Mecanismos e Práticas de Segurança
IDS Saúde versão 5.17.2

Avenida Brasil, 922 SL01, Centro - Pato Branco PR
(046) 3225.8383 | treinamento@ids.inf.br | www.ids.inf.br
IDS Desenvolvimento de Software e Assessoria Ltda.

HISTÓRICO DE REVISÃO

VERSÃO	DATA	AUTOR(ES)	DESCRIÇÃO
1.0	08/04/2015	André Luiz Varnier (Analista)	Criação do documento (Manual)
1.0	17/04/2015	Greice B Uberti (Suporte Técnico)	Elaborado contexto do documento
1.0	20/04/2015	André Luiz Varnier (Analista)	Revisado, finalizado a elaboração dos de Mecanismos de Segurança para a TI e Usuários
2.0	11/11/2020	Greice B Uberti (Treinamentos)	Atualização do documento. Regras baseadas a partir das mudanças nas versões de sistema: 5.16.2, 5.16.4 e 5.16.5
2.1	01/12/2020	Greice B Uberti (Treinamentos)	Alterações no documento conforme regras da versão 5.17.0
2.2	10/03/2021	Greice B Uberti (Treinamentos)	Manual com funcionalidades de acordo com a versão 5.17.2

ÍNDICE

Introdução

Este manual procura reunir um conjunto de mecanismos e boas práticas de segurança em relação à utilização do sistema IDS Saúde. A implantação destas práticas minimiza as chances de ocorrerem problemas de segurança e facilita a utilização/administração do sistema de forma segura. É importante ressaltar que este conjunto representa o mínimo indispensável dentro de um grande universo de boas práticas de segurança. As recomendações apresentadas são mais superiores que na prática e, tanto quanto possível, independentes de plataforma. A maioria dos princípios aqui expostos pode ser considerada como genérica.

Este documento é direcionado à equipe de tecnologia, especialmente aos administradores de redes, sistemas e/ou segurança, que são os responsáveis pelo planejamento, implementação ou operação de redes e sistemas nas unidades. E também podem se beneficiar da sua leitura os usuários do sistema, ao qual são repassados vários mecanismos quanto à segurança da informação.

Visão Geral

Através deste manual serão compreendidos e apontados os principais Mecanismos de Segurança para a Tecnologia da Informação - TI do Cliente e Mecanismos de Segurança para os Usuários.

Destacando-se as situações envolvendo vulnerabilidades, perigos e ameaças à segurança, bem como a segurança na estação de trabalho, a segurança no meio de transporte dos dados pela rede, a segurança do servidor, na rede interna, além de abranger os pontos de controle de segurança.

É de enorme relevância frisar a segurança do banco de dados utilizado e a forma de realização do backup. A fim de preservar as informações que são de suma importância para as tomadas de decisões e controles operacionais e gerenciais.

Mecanismos de segurança para a TI do cliente

Os mecanismos de segurança para ambientes e softwares em plataforma Web quando bem projetados, apresentam aspectos de segurança revistos e bem estruturados. Estas ações evitam que sejam fraudadas e tenham seus dados expostos a indivíduos não autorizados. As aplicações são providas de uma segurança adicional para que o sistema esteja sempre disponível para apoiar os processos operacionais e gerenciais, entretanto segura a intrusos ou hackers.

A escolha das tecnologias para desenvolvimento do sistema IDS Saúde vão de encontro com os critérios de segurança, e da mesma forma como as informações são armazenadas no banco de dados. Para se ter domínio sobre a segurança da informação faz se necessário ter domínio do controle de acesso lógico, que por sua vez tem como principal objetivo a correta definição de uma política de senhas e de acesso aos ambientes e aplicativos.

Por isso, é extremamente importante ter-se a prevenção de desenvolver um sistema possuindo controles específicos, como por exemplo: rotina de backup, gerenciamento de acessos, histórico de exclusões, parâmetros de acesso e autenticação, dentre outros. Além de controles gerais, que irão englobar todos os aspectos físicos dos equipamentos até o uso do sistema pelos operadores (recomendável efetuar treinamento antes de disponibilizar o sistema aos operadores).

1. Vulnerabilidades, Perigos e Ameaças à Segurança

As vulnerabilidades, perigos e ameaças à segurança podem ocorrer nas mais variadas formas, como: desastres envolvendo incêndios, inundações, vendavais ou até mesmo falhas na energia elétrica. Além desses fatores externos, há uma grande preocupação interna em relação a acidentes com equipamentos, espionagem, roubo de dados, acesso indevido a informações sigilosas, uso indevido de informações para beneficiar-se a si ou outros. De forma semelhante, vale lembrar que o uso da internet e o uso da rede interna trazem novas vulnerabilidades na rede, como: hackers, invasões, vírus, dispositivos externos e outras ameaças que podem ocasionar roubo ou danos a informação.

Os sistemas de informação, aplicações, redes de computadores, banco de dados, sistema de comunicação, sistema de energia além de outros são um dos pontos mais procurados quanto à vulnerabilidade e risco. Para obter tal segurança em uma aplicação para Internet ou Intranet, é necessário atentar-se de alguns elementos básicos, que estão mostrados e detalhados a seguir:

- Segurança na estação (cliente);
- Segurança no meio de transporte;
- Segurança nos servidores;
- Segurança na Rede Interna;
- Pontos de controle de segurança;
- Segurança no Banco de Dados utilizado;
- Segurança na comunicação entre o Cliente e Servidor;
- Proteção de parâmetros de autenticação.

