gibson”

“Jan Michelini nunca mais vai dizer que um raio não cai duas vezes no mesmo lugar. Diretor-assistente de A Paixão de Cristo, o polêmico filme de Mel Gibson, Michelini ganhou o apelido de ‘garoto relâmpago’ depois que um raio atingiu seu guarda-chuva durante as filmagens em Matera, na Itália, queimando a ponta de seus dedos.

Passados alguns meses, quando a equipe estava numa locação a algumas horas de Roma, nova tempestade. Michelini, outra vez, levava um guarda-chuva, desta vez ao lado de Jim Caviezel, astro do filme, que faz o papel de Cristo. ‘Eu estava a uns 3 metros dos dois quando vi um raio saindo das orelhas deles. Dessa vez os dois foram atingidos’, contou o produtor Steve McEveety. ‘O maior raio caiu em Caviezel e parte atingiu Michelini, mas eles não ficaram feridos.’ (...)”

Fonte: www.estadao.com.br

Data: 27/10/2003

Segurança da Informação
Produtos Homologados

A organização para a qual você trabalha ou presta serviços define um conjunto de ferramentas de tecnologia que formam o padrão dos produtos que estão autorizados para utilização por todos os usuários. São os chamados produtos homologados.

Quando uma organização homologa um produto, ela considera várias questões, tais como:

- **Manutenção de versões**
- **Treinamento de usuários**
- **Conhecimento coletivo**
- **Possibilidade de Suporte ao Usuário**
- **Licenciamento para uso do produto por toda a organização**

Segurança da Informação
Produtos Homologados - Para refletir

- **Você conhece os produtos homologados pela sua organização?**
- **Você sabe qual área procurar caso deseje encaminhar um produto para ser homologado?**
- **Você utiliza no computador da organização algum programa não homologado que necessita para o desempenho de suas atividades profissionais na empresa? Se sim, sua organização orienta o que deve ser feito?**

Segurança da Informação
Uso de Antivírus

Os vírus são programas que penetram no computador que utilizamos sem a nossa autorização e executam ações que não solicitamos. Normalmente, essas ações prejudicam o equipamento ou seu desempenho.

Alguns motivos para a criação de vírus:

a) **Demonstração de conhecimento técnico**
b) **Protesto**
c) **Chantagem**
d) **Crime organizado e desorganizado**
e) **Destruir por destruir**

Segurança da Informação
Uso de Antivírus

Você deve garantir, em casa ou no trabalho, que o programa antivírus esteja ativo no seu computador e corresponda à versão mais atualizada.

Tão importantes quanto o uso de programa antivírus são algumas ações complementares tais como:

a) **Ao receber qualquer arquivo anexo, não o execute sem antes passar o programa antivírus.**
b) **Se você não estava esperando o arquivo, não execute nenhum programa enviado anexo. Se conhecer o remetente, entre em contato com ele.**
c) **Na internet, somente baixe alguma informação em forma de arquivo quando estiver navegando em locais (*sites*) seguros e reconhecidamente de organizações sérias e profissionais que zelam pela segurança da informação.**
d) **Mantenha atualizadas as cópias de segurança dos arquivos de dados que você gerou. Garanta a possibilidade de recuperação da informação a partir dessas cópias.**

Segurança da Informação
Uso de Antivírus - Para refletir

- O computador que você utiliza na organização possui um programa antivírus?
- O programa antivírus que você utiliza está atualizado? Ele é um produto homologado pela organização?
- Você sabe como ocorre a atualização do programa antivírus?
- Você conhece o que a política de segurança da sua organização define sobre o uso de programas antivírus?
- Você utiliza programa antivírus no computador da sua residência? Os demais usuários do equipamento doméstico conhecem a importância desse tipo de programa?
- Você já sofreu uma ação de vírus? Foi prejudicado? O que aconteceu?
- Caso um vírus seja identificado no computador que você utiliza, saberia quem acionar na sua organização?

Segurança da Informação
Uso de Antivírus - Caso real

“Vírus sérvio espalha mensagem política”

“A Sophos divulgou nesta quarta-feira (16/02) a descoberta de um vírus de origem sérvia que espalha uma mensagem política utilizada por Tomislav Nicolic, político de um partido radical daquele país, além de modificar arquivos executáveis do sistema operacional Windows, da Microsoft.

