MINISTÉRIO DA SAÚDE

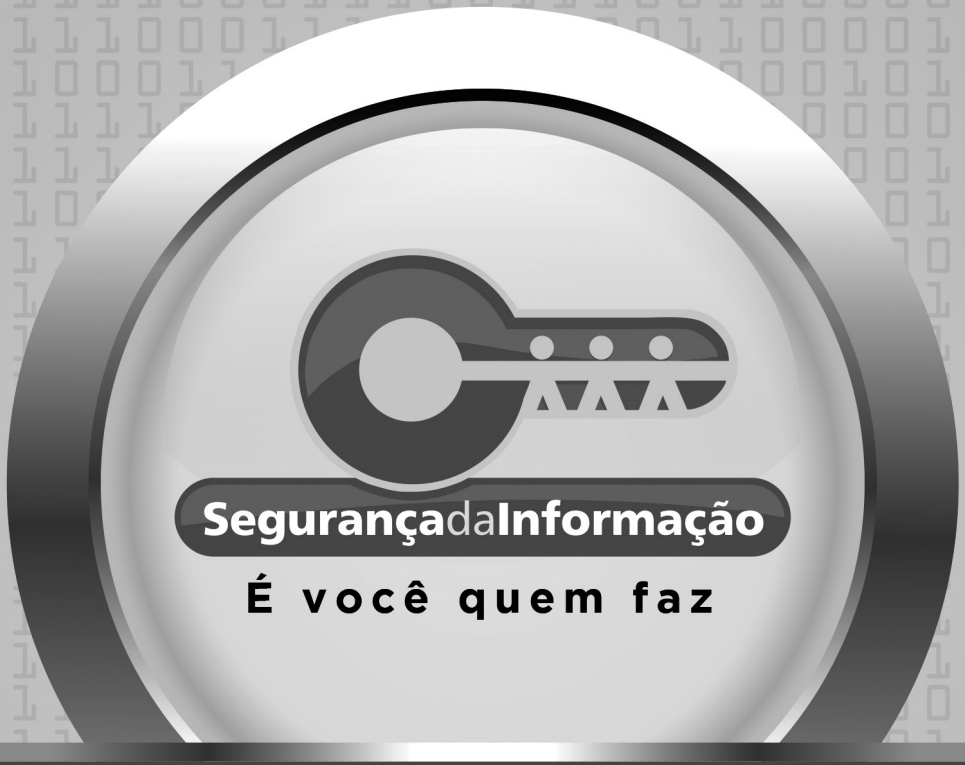
DISTRIBUIÇÃO GRATUITA VENDA PROIBIDA

Cartilha de SIC

Brasília - DF
2016

DATASUS
Departamento de Informática do SUS

MINISTÉRIO DA SAÚDE



Cartilha de SIC

Brasília - DF
2016

DATASUS
Departamento de Informática do SUS

Referência Bibliográfica
Portal Cert.Br – Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil, Cartilha de Segurança para Internet. Disponível em: <http://cartilha.cert.br/>. Acesso em 30 de março de 2016.

Portal Ministério do Planejamento, Cartilha SIC. Disponível em: <http://www.planejamento.gov.br/servicos/central-de-conteudos/publicacoes/cartilha_sic.pdf>. Acesso em 17 de março de 2016.

Elaboração, distribuição e informações:
MINISTÉRIO DA SAÚDE
Secretaria Executiva
DATASUS – Departamento de Informática do SUS
Esplanada dos Ministérios, Bloco G, Anexo, Ala A Sala 102
Tel.: +55 (61) 3315-3808/ 3315-3944
datasus.csic@saude.gov.br

MINISTÉRIO DA SAÚDE
Secretaria Executiva
DATASUS
Central de Segurança de Informação e Comunicação – CSIC

Tel.: +55 (61) 3315.3808/3944
datasus.csic@saude.gov.br

Organização e Elaboração
Central de Segurança da Informação para NSIC - Núcleo de Segurança da Informação e Comunicações

Editora responsável

Equipe editorial
Normalização:
Revisão:
Ilustrações
Capa, projeto gráfico e diagramação:
NUCOM/DATASUS

Ficha Catalográfica

Brasil. Ministério da Saúde. Secretaria Executiva. DATASUS – Departamento de Informática do SUS.
Cartilha de SIC – Segurança da Informação é você quem faz / Ministério da Saúde. Secretaria Executiva. DATASUS – Departamento de Informática do SUS. – Brasília: Ministério da Saúde, 2016.