1.1 Segurança na estação

Nas estações de trabalho geralmente não ocorrem situações de ataques tanto quanto nas redes ou servidores dos sistemas ou de recuperação de informações. Estas estações comumente também podem conter informações delicadas e sigilosas o que não impedem de serem alvos de invasões.

As estações de trabalho também podem ser invadidas sem o conhecimento do usuário e utilizadas por atacantes como máquinas "escravas" em ataques coordenados. Por estas razões, saber das vulnerabilidades de uma estação de trabalho pode evitar aos profissionais de TI a manutenção.

Senhas ruins representam um dos métodos mais fáceis para um atacante obter acesso a um sistema. Apesar de um administrador conter de um servidor completamente seguro e conservado, isto não significa que usuários remotos estão seguros ao acessá-lo. Por exemplo, se o servidor oferece os serviços Telnet e FTP através de uma rede pública, um atacante pode capturar os nomes de usuário e senhas (somente-texto) ao longo da rede, e então usar as informações da conta para acessar a estação de trabalho do usuário remoto.

1.2 Segurança no meio de transporte

A segurança no meio de Transporte é um método para garantir a privacidade e a integridade das informações enviadas pela Internet. O Transport Layer Security (TLS ou Segurança da Camada de Transporte) assim como o Secure Sockets Layer (SSL ou Protocolo de Camada Segura de Soquetes) é um protocolo de segurança que protege as telecomunicações via internet para serviços como e-mail (SMTP), navegação por páginas (HTTPS) e outros tipos de transferência de dados.

O protocolo SSL favorece a privacidade e a integridade de dados entre duas aplicações que comuniquem pela internet. Isso ocorre por intermédio da autenticação das partes envolvidas e da cifragem dos dados transmitidos entre as partes. Esse protocolo ainda ajuda a prevenir que intermediários entre as duas extremidades das comunicações obtenham acesso indevido ou falsifiquem os dados que estão sendo transmitidos.

O funcionamento ocorre da seguinte forma: o servidor do site que está sendo acessado envia uma chave pública ao browser, usada por este para enviar uma "conexão secreta", criada aleatoriamente. Desta forma, fica estabelecida a troca de dados criptografados entre dois computadores. A criptografia transforma as informações em textos que são impossíveis de serem compreendidos enquanto a informação não chegou a seu local de destino, quando a informação está no seu destino torna compreensivo para seu remetente, por isso é uma ferramenta de alta segurança.

O sistema IDS Saúde utiliza de alguns protocolos de segurança e faz utilização do protocolo HTTPS (Protocolo de Transferência de Hipertexto Seguro) é uma implementação do protocolo HTTP sobre uma camada adicional de segurança que utiliza o protocolo SSL/TLS. Essa camada adicional permite que os dados sejam transmitidos por meio de uma conexão criptografada e que se verifique a autenticidade do servidor e do cliente por meio de certificados digitais. Por exemplo, a existência na barra de endereços de um cadeado (que pode ficar do lado esquerdo ou direito, dependendo do navegador utilizado) demonstra a certificação de página segura (SSL). A existência desse certificado indica o uso do protocolo HTTPS e que a comunicação entre o browser e o servidor se dará de forma segura. Para verificar a identidade do servidor é necessário abrir esse certificado com um duplo clique no cadeado para exibição do certificado.

Para complementar a segurança de todo esse processo de transporte é necessário atentar-se que o firewall tem papel fundamental em deixar passar o conteúdo somente condizente com sua configuração e permissão. A utilização de proxy também auxilia nesses filtros e permite que somente a informação necessária e verdadeira chegue no seu destino correto.

1.3 Segurança nos Servidores

É muito amplo o campo de segurança para servidores e cada organização deve atentar-se em aplicar os recursos e mecanismos que estiverem ao seu alcance, é válido ressaltar que quanto mais segurança é melhor. Devem ser levados em consideração tanto os aspectos físicos quanto lógicos para manter um servidor principal em segurança.

Aos **aspectos físicos** deve-se atentar aos principais tópicos listados abaixo:

- ✓ A estrutura para armazenar um servidor físico não precisa ser complexa, mas requer temperaturas não elevadas e com boa ventilação;
- ✓ É recomendado a ter equipamentos de reserva, caso algum hardware precise ser substituído;
- ✓ Mantenha a sala de servidores longe de áreas que tenham contatos com inflamáveis ou umidade. Da mesma forma mantenha-o longe de locais que possam ter inundações;
- ✓ Utilize nobreak;
- ✓ Deve ser de acesso restrito a entrada na sala de Centro de Processamento de Dados - CPD e manutenção dos equipamentos;
- ✓ Utilize senhas fortes para os controles, que sejam com no mínimo oito caracteres e procure combinar aleatoriamente números, letras em caixa alta e baixa e caracteres especiais;
- ✓ Configure o seu Sistema Operacional para solicitar a senha do root sempre que acessado, para evitar vulnerabilidades;
- ✓ Desabilite boots através de unidades;
- ✓ Cuidado com o lixo eliminado, nunca anote senhas ou configurações realizados em "papel/documentos" que depois serão jogados no lixo de forma íntegra.