O vírus que chega ao usuário por meio de arquivos executáveis (com extensão .exe) infectados mostra a mensagem ‘Long Live Great SERBIA’ (Vida longa grande Sérvia, em inglês) após infectar.”

Fonte: www.idgnow.com.br

Data: 16/02/2005

Segurança da Informação
Uso de Antivírus - Importante

Quando a organização define uma política de segurança, seu objetivo é explicitar aos usuários que acessam e utilizam a informação qual é a filosofia e quais são as regras sobre esse recurso.

A organização busca garantir que a informação esteja protegida contra possíveis perdas, danos, destruição e/ou mau uso.

Segurança da Informação
Uso da Internet

- A Internet é uma nova forma de acessar informações;
- Dificuldade em achar exatamente aquilo que queremos;
- Na Internet é o usuário quem busca a informação;
- Informações que deveriam ser acessadas apenas por adultos podem ser facilmente vistas por crianças e adolescentes;
- As empresas disponibilizam acesso à Internet como uma fonte de informações para que os colaboradores atualizem e enriqueçam seu conhecimento;
- Legislação em termos de direito autoral, propriedade industrial e outras irregularidades;
- Você é responsável pelos acessos que realiza na Internet;
- Privacidade do usuário ao acessar sites que monitoram tudo o que você faz.

Segurança da Informação
Uso da Internet - Para refletir

- **Você utiliza os recursos da organização para acessos na Internet somente para assuntos profissionais?**
- **Ao utilizar a Internet para assuntos pessoais, você utiliza em tempo adequado de maneira a não prejudicar suas atividades profissionais?**
- **Você conhece qual é a política de acesso à Internet de sua organização?**
- **Você sabe que pode ser monitorado quando acessa locais *(sites)* na Internet?**
- **Você ficaria em situação constrangedora se sua chefia (e seus subordinados) soubessem os acessos que realizou na Internet por meio de recursos da organização? Pense que seus acessos serão publicados no jornal da empresa.**
- **Você evita circular na Internet por locais *(sites)* que não conhecem a seriedade e o profissionalismo?**
- **Você costuma ler a política de privacidade dos locais *(sites)* que acessa na Internet?**
- **Qual a sua opinião sobre o seguinte procedimento: a lista de acessos feitos por cada usuário, independentemente de seu nível hierárquico, será uma informação disponível para qualquer usuário da organização. Você é a favor de implementar esse procedimento na sua organização?**

Segurança da Informação
Uso da Internet - Caso real

“Kits ensinam como aplicar golpes e fraudes pela Internet”

“Os candidatos a golpistas virtuais contam agora com uma nova ferramenta para tentar enganar os internautas: um kit tipo ‘faça você mesmo’ que pode ser baixado gratuitamente da rede mundial de computadores.

De acordo com Sophos, empresa que desenvolve antivírus e outras soluções de segurança, os kits ensinam como criar páginas falsas de bancos e fazer com que os usuários digitem seus números de conta bancária e senha nos sites falsos.”

Fonte: www.folhaonline.com.br
Data: 19/08/2004

Segurança da Informação
Uso do Correio Eletrônico

- Faz parte do nosso dia-a-dia, seja no âmbito pessoal ou profissional.
- Ferramenta disponibilizada para tornar mais eficientes nossas atividades profissionais.
- Devem ir de encontro à legislação vigente e princípios éticos.
- Cuidado com mensagens obscenas, discriminatórias, racistas ou similares.
- Soluções seguras que permitem a confidencialidade do conteúdo de uma mensagem.
- Utilize o correio eletrônico da organização para mensagens de assuntos profissionais.
- Para assuntos pessoais, utilize-o de forma responsável.

Segurança da Informação
Uso do Correio Eletrônico - Para refletir

- Você conhece a política e as normas de correio eletrônico de sua organização?
- Você considera que utiliza de forma adequada o correio eletrônico para a comunicação pessoal? E seus subordinados?
- O que seria utilizar o correio eletrônico da organização de forma irresponsável?
- Ao receber uma mensagem com conteúdo indevido, qual deve ser sua ação?
- Você está lembrado que normalmente a mensagem de correio eletrônico circula pela Internet de forma aberta, possibilitando sua leitura por pessoas que não deveriam ter acesso ao conteúdo da mensagem?
- Na sua organização, qual é a orientação caso você necessite enviar uma mensagem eletrônica confidencial para outra empresa?
- Como você avalia o nível de conscientização das pessoas em relação à segurança do correio eletrônico?