1. Segurança da Informação. 2. Tecnologia

Sumário

Apresentação

O Ministério da Saúde planejou a campanha "É você quem faz", com o objetivo de conscientizar seus servidores e colaboradores em relação às medidas que devem ser adotadas internamente para garantir a SIC - Segurança da Informação e Comunicações no ambiente de trabalho. O grande resultado que se pretende alcançar é a mudança de hábitos diários que, por vezes, permitem o vazamento de informações relevantes que envolvem o órgão.

Para que a campanha obtenha sucesso, é imprescindível que você participe ativamente, incentivando suas equipes a seguir todas as recomendações e dicas de boas práticas aqui apresentadas, que incluem cuidados com contas e senhas, controle de acesso, integridade de sistema, utilização adequada dos recursos, classificação da informação, identificação e autenticação, ambiente de trabalho e incidentes de segurança.

A Segurança da Informação e Comunicações é um assunto muito importante e que diz respeito a todos. E você, como um dos comunicadores do Ministério da Saúde, tem papel essencial na divulgação desta campanha. Tenha em mente que tudo o que você aprender aqui será de grande utilidade no desempenho de suas funções no MS, mas também em sua casa, onde estão as suas informações.

O principal objetivo é levar ao conhecimento dos Agentes Públicos do Ministério da Saúde e Regionais a importância da Segurança da Informação, boas práticas de SIC, assim como os normativos e a POSIC-MS (Política de Segurança da Informação e Comunicações). Reforçar o comprometimento do MS em todos o níveis hierárquicos em relação a POSIC e Normas publicadas.

Boa leitura!

O que é Segurança da Informação?

Segurança da Informação é o conjunto de procedimentos que você e seus colegas de trabalho devem adotar para proteger as informações pessoais e as relacionadas a qualquer projeto, ação ou trabalho do Ministério da Saúde.

Preparamos este material com dicas simples, mas muito importantes, que você deve adotar em sua rotina de trabalho para deixar seu dia a dia mais eficiente e ainda mais seguro.

É você quem faz

D.I.C.A

Propriedades básicas da Segurança da Informação e Comunicações – SIC

DICA (Disponibilidade, Integridade, Confidencialidade e Autenticidade).

Disponibilidade: propriedade de que a informação esteja acessível e utilizável, sob demanda, por uma pessoa física ou determinado sistema, órgão ou entidade. Proteger essa propriedade significa assegurar ao usuário o acesso à informação, sempre que dela precisar.

Integridade: propriedade de que a informação não seja modificada ou destruída de maneira não autorizada ou acidental. Protegê-la significa assegurar que nada foi acrescentado, retirado ou modificado sem a explícita permissão do seu proprietário.

Confidencialidade: propriedade de que a informação não seja revelada ou disponibilizada a indivíduo, entidade, órgão ou sistema, não autorizado ou não credenciado. Dados privados ou com algum grau de sigilo devem ser apresentados somente ao(s) seu(s) dono(s) ou ao(s) grupo(s) com a devida permissão para tal.

Autenticidade: propriedade de que a informação seja produzida, expedida, modificada ou destruída por indivíduo, entidade, órgão ou sistema, devidamente identificado ou certificado.

Contas e Senhas

CONTAS E SENHAS

A senha de sua conta de usuário é chave da porta que possibilita o acesso aos sistemas e, consequentemente, o acesso às informações. Por isso, é de vital importância que você tome muito cuidado com ela.

TROQUE PERIODICAMENTE SUA SENHA

O uso prolongado de uma mesma senha facilita sua quebra, ou seja, a descoberta da senha por pessoas não autorizadas, possibilitando o acesso a informações sigilosas.

É recomendável que você troque-a a cada seis meses ou sempre que existir qualquer comprometimento da própria senha. Lembre-se: utilize sempre as chamadas senhas fortes – que contenham vários números, letras e caracteres especiais – para dificultar sua quebra.

Fique Ligado

GUARDE-A EM UM LUGAR SEGURO

De nada adianta o uso de senhas fortes se estas forem anotadas em locais visíveis, como lembretes adesivos, bloco de notas, arquivos ou dispositivos móveis.

Alguém pode usar sua senha para acessar o sistema e, se passando por você, cometer uma série de delitos em seu nome.

