casa do concurseiro
sinta-se em casa para estudar conosco

Informática

Segurança da Informação

Professor Márcio Hunecke

SEGURANÇA DA INFORMAÇÃO – CONCEITOS GERAIS

Triade CIDA

A Segurança da Informação se refere à proteção existente sobre as informações de uma determinada empresa ou pessoa, isto é, aplica-se tanto às informações corporativas quanto às informações pessoais. Entende-se por informação todo e qualquer conteúdo ou dado que tenha valor para alguma organização ou pessoa. Ela pode estar guardada para uso restrito ou exposta ao público para consulta ou aquisição.

Podem ser estabelecidas métricas (com o uso ou não de ferramentas) para a definição do nível de segurança existente e, com isto, serem estabelecidas as bases para análise da melhoria ou piora da situação de segurança existente. A segurança de uma determinada informação pode ser afetada por fatores comportamentais e de uso de quem se utiliza dela, pelo ambiente ou infraestrutura que a cerca ou por pessoas mal-intencionadas que têm o objetivo de furtar, destruir ou modificar tal informação.

A tríade CIA (*Confidentiality, Integrity and Availability*) – Confidencialidade, Integridade e Disponibilidade – representa os principais atributos que, atualmente, orientam a análise, o planejamento e a implementação da segurança para um determinado grupo de informações que se deseja proteger. Outros atributos importantes são a irretratabilidade e a autenticidade. Com a evolução do comércio eletrônico e da sociedade da informação, a privacidade é também uma grande preocupação.

Portanto, os atributos básicos, segundo os padrões internacionais (ISO/IEC 17799:2005), são os seguintes:

Confidencialidade – propriedade que limita o acesso a informação tão somente às entidades legítimas, ou seja, àquelas autorizadas pelo proprietário da informação. A **criptografia** é a principal técnica utilizada para proteger a confidencialidade.

Integridade – propriedade que garante que à informação manipulada mantenha todas as características originais estabelecidas pelo proprietário da informação, incluindo controle de mudanças e garantia do seu ciclo de vida (nascimento, manutenção e destruição). A **assinatura digital** é a principal técnica utilizada para proteger a integridade.

Disponibilidade – propriedade que garante que a informação esteja sempre disponível para o uso legítimo, ou seja, por aqueles usuários autorizados pelo proprietário da informação. O **backup** (becape) é uma das técnicas utilizadas para proteger a disponibilidade.

Autenticidade – propriedade que garante que a informação é proveniente da fonte anunciada e que não foi alvo de mutações ao longo de um processo. A **assinatura digital** é utilizada para proteger a integridade.

Irretratabilidade ou não repúdio – propriedade que garante a impossibilidade de negar a autoria em relação a uma transação anteriormente feita.

Autenticação, Autorização e Auditoria (AAA)

Autenticação é o ato de estabelecer ou confirmar algo (ou alguém) como autêntico, isto é, que reivindica a autoria ou a veracidade de alguma coisa. A autenticação também remete à confirmação da procedência de um objeto ou pessoa, neste caso, frequentemente relacionada com a verificação da sua identidade.

Mecanismos ou Fatores de Autenticação:

1. Autenticação baseada no conhecimento (SABER) – Login e senha

2. Autenticação baseada na propriedade (TER) – Token / Smart card com PIN (senha do cartão)

3. Autenticação baseada na característica (SER) – Digital / Palma da mão / Íris

Cada mecanismo possui suas vantagens e desvantagens, devendo ser os mesmos aplicados de modo a atender à necessidade do negócio visando garantir a autenticidade das entidades envolvidas. O que vai definir qual dos métodos será adotado é o valor da informação a ser protegida para as entidades envolvidas, cujo o risco deverá ser aceito em níveis aceitáveis. Frequentemente é utilizada uma combinação de dois ou mais métodos.

Autorização é o mecanismo responsável por garantir que apenas usuários autorizados consumam os recursos protegidos de um sistema computacional. Os recursos incluem arquivos, programas de computador, dispositivos de hardware e funcionalidades disponibilizadas por aplicações instaladas em um sistema. Podem ser consideradas consumidores de recursos as pessoas que utilizam um sistema através de uma interface, programas e outros dispositivos de um computador.