Segurança da Informação
Uso do Correio Eletrônico - Caso real

“Familiares de pessoas falecidas podem acessar seus e-mails?”

“O pai de um fuzileiro naval norte-americano morto em confronto no Iraque quer ter acesso aos e-mails de seu filho no Webmail do Yahoo! A empresa negou esse direito e, com isso, criou uma polêmica. O que você acha sobre o assunto? (...)”

Fonte: www.folhaonline.com.br

Data: 06/01/2005

Argumentos

- **Ninguém tem o direito de acessar o Webmail de uma pessoa falecida. Isso vai totalmente contra a política de privacidade com a qual empresas como o Yahoo! Dizem proteger informações dos seus usuários.**
- **O pai tem o direito de acessar os e-mails do filho. É possível até que ele encontre informações preciosas, caso o fuzileiro tenha salvado mensagens enviadas a amigos.**

Segurança da Informação
Uso do Correio Eletrônico - Importante

Caso você não utilize certificado digital, que possibilita o sigilo e não o repúdio à mensagem de correio eletrônico, não envie informação para fora do ambiente da organização – ou seja, mensagens em que a organização ou o destinatário ficariam constrangidos caso seu conteúdo fosse publicado em um jornal.

Uma mensagem via correio eletrônico pode ser considerada um documento formal da organização. Seja cuidadoso no uso dessa ferramenta.

Segurança da Informação

Mensagens encadeadas e anexos no correio eletrônico

- **Facilidade de se registrar o histórico do assunto.**
- **Ao responder uma mensagem, devemos deixar parte do texto original para que a pessoa que enviou a primeira mensagem saiba do que estamos falando.**
- **Circulação desnecessária de arquivos anexados.**
- **Confidencialidade da informação encaminhada ou respondida.**
- **Verifique sempre se é necessário realmente enviar mensagens encadeadas. Às vezes uma reunião pode resolver o problema.**
- **Somente envie arquivos anexados quando for realmente imprescindível.**
- **Exerça a proteção: descarte arquivos não esperados!**
- **Não incentive o encadeamento de mensagens de correio eletrônico.**

Segurança da Informação

Mensagens encadeadas e anexos no correio eletrônico - Para refletir

- Ao repassar mensagens anexadas, você analisa o conteúdo das mensagens e a confidencialidade em relação aos destinatários?
- Você analisa se é imprescindível repassar arquivos anexados?
- Você conhece alguma situação em que alguém ou alguma corporação em situação delicada por repassar informação indevida por meio de arquivos ou mensagens anexadas?
- Sua organização orienta os usuários sobre esse assunto? E você orienta os mais jovens na organização sobre este tema?
- Você conhece a área técnica da sua organização que pode ajudá-lo caso tenha dúvidas sobre um arquivo anexado que recebeu?
- Você sabe se sua organização bloqueia o recebimento de determinados tipos de arquivos vindos em mensagens do correio eletrônico? A organização divulgou quais são esses tipos de arquivos bloqueados?

Segurança da Informação

Mensagens encadeadas e anexos no correio eletrônico - Caso real

“E-mails sobre armas nucleares podem ter vazado”

“Oficiais do Laboratório Nacional Los Alamos, nos Estados Unidos, confirmaram que vários e-mails com dados sigilosos sobre armas nucleares foram enviados por um sistema inseguro de e-mail. Essa circulação poderia dar chance a vazamento de informações.

A revelação vem menos de duas semanas depois de o laboratório anunciar que dois discos removíveis com informações sobre armas nucleares desapareceram de suas instalações. Esta é a terceira vez desde o ano de 2000 que discos de armazenamento com informações confidenciais desaparecem da base. (...)”