Evite usar a mesma senha para diferentes serviços, em caso de comprometimento de uma senha, os demais serviços estarão protegidos.

O Ministério da Saúde possui uma Norma de Segurança que dispõe das regras de criação e manutenção de contas de acesso aos recursos de TIC.

São alguns itens da norma:

- A conta de acesso é pessoal e intransferível, sendo de responsabilidade do usuário manter a confidencialidade de sua senha pessoal;

- O uso prolongado de uma mesma senha facilita sua quebra, ou seja, a descoberta da senha por pessoas não autorizadas, possibilitando o acesso a informações sigilosas;

- Os direitos de acesso devem ser solicitados de acordo com as necessidades do setor para a execução das suas atividades;

- O nome de usuário seguirá a nomenclatura padronizada pelas Regras de formação de nomes para a composição de endereço eletrônico (e-mail) no Governo Federal, qual seja um nome seguido de ponto e de um sobrenome;

- A senha de acesso aos recursos de TI deve ser obrigatoriamente alterada a cada 90 (noventa) dias ou sempre que o Usuário da Rede desejar;

- A senha deve ser composta obrigatoriamente por, no mínimo, 8 (oito) caracteres, sendo, pelo menos, 4 (quatro) deles numéricos ou especiais e os demais, alfabéticos;

Saiba mais em: http://datasus.saude.gov.br/seguranca-da-informacao/legislacao-seguranca-da-informacao

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.

Sequências de teclado: evite senhas associadas à proximidade entre os caracteres no teclado, como "1qaz2wsx" e "QwerTAsdfG".

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

Números aleatórios: quanto mais ao acaso forem os números usados melhor.

Grande quantidade de caracteres: quanto mais longa for a senha mais difícil será descobri-la.

Diferentes tipos de caracteres: quanto mais "bagunçada" for a senha mais difícil será descobri-la.

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

Faça substituições de caracteres: crie 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".

Controle de Acesso

Controle de acesso

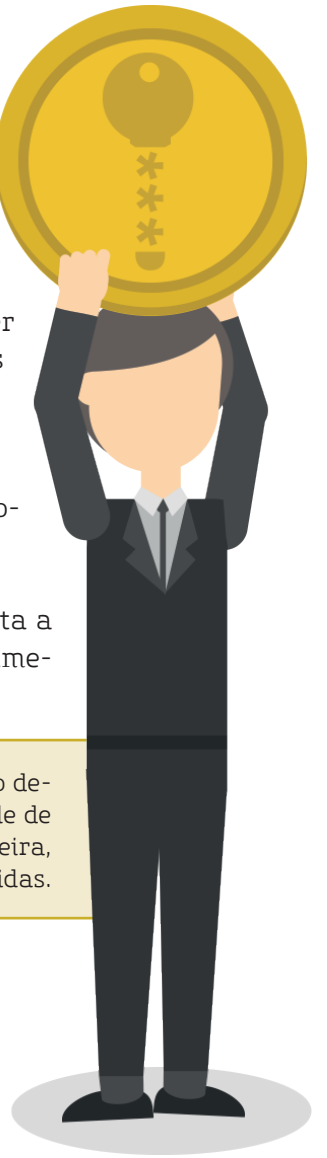
Controle de acesso é o processo de autorização a pessoas acessarem algo. Na Segurança da Informação, o controle de acesso é composto dos processos de autenticação, autorização e auditoria.

O acesso às informações e aos recursos de tecnologia deve ser limitado àqueles que possuem permissão para utilizá-las em suas funções. Qualquer outra forma de acesso físico ou lógico necessita de autorização prévia.

Sempre que houver mudança nas atribuições de qualquer funcionário do MS, esses privilégios devem ser readequados.

Assim, quando um funcionário é desligado do MS, deve ser feita a comunicação do desligamento e sua conta deve ser cancelada imediatamente.

Sua conta é pessoal e intransferível, e seus privilégios de acesso são definidos pelo gestor da informação. Lembre-se: todos os acessos à rede de comunicação são registrados e sujeitos a rastreabilidade. Dessa maneira, fica mais fácil identificar os usuários que realizam operações indevidas.



Controle de acesso físico

O controle de acesso físico é o controle do acesso físico a uma determinada área, como, por exemplo, um prédio, uma sala, uma empresa, uma casa, etc., sendo que somente pessoas autorizadas são permitidas o acesso.