O processo de autorização decide se uma pessoa, programa ou dispositivo X tem permissão para acessar determinado dado, programa de computador ou serviço Y. A maioria dos sistemas operacionais modernos possuem processos de autorização. Após um usuário ser autenticado, o sistema de autorização verifica se foi concedida permissão para o uso de determinado recurso. As permissões são normalmente definidas por um administrador do sistema na forma de "políticas de aplicação de segurança", como as ACLs (listas de controle de acesso) ou uma "capacidade", com base no "princípio do privilégio mínimo": os consumidores terão permissão apenas para acessar os recursos necessários para realizar a sua tarefa.

Auditoria é uma referência à coleta da informação relacionada à utilização de recursos de rede pelos usuários. Esta informação pode ser utilizada para gerenciamento, planejamento, cobrança, etc. A auditoria em tempo real ocorre quando as informações relativas aos usuários são trafegadas no momento do consumo dos recursos. Na auditoria em batch as informações

são gravadas e enviadas posteriormente. As informações que são tipicamente relacionadas com este processo são a identidade do usuário, a natureza do serviço entregue, o momento em que o serviço se inicia e o momento do seu término.

Contas e senhas

Uma conta de usuário, também chamada de "nome de usuário", "nome de login" e username, corresponde à identificação única de um usuário em um computador ou serviço. Por meio das contas de usuário, é possível que um mesmo computador ou serviço seja compartilhado por diversas pessoas, pois permite, por exemplo, identificar unicamente cada usuário, separar as configurações específicas de cada um e controlar as permissões de acesso.

A sua conta de usuário é de conhecimento geral e é o que permite a sua identificação. Ela é, muitas vezes, derivada do seu próprio nome, mas pode ser qualquer sequência de caracteres que permita que você seja identificado unicamente, como o seu endereço de e-mail. Para garantir que ela seja usada apenas por você, e por mais ninguém, é que existem os mecanismos de autenticação.

Existem três grupos básicos de mecanismos de autenticação, que se utilizam de: aquilo que você é (informações biométricas, como a sua impressão digital, a palma da sua mão, a sua voz e o seu olho), aquilo que apenas você possui (como seu cartão de senhas bancárias e um token gerador de senhas) e, finalmente, aquilo que apenas você sabe (como perguntas de segurança e suas senhas).

Uma senha, ou password, serve para autenticar uma conta, ou seja, é usada no processo de verificação da sua identidade, assegurando que você é realmente quem diz ser e que possui o direito de acessar o recurso em questão. É um dos principais mecanismos de autenticação usados na Internet devido, principalmente, à simplicidade que possui.

Se uma outra pessoa souber a sua conta de usuário e tiver acesso à sua senha ela poderá usá-las para se passar por você na Internet e realizar ações em seu nome, como:

- Acessar a sua conta de correio eletrônico e ler seus e-mails, enviar mensagens de spam e/ou contendo phishing e códigos maliciosos, furtar sua lista de contatos e pedir o reenvio de senhas de outras contas para este endereço de e-mail (e assim conseguir acesso a elas);
- Acessar o seu computador e obter informações sensíveis nele armazenadas, como senhas e números de cartões de crédito;
- Utilizar o seu computador para esconder a real identidade desta pessoa (o invasor) e, então, desferir ataques contra computadores de terceiros;
- Acessar sites e alterar as configurações feitas por você, de forma a tornar públicas informações que deveriam ser privadas;
- Acessar a sua rede social e usar a confiança que as pessoas da sua rede de relacionamento depositam em você para obter informações sensíveis ou para o envio de boatos, mensagens de spam e/ou códigos maliciosos.

Algumas das formas como a sua senha pode ser descoberta são:

- Ao ser usada em computadores infectados. Muitos códigos maliciosos, ao infectar um computador, armazenam as teclas digitadas (inclusive senhas), espionam o teclado pela webcam (caso você possua uma e ela esteja apontada para o teclado) e gravam a posição da tela onde o mouse foi clicado;
- Ao ser usada em sites falsos. Ao digitar a sua senha em um site falso, achando que está no site verdadeiro, um atacante pode armazená-la e, posteriormente, usá-la para acessar o site verdadeiro e realizar operações em seu nome;
- Por meio de tentativas de adivinhação;
- Ao ser capturada enquanto trafega na rede, sem estar criptografada;
- Por meio do acesso ao arquivo onde a senha foi armazenada, caso ela não tenha sido gravada de forma criptografada;
- Com o uso de técnicas de engenharia social, como forma a persuadi-lo a entregá-la voluntariamente;
- Pela observação da movimentação dos seus dedos no teclado ou dos cliques do mouse em teclados virtuais.