Para os **aspectos lógicos** deve-se atentar aos principais tópicos listados abaixo:

- ✓ Configuração do Firewall;
- ✓ Controle de portas de entrada e saída da rede (fechar portas e desativar serviços não utilizados);
- ✓ Criptografia de Discos Rígidos;
- ✓ Proteção a Acesso Remoto;
- ✓ Controle de Backup e Recuperação de dados;
- ✓ Controle de atualização de softwares (antivírus, sistema utilizado para armazenar informações entre outros);
- ✓ Desenvolver Políticas de Segurança para sistemas de arquivos de rede e serviços de informação;
- ✓ Consultar diariamente os arquivos de LOG. Será através deles que será possível obter registros de tudo o que ocorrer em seu servidor além também de poder identificar os possíveis indícios e tentativas de violação quando houver.

1.4 Segurança na Rede Interna

A segurança deve prever a proteção e controle da Rede Interna. Em certos casos profissionais de TI responsáveis pela segurança das redes tem dado maior valor que o fator prejudicial está do lado de fora da organização, e considerando que dentro, todos são confiáveis. Porém, a maior parte dos problemas ocorre em função de ameaças internas.

E uma das soluções proposta para essas situações é abranger o desenvolvimento e acompanhamento de:

- ✓ Políticas de Segurança corporativa com definição das diretrizes, normas, padrões e procedimentos que devem ser seguidos por todos os usuários da organização e se houver terceirizado no processo a regra deve ser da mesma forma aplicada;

- ✓ Treinamento e capacitação dos usuários, a fim de minimizar entrada de dados incorretos e melhor operabilidade dos sistemas;
- ✓ Recursos e ferramentas específicas para a segurança, com logs e registros para auditoria;
- ✓ Monitoração constante de acesso à Internet /Intranet.

1.5 Pontos de controle de segurança

Em quaisquer organizações que contenham sistemas de informações, é fundamental a existência de pontos de controle de segurança, é com eles a importância de levar em consideração os principais fatores que envolvem a segurança:

- **Políticas de Segurança da informação:** Conjunto de princípios que norteia a gestão da segurança das informações. Esta política deve ser divulgada/atualizada a todos os funcionários e partes externas relevantes para a proteção das informações do negócio da organização, além de definir as responsabilidades;
- **Organização da Segurança da Informação**: Geralmente realizada por representantes de diferentes partes da organização, com funções e papéis relevantes na coordenação das atividades operacionais de segurança da informação;
- **Acordos de confidencialidade (Controle de Acessos)**: Pode-se evitar a utilização indevida de informações sensíveis, no que diz respeito à questão de sigilo e condições de uso das informações confiadas aos funcionários, prestadores e partes externas relevantes;
- **Gestão e Controle de Ativos**: Registro de identificação, localização e funcionalidade dos ativos de informação de valor relevante, para que a organização possa avaliar quais são os controles de segurança adequados. É recomendado que o inventário deva incluir uma identificação clara dos seguintes tipos de ativos: Informações, Software, Hardwares e Infraestrutura;
- **Gestão e Controle de Devolução de Ativos**: Definição de um processo para a proteção das informações e preservação do patrimônio da organização no processo de encerramento ou transferência de atividades. Os ativos que devem ser devolvidos incluem, mas não se restringem a: Equipamentos, Documentos corporativos, Softwares entregues à pessoa, Dispositivos de comunicação móvel e Manuais;
- **Segurança em Recursos Humanos**: Sensibilização constante de funcionários e partes externas relevantes, por exemplo, prestadores de serviço, da necessidade de segurança da informação, a partir de treinamentos e esclarecimentos de conscientização sobre segurança da informação, com foco nos dados sensíveis para a organização. Esse processo deve ocorrer desde a contratação, e ser realizado de forma periódica, e assegurar através de formalização o reconhecimento do conteúdo da política de segurança da informação;
- **Segurança Física e do ambiente**: Acesso a áreas de segurança, como escritório, sala ou instalação de processamento e armazenamento de informações sensíveis ao negócio da organização, liberado somente para pessoas autorizadas, com entrada e saída controladas e registradas por meio de mecanismos apropriados;
- **Gestão das Operações e Comunicações**: Conjunto de ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;
- **Legislação aplicada**: São controles destinados a tratar as leis, estatutos, regulamentações, normas e requisitos de segurança que garante uma confiabilidade e o comprometimento da organização junto aos órgãos regulatórios.

1.6 Segurança no Banco de Dados utilizado

O sistema IDS Saúde para atender a restrição de acesso a entidades não autenticadas e autorizadas foi estruturado de forma a não deixar a senha de acesso ao banco de dados visível em nenhum arquivo de

configuração do sistema, esta configuração de conexão da aplicação com o banco de dados por questões de segurança está exposta no arquivo de configuração de maneira criptografada evitando assim que terceiros possam utilizar de má fé, o IDS Saúde criptografa este arquivo.

Além das senhas criptografadas, o acesso pelas ferramentas de manipulação de Banco de dados também é restrito a administradores do Sistema, pois as senhas são cadastradas diferentemente das senhas padrões de banco de dados, onde é necessário conhecer esta senha que está totalmente restringida à empresa provedora da aplicação, sem essa senha fica impossível acessar o banco de dados.

1.7 Segurança da comunicação entre Cliente e Servidor

As informações digitais estão sujeitas a uma série de inconvenientes, que podem ser intencionais ou não. E são através da segurança da informação que é tratado esses conceitos, técnicas e recursos que conseguem minimizar essa fragilidade, dando níveis de confiabilidade altos as informações digitais. Atualmente existem alguns pilares nos quais se apoia a Segurança dos sistemas de Informação, desde a sessão de comunicação entre o componente cliente (do lado do usuário) e o componente servidor.

