

## Normas de Segurança da Informação

### Introdução

Ninguém passa a noite com a porta de casa aberta para não ter que abrir de novo no dia seguinte. Mas muita gente deixa o computador ligado, o e-mail aberto e senha no modo automático para não ter que inicializar tudo de novo. **Por que as pessoas têm menos cuidado quando estão em ambiente eletrônico, cujos dados hoje representam o patrimônio da pessoa e da empresa?**

A invasão de sua residência torna-se mais difícil quando há um trinco na porta, mas seu computador (tanto o pessoal como sua estação de trabalho) está altamente suscetível a diversos riscos se não forem observadas as mínimas regras de segurança da informação. **Você sabe se está deixando a porta eletrônica aberta?**

Com este guia, você poderá fazer uma consulta rápida sobre o que é certo e o que é errado na Sociedade Digital, no uso da tecnologia e dos ambientes eletrônicos. As afirmações contidas foram baseadas em nossa legislação vigente, bem como em princípios éticos, de cidadania e de boas práticas digitais.

### 1. Senhas

**Você já emprestou sua senha da rede da ESHO para alguém, ou usou a de algum colega? Já emprestou sua senha de e-mail?**

Estas atitudes geram um grave risco, uma vez que as **senhas** hoje são consideradas **evidência de identidade digital**. Ou seja, elas demonstram quem é o autor de determinado e-mail, acesso ou transação. Logo, se esta pessoa utilizar sua senha para fazer algo de errado em ambiente eletrônico, como retirar conteúdos da rede ou enviar uma mensagem ofensiva, **o principal suspeito será você**.

Além disso, você incorre no crime de **“falsa identidade”**, como prevê o código penal.

**“De olho na Lei”**

#### Código Penal - Falsa identidade

Art. 307 - Atribuir-se ou atribuir a terceiro falsa identidade para obter vantagem, em proveito próprio ou alheio, ou para causar dano a outrem:

Pena - detenção, de três meses a um ano, ou multa, se o fato não constitui elemento de crime mais grave.

Art. 308 - Usar, como próprio, passaporte, título de eleitor, caderneta de reservista ou qualquer documento de identidade alheia ou ceder a outrem, para que dele se utilize, documento dessa natureza, próprio ou de terceiro:

Pena - detenção, de quatro meses a dois anos, e multa, se o fato não constitui elemento de crime mais grave.

Tudo isso por emprestar a senha. Por isso, **proteja sua IDENTIDADE DIGITAL!**

### Dicas

- não empreste sua senha;
- não use a senha de outra pessoa;
- não empreste seu computador;
- evite usar o computador de outra pessoa;
- evite colocar sua senha em módulos automáticos;
- evite usar computadores com pouca segurança, como cyber-café, para operações que exijam maior segurança;
- se for necessário utilizar seu computador pessoal, verifique se os documentos da empresa não estarão disponíveis para serem baixados por programas de troca de arquivos.

### Você sabe escolher sua senha de uma forma segura?

As senhas caracterizam a privacidade do acesso de pessoas a determinados recursos e informações restritas. Escolha um código que seja fácil de ser memorizado apenas por você. Siga as orientações abaixo para as regras de senhas da ESHO e adote o mesmo método para sua vida pessoal, em senhas de acesso a banco, sites ou correio, trocando-as periodicamente, mesmo que não seja solicitada:

- Sempre altere sua senha caso suspeite que foi "descoberta";
- O tamanho mínimo da senha deve ser de 6 caracteres;
- Troque sua senha no mínimo a cada quatro meses;
- Combine caracteres maiúsculos e minúsculos, sinais e números, que devem ser fáceis de lembrar, porém difíceis de serem descobertos;
- Não baseie sua senha em informações pessoais, como próprio nome, nome de familiares, bichos de estimação, nome de time de futebol, placa do automóvel, nome da empresa ou departamento, etc.;
- Não inclua senhas em processos automáticos de acesso ao sistema;
- Toda senha possui caráter individual e não deve ser fornecida em hipótese alguma a outras pessoas, quer sejam da sua família, empregados, amigos ou terceiros;
- Memorize as suas senhas, não escreva no monitor, papel, etc.

Apesar da segurança, existem programas específicos criados para captar e decifrar senhas que circulam na rede. Senhas como data de aniversário, nomes próprios ou nomes de fácil conhecimento, facilitam para que estes softwares decifrem sua senha.