Cuidados a serem tomados ao usar suas contas e senhas:

- Certifique-se de não estar sendo observado ao digitar as suas senhas;
- Não forneça as suas senhas para outra pessoa, em hipótese alguma;
- Certifique-se de fechar a sua sessão ao acessar sites que requeiram o uso de senhas. Use a opção de sair (logout), pois isso evita que suas informações sejam mantidas no navegador;
- Elabore boas senhas;
- Altere as suas senhas sempre que julgar necessário;
- Não use a mesma senha para todos os serviços que acessa;
- Ao usar perguntas de segurança para facilitar a recuperação de senhas, evite escolher questões cujas respostas possam ser facilmente adivinhadas;
- Certifique-se de utilizar serviços criptografados quando o acesso a um site envolver o fornecimento de senha;
- Procure manter sua privacidade, reduzindo a quantidade de informações que possam ser coletadas sobre você, pois elas podem ser usadas para adivinhar a sua senha, caso você não tenha sido cuidadoso ao elaborá-la;
- Mantenha a segurança do seu computador;
- Seja cuidadoso ao usar a sua senha em computadores potencialmente infectados ou comprometidos. Procure, sempre que possível, utilizar opções de navegação anônima.

- Uma senha boa, bem elaborada, é aquela que é difícil de ser descoberta (forte) e fácil de ser lembrada. Não convém que você crie uma senha forte se, quando for usá-la, não conseguir recordá-la. Também não convém que você crie uma senha fácil de ser lembrada se ela puder ser facilmente descoberta por um atacante.

Alguns elementos que você **não deve** usar na elaboração de suas senhas são:

Qualquer tipo de dado pessoal: evite nomes, sobrenomes, contas de usuário, números de documentos, placas de carros, números de telefones e datas (estes dados podem ser facilmente obtidos e usados por pessoas que queiram tentar se autenticar como você).

Sequências de teclado: evite senhas associadas à proximidade entre os caracteres no teclado, como "1qaz2wsx" e "QwerTAsdfG", pois são bastante conhecidas e podem ser facilmente observadas ao serem digitadas.

Palavras que façam parte de listas: evite palavras presentes em listas publicamente conhecidas, como nomes de músicas, times de futebol, personagens de filmes, dicionários de diferentes idiomas, etc. Existem programas que tentam descobrir senhas combinando e testando estas palavras e que, portanto, não devem ser usadas.

Alguns elementos que você **deve** usar na elaboração de suas senhas são:

Números aleatórios: quanto mais ao acaso forem os números usados melhor, principalmente em sistemas que aceitem **exclusivamente** caracteres numéricos.

Grande quantidade de caracteres: quanto mais longa for a senha, mais difícil será descobri-la. Apesar de senhas longas parecerem, a princípio, difíceis de serem digitadas, com o uso frequente elas acabam sendo digitadas facilmente.

Diferentes tipos de caracteres: quanto mais "bagunçada" for a senha mais difícil será descobri-la. Procure misturar caracteres, como números, sinais de pontuação e letras maiúsculas e minúsculas. O uso de sinais de pontuação pode dificultar bastante que a senha seja descoberta, sem necessariamente torná-la difícil de ser lembrada.

Algumas dicas práticas que você pode usar na elaboração de boas senhas são:

Selecione caracteres de uma frase: baseie-se em uma frase e selecione a primeira, a segunda ou a última letra de cada palavra. Exemplo: com a frase "O Cravo brigou com a Rosa debaixo de uma sacada" você pode gerar a senha "?OCbcaRddus" (o sinal de interrogação foi colocado no início para acrescentar um símbolo à senha).