Esses principais pilares são praticamente pré-requisitos para que se considere um sistema de informação seguro:

Confidencialidade: É a garantia de que uma informação não será acessada por pessoas não autorizadas, ou seja, ser confidencial/sigiloso. Podemos mencionar os recursos de criptografia que "escondem" a informação e os limites de acesso dos usuários como o uso de senhas privadas.

Integridade: É a garantia de que uma informação não será alterada sem autorização (durante seu trajeto ou armazenamento, equivale a informar que irá manter-se íntegro). Podemos mencionar o recurso de hash (ou Resumo - qualquer algoritmo que mapeie dados grandes e de tamanho variável para pequenos dados de tamanho fixo) que permite saber se a informação foi, ou não, alterada, e assim forneça essa garantia.

Disponibilidade: É a garantia de que um sistema de informações estará sempre disponível aos usuários quando a informação for requisitada. Podemos associar ao sistema estar sempre on-line e disponível aos usuários. E para que isso seja possível devem-se tomar medidas como geradores de energia, computadores de reserva e backup das informações caso ocorram situações especificas de fatores externos e internos.

Autenticidade: É a garantia de conhecer a identidade de um usuário ou sistema de informações com quem se vai estabelecer comunicação. Podemos reconhecer esse pilar como ser quem diz que é, ser autêntico. Recursos como senhas que somente o usuário tem conhecimento, ou biometria, assinatura digital e certificação digital são utilizados para esse propósito.

Confiabilidade: sendo o objetivo maior da Segurança. Garantir que o sistema irá se "comportar" como o esperado e projetado para prestar o serviço. Para se alcançar esse pilar todos os demais devem ter sido alcançados primeiro.

Em se tratar de segurança, o sistema IDS Saúde utiliza-se do protocolo de segurança HTTPS (Protocolo de Transferência de Hipertexto Seguro) que substitui o acesso pelo protocolo HTTP. A principal diferença é que o HTTPS possui uma camada adicional de segurança que utiliza o protocolo SSL/TLS. Essa camada adicional permite que os dados sejam transmitidos por meio de uma conexão criptografada e que se verifique a autenticidade do servidor e do cliente por meio de certificados digitais. Dessa forma evita-se que a informação seja transmitida entre o cliente e servidor e que seja visualizada por terceiros.

1.8 Proteção de parâmetros de autenticação

Para realizar a Autenticação, o sistema IDS Saúde utiliza o protocolo de segurança HTTPS (Protocolo de Transferência de Hipertexto Seguro) ao qual possui uma camada adicional de segurança que utiliza o

protocolo SSL/TLS. Essa camada adicional permite que os dados sejam transmitidos por meio de uma conexão criptografada e que se verifique a autenticidade do servidor e do cliente por meio de certificados digitais. Dessa forma evita que a informação seja transmitida entre o cliente e o servidor e seja visualizada por terceiros.

Essa criptografia consiste num método de proteger determinado conteúdo desde sua origem até destino, para que estas não sofram alterações indevidas ou apenas para evitar que pessoas não autorizadas tenham conhecimento das mesmas. A criptografia dos dados conceitua-se na transformação das mensagens de documento em textos cifrados que é reprocessado por quem recebe e o transforma em texto para que se possa ler. Quem faz essa transformação de texto claro ao cifrado é um algoritmo. As senhas do sistema IDS Saúde são criptografas em banco de dados e o banco de dados possui proteção de acesso por senha.

O IDS Saúde disponibiliza de mecanismos de usuário por Login e Senha além de acesso por Biometria e Certificação Digital, ambos os parâmetros de autenticação são seguros. O sistema também disponibiliza de um processo de criptografia de dados na comunicação entre os componentes da aplicação (Cliente, Servidor de Aplicação e Banco de dados).

2. MECANISMOS DE SEGURANÇA OS USUÁRIOS

Para evitar alvos de ataques pela Internet ou pela Rede, qualquer usuário que tenha uma simples conexão na rede e não tome as devidas precauções está passível de ter seu computador comprometido.

Com o avanço das novas tecnologias, os ataques através códigos maliciosos ou outros meios, buscam sistemas vulneráveis onde possam coletar senhas, dados pessoais e dados sigilosos. Além disso, uma vez que a máquina foi invadida, o atacante pode assumir total controle sobre o sistema e usá-lo como ponte para atividades ilícitas como exemplo ataques automatizados.

Mais adiante serão apresentados para usuários não-técnicos, breves tópicos com sugestões, dicas e boas práticas recomendadas para garantir a segurança.

2.1 Login e Senhas

Para realizar o cadastro de Login e Senha, alguns cuidados devem ser tomados, segue alguns exemplos:

- Certificar de não estar sendo observado ao digitar o Login e senha;
- Não fornecer Login e senha para terceiros ou outras pessoas, em hipótese alguma;
- Elaborar boas senhas, as senhas bem elaboradas consideradas de nível alto ou fortes, são senhas difíceis de serem descobertas e de fácil memorização. Abaixo segue alguns exemplos para a elaboração de uma boa senha:
  - ✓ Números Aleatórios: Evitar usar números sequenciais, exemplo 222 ou 123456, utilizar números aleatórios de preferência misturados com caracteres;
  - ✓ Quantidade elevada de Caracteres: Tentar elaborar senhas longas, quanto maior for à senha mais difícil de ser descoberta;
  - ✓ Diferentes Tipos de Caracteres: Tentar elaborar senhas misturando os caracteres, exemplo: Utilizar Letras, Números, Acentuação e Caracteres especiais em uma única senha;
  - ✓ Letras Maiúsculas e Minúsculas: Tentar alternar as letras de senhas com uso de letras maiúsculas e minúsculas;
  - ✓ Substituição de caracteres: Invente um padrão de substituição de caracteres, ou seja, um padrão que possa ser identificado visualmente. Exemplo: a letra **w** por **VV**, a letra **O** pelo **Ø,** a letra **S** pelo **$** ou **5** entre outros meios.