## 2. Descarte de Informações

**Você já jogou fora algum CD ou disquete com informações pessoais ou pertencentes à ESHO, sem apagá-las ou destruir a mídia?**

O **descarte de mídias** deve ser realizado de forma consciente e seguro. Da mesma forma que cuidamos de nossas informações pessoais devemos cuidar das informações da empresa. Quando enviamos para a impressora nossa posição de extrato bancário ou uma transação bancária, imediatamente temos o cuidado de buscá-las, assim também deve ser com as informações da empresa!

Documentos esquecidos ou abandonados em impressoras, copiadoras e fax são risco de vazamento de informação ou divulgação indevida.

Material armazenado embaixo de mesas ou em outros locais inadequados são possíveis focos de incêndio; são chamados de carga de fogo e devem ser controlados, pois podem colocar em risco não apenas as informações da empresa, mas suas instalações e seu pessoal.

É de responsabilidade de todos os colaboradores da ESHO zelar pelas informações que lhes foram confiadas!

O mesmo vale para o lixo que você joga fora. É preciso picotar o mesmo, inclusive papéis com informações bancárias (extrato de banco) ou de fatura de cartão de crédito. Documentos confidenciais jamais podem ser jogados no lixo sem observar estes cuidados.

### **Informações Confidenciais:**

São informações com potencial para gerar vantagens competitivas ou capazes de exercer impactos significativos (financeiros, de imagem, jurídico) caso sejam divulgadas para pessoas não autorizadas. São exemplos de informações confidenciais: informações cadastrais de clientes, fornecedores, filiais, parceiros e funcionários.

### **Como descartar os materiais mais comuns :**

- Papel: rasgue o papel antes do descarte;
- CDs e DVDs: quebre a mídia em alguns pedaços, tomando cuidado para evitar acidentes;
- Cartões de crédito ou banco: corte em pedaços, invalidando a área magnética;
- Disquetes e fitas magnéticas: corte a área magnética em pedaços.

### **Dicas:**

- Ao se ausentar por um longo período de sua estação de trabalho, lembre-se sempre de trancar gavetas e armários e não armazenar informações da empresa sobre a mesa; e, mesmo que por um breve período, trave o acesso a seu computador com <Ctrl + Alt + Del>.
- Ao selecionar o comando "imprimir", vá até a impressora retirar seus documentos. Esse cuidado também deve ocorrer com originais em copiadoras e fax.
- Não armazene material embaixo das mesas. Quando não for mais necessário, solicite à manutenção sua retirada.
- Utilize as caixas de destruição dos andares para o descarte de papéis e mídias com informações confidenciais.

### Importante:

Divulgação indevida de informações – o que pode acontecer com você se isso ocorrer? Você pode vir a ser responsabilizado por danos causados por sua omissão ou negligência. Se sua função for de **gerente** ou **gestor**, há a responsabilidade solidária, bem como pode ainda incorrer em infração a Consolidação das Leis do Trabalho por quebra de sigilo profissional.

### De olho na Lei:

**Código Civil: Artigo 186** - Aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito.

**Art.1016.** Os administradores (cargo de gerente para cima) respondem solidariamente perante a sociedade e os terceiros prejudicados, **por culpa no desempenho de suas funções**.

**Art. 482** - Constituem justa causa para rescisão do contrato de trabalho pelo empregador:

(...) g) violação de segredo da empresa;

## 3. Engenharia Social

**Você já foi abordado por alguém pedindo sua senha ou informação confidencial para algum fim duvidoso?**

Se a resposta for sim, é muito possível que você tenha tido contato com o golpe denominado **engenharia social**. Essa forma de ataque é a favorita de muitos criminosos, já que muitas pessoas são bem mais vulneráveis e mais fáceis de “burlar” que os firewalls e sistemas de segurança. Se alguém abordar você pedindo uma senha ou informação da ESHO, procure saber mais sobre a pessoa e confira sua identidade. Nunca responda a mensagens de conteúdo duvidoso, como cartões românticos, promoções, relacionadas à Receita Federal, ao SPC e cancelamento de Título de Eleitor. A maioria dos casos explora a curiosidade das pessoas, para, por meio de uma “máscara”, pegar seus dados ou infectar sua máquina. Portanto, tenha muita cautela nessas ocasiões. Desconfie sempre!