Utilize uma frase longa: escolha uma frase longa, que faça sentido para você, que seja fácil de ser memorizada e que, se possível, tenha diferentes tipos de caracteres. Evite citações comuns (como ditados populares) e frases que possam ser diretamente ligadas a você (como o refrão de sua música preferida). Exemplo: se quando criança você sonhava em ser astronauta, pode usar como senha "1 dia ainda verei os anéis de Saturno!!!".

Faça substituições de caracteres: invente um padrão de substituição baseado, por exemplo, na semelhança visual ("w" e "vv") ou de fonética ("ca" e "k") entre os caracteres. Crie o seu próprio padrão pois algumas trocas já são bastante óbvias. Exemplo: duplicando as letras "s" e "r", substituindo "o" por "0" (número zero) e usando a frase "Sol, astro-rei do Sistema Solar" você pode gerar a senha "SS0l, asstrr0-rrei d0 SSisstema SS0larr".

Existem serviços que permitem que você teste a complexidade de uma senha e que, de acordo com critérios, podem classificá-la como sendo, por exemplo, "muito fraca", "fraca", "forte" ou "muito forte". Ao usar estes serviços, é importante ter em mente que, mesmo que uma senha tenha sido classificada como "muito forte", pode ser que ela não seja uma boa senha caso contenha dados pessoais que não são de conhecimento do serviço, mas que podem ser de conhecimento de um atacante. Apenas você é capaz de definir se a senha elaborada é realmente boa!

Ameaças e Riscos

Acesso a conteúdo impróprios ou ofensivos: ao navegar você pode se deparar com páginas que contenham pornografia, que atentem contra a honra ou que incitem o ódio e o racismo.

Contato com pessoas mal-intencionadas: existem pessoas que se aproveitam da falsa sensação de anonimato da Internet para aplicar golpes, tentar se passar por outras pessoas e cometer crimes como, por exemplo, estelionato, pornografia infantil e sequestro.

Furto de identidade: assim como você pode ter contato direto com impostores, também pode ocorrer de alguém tentar se passar por você e executar ações em seu nome, levando outras pessoas a acreditarem que estão se relacionando com você, e colocando em risco a sua imagem ou reputação.

Furto e perda de dados: os dados presentes em seus equipamentos conectados à Internet podem ser furtados e apagados, pela ação de ladrões, atacantes e códigos maliciosos.

Invasão de privacidade: a divulgação de informações pessoais pode comprometer a sua privacidade, de seus amigos e familiares e, mesmo que você restrinja o acesso, não há como controlar que elas não serão repassadas. Além disso, os sites costumam ter políticas próprias de privacidade e podem alterá-las sem aviso prévio, tornando público aquilo que antes era privado.

Divulgação de boatos: as informações na Internet podem se propagar rapidamente e atingir um grande número de pessoas em curto período de tempo. Enquanto isto pode ser desejável em certos casos, também pode ser usado para a divulgação de informações falsas, que podem gerar pânico e prejudicar pessoas e empresas.

Dificuldade de exclusão: aquilo que é divulgado na Internet nem sempre pode ser totalmente excluído ou ter o acesso controlado. Uma opinião dada em um momento de impulso pode ficar acessível por tempo indeterminado e pode, de alguma forma, ser usada contra você e acessada por diferentes pessoas, desde seus familiares até seus chefes.

Dificuldade de detectar e expressar sentimentos: quando você se comunica via Internet não há como observar as expressões faciais ou o tom da voz das outras pessoas, assim como elas

não podem observar você (a não ser que você esteja utilizando webcams e microfones). Isso pode dificultar a percepção do risco, gerar mal-entendidos e interpretações dúbias.

Dificuldade de manter sigilo: no seu dia a dia é possível ter uma conversa confidencial com alguém e tomar cuidados para que ninguém mais tenha acesso ao que está sendo dito. Na Internet, caso não sejam tomados os devidos cuidados, as informações podem trafegar ou ficar armazenadas de forma que outras pessoas tenham acesso ao conteúdo.