Utilizando as dicas para elaboração de senha, é possível criar boas senhas, segue algumas Dicas:

- Memorizar uma frase qualquer de seu conhecimento e atribuir esta frase como senha.
  Frase de exemplo: Tenho cinco Senhas Fortes Super Seguras para acessar o sistema:
  Senha: T5$F$$P/aØ$!
- A palavra **criptografia** poderia se transformar em **cr1p+Øgraf1a**
- Altere as senhas sempre que julgar necessário;
- Evitar utilizar a mesma senha em diferentes serviços;
- Evitar utilizar respostas de perguntas de recuperação de senhas que possam ser facilmente adivinhadas;
- Procurar 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;
- Ser cuidadoso ao usar a sua senha em computadores potencialmente infectados ou comprometidos. Procure, sempre que possível, utilizar opções de navegação anônima ou teclados virtuais;
- Evitar usar opções como "Lembre-se de mim", "Manter conectado e outros.

2.2 Navegando na internet (Web)

Em se tratar de acesso à internet, qualquer usuário deve estar ciente das precauções que devem ser tomadas em uma navegação web. A navegação com segurança está ganhando cada vez mais e atualmente não é questão de escolha, deve ser utilizados mecanismos para proteção contra fraudes, roubo de dados, dentre outros meios.

Para proteção em relação às fraudes é importante manter sempre o Sistema Operacional e antivírus atualizado, não clicar em links recebidos por e-mails caso não seja de remetente confiável, não executar arquivos recebidos por e-mail ou via serviços de mensagem instantânea. Desative o compartilhamento de recursos ou pastas em redes além de outros mecanismos de não conhecimento do usuário.

Proteja-se dos vírus mantendo todos os programas que você usa preferencialmente atualizados. Instale todas as correções de segurança quando existirem envolvendo os sistemas de antivírus, firewall pessoal e anti-spyware. Mantenha seu navegador sempre atualizado, pois é um dos meios de entradas para que ocorra invasões sem que o usuário perceba. Desative Java e ActiveX, use-os apenas se for estritamente necessário, e só habilite JavaScript, cookies e pop-up ao acessar sites confiáveis.

Se possível mantenha o programa de leitor de e-mails sempre atualizado ou de preferência de correios eletrônicos online e não armazene senhas no seu navegador. Desative a visualização de e-mails em HTML e as opções de execução automática de arquivos anexados. É recomendado que sejam usadas senhas com letras, números e símbolos. E preferencialmente nunca use como senha dados pessoais ou palavras chaves usadas no seu dia a dia. Evite expor os dados pessoais em páginas Web, blogs ou sites de redes de relacionamentos.

2.3 Baixando e Instalando Programas

Sempre que for instalar um programa, é importante ler a licença de instalação e termos de utilização. Certificar-se que esse programa é de uma fonte confiável e que não irá instalar outros programas "não autorizados" em seu computador, que irão "pegar" dados e repassá-los a outros meios não autorizados.

Em situações de realizar downloads de arquivos de sites ou de anexos de e-mails, é primordial somente abrir de remetentes confiáveis e mesmo assim se houver suspeita verificar o arquivo com o antivírus antes de descompactá-lo ou executar. Isso ajudará a evitar que vírus sejam instalados no computador e se propaguem pela rede. Da mesma forma ajudará a não sofrer ataques de cavalo de tróia, phishing, spywares e outros.

Outro cuidado que os usuários devem ter é nas execuções automáticas de programas e mensagens que solicitem execução no momento em que um determinado site é visitado ou na execução de algum arquivo salvo no computador. Evite instalar programas piratas em seu computador, eles podem trazer vírus ou outros programas perigosos, toda a atenção é necessária quando se trata da segurança de informação e de dados.

2.4 Dados Pessoais

Os dados pessoais são informações confidenciais e é nestes casos que é necessário tomar precauções, evite fornecer seus dados pessoais, como: nome, e-mail, telefone, endereço e números de documentos para terceiros. Também evite fornecer informações delicadas, como: senhas e números de cartão de crédito (somente se estiver realizando uma transação comercial ou financeira e se tenha certeza da idoneidade da instituição que mantém o site). Pois estas informações geralmente são armazenadas em servidores das instituições que mantêm os sites e corre-se o risco destas informações serem repassadas sem sua autorização para outras instituições ou de um atacante comprometer este servidor e obter acesso a todas as informações.

Um site de redes de relacionamento normalmente permite que o usuário cadastre informações pessoais, como: nome, endereços residencial e comercial, telefones, endereços de e-mail, data de nascimento, quem são seus familiares, além de outros dados que irão compor o seu perfil. Se o usuário não limitar o acesso aos seus dados para apenas aqueles de interesse, todas as suas informações poderão ser visualizadas por qualquer um que utilize este site. Além disso, é recomendável que o usuário evite fornecer muita informação a seu respeito, pois nenhum site está isento do risco de ser invadido e de ter suas informações furtadas por um invasor.