Fonte: www.idgnow.com.br

Data: 20/07/2004

Segurança da Informação

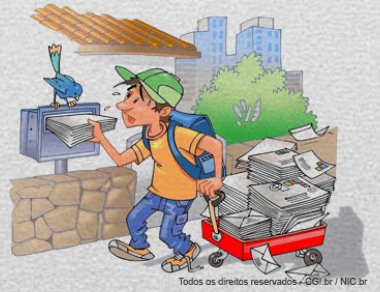
Mensagens encadeadas e anexos no correio eletrônico - Importante

Caso uma negociação precise ser feita via correio eletrônico, e não esteja sendo utilizada uma proteção segura tipo certificado digital e sigilo do texto, a direção da organização deverá estar ciente do fato e do risco da não confidencialidade das mensagens trocadas entre as partes, bem como da possibilidade de repúdio de autoria.

Ao indicar o destinatário em uma mensagem de correio eletrônico, tenha certeza de que o endereço indicado é realmente aquele para quem você deseja enviar a mensagem.

Segurança da Informação
Notícias e orientações via correio eletrônico

- **O uso do correio eletrônico facilitou muito a comunicação entre as pessoas que possuem acesso a esse recurso. De uma maneira diferente, a comunicação com outras pessoas pela escrita voltou a ser sucesso.**
- **Não acredite em tudo que chega ao seu correio eletrônico. Se você realmente se interessou por uma determinada situação, utilize outros meios para validar a veracidade da situação relatada.**
- **Não acesse uma instituição financeira por meio de endereços vindos em mensagens duvidosas. Normalmente, esses endereços apresentam apenas números e você não tem como comprovar sua veracidade.**



Segurança da Informação

Notícias e orientações via correio eletrônico - Para refletir

- Você já recebeu mensagem de correio eletrônico do banco em que tem conta corrente? Procurou identificar se a mensagem era verdadeira? E de bancos em que você não tem conta? Você imagina por que recebeu essa mensagem?
- Você repassa imediatamente para seus amigos mensagens recebidas via correio eletrônico sobre descobertas, novos vírus e outros assuntos de interesse geral? Já parou para pensar que essas mensagens podem não ser verdadeiras e que você pode estar sendo usado para divulgar boatos?
- Já foi escolhido entre milhões de internautas para receber uma superoferta à qual somente você tem direito? Isso, logicamente, apenas de responder imediatamente! Você procurou avaliar que isso pode ser um golpe?
- Você desconfia de mensagens de remetentes desconhecidos?
- Você repassa corrente de mensagens? E aquelas que informam que repassar a mensagem traz muito dinheiro para quem o faz e desgraça para quem não repassa?
- Sua organização orienta sobre a postura diante desse tipo de mensagens?

Segurança da Informação

Notícias e orientações via correio eletrônico - Caso real

“Banco do Brasil é alvo de fraude eletrônica”

“Um e-mail falso disparado durante o Carnaval para diversos correntistas do Banco do Brasil obrigava o recadastramento das contas num prazo de 48 horas.

Site do Banco foi forjado no domínio do Instituto Nacional de Tecnologia, órgão vinculado ao Ministério da Ciência e Tecnologia. Polícia Federal está investigando o caso.

Aproveitando-se do Carnaval, fraudadores dispararam e-mail para diversos clientes do BB informando que eles deveriam acessar o site www.bancodobrasil.int.gov.br e fazer o recadastramento. (...)”

Fonte: www.computerworld.com.br

Data: 06/03/2003

Segurança da Informação

Notícias e orientações via correio eletrônico - Importante

A proteção do recurso computacional de uso individual é de responsabilidade do usuário.

Verifique na sua organização os procedimentos em caso de perda ou roubo.

Segurança da Informação
Fraude que utiliza a tecnologia

- **A fraude é uma ação tão velha quanto a história da humanidade. A própria Bíblia relata a fraude em que Jacó enganou seu pai Isaque, quando se fez passar por Esaú, seu irmão. Há também a história da serpente do Éden!**

- **Pedidos de ajuda para pessoas doentes e situações similares são potencialmente fraudes utilizando o ambiente de tecnologia.**

- **A fraude que utiliza o ambiente de tecnologia continuará acontecendo, mas você tem condições de evitá-la.**

Segurança da Informação

Fraude que utiliza a tecnologia - Para refletir

- Você já recebeu mensagem de correio eletrônico oferecendo vantagens que pareciam fraude?
- Por que você acha que as pessoas caem em malandragens eletrônicas?
- Como podemos evitar cair em uma fraude eletrônica?
- Você acha que as fraudes eletrônicas que já ocorreram devem ser divulgadas para que todos saibam dos riscos? Com essa divulgação, você não acredita que os fraudadores ficariam sabendo de vulnerabilidades que não conheciam?
- Que ações concretas e visíveis a sua organização tem realizado para evitar a fraude eletrônica?
- Você verifica a veracidade das mensagens antes de passá-las adiante?
- Você já alertou seus familiares sobre a possibilidade de fraudes no ambiente de tecnologia?
- Você conhece alguém que já foi vítima de fraude realizada por meio do ambiente computacional?