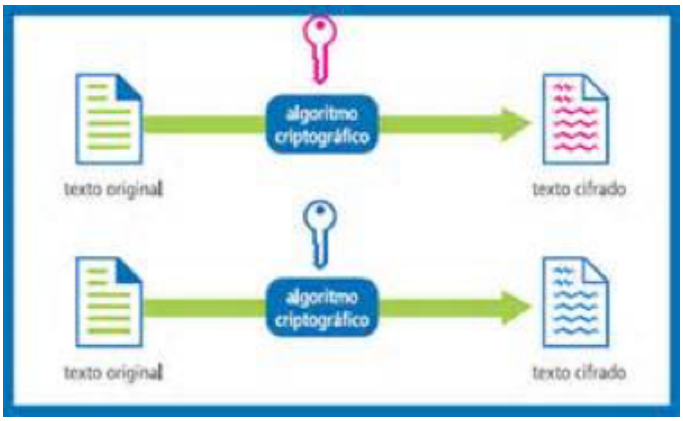
Uso excessivo: o uso desmedido da Internet, assim como de outras tecnologias, pode colocar em risco a sua saúde física, diminuir a sua produtividade e afetar a sua vida social ou profissional.

Plágio e violação de direitos autorais: a cópia, alteração ou distribuição não autorizada de conteúdos e materiais protegidos pode contrariar a lei de direitos autorais e resultar em problemas jurídicos e em perdas financeiras.

Criptografia

A palavra criptografia tem origem grega e significa a arte de escrever em códigos de forma a esconder a informação na forma de um texto incompreensível. A informação codificada é chamada de texto cifrado. O processo de codificação ou ocultação é chamado de cifragem, e o processo inverso, ou seja, obter a informação original a partir do texto cifrado, chama-se decifragem.

A cifragem e a decifragem são realizadas por programas de computador chamados de cifradores e decifradores. Um programa cifrador ou decifrador, além de receber a informação a ser cifrada ou decifrada, recebe um número-chave que é utilizado para definir como o programa irá se comportar. Os cifradores e decifradores se comportam de maneira diferente para cada valor da chave. Sem o conhecimento da chave correta não é possível decifrar um dado texto cifrado. Assim, para manter uma informação secreta, basta cifrar a informação e manter em sigilo a chave.



Atualmente existem dois tipos de criptografia: a simétrica e a de chave pública. A criptografia simétrica realiza a cifragem e a decifragem de uma informação por meio de algoritmos que utilizam a mesma chave, garantindo sigilo na transmissão e armazenamento de dados. Como a mesma chave deve ser utilizada na cifragem e na decifragem, a chave deve ser compartilhada entre quem cifra e quem decifra os dados. O processo de compartilhar uma chave é conhecido como troca de chaves. A troca de chaves deve ser feita de forma segura, uma vez que todos que conhecem a chave podem decifrar a informação cifrada ou mesmo reproduzir uma informação cifrada.

Os algoritmos de chave pública operam com duas chaves distintas: chave privada e chave pública. Essas chaves são geradas simultaneamente e são relacionadas entre si, o que possibilita que a operação executada por uma seja revertida pela outra. A chave privada deve ser mantida em sigilo e protegida por quem gerou as chaves. A chave pública é disponibilizada e tornada acessível a qualquer indivíduo que deseje se comunicar com o proprietário da chave privada correspondente.

Assinatura Digital

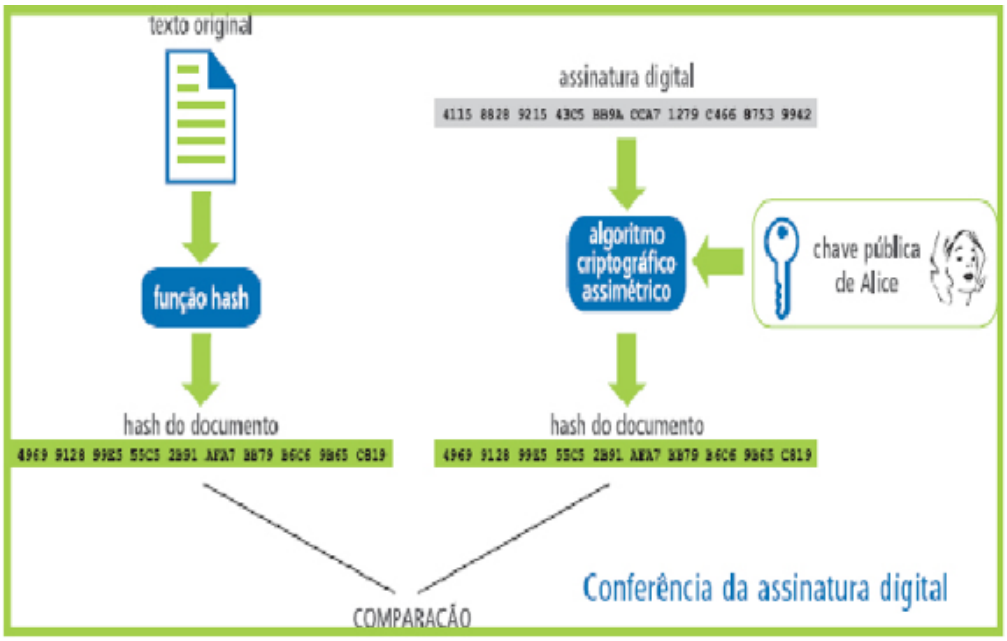
Existem diversos métodos para assinar digitalmente documentos, os quais estão em constante evolução. Porém de maneira resumida uma assinatura típica envolve dois processos criptográficos: o hash (resumo criptográfico) e a encriptação deste hash.