Desta forma, é extremamente importante estar atento e avaliar que informações serão disponibilizadas nesse tipo de site, principalmente aquelas que poderão ser vistas por todos. Em resumo as principais situações a serem verificadas, são:

- Evite colocar dados pessoais (endereço, nome completo, instituição onde estuda entre outros) em sites de relacionamentos como exemplo, Facebook e Twitter;
- Evite digitar senhas e dados pessoais em computadores públicos, por exemplo, em Lan Houses, empresa, computadores compartilhados e afins;
- Evite criar senhas com datas de aniversários, sequências numéricas de fácil adivinhação ou nome de pessoas. Uma sugestão é criar senhas intercalando letras e números (se possível também com caracteres) e que tenham tamanho mínimo de oito caracteres;
- Mude de senha regularmente, principalmente se utilizar máquinas compartilhadas e/ou administradas por pessoas;
- Não clique em links mostrados por e-mails desconhecidos. Eles costumam instalar vírus ou outras ameaças que roubam dados do computador;
- Evite abrir arquivos anexados a e-mails de pessoas ou empresas desconhecidas. E mesmo que o remetente seja conhecido, certifique-se do remetente ou passe um bom antivírus antes de abrir o arquivo;
- Não divulgue e nem compartilhe suas senhas.

2.5 Segurança Física

Quando usar seu computador ou qualquer dispositivo com acesso a rede em ambiente público, é importante tomar cuidados para evitar que ele seja furtado ou indevidamente utilizado por outras pessoas. Por isso procure manter seu computador bloqueado, para evitar que seja usado quando você não estiver por perto (isso pode ser feito utilizando protetores de tela com senha ou com programas que impedem o uso do computador caso um dispositivo específico não esteja conectado). Para segurança em relação a esse item, o sistema IDS Saúde já possui um recurso para inativar a tela do sistema, caso tenha "x" minutos sem atividade no sistema solicitando novamente a senha para liberar acesso (isso com o específico operador conectado).

Se necessário procure manter a segurança física do seu computador, utilizando travas que dificultem que ele seja aberto, que tenha peças retiradas ou que seja furtado, como cadeados e cabos de aço. Se possível utilize criptografia de disco para que, em caso de perda ou furto, seus dados não sejam indevidamente acessados.

É interessante configurar seu computador para solicitar senha na tela inicial, isso impede que alguém reinicie seu computador e o acesse diretamente. E por fim não é recomendado que insira dispositivos externos de outras pessoas sem antes certificar do remetente e também realizar uma varredura nos dados com o antivírus.

2.6 Antivirus, Antispyware, Firewall e outros

No ambiente tecnológico contamos com recursos e softwares específicos que auxiliam na proteção de nossos computadores e redes. É válido ressaltar que esses mecanismos devem estar devidamente instalados, atualizados e configurados para que a segurança possa de fato acontecer. A seguir são listados alguns dos principais recursos utilizados:

- **Antivírus**: São programas que protegem os sistemas de informação contra vírus de computador. São ferramentas preventivas e corretivas, que detectam e, em muitos casos, removem vírus de computador e outros programas maliciosos (como spywares e cavalos de tróia).
- **Antispyware**: São programas espiões (um tipo de malware), responsável por invadir o seu computador e, sem o seu conhecimento ou autorização, transmitir dados confidenciais (como sua senha do banco, e-mail ou rede social) para uma rede externa. Então da mesma forma que os programas antivírus, os antispywares têm a função de impedir o acesso de invasores aos dados, identificando e removendo as que, eventualmente, já tenham sido instaladas.
- **Firewall**: É uma espécie de barreira que não permite que intrusos acessem a rede interna. É um sistema baseado em software ou hardware capaz de controlar o acesso entre duas redes ou sistemas, impedindo acessos indevidos e ataques. Geralmente é posicionado entre a rede privada e a rede externa. Dessa forma o firewall deve permitir acesso entre as duas interfaces através de autenticação. Ele é usado para múltiplos propósitos: restringe a entrada de dados utilizando um ponto de acesso controlado; evita que os invasores cheguem perto dos sistemas em questão, além de restringir a saída de dados utilizando um ponto de acesso controlado. Existem muitas maneiras de configurar um firewall e a configuração dependerá da política de segurança local e dos serviços utilizados.

2.7 Atualizações

É de extrema importância que o usuário sempre esteja com seu Sistema Operacional atualizado, a fim de já estar seguro em relação às correções que são constantemente realizadas pelos fabricantes de Sistemas Operacionais. Ressaltando que da mesma forma o sistema utilizado IDS Saúde preferencialmente deve estar

atualizado para suas últimas versões. Ficando a responsabilidade por parte do cliente em solicitar as atualizações à desenvolvedora de software IDS.

2.8 Correio Eletrônico

A utilização de correio eletrônico (e-mails) surgiu tendo como principal característica a simplicidade no envio e recebimento de mensagens. Contudo esse ambiente virtual proporciona muitas vantagens e agilidades, no entanto é importante se proteger contra ameaças na utilização de e-mails.

Manter sempre a versão mais atualizada do seu programa de e-mail, desabilitar as opções que permitem abrir ou executar automaticamente arquivos ou programas anexados às mensagens e evitar abrir arquivos ou executar programas anexados aos e-mails sem antes verificá-los com algum antivírus. Além disso, constatar a procedência de e-mails quanto ao remetente. Como dica priorizar a utilização de recursos de e-mails online em vez de correios eletrônicos off-line.