Exemplos:

guarda, segurança ou mesmo um recepcionista;

chaves e fechaduras;

cartões de acesso.

Controle de acesso lógico

O controle de acesso lógico permite que os sistemas verifiquem a autenticidade e a identidade dos usuários para acessarem sistemas de tecnologia da informação.

Exemplos:

"login" e Senha

biometria (íris, digital)

tokens

A Norma de Segurança para Controle de Acesso Remoto do Ministério da Saúde tem como objetivo definir critérios de segurança no âmbito da Rede Corporativa do MS.

Descreve regras gerais como acesso à rede Corporativa assim como o acesso remoto.

Saiba mais em: http://datasus.saude.gov.br/seguranca-da-informacao/legislacao-seguranca-da-informacao

Utilização adequada dos recursos

Utilização adequada dos recursos

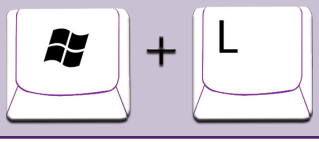
Sempre que você usa seu e-mail corporativo, mesmo que para assuntos particulares, é a imagem do MS que está sendo exposta. Um usuário que utilize o e-mail corporativo para envio de correntes, spams, comentários difamatórios, vírus ou propagandas pode acarretar sanções legais ao MS.

E, consequentemente, estas sanções chegarão até você.

O envio desnecessário de mensagens pode deixar o serviço de e-mail congestionado, causando a sobrecarga da rede e a lentidão de todo o sistema.

Por isso, use seu e-mail corporativo apenas para assuntos relacionados a sua função. Você é responsável não apenas pela sua conta de usuário, mas também pelos e-mails que envia e que recebe dentro do MS.

Fique Ligado



Tome cuidado com informações sigilosas em exibição em sua tela. Ao se ausentar, ative sempre o descanso de tela com bloqueio de senha para evitar que pessoas tenham acesso a esse tipo de dado, pressionando as teclas **WINDOWS** + **L.**

O Ministério da Saúde permite o uso da internet para interesses particulares dos Usuários da Rede, desde que este uso não exceda os limites da ética, bom senso e razoabilidade.

No ambiente do MS fica vedado:

I. Acessar sites com códigos maliciosos e vírus de computador;

II. Acessar sites com materiais pornográficos, atentatórios à moral e aos bons costumes ou ofensivos;

III. Acessar sites ou arquivos que contenham conteúdo criminoso ou ilegal, ou que façam sua apologia, incluindo os de pirataria ou que divulguem número de série para registro de softwares;

IV. Acessar sites ou arquivos com conteúdo de incitação à violência, que não respeitem os direitos autorais ou com objetivos comerciais particulares;

V. Realizar download de arquivos que não estejam relacionados às necessidades de trabalho do Ministério da Saúde, em especial arquivos que contenham materiais ilegais ou que não respeitem os direitos autorais;

VI. Realizar atividades relacionadas a jogos eletrônicos pela internet;

VII. Escutar música ou assistir programas de TV, exceto nos casos em que tais ações sejam condizentes com atividades de trabalho do Ministério da Saúde; e

VIII. Transferir e armazenar informações do MS em sites com os quais não haja um contrato ou acordo de responsabilidade estabelecido com o MS.

Saiba mais em: http://datasus.saude.gov.br/seguranca-da-informacao/legislacao-seguranca-da-informacao

Fique Ligado

Não seja curioso!!! Se você vê um link em redes sociais ou e-mail, com temas de acontecimentos recentes e chamativos, não clique pois pode se tratar de algum tipo de fraude.

Identificação e autenticação

Identificação e autenticação

A identificação permite a entrada de um nome, smartcard, ou algo que indica aquele usuário.

Já a autenticação do usuário pode ser entendida como o processo no qual esse prova ser quem ele diz que é, digitando uma senha, inserindo um token ou realizando a leitura biométrica em algum dispositivo.

Por vezes, determinados usuários, por questão de comodidade, emprestam sua conta e senha de acesso a outros usuários.

O compartilhamento de conta e outros mecanismos de autenticação comprometem a rastreabilidade das ações realizadas no sistema e podem fazer que você responda por crimes cometidos por outras pessoas.

Saiba mais em: http://datasus.saude.gov.br/seguranca-da-informacao/legislacao-seguranca-da-informacao

1. Você costuma emprestar ou compartilhar crachás ou outros recursos de autenticação, tais como "Security Tokens", certificados digitais, etc?