Para solicitações de informações confidenciais, peça que a pessoa faça por escrito, com cópia para outras pessoas – como, por exemplo, o gestor dela ou o seu gestor.

O acesso às instalações da ESHO também é controlado pelo uso de crachás.

Visitantes devem ser identificados na recepção e possuem acesso liberado apenas para o departamento informado e autorizado pelo anfitrião. **Não dê carona com seu crachá** para facilitar o acesso de desconhecidos e, no caso de identificar alguém desconhecido desacompanhado, questione: No que posso ajudá-lo? Quem você procura? Dessa forma você estará sendo gentil e ao mesmo tempo inibindo uma possível tentativa de acesso indevido. E, a qualquer suspeita, avise a área de Segurança Patrimonial

### Falando nisso...

Evite também falar sobre assuntos confidenciais em ambientes não-privativos, elevadores, restaurantes, ônibus e ruas. O mesmo vale para mensagens em secretárias eletrônicas e caixas postais. Nunca se sabe quem está a seu lado e que poderá ouvir sua conversa.

## 4. Acesso à Internet e a e-mails

**Você já freqüentou, ou até mesmo criou, uma comunidade virtual com o nome da ESHO? Será que algum assunto discutido era sigiloso e não deveria ter sido divulgado amplamente? Será que o assunto é ilegal?**

**Comunidades virtuais** podem ser muito úteis para discutir assuntos profissionais, mas é muito importante que você saiba que esses ambientes não são privativos, podendo causar diversos danos à empresa. Um concorrente, por exemplo, pode facilmente ter acesso a informações estratégicas apenas acompanhando conversas de colaboradores da ESHO em comunidades. Um simples comentário sobre novos projetos ou sobre como foi seu dia pode ser um prato cheio para quem quer ter acesso a detalhes e segredos corporativos.

Cuidado com as comunidades de um modo geral, em especial porque você pode ser responsabilizado pelo conteúdo dela, pelo que você escreveu e até pelo que outras pessoas escreveram, situação na qual você se transforma em **co-autor**. Isso ocorre muito em comunidades que debatem temas ilícitos, ou que utilizem fotos não autorizadas de terceiros, ou cujo texto venha a ser considerado ofensivo a alguém, participante da comunidade ou terceiro.

Além de comunidades virtuais, evite publicar assuntos profissionais em blogs, fotologs, sites e demais ambientes eletrônicos.

### De olho na Lei:

#### CLT

**Artigo 482** - Constituem justa causa para rescisão do contrato de trabalho pelo empregador:(...)

g) violação de segredo da empresa;

#### Crime de Racismo - Lei nº 7716/89

**Artigo 20** - Pena: reclusão de um a três anos e multa.

#### Código Penal

**Artigo 138** - caluniar alguém imputando-lhe falsamente fato definido como crime.

Pena: 6 meses a 2 anos, e multa.

*Parágrafo 1º* – Na mesma pena incorre quem, sabendo falsa a imputação, a propaga ou divulga (dá forward, faz link...).

**Ao receber um e-mail, você já ficou em dúvida sobre sua real procedência ou sobre a identidade do remetente?**

É muito provável que sim. O remetente confuso é um dos principais indícios de que o **e-mail é indesejado** e que pode, até mesmo, conter alguma praga virtual anexa, como um vírus ou um arquivo malicioso.

## Normas de Segurança

Versão 1

Mas também esse mesmo remetente pode ser de uma mensagem muito importante, porém mal identificada por seu autor. Para que isso não aconteça com os seus e-mails enviados, identifique-se sempre. Coloque de maneira clara seu nome, cargo, departamento, e-mail, telefone para contato e o nome da ESHO.

Caso você perceba que a mensagem realmente foi enviada por alguém que você não conhece e que seu conteúdo não foi solicitado, envie-a para o Departamento de Tecnologia – [suporte@ESHO.com.br](mailto:suporte@ESHO.com.br) e apague-a. Também desconfie quando receber e-mails com remetente conhecido, mas que não costuma enviar determinado tipo de e-mail, fax, SMS, etc. **Na dúvida, não abra a mensagem, muito menos execute seus anexos**, e contate nosso help-desk.