2.9 Bom Senso

Aos usuários, é fundamental que tenham o mínimo de conhecimento sobre seus direitos e deveres dentro da organização a qual atuam. É interessante que recebam informações da utilização de softwares e contas de acesso, proteção e uso de informações como senhas, utilização do sistema e dados confidenciais da organização. Devem, ainda, ter conhecimento da importância da utilização de mecanismos de segurança como Antivírus, Firewall, Proxy e outros.

Além de todos os tópicos citados nesse manual, é impossível elaborar um roteiro completo ao usuário do que prevenir para a segurança. O usuário tem que ter bom senso no uso de sistemas digitais e no uso da internet com o intuito de manter os padrões de segurança necessários.

3. Lei Geral de Proteção de Dados (LGPD)

Com a iminência da Lei Geral de Proteção de Dados (LGPD, nº 13.709/2018) entrar em vigor, é fundamental a segurança em sistema e em dados. A LGPD regulamenta a coleta e o processamento de informações pessoais, seja por empresas públicas ou privadas. Em relação às áreas atendidas pela IDS, um dos principais pontos refere-se ao armazenamento de dados sensíveis que podem gerar alguma discriminação da pessoa, a exemplo de diagnósticos e doenças salvos em sistemas online. Sendo assim, é preciso adotar ferramentas com rigorosa certificação de segurança para proteger tais informações.

Para adequação de seu Município à LGPD, no que se refere a utilização do Software de Gestão, é necessário que sejam utilizadas algumas funcionalidades já disponíveis em nossos softwares, tais como:

- Controle avançado de senha de acesso para operadores;
- Controle de e-mail do operador para redefinição de senha de acesso;
- Controle de validade da senha do operador (dias);
- Controle de inatividade da sessão;
- Controle de operadores ativos e inativos;
- Controle de data de expiração da senha do cadastro dos operadores;
- Monitoramento de operador;
- Restrição de horário de acesso do operador;
- Certificado digital para médicos e profissionais do laboratório no padrão ICP-Brasil;

No caso de municípios que possuem estrutura de servidor própria, além das especificações acima, são necessárias algumas adequações para garantir o controle e a segurança dos dados:

- HTTPS – SSL: O HTTPS é uma extensão segura do HTTP. Os sites que configurarem um certificado SSL/TLS podem utilizar o protocolo HTTPS para estabelecer uma comunicação segura com o servidor. O objetivo do SSL/TLS é tornar segura a transmissão de informações sensíveis como dados pessoais, de pagamento ou de login;
- Acessos nominais para qualquer usuário que realize acesso aos servidores;
- Firewall habilitado em todos os servidores (controle de portas);
- Senhas fortes, com no mínimo 8 caracteres incluindo letras, números e caracteres especiais;
- Rotina de backups conforme políticas mundiais de backup, sendo estes realizados conforme descrição abaixo e armazenados em estrutura fora do servidor:
  Backup diário (full) com retenção de 7 dias (7 backups);
  Backup semanal (full) com retenção de 30 dias (4 backups);
  Backup mensal (full) com retenção de 365 dias (12 backups);
  Backup anual (full) com retenção de 5 anos (5 backups);

SAIBA MAIS

- Bases legais de sistemas: https://triplait.com/bases-legais-para-tratamento-de-dados-da-lgpd
- Lei da LGPD: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm

Glossário

Termo	Definição
Activex	É um conjunto de tecnologias software framework criado pela Microsoft facilitar a integração entre diversas aplicações
Adobe flex	O Adobe Flex é o nome de uma tecnologia lançada pela Macromedia, que suporta o desenvolvimento de aplicações ricas para a Internet, baseadas na plataforma do Macromedia Flash
AES	Advanced Encryption Standard ou Padrão de Criptografia Avançada
Antispyware	São programas cujo objetivo é tentar eliminar do sistema, através de uma varredura, spywares, adwares, keyloggers, trojans e outros malwares
Antivírus	São programas de computador concebidos para prevenir, detectar e eliminar vírus de computadores.
Back-end	É responsável por coletar a entrada do usuário em várias formas e processá-la para adequá-la a uma especificação em que o back-end possa utilizar
Backup	Termo em inglês que tem o significado de Cópia de segurança
Biometria	Do ponto de vista da tecnologia da informação, é a técnica utilizada para medir e se obter determinadas informações físicas sobre um indivíduo e, com base nessas informações, gerar uma identificação única para o mesmo
Bits	Dígito binário (Menor unidade de informação)
Blog	É um site cuja estrutura permite a atualização rápida a partir de acréscimos dos chamados artigos, ou posts
Boot	Processo de iniciação do computador que carrega o sistema operacional quando a máquina é ligada
Browser	Navegador, também conhecido pelos termos em inglês web browser ou simplesmente browser
Cloud Computing	Computação nas nuvens
Cookies	É um pequeno pedaço de dados enviado a partir de um site web e armazenado em um arquivo (ficheiro) de texto criado no computador do usuário enquanto ele está navegando naquele site