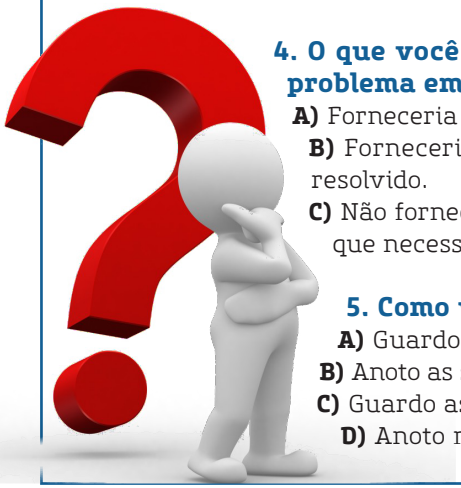
A) Não utilizo recursos de autenticação
B) Sim
C) Apenas quando estritamente necessário
D) Não

2. Você costuma emprestar ou compartilhar contas de acesso com outros usuários?

A) Sim
B) Apenas quando estritamente necessário
C) Não

3. Você costuma trocar suas senhas com frequência?

A) Sim, constantemente
B) Sim, ocasionalmente
C) Sim, raramente
D) Não troco minhas senhas



4. O que você faria se sua senha fosse pedida para resolver um problema em seu computador?

A) Forneceria minha senha para que o problema fosse resolvido.
B) Forneceria minha senha, mas trocaria depois que o problema fosse resolvido.
C) Não forneceria minha senha, mas estaria disposto a digitá-la sempre que necessário.

5. Como você costuma guardar suas senhas?

A) Guardo apenas mentalmente.
B) Anoto as senhas em um papel, bloco ou livro que sempre esteja comigo.
C) Guardo as senhas em um arquivo em meu computador.
D) Anoto minhas senhas em um local visível para não esquecer.

Resposta: 1: D, 2: C, 3: A, 4: C e 5: A

Ambiente de trabalho

Ambiente de trabalho

O hábito de comer e beber junto aos equipamentos de TI coloca em risco o bom funcionamento destes, podendo causar desde sujeira e mau cheiro até danos mais graves, como deterioração das mídias magnéticas, sobrecargas e curtos-circuitos.

No caso de equipamentos de uso compartilhado, como servidores de rede, a interrupção dos serviços pode gerar grandes problemas.

Por isso, evite fazer suas refeições próximo a estes equipamentos pois acidentes podem ocorrer. Procure as áreas destinadas a esse fim ou locais sem a instalação de equipamentos.

No ambiente de trabalho também devemos adotar certas atitudes para garantir a segurança da informação. Ao deixar sua estação de trabalho, guarde todo documento que possa conter informação restrita. Ao se ausentar lembre-se de desligar ou bloquear o computador, e não deixe a sala aberta, pois facilita o acesso de pessoas alheias.

Fique Ligado

Na hora do lanche, procure um lugar adequado, comida e bebida são verdadeiros inimigos de equipamentos eletrônicos de trabalho.

Adotar um comportamento de “mesa limpa” e de “tela limpa” e de “telas limpas” ajuda a reduzir os riscos de perda e danos de informações.

São alguns controles que devem ser considerados:

- Documentos impressos e mídias eletrônicas devem ser armazenados em armários trancados;
- Estações de trabalho não devem ser deixados “logados” quando não houver um operador;
- Ao imprimir um documento, esses devem ser retirados da impressora imediatamente;
- Mantenha um comportamento de “mesa limpa” retirando papéis, anotações e lembretes da sua mesa de trabalho;
- Não deixe papéis, livros ou qualquer informação na sua mesa;
- Utilize um protetor de tela que solicite uma senha para acesso;
- As informações da sua organização são de sua responsabilidade! (mesmo em sua casa!).

Saiba mais em: http://datasus.saude.gov.br/seguranca-da-informacao/legislacao-seguranca-da-informacao

Incidentes de segurança

Incidentes de segurança

Ameaças à Segurança da Informação são hoje mais reais do que nunca.

Ataques automáticos, sequestro de ativos de TI, máquinas zumbis e roubo de informações confidenciais comprometem não apenas a integridade de sua organização como também a utilização de seus serviços.