### **Ao receber um boato eletrônico, você já encaminhou a mensagem sem verificar a veracidade da informação, mesmo que fosse uma mensagem falando mal de alguém?**

Uma mensagem alarmante pode ser bem convincente. Ela ainda ganha mais credibilidade quando tem uma observação do tipo “É verdade! Eu mesmo liguei lá e confirmei a informação!” mas muitas vezes esses e-mails não passam de **boatos**, de **informação falsa**, que têm por finalidade causar desinformação a um grande número de pessoas ou, até mesmo, disseminar vírus ou outras pragas virtuais.

Ao receber uma mensagem que agride terceiros com imagens, vídeos ou textos, nunca passe para a frente, principalmente por seu e-mail [@esho.com.br](mailto:@esho.com.br), [@saolucascopacabana.com.br](mailto:@saolucascopacabana.com.br), [@hcniteroi.com.br](mailto:@hcniteroi.com.br), [@cardiotrauma.com.br](mailto:@cardiotrauma.com.br), [@suprim-esho.com.br](mailto:@suprim-esho.com.br), [@servbaby.com.br](mailto:@servbaby.com.br), [@hcml.com.br](mailto:@hcml.com.br). Você pode não ser responsabilizado por ter recebido a mensagem, mas passa a ser responsável quando a envia, quando passa para a frente, pois está assinando embaixo do conteúdo.

O mesmo vale para aquelas mensagens alarmantes como o câncer causado pelo desodorante, o hambúrguer feito de minhoca ou a criança com doença grave que precisa de doações. Se você realmente considera a informação importante, verifique sua **veracidade** antes de retransmiti-la. E evite fazê-lo pelo e-mail da empresa, uma vez que este assunto não está relacionado ao trabalho.

Use o correio eletrônico com cautela, principalmente em seu ambiente de trabalho, para fins éticos e com redação objetiva. Na dúvida, peça autorização ao destinatário antes de enviar anúncios, mensagens, arquivos, imagens e piadas. Determinado assunto pode ser de seu interesse, mas nem sempre terá alguma utilidade para quem você está enviando.

### **Falando nisso...**

Certamente você já recebeu algum e-mail sobre alguém (geralmente uma criança) que possui uma doença muito grave e que determinada empresa doará certa quantia se você retransmitir a mensagem para sua lista de contatos. Esse tipo de “caridade virtual” não existe. Não é possível rastrear mensagens para determinar quantas pessoas a receberam. Apesar de parecer um belo gesto, o repasse desse tipo de informação expõe empresas e pessoas e também entope as contas de e-mails com recados inúteis.

### **Você já recebeu um e-mail de alguma instituição, como um banco ou o Serasa, pedindo para que você efetue algum tipo de cadastro, fornecendo dados secretos como senhas bancárias? E você respondeu à solicitação da mensagem?**

Este pode ser o golpe do **phishing scam**, que consiste em se aproveitar da inocência ou falta de atenção do usuário para obter informações sigilosas para realizar diversos golpes.

# ESHO - Empresa de Serv. Hosp. Ltda

## Normas de Segurança

Versão 1

Tome muito cuidado por onde anda pelo mundo virtual. No mundo palpável é mais fácil identificar locais perigosos e que não devem ser freqüentados, como ruas escuras e sem policiamento; na Internet, nem sempre é possível, julgarmos se um site é o que ele aparenta ser. Fique atento às circunstâncias que levaram você a determinado endereço: muitos **fraudadores abordam suas vítimas com alguma vantagem financeira**, concedida mediante um cadastro com informações como **senha bancária**. Desconfie! Não forneça dados sigilosos e nem baixe arquivos de sites com informações desconstruídas ou promessas mirabolantes. Na dúvida, entre em contato com a instituição e confira se realmente está sendo enviada a campanha recebida ou se determinados dados estão sendo solicitados.

### Falando nisso...

#### Você sabe reconhecer um site seguro?

Existem vários elementos que garantem a segurança de uma página. Veja os mais freqüentes:

- Exibição de um pequeno cadeado (🔒) na parte inferior de seu navegador;
- Endereço do site começando por **https://** ao invés de apenas **http://**;
- Selo de site seguro (clique sobre o selo para conferir sua autenticidade).

### Você sabia?

#### Que todos ambientes eletrônicos da ESHO são monitorados?

A empresa é responsável pelo mau uso das ferramentas de trabalho pelos colaboradores e, portanto, já há decisão judicial autorizando o monitoramento corporativo. Isso quer dizer que tanto sua navegação como seu e-mail profissional estão sujeitos a restrições de uso, bem como estão tendo acompanhamento de segurança e guarda, já que são a prova digital da empresa. Por isso, é recomendável que você utilize os recursos da ESHO apenas para fins profissionais, prezando sempre pela ética e pelo bom senso. Consulte a Política de Segurança da Informação da ESHO para obter mais detalhes sobre condutas e restrições da empresa. E se for assunto particular, use e-mail pessoal e um computador que não esteja ligado na rede.