Em um primeiro momento, é gerado um resumo criptográfico da mensagem por meio de algoritmos complexos (exemplos: MD5, SHA-1, SHA-256) que reduzem qualquer mensagem sempre a um resumo de mesmo tamanho. A este resumo criptográfico se dá o nome de hash.

O mesmo método de autenticação dos algoritmos de criptografia de chave pública operando em conjunto com uma função resumo, também conhecido como função de hash, é chamado de assinatura digital.

O resumo criptográfico é o resultado retornado por uma função de hash. Este pode ser comparado a uma impressão digital, pois cada documento possui um valor único de resumo e até mesmo uma pequena alteração no documento, como a inserção de um espaço em branco, resulta em um resumo completamente diferente.

A vantagem da utilização de resumos criptográficos no processo de autenticação é o aumento de desempenho, pois os algoritmos de criptografia assimétrica são muito lentos. A submissão de resumos criptográficos ao processo de cifragem com a chave privada reduz o tempo de operação para gerar uma assinatura por serem os resumos, em geral, muito menores que o documento em si. Assim, consomem um tempo baixo e uniforme, independentemente do tamanho do documento a ser assinado.



Na assinatura digital, o documento não sofre qualquer alteração e o hash cifrado com a chave privada é anexado ao documento.

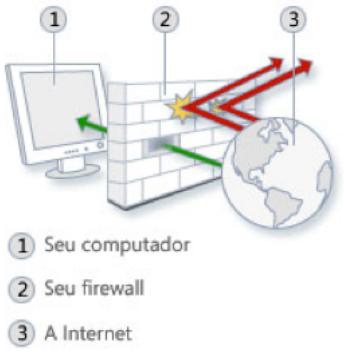
Para comprovar uma assinatura digital, é necessário inicialmente realizar duas operações: calcular o resumo criptográfico do documento e decifrar a assinatura com a chave pública do signatário. Se forem iguais, a assinatura está correta, o que significa que foi gerada pela chave privada corresponde à chave pública utilizada na verificação e que o documento está íntegro. Caso sejam diferentes, a assinatura está incorreta, o que significa que pode ter havido alterações no documento ou na assinatura pública.

A semelhança entre a assinatura digital e a assinatura manuscrita restringe-se ao princípio de atribuição de autoria a um documento. Na manuscrita, as assinaturas seguem um padrão, sendo semelhantes entre si e possuindo características pessoais e biométricas de cada indivíduo. Ela é feita sobre algo tangível, o papel, responsável pela vinculação da informação impressa à assinatura. A veracidade da assinatura manuscrita é feita por uma comparação visual a uma assinatura verdadeira tal como aquela do documento de identidade oficial.

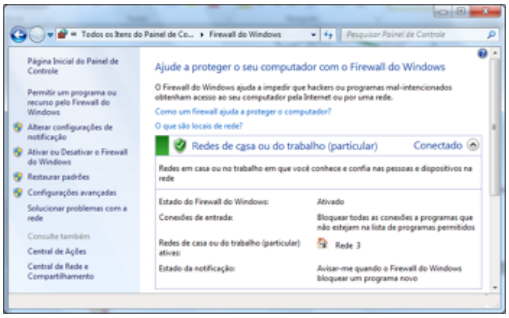
Firewall

Firewall é um software ou hardware que verifica informações vindas da Internet ou de uma rede, rejeitando-as ou permitindo que elas passem e entrem no seu computador, dependendo das configurações definidas. Com isso, o firewall pode ajudar a impedir o acesso de hackers e software mal-intencionado ao seu computador.