Dessa maneira, torna-se essencial que as áreas da organização, principalmente as mais relevantes, que estão mais sujeitas a este tipo de ameaça, adotem procedimentos para evitar ou minimizar os danos causados por estes incidentes, permitindo recuperar a capacidade operacional no menor tempo possível.

Os principais pontos relacionados aos incidentes de segurança são:

• A importância do Certificado de Segurança.

• Destacar quais os incidentes de segurança que podem gerar crises organizacionais.

• Divulgar os principais incidentes de segurança que afetam a instituição.

• Conscientizar os gestores da informação sobre a importância de adotar os procedimentos documentados e definir o pessoal apropriado para liderar as ações em situações de crise.

Os usuários do Ministério da Saúde devem estar cientes das regras de informação, evitando incidentes de manipulação das informações, recursos computacionais ou de rede. Comunique qualquer incidente de segurança imediatamente, para que as providências necessárias sejam tomadas a tempo.

Fique Ligado

Os golpes na Internet são cada vez mais recorrentes devido a facilidade que golpistas encontram em obter informações pessoais de suas vítimas.

Pessoas com más intenções procuram enganar e persuadir suas vítimas a fornecerem informações sensíveis ou a realizarem ações, como executar códigos maliciosos e acessar páginas falsas. De posse dos dados das vítimas, os golpistas costumam efetuar transações financeiras, acessar sites, enviar mensagens eletrônicas, abrir empresas fantasmas e criar contas bancárias ilegítimas, entre outras atividades maliciosas.

Existem alguns meios que golpistas utilizam para obtenção de informações de suas vítimas. São algumas:

Engenharia Social – termo utilizado para descrever um método de ataque, onde alguém faz uso da persuasão, muitas vezes abusando da ingenuidade ou confiança do usuário, para obter informações que podem ser utilizadas para ter acesso não autorizado a computadores ou informações.

Phishing – é uma técnica de fraude online, utilizada para roubar senhas de banco e demais informações pessoais, usando-as de maneira fraudulenta. Tentam se passar pela comunicação oficial de uma instituição conhecida, como um banco, uma empresa ou um site popular e procuram atrair a atenção do usuário, seja por curiosidade, por caridade ou pela possibilidade de obter alguma vantagem financeira.

Spam – é o termo usado para se referir aos e-mails não solicitados, que geralmente são enviados para um grande número de pessoas. Muitas vezes esses e-mails contem códigos maliciosos com o objetivo de furto de informações.

Códigos maliciosos

Códigos maliciosos

Códigos maliciosos (malware) são programas desenvolvidos para executar ações danosas e atividades maliciosas em um computador. Os principais motivos que levam um atacante a desenvolver e a propagar códigos maliciosos são a obtenção de vantagens financeiras, a coleta de informações confidenciais, o desejo de autopromoção e o vandalismo.

Alguns procuram permanecer ocultos, infectando arquivos do disco e executando uma série de atividades sem o conhecimento do usuário. Há outros que permanecem inativos durante certos períodos, entrando em atividade apenas em datas específicas.

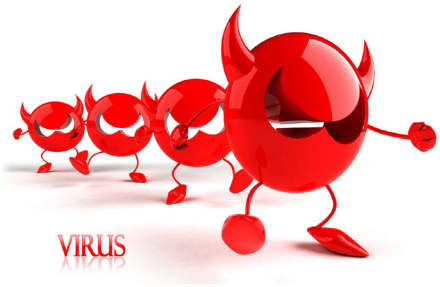
As mídias removíveis tornaram-se o principal meio de propagação, principalmente, pelo uso de pen-drives. Há diferentes tipos de vírus.

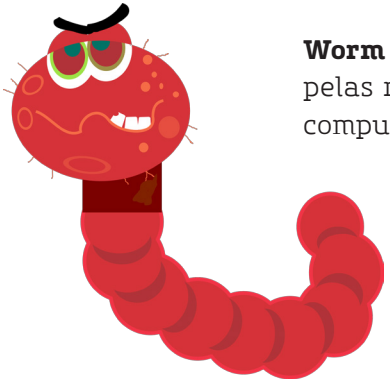
Fique Ligado

Execute o antivírus para executar varreduras em arquivos recebidos via e-mail e em mídias removíveis.

QUEM SOU?

Vírus - é um programa ou parte de um programa de computador, normalmente malicioso, que se propaga inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos.





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

Spyware - é um programa projetado para monitorar as atividades de um sistema e enviar as informações coletadas para terceiros.