CPD	Centro de processamento de dados. Local onde são concentrados os equipamentos de processamento e armazenamento de dados de uma empresa ou organização
Criptografar	Conjunto de regras que visa codificar a informação
DatabaseSecure	Refere-se à utilização de uma ampla gama de controles de segurança da informação para proteger o banco de dados
Download	Transferir (baixar) um ou mais arquivos de um servidor remoto para um host local
DVD	Disco Digital Versátil é um formato digital para arquivar ou guardar dados
e-mail	Correio eletrônico, é um método que permite compor, enviar e receber mensagens através de sistemas eletrônicos de comunicação
Firewall	Parede de fogo. É um dispositivo de uma rede de computadores que tem por objetivo aplicar uma política de segurança a um determinado ponto da rede
Front-end	É responsável por coletar a entrada do usuário em várias formas e processá-la para adequá-la a uma especificação em que o back-end possa utilizar
FTP	Protocolo de Transferência de Arquivos. É uma forma bastante rápida e versátil de transferência de arquivos
Função hash	É um algoritmo que mapeia dados de comprimento variável para dados de comprimento fixo
Hacker	É um indivíduo que se dedica, com intensidade incomum, a conhecer e modificar os aspectos mais internos de dispositivos, programas e redes de computadores
Hardware	Todos os dispositivos físicos e equipamentos utilizados no processo de informações
HTML	Linguagem de Marcação de Hipertexto. È uma linguagem de marcação utilizada para produzir páginas na Web
HTTP	Protocolo de Transferência de Hipertexto
HTTPS	Protocolo de Transferência de Hipertexto Seguro. É uma implementação do protocolo HTTP sobre uma camada adicional de segurança que utiliza o protocolo SSL/TLS
Internet	É um sistema global de redes de computadores interligadas que utilizam o conjunto de protocolos padrão da internet (TCP/IP) para servir vários bilhões de usuários no mundo inteiro
Intranet	Rede de computadores privada que assenta sobre a suíte de protocolos da Internet, porém, de uso exclusivo de um determinado local
Java	É uma linguagem de programação e plataforma computacional
JavaScript	Linguagem de programação interpretada

Lan House É um estabelecimento comercial onde, à semelhança de um cyber café, os usuários podem pagar para utilizar um PC com acesso à Internet e a uma rede local

Link Uma ligação. Também conhecida em português pelos correspondentes termos ingleses, hyperlink e link

Log Arquivo utilizado para auditoria e diagnóstico

Login Define o processo através do qual o acesso a um sistema informático é controlado através da identificação e autenticação do utilizador através de credenciais fornecidas por esse mesmo utilizador

Malware Software malicioso ou mal-intencionado. É um software destinado a infiltrar-se em um sistema de computador alheio de forma ilícita

Md5 Message-Digest algorithm 5. É um algoritmo de hash de 128 bits unidirecional

Nobreak Fonte de alimentação ininterrupta. É um sistema de alimentação secundário de energia elétrica que entra em ação, alimentando os dispositivos a ele ligados, quando há interrupção no fornecimento de energia primária

Offline Fora de Linha, representa a indisponibilidade de acesso do usuário à rede ou ao sistema de comunicações

Online Estar online ou estar em linha significa estar disponível para acesso

Oracle Sistema de gerenciamento de banco de dados

Pendrives Memória USB Flash Drive. É um dispositivo de memória construído por memória flash

Phishing É uma forma de fraude eletrônica, caracterizada por tentativas de adquirir dados pessoais de diversos tipos; senhas, dados financeiros como número de cartões de crédito e outros dados pessoais

Pop-up Janela que abre no navegador ao visitar uma página web ou acessar uma hiperligação específica

Proxy Em português procurador. É um servidor (um sistema de computador ou uma aplicação) que age como um intermediário para requisições de clientes solicitando recursos de outros servidores

Required Requerido, obrigatório

Root Super Usuário ou Super Utilizador

Sgdb Abreviação de Sistema de Gerenciamento de Banco de Dados

Site Website ou Site. É um conjunto de páginas web

SMTP Protocolo de Transferência de Correio Simples. È o protocolo padrão para envio de e-mails através da Internet

Software Conjunto de componentes lógicos de um computador ou sistema de processamento de dados; programa, rotina ou conjunto de instruções que controlam o funcionamento de um computador; suporte lógico

Spyware Programa automático de computador, que recolhe informações sobre o usuário, sobre os seus costumes na Internet e transmite essa informação a uma entidade externa na Internet, sem o conhecimento e consentimento do usuário.

Telnet É um protocolo de rede utilizado na Internet ou redes locais para proporcionar uma facilidade de comunicação baseada em texto interativo bidirecional usando uma conexão de terminal virtual

TI Tecnologia da Informação (TI) pode ser definida como o conjunto de todas as atividades e soluções providas por recursos de computação que visam permitir a produção, armazenamento, transmissão, acesso, segurança e o uso das informações

TLS/SSL O Transport Layer Security - TLS, assim como o seu antecessor Secure Sockets Layer - SSL. É um protocolo de segurança que protege as telecomunicações via internet para serviços como e-mail (SMTP), navegação por páginas (HTTPS) e outros tipos de transferência de dados

Vírus É um software malicioso que vem sendo desenvolvido por programadores que, tal como um vírus biológico, infecta o sistema, faz cópias de si mesmo e tenta se espalhar para outros computadores, utilizando-se de diversos meios

Web Designa a rede que conecta computadores por todo mundo, a World Wide Web (WWW)

Conheça os produtos IDS

Encontre mais informações através da Universidade IDS

O conhecimento é o fator principal para realização eficiente do nosso trabalho diário, seja ele no ambiente tecnológico ou nas áreas da Saúde, Social e Educação. E para facilitar esse conhecimento se faz necessária a utilização de novas tecnologias e recursos que possibilite acesso à cursos e treinamentos. Com conteúdo de fácil aprendizagem, horário flexível e de fácil acesso, que permita à todos os envolvidos capacitação e ampliação dos seus conhecimentos.

Acesse a Universidade IDS
https://treinamento.ids.inf.br/moodle/login/index.php

Encontre-nos em nossas redes sociais e
visite nosso site | **www.ids.inf.br**