Segurança da Informação
Fraude que utiliza a tecnologia - Caso real

“Dados confidenciais são recuperados em 47% dos PCs inutilizados”

“Cerca de 47% dos computadores inutilizados nas empresas contém informações em seus discos rígidos sobre a própria organização ou seus funcionários – dados pessoais, financeiros e relatórios foram alguns dos ‘achados’.

Isso é o que mostra um estudo da University of Glamorgan, no Reino Unido. Os pesquisadores compraram computadores no site de leilões eBay e fizeram a análise nos discos de 92 máquinas.”

Fonte: www.folhaonline.com.br

Data: 28/02/2005

A divulgação não autorizada de informação confidencial pode causar impacto (financeiro, de imagem ou operacional) ao negócio da organização.

Segurança da Informação
Legislação

- **Ela atende grande parte do mundo virtual.**
- **Acessos indevidos, ações de destruição ou alteração em ambientes de terceiros;**
- **Normas e regulamentos da organização;**
- **Legislação vigente sobre o uso da informação no mundo virtual.**

Viva no seu ambiente virtual com a mesma responsabilidade com que vive no mundo real. Afinal, pode ser virtual, mas a penalização é real e dura!

Segurança da Informação
Legislação - Para refletir

- Você conhece suas responsabilidades legais como usuário ou como gestor da organização?
- Você sabe que pessoas já foram condenadas pela justiça brasileira por ações de má-fé utilizando o ambiente virtual?
- A área jurídica de sua organização orienta você sobre esse aspecto?
- Você tem acompanhado as decisões da justiça sobre situações complexas no ambiente virtual?

Segurança da Informação
Legislação - Caso real

“Bandidos usam pornografia infantil para extorquir internautas”

“Naquilo que parece ser um novo esquema on-line, funcionários vêm sendo chantageados por supostos downloads de fotos pornográficas de crianças em seus computadores. Na verdade, porém, as imagens são baixadas no PC da vítima sem o seu conhecimento.

O esquema usa uma série de técnicas de extorsão atualmente comuns, mas explora o fato de tratar-se de material ilegal, que poderia facilmente colocar a vítima em mais lençóis.

Descrito pela primeira vez na edição de fevereiro da revista ‘CSO Magazine’, a ação dos bandidos começa com um e-mail não solicitado contendo um link para um site aparentemente inofensivo – no caso descrito pela revista, o site faz referência aos Jogos Olímpicos da Grécia. (...)”

Fonte: www.jconline.com.br

Data: 19/02/2003

Segurança da Informação
Privacidade

- **Não deve ser violada!**
- **Mais segurança → menos privacidade.**
- **Segurança física: controle e registro de acesso por meio do uso de crachás, filmagem de ambientes, barreiras com catracas, vigilância com guardas e áreas restritas.**
- **Segurança da informação: identificação e autenticação de usuários, uso restrito de recursos (transações) e registro dos acessos realizados por cada usuário.**
- **Política de privacidade para uso do correio eletrônico e da Internet.**

Segurança da Informação
Privacidade - Para refletir

- Você conhece a legislação que sua organização é obrigada a cumprir em função do tipo de negócio?
- Você conhece a política e as normas de sua organização em relação à privacidade dos funcionários, dos prestadores de serviço e dos clientes?
- Você conhece a legislação federal sobre a privacidade do cidadão?
- Você já sentiu, em algum momento, que sua privacidade foi invadida como cidadão? E como colaborador da organização?
- Você já teve acesso à informação de outras pessoas, mesmo sabendo que não deveria tê-lo?
- Para você o monitoramento de câmeras nas ruas das grandes cidades invade a privacidade do cidadão? E na empresa?
- O que você acha das notícias sobre a venda ilegal de banco de dados com informação de cidadãos? Alguma sugestão para combater essa prática?