### Falando Nisso...

A ESHO possui controles anti-vírus para toda a rede, bem como a proteção de firewall. Para seu uso pessoal em casa ou com a utilização de notebooks há softwares sem custo (free) disponíveis para download na Internet e que podem ajudar a proteger suas informações, como:

Firewall pessoal – Sygate/Zone Alarm;  
Antivírus – AVG;  
Anti-spywares – SpyBot

### De olho na Lei

#### Código Penal

Calúnia

Artigo 138 - Caluniar alguém, imputando-lhe falsamente fato definido como crime:

Pena - detenção, de seis meses a dois anos, e multa.

### Difamação

Artigo 139 - Difamar alguém, imputando-lhe fato ofensivo à sua reputação:

Pena - detenção, de três meses a um ano, e multa.

### Injúria

Artigo 140 - Injuriar alguém, ofendendo-lhe a dignidade ou o decoro:

Pena - detenção, de um a seis meses, ou multa.

**Você já instalou nos computadores da ESHO algum programa cujo uso não estava relacionado a suas atividades profissionais? Isso pode alterar as configurações-padrão da empresa, pois um simples “papel de parede” pode conter códigos maliciosos e impactar não somente a estação de trabalho de quem instalou, mas toda a rede. E no computador da sua casa, você já instalou algum programa, baixou música de MP3, que pode configurar pirataria?**

É recomendável que você utilize apenas programas disponibilizados pela própria ESHO em suas dependências e não instale nada sem autorização prévia de um superior. **Em hipótese alguma duplique softwares sem a autorização da área de informática nem copie ou reproduza documentos ou qualquer tipo de informação sem a autorização do responsável pela sua guarda.**

### **Você já instalou algum software sem ter licença para tanto?**

É muito importante que você respeite todas as regras de proteção de **direitos autorais**. O descumprimento dessas normas pode resultar em penalidades como **multa e prisão**, tanto para quem copia ou instala o software como para a empresa responsável pelos equipamentos utilizados.

Caso você não possa ou não queira pagar por um programa, procure alternativas gratuitas, mas nunca se arrisque contrariando a lei.

### **De olho na lei**

#### **Lei nº 9609/98**

**Artigo 12** - Violar direitos de autor de programa de computador:

Pena - Detenção de seis meses a dois anos ou multa.

#### **Código Penal**

**Artigo 184** - Determina pena de detenção de 3 meses a um ano ou multa para aquele que infringe direito autoral. A pena pode aumentar se o crime for cometido para obter lucro, como “piratear” um CD e depois vendê-lo.

## **5. Glossário**

### **Adware**

Qualquer aplicativo no qual são exibidos banners de propaganda durante a execução do programa. Os autores desses aplicativos incluem códigos que apresentam os anúncios, os quais podem ser vistos em janelas instantâneas (pop-ups) ou através de uma barra que aparece na tela do computador.

### **Assinatura Digital**

Uma assinatura eletrônica impossível de falsificar que autentica o remetente de uma mensagem e garante, ao mesmo tempo, a integridade dessa mensagem.

### **Ataque**

Uma "agressão" eletrônica (normalmente não provocada) cujo objetivo é, de alguma forma, prejudicar os computadores, as redes e os mecanismos de segurança que constituem os alvos.

### **Ataque de Espionagem**

Espionar passivamente o tráfego da rede para coletar dados ou segredos valiosos tais como senhas do usuário.

### **Autenticação**

Um método sistemático de estabelecer a comprovação da identidade entre duas ou mais entidades, normalmente usuários e hosts.

### **Autoridade de Certificação (CA)**

Uma entidade confiável que assina digitalmente os certificados para confirmar a propriedade de chaves públicas.

### **Autorização**

Direito predeterminado de acesso a um objetivo ou serviço, com base em informações de autenticação.

### **Cavalos de Tróia**

Conta a mitologia grega que o "Cavalo de Tróia" foi uma grande estátua, utilizada como instrumento de guerra pelos gregos para obter acesso a cidade de Tróia. A estátua do cavalo foi recheada com soldados que, durante a noite, abriram os portões da cidade possibilitando a entrada dos gregos e a dominação de Tróia. Daí surgiram os termos "Presente de Grego" e "Cavalo de Tróia".