Trojan - é um programa que, além de executar as funções para as quais foi aparentemente projetado, também executa outras funções, normalmente maliciosas, e sem o conhecimento do usuário

Bot - é um programa que possibilita o controle de um computador acessado remotamente. Semelhante ao worm, ele é capaz de se propagar automaticamente, explorando vulnerabilidades existentes em programas instalados em computadores. Botnet é uma rede formada por centenas ou milhares de computadores zumbis e que permite potencializar as ações danosas executadas pelos bots.

Prevenção

Prevenção

O que define as chances de um ataque na Internet ser ou não bem sucedido é o conjunto de medidas preventivas tomadas pelos usuários.

Se cada um fizer a sua parte, muitos dos ataques realizados via Internet podem ser evitados ou, ao menos, minimizados.

A parte que cabe a você, como usuário da Internet, é proteger os seus dados, fazer uso dos mecanismos de proteção disponíveis e manter o seu computador atualizado e livre de códigos maliciosos. Ao fazer isto, você estará contribuindo para a segurança geral da Internet, pois:

- Quanto menor a quantidade de computadores vulneráveis e infectados, menor será a potência das botnets e menos eficazes serão os ataques de negação de serviço;

- Quanto mais consciente dos mecanismos de segurança você estiver, menores serão as chances de sucesso dos atacantes;

- Quanto melhores forem as suas senhas, menores serão as chances de sucesso de ataques de força bruta e, consequentemente, de suas contas serem invadidas;

- Quanto mais os usuários usarem criptografia para proteger os dados armazenados nos computadores ou aqueles transmitidos pela Internet, menores serão as chances de tráfego em texto claro ser interceptado por atacantes;

- Quanto menor a quantidade de vulnerabilidades existentes em seu computador, menores serão as chances de ele ser invadido ou infectado.

SIC no MS

O Ministério da Saúde instituiu a sua Política de Segurança da Informação e Comunicações do Ministério da Saúde – POSIC/MS pela Portaria Nº. 3.207, DE 20 DE OUTUBRO DE 2010.

A POSIC/MS aprovada pelo Comitê de Informação e Informática em Saúde (CIINFO) é constituída por objetivos e diretrizes que se aplicam às informações armazenadas e transmitidas. E, portanto, incubem a todos os agentes públicos do Ministério da Saúde, que tenham acesso às informações e recursos de tecnologia da informação e comunicações – TIC, a responsabilidade, o comprometimento e obrigações quanto a sua aplicação no ambiente de trabalho.

A POSIC/MS foi elaborada pelo Subcomitê Gestor de Segurança da Informação e Comunicações constituído por representantes de todas as Secretarias que compõe o MS e pelas entidades vinculadas.

O MS também possui quatro normas de Segurança da Informação e Comunicações publicadas pela Portaria nº 85, DE 31 DE JANEIRO DE 2012.

São elas:

- Criação e Manutenção de Contas de Acesso aos Recursos de TIC;
- Segurança para o Uso do Correio Eletrônico;
- Segurança para Controle de Acesso Remoto; e
- Segurança para Uso de Internet.

Saiba mais em: http://datasus.saude.gov.br/seguranca-da-informacao/legislacao-seguranca-da-informacao

COM QUEM POSSO CONVERSAR EM CASO DE DÚVIDAS, SUSPEITA, DENÚNCIAS OU PROBLEMAS RELACIONADOS À SIC NO MS?

Central de Segurança da Informação e Comunicações - CSIC, por meio dos seguintes canais:

E-mails: datasus.csic@saude.gov.br abuse@saude.gov.br

datasus.cqa@saude.gov.br

Telefones: Suporte Técnico - 2222

CSIC - (61) 3315-3944/3808

Central de Qualidade no atendimento - CQA - (62) 3315-2614/2664

• É importante informar todo e qualquer incidente identificado a Central de Segurança da ação e Comunicações do MS:

datasus.csic@saude.gov.br

• Em casos específicos de suspeita de e-mails maliciosos, encaminhe-os para:

abuse@saude.gov.br

Biblioteca Virtual em
Saúde do Ministério da Saúde
www.saude.gov.br/bvs

DISQUE SAÚDE
136
Ouvidoria Geral do SUS.
www.saude.gov.br

SUS
MINISTÉRIO DA SAÚDE
BRASIL
GOVERNO FEDERAL