Segurança da Informação
Privacidade - Caso real

“Espanha multa jovem por espionagem via *Webcam*”

“Um estudante foi multado pela Corte espanhola por espionar uma jovem por meio de sua Webcam, anunciou nesta segunda-feira (28/02) a empresa de segurança Sophos.

Segundo a Corte de Málaga, o rapaz utilizou o cavalo de Tróia Subseven para monitorar a garota sem o seu conhecimento e também para espionar conversas on-line da vítima.

O rapaz, que não foi identificado, afirmou ter escolhido sua vítima aleatoriamente em janeiro de 2002 pela Internet, então, ativou o cavalo de Tróia.

Uma vez ativado, o programa conseguia monitorar de maneira invisível e-mails, chats e capturar imagens pela Webcam da vítima. (...)

A Corte denunciou o estudante por invasão de privacidade e captura ilícita de imagens. (...)”

Fonte: www.idgnow.com.br
Data: 28/02/2005

Segurança da Informação
Informações Pessoais

- **Dados cadastrais, médicos, de desempenho profissional e vida acadêmica.**
- **Não devem ser mantidas nas bases de dados da organização informações pessoais que não sejam relevantes ou não sejam exigidas legalmente para o funcionamento do negócio e da infraestrutura administrativa.**
- **Proteja suas informações pessoais e das demais pessoas que você conhece. Procure saber como as organizações com as quais você se relaciona tratam esse tipo de informação.**
- **Não deixe a informação pessoal virar informação do pessoal! Evite fraudes!**

Segurança da Informação
Informações Pessoais - Para refletir

- Você preenche folhetos de promoções com várias informações pessoas apenas para concorrer a um sorteio? Não acha barato demais o preço pago a você pelas suas informações?
- Você indica endereços de correio eletrônico de amigos para organizações que lhe pedem isso?
- Você conhece a política de sua organização para os dados pessoais dos colaboradores e clientes?
- Você conhece a política dos parceiros de sua organização em relação aos dados pessoais dos colaboradores e clientes para os quais realiza suas atividades profissionais?
- Como seu convênio médico protege suas informações pessoais e dos demais clientes?
- Você começa a responder rapidamente a qualquer pesquisa que é feita por telefone?