Na informática, um cavalo de tróia (trojan horse) é um programa, normalmente recebido como um "presente" (por exemplo, cartão virtual, álbum de fotos, protetor de tela, jogo, etc), que além de executar funções para as quais foi aparentemente projetado, também executa outras funções normalmente maliciosas e sem o conhecimento do usuário.

### **Certificação digital**

O certificado digital é um documento eletrônico de identificação que permite comprovar a identidade de uma pessoa, empresa ou site, para assegurar as transações online e a troca eletrônica de documentos, mensagens e dados.

Esta tecnologia permite assinar digitalmente qualquer tipo de documento, conferindo-lhe a mesma validade jurídica dos equivalentes em papel assinados de próprio punho.

Além disso, os certificados digitais permitem acessar os serviços virtuais da Secretaria da Receita Federal, o que representa uma grande economia de tempo para o contribuinte, que não precisa comparecer pessoalmente a uma unidade de atendimento da Secretaria da Receita Federal.

Os documentos assinados digitalmente atendem aos principais requisitos de segurança para a realização de negócios eletrônicos, são eles:

Autenticidade: garante a identidade de todas as partes envolvidas.  
Confidencialidade: assegura o sigilo das informações, que são resguardadas de pessoas desautorizadas.

**Integridade:** protege contra a modificação imprópria da mensagem, garantindo o seu conteúdo original.

**Não Repúdio:** impede as partes de negarem a participação no negócio eletrônico.

### **Chave**

Um entre todos os valores possíveis que podem ser aplicados ao texto simples com um algoritmo de criptografia para gerar texto codificado, ou vice-versa.

### **Controle de Acesso**

Técnicas de limitação do acesso a recursos com base em informações de autenticação e regras de acesso.

### **Conversão de Nomes**

Processo de correlação do nome de um host a um endereço IP. O DNS é o principal sistema da Internet para conversão de nomes de host.

### **Cracker**

1º - Pessoa que faz tentativas de quebrar a segurança de um sistema com a finalidade de invadir ou roubar informações;

2º - Um hacker que utiliza os seus conhecimentos para entrar em sistemas informáticos alheios, quebrando sistemas de segurança e eventualmente para causar danos.

### **Criptoanálise**

Ciência de análise e decodificação de comunicações seguras.

### **Criptografia**

Processo de conversão de dados de um formato facilmente compreensível (texto simples) no que parece ser texto aleatório e inútil (texto grifado), até ser posteriormente decodificado.

### **Criptologia**

Estudo das comunicações secretas, inclusive a criptografia e a criptoanálise.

### **Decodificadores de Senhas**

Programas que permitem a um hacker adivinhar a senha de um computador ou de um usuário, usando dicionários ou a técnica conhecida como "força bruta".

### **Discadores**

Programas que usam o modem do computador para conexão com um número pago ou site da Internet, normalmente para cobrança de tarifas. Esses programas são muito pequenos, +/- 100Kb.

### **DNS (Sistema de Nomes de Domínio)**

Um banco de dados distribuído usado para correlacionar endereços IP com nomes de host. O DNS também possui informações para troca de emails.

### **e-CPF**

É identificação eletrônica da pessoa física. Possibilita acessar os serviços virtuais da Secretaria da Receita Federal, além de permitir assinar digitalmente qualquer tipo de documento, conferindo-lhe o mesmo valor legal dos equivalentes em papel.

No Sistema da Receita Federal, o e-CPF permite que a pessoa física acesse dados e serviços relacionados a seu CPF e aos CNPJs dos quais é representante legal.

### **e-CNPJ**

O e-CNPJ é a identificação eletrônica que permite aos representantes legais das empresas acessarem os serviços virtuais da Secretaria da Receita Federal além possibilitar assinar digitalmente qualquer tipo de documento, assegurando as transações comerciais e a troca eletrônica de documentos, mensagens e dados.

### **Engenharia Social**

Uso de mentiras, fraudes, representação e engenhosidade verbal para induzir usuários legítimos a divulgar segredos.

### **Firewall**

Um ou mais filtros e gateways de pacotes que blindam as redes confiáveis "internas" das redes não-confiáveis "externas", tais como a Internet.