O Firewall do Windows vem incorporado ao Windows e é ativado automaticamente.



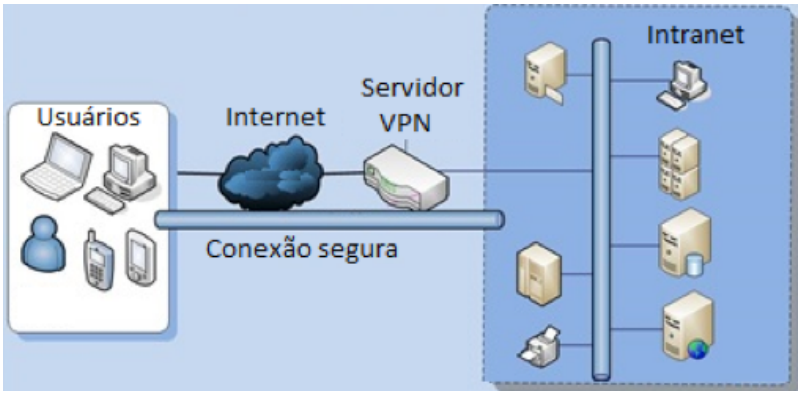
Se você executar um programa como o de mensagens instantâneas (Skype) ou um jogo em rede com vários participantes, que precise receber informações da Internet ou de uma rede, o firewall perguntará se você deseja bloquear ou desbloquear (permitir) a conexão. Se você optar por desbloquear a conexão, o Firewall do Windows criará uma exceção para que você não se preocupe com o firewall quando esse programa precisar receber informações no futuro.



VPN

Rede Privada Virtual (VPN) é uma rede de comunicações privada normalmente utilizada por uma empresa ou um conjunto de empresas e/ou instituições, construída em cima de uma rede de comunicações pública (como, por exemplo, a Internet). O tráfego de dados é levado pela rede pública utilizando protocolos padrão, normalmente seguros.

Uma VPN é uma conexão estabelecida sobre uma infraestrutura pública ou compartilhada, usando tecnologias de tunelamento e criptografia para manter seguros os dados trafegados. VPNs seguras usam protocolos de criptografia por tunelamento que fornecem confidencialidade, autenticação e integridade necessárias para garantir a privacidade das comunicações requeridas. Quando adequadamente implementados, estes protocolos podem assegurar comunicações seguras através de redes inseguras.



Políticas de Segurança

De acordo com o RFC 2196 (The Site Security Handbook), uma política de segurança consiste num conjunto formal de regras que devem ser seguidas pelos utilizadores dos recursos de uma organização.

As políticas de segurança devem ter implementação realista e definir claramente as áreas de responsabilidade dos utilizadores, do pessoal de gestão de sistemas e redes e da direção. Deve também se adaptar às alterações na organização. As políticas de segurança fornecem um enquadramento para a implementação de mecanismos de segurança, definem procedimentos de segurança adequados, processos de auditoria à segurança e estabelecem uma base para procedimentos legais na sequência de ataques.

O documento que define a política de segurança deve deixar de fora todos os aspectos técnicos de implementação dos mecanismos de segurança, pois essa implementação pode variar ao longo do tempo. Deve ser também um documento de fácil leitura e compreensão, além de resumido.

Algumas normas definem aspectos que devem ser levados em consideração ao elaborar políticas de segurança. Entre essas normas estão a BS 7799 (elaborada pela British Standards Institution) e a NBR ISO/IEC 17799 (a versão brasileira desta primeira). A ISO começou a publicar a série de normas 27000, em substituição à ISO 17799 (e por conseguinte à BS 7799), das quais a primeira, ISO 27001, foi publicada em 2005.

Existem duas filosofias por trás de qualquer política de segurança: a proibitiva (tudo que não é expressamente permitido é proibido) e a permissiva (tudo que não é proibido é permitido).