Segurança da Informação
Informações Pessoais - Caso real

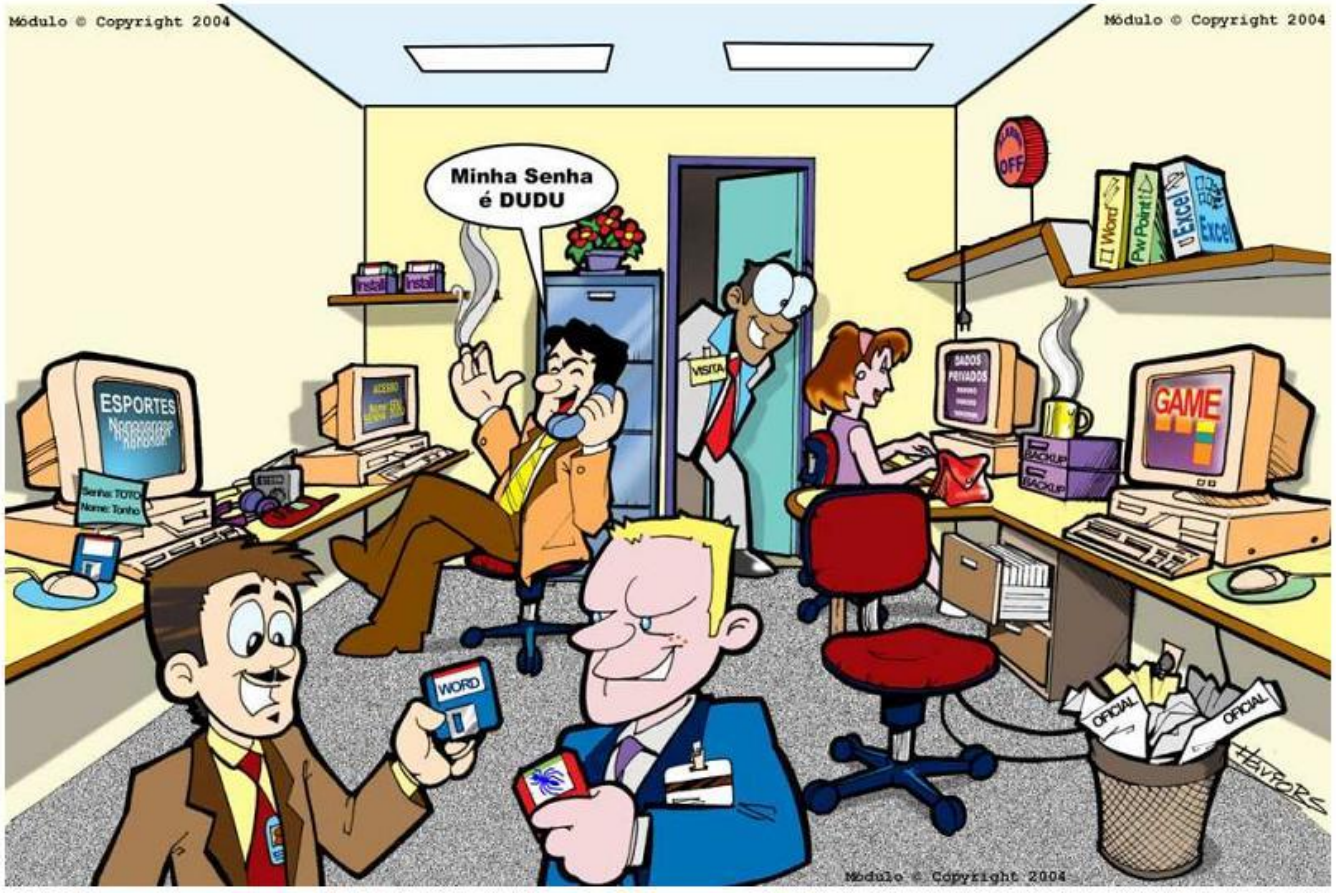
"*Hacker* quebra banco de dados de universidade nos EUA"

"Em um ataque à rede de computadores da Universidade do Texas (UT), em Austin (EUA), um hacker conseguiu coletar informações a respeito de mais de 55 mil pessoas, incluindo estudantes, membros da equipe da faculdade e profissionais em busca de vagas, informou a Universidade em um comunicado, nesta quinta-feira (06/03).

O ataque foi detectado no domingo (02/03) quando a equipe de sistemas da universidade notou que um computador não estava funcionando bem. Análises do problema revelaram que o mau funcionamento da máquina resultava de um ataque e que o sistema de usuários da rede estava comprometido. (...)"

Fonte: www.idgnow.com.br
Data: 28/02/2005

Segurança da Informação
Engenharia Social



Segurança da Informação
Engenharia Social

- **Conjunto de procedimentos e ações que são utilizados para adquirir informações de uma organização ou de uma pessoa por meio de contatos falsos sem o uso da força, do arrombamento físico ou de qualquer brutalidade. É a velha conversa do malandro!**
- **Os engenheiros sociais agem e buscam informações da organização usando pessoas como você. Eles usam as seguintes táticas:**
  a) **Falam com conhecimento**
  b) **Adquirem a confiança do interlocutor**
  c) **Prestam favores**

Segurança da Informação
Engenharia Social - Para refletir

- Você recebeu orientação da organização sobre os cuidados para contatos com estranhos?
- A organização garante que os papéis destinados à destruição sejam realmente destruídos?
- Você destrói seus documentos confidenciais antes de jogar no lixo?
- Os funcionários ou prestadores de serviços que atuam diretamente com o público externo estão atentos para os golpes aplicados pelos engenheiros sociais?
- Você considera dados pessoais o endereço residencial, o telefone celular, o time de futebol que torce, a data de nascimento, o telefone comercial?
- Você acha que a sua organização está preparada para evitar os engenheiros sociais?
- Você está preparado para enfrentar situações-surpresa se alguém aplicar táticas de engenharia social?
- Você orientou seus familiares sobre o perigo dos golpes por intermédio de engenharia social?