### **Força Bruta**

Também conhecido como "decodificação por força bruta", é um método de tentativa e erro usado por aplicativos para decodificar dados criptografados tais como senhas ou chaves do Padrão de Codificação de Dados (DES), através de um esforço exaustivo (utilizando força bruta) em vez de estratégias intelectuais

### **HTTP (Protocolo de Transferência de Hipertexto)**

Protocolo de camada de aplicativos usado para distribuir texto, gráficos, sons, filmes e outros dados através da WWW, com a interface intuitiva de hipertexto de um navegador de Web.

### **IP (Protocolo de Internet)**

Junto com o TCP, um dos protocolos mais fundamentais das redes TCP/IP. O IP é responsável pelo endereçamento e pela distribuição de datagramas pela Internet.

### **Java**

Uma linguagem orientada a objetos, baseada em C++, que permite que os desenvolvedores desenvolvam aplicativos independentes de plataformas.

### **Negação de Serviço (DoS)**

Interrupção de serviços de Internet ou de IP por uma inundação de tráfego falso que entope a rede do provedor. SYN Flood, Ping o' Death e Ping Flooding são alguns exemplos de ataques de Negação de Serviço.

### **Phishing**

Na Internet, o phishing (às vezes chamado de carding ou brand spoofing) é um golpe no qual o autor distribui e-mails com aspecto legítimo, aparentemente vindos de alguns dos mais importantes sites da Web, com a intenção de roubar informações particulares e obter acesso às contas bancárias ou aos serviços por assinatura da vítima.

### **Porta**

Identificadores de 16 bits, usados pelo TCP e pelo UDP, que servem para especificar qual processo ou aplicativo está enviando ou recebendo dados.

### **Protocolo**

Um conjunto de regras usadas para controlar a transmissão e o recebimento de dados.

### **Spam**

O spam é uma mensagem de e-mail não-solicitada. (As mensagens desejadas são, algumas vezes, chamadas de ham) Do ponto de vista do remetente, o spam é uma forma de mala direta, muitas vezes enviada a uma lista obtida através de um spambot, ou a uma lista obtida por empresas especializadas em criar listas de distribuição de e-mail. Para o destinatário, normalmente se trata de lixo eletrônico.

### **Spambot**

Um spambot é um programa projetado para coletar, ou “colher”, endereços de e-mail na Internet para criar listas de envio de e-mail no sentido de enviar mensagens não-solicitadas. Um spambot pode coletar endereços de e-mail em sites, grupos de notícias, publicações em grupos de interesse especial (SIG) e diálogos em salas de bate-papo. Como os endereços de e-mail possuem um formato distintivo, é fácil escrever spambots.

### **Spammer**

Pessoa que distribui mensagens não-solicitadas. (Veja SPAM)

### **Spyware (Programas Espiões)**

Programas espiões são tecnologias que auxiliam na coleta de informações sobre uma pessoa ou empresa sem seu conhecimento. Na Internet (onde também são conhecidos como spybots ou software de rastreamento), os programas espiões são códigos inseridos no computador de uma pessoa para coletar secretamente informações sobre o usuário e enviá-las a anunciantes ou outras partes interessadas. Os programas espiões podem entrar em um computador como um vírus ou devido à instalação de um novo programa.

### **SSL (Secure Sockets Layer)**

Uma camada de segurança intermediária entre as camadas de aplicativos e de transporte. A SSL protege discretamente os protocolos da camada de aplicativos (tais como o HTTP, para o qual ela foi concebida inicialmente) e de dados, com pouco esforço por parte do desenvolvedor de aplicativos.

### **TCP (Protocolo de Controle de Transmissão)**

Protocolo de transporte voltado para a conexão, que permite uma transmissão bidirecional completa (full duplex) de dados entre duas entidades, freqüentemente entre um aplicativo cliente e um servidor.

### **Worms**

Worm é um programa capaz de se propagar automaticamente através de redes, enviando cópias de si mesmo de computador para computador.

Diferente do vírus, o worm não embute cópias de si mesmo em outros programas ou arquivos e não necessita ser explicitamente executado para se propagar. Sua propagação se dá através da exploração de vulnerabilidades existentes ou falhas na configuração de softwares instalados em computadores.

### **WWW (World Wide Web, ou “Rede Mundial”)**

Uma visão coesa e intuitiva da Internet através de muitos protocolos, especialmente o HTTP.