Segurança da Informação
Engenharia Social - Caso real

“Mitnick reforça o aspecto humano na segurança das redes corporativas”

“Se o passado o condenou, o presente está sendo de grande profundidade para Kevin Mitnick. De ex-hacker, passou oitos anos na prisão por invasão de computadores, Mitnick é atualmente um promissor consultor de segurança e também escritor. O dono da Defensive Thinking e autor do livro The art of deception: Controling the human element of security reforça o fator humano, mais até que o tecnológico, para aumentar a segurança em redes corporativas, que anda tirando o sono de muitos CIOs.

Além desse aspecto, o executivo sugere que a política de segurança deve vir antes até da construção física da rede. ‘Deve ser como um carro novo, quando compramos, ninguém espera que ele seja abalroado ou roubado para adquirir um seguro. Com as corporações é a mesma coisa, o investimento deve preceder o problema’, ensina Mitnick, em entrevista exclusiva à revista Network.

O consultor aborda ainda a importância da análise dos valores das informações no caso destas serem roubadas. (...)”

Fonte: www.itweb.com.br, por Tereza Santos
Data: 23/04/2003

Segurança da Informação
Engenharia Social - Importante

Tenha cuidado ao falar e conversar com outras pessoas.

Não discuta assuntos da organização em ambientes em que não se possa garantir o sigilo da informação.

Todos os locais físicos em que se encontram recursos de informação devem possuir proteção de controle de acesso.

Segurança da Informação
Ambiente Convencional

- **Alguns cuidados a serem tomados ao tratar a informação da organização:**

a) **Falar em ambiente não seguro**
b) **Mostrar a informação**
c) **Deixar a informação**
d) **Entregar informação**
e) **Acesso físico**

Segurança da Informação
Ambiente Convencional - Para refletir

- Você costuma comentar assuntos da organização quando está em um táxi?
- Após o expediente, os documentos confidenciais são trancados em gavetas ou armários? Os computadores portáteis também são guardados ou ficam protegidos?
- Existe restrição de acesso físico para os visitantes? Como a organização garante que os visitantes terão acesso apenas a uma área específica?
- Você pode solicitar a alguma pessoa na organização que não está utilizando o crachá de identificação que o coloque? Se você fizer isso, será mal interpretado?
- O visitante, na sua organização, recebe orientação sobre os critérios de segurança física adotados no ambiente da visita?
- Se um vigilante recém-contratado pela organização impedir o acesso do presidente a uma área restrita porque ele está desacompanhado e sem crachá, o que acontecerá no dia seguinte?

Segurança da Informação
Ambiente Convencional - Caso real

“CEU é roubado pelo próprio vigia”

“Trabalhando há três semanas no escolão Navegantes, na Zona Sul, o segurança foi flagrado furtando câmeras e aparelhos eletrônicos.

O Centro Educacional Unificado (CEU) Navegantes, no Grajaú, Zona Sul, foi alvo ontem do seu quarto ataque por bandidos. Desta vez, houve um preso. Os guardas-civis que realizaram a ação se surpreenderam ao identificar o suspeito: Edvan Gonçalves da Silva, de 31 anos, trabalhava havia três semanas como segurança do próprio escolão. (...)”

Fonte: www.diariosp.com.br

Data: 22/12/2003

Segurança da Informação
Dez Direitos do Usuário

Todo usuário, de qualquer nível hierárquico e de qualquer relação profissional com a organização, tem o direito de:

1. **Ter acesso individual.**
2. **Acessar as informações necessárias para o desempenho de suas atividades profissionais.**
3. **Saber quais informações existem a seu respeito e poder indicar correções.**
4. **Saber as situações em que seu acesso à informação será registrado em trilha (*log*) de auditoria.**
5. **Ser informado de forma explícita, clara e contínua sobre a política e os demais regulamentos de segurança da informação.**
6. **Ser avisado quando ocorrer tentativas de acesso inválido utilizando sua identificação.**
7. **Receber treinamento adequado sobre os mecanismos de segurança de informação, que devem ser de fácil utilização.**
8. **Poder comunicar qualquer ocorrência ou suspeita de ocorrência que comprometa a segurança da informação.**
9. **Ter garantida sua privacidade pessoal.**
10. **Ser considerado mais importante do que qualquer recurso tecnológico.**

Segurança da Informação
Referências Bibliográficas

- **FONTES, E. Segurança da Informação. São Paulo: Saraiva, 2006.**