POLITICA DE SEGURANÇA

ÁREA DE TECNOLOGIA

UNISEPE–UNIÃO DAS INSTITUIÇÕES DE SERVIÇOS, ENSINO E PESQUISA LTDA.

1. Introdução

A **segurança** é um dos assuntos mais importantes dentre as preocupações da UNIÃO DAS INSTITUIÇÕES DE SERVIÇOS, ENSINO E PESQUISA - UNISEPE.

Temos nesse documento um conjunto de instruções e procedimentos para normatizar e melhorar nossa visão e atuação em segurança.

A Informação é um ativo que, como qualquer outro importante para os negócios, tem um valor para a UNIÃO DAS INSTITUIÇÕES DE SERVIÇOS, ENSINO E PESQUISA - UNISEPE e consequentemente necessita ser adequadamente protegida. A informação pode existir de diversas formas. Ela pode ser impressa ou escrita em papel, armazenada eletronicamente, transmitida pelo correio ou através de meios eletrônicos, mostrada

em filmes ou falada em conversas. Seja qual for a forma pela qual a mesma é apresentada, transmitida, armazenada ou compartilhada, é recomendado que a mesma seja protegida adequadamente.

A Segurança da Informação protege a Informação de diversas ameaças para garantir a continuidade dos negócios, a integridade e a disponibilidade da mesma.

Política de Segurança são normas internas padronizadas pela empresa que devem ser seguidas à risca para que todas as possíveis ameaças sejam minimizadas e combatidas eficientemente pela equipe de segurança.

Todas as normas estabelecidas neste documento deverão ser cumpridas por todos os funcionários, parceiros e prestadores de serviços da UNIÃO DAS INSTITUIÇÕES DE SERVIÇOS, ENSINO E PESQUISA - UNISEPE. Ao receber essa cópia da Política de Segurança, você comprometeu-se a respeitar todos os tópicos aqui abordados e está ciente de que seus emails e navegação na internet/intranet podem estar sendo monitorados. A equipe de informática encontra-se a total disposição para saneamento de dúvidas e auxílio técnico.

2. Política de Senhas

Uma senha segura deverá conter no mínimo 7 caracteres compostos por letras, números e símbolos, diferenciando letras maiúsculas e minúsculas.

Você deve trocar todas as senhas (rede, e-mails, acessos bancários, etc.) periodicamente, preferencialmente a cada dois ou três meses.

Jamais utilizar palavras que façam parte de dicionários. Existem softwares que tentam descobrir senhas combinando e testando palavras em diversos idiomas e geralmente possuem listas de palavras (dicionários) e listas de nomes (nomes próprios, músicas, filmes, etc.). Não elaborar senhas utilizando:

- Nomes;
- Sobrenomes;
- Números de documentos;
- Placas de carros;
- Números de telefones;
- Datas.

Utilizar uma senha diferente para cada finalidade, ou seja, se você acessa a rede, o e-mail e duas contas bancárias, utilizar quatro senhas diferentes, uma para cada finalidade.

Certifique-se que não está sendo observado ao digitar sua senha.

Não utilize sua senha em computadores de terceiros (Lan Houses, por exemplo).

Sua senha não deve ser jamais passada a ninguém, nem mesmo da equipe de tecnologia. Caso desconfie que sua senha não esteja mais segura, sinta-se à vontade para mudá-la, mesmo antes do prazo determinado de validade.

Dicas para elaborar uma boa senha:

- Utilizar ao menos sete caracteres;
- Combinar letras, números e símbolos;
- Diferenciar maiúsculas e minúsculas;

2.1. Políticas de senhas de rede

Obrigatoriedade de cadastro de senhas complexas:

- Não conter toda ou parte do nome do usuário;
- Ter no mínimo sete caracteres;
- Conter combinações de números, letras maiúsculas e minúsculas, caracteres; As senhas expiram a cada 42 dias e o usuário não poderá utilizar-se novamente das últimas 11 senhas usadas. Digitando a senha errada por quatro vezes, o login será bloqueado por 3 horas ou até a liberação do administrador da rede.

3. Política de E-mail

Grande parte dos problemas de segurança envolvendo e-mails está relacionada aos conteúdo das mensagens, que normalmente abusam das técnicas de ataque ou de características de determinados programas leitores de e-mails, que permitem abrir arquivos ou executar programas anexados às mensagens automaticamente.

Nossos servidores de e-mail encontram-se protegidos contra vírus e códigos maliciosos, mas algumas atitudes do usuário final são requeridas:

- Não abra anexos com as extensões (bat, .exe, .src, .lnk e .com) se não tiver certeza absoluta de que solicitou esse e-mail;
- Desconfie de todos os e-mails com assuntos estranhos e/ou em inglês;
- Não reenvie e-mails do tipo corrente, aviso de vírus, avisos da Microsoft/AOL/Symantec, criança desaparecida, criança doente, pague menos em alguma coisa, não pague alguma coisa, etc.;
- Não utilize o e-mail da UNISEPE–UNIÃO DAS INSTITUIÇÕES DE SERVIÇOS, ENSINO E PESQUISA LTDA para assuntos pessoais;
- Evite anexos muito grandes;
- É proibido o assédio ou perturbação de outrem, seja através de linguagem utilizada, frequência ou tamanho das mensagens;
- É proibido o envio de e-mail a qualquer pessoa que não o deseje receber. Se o destinatário solicitar a interrupção de envio e-mails, o usuário deve acatar tal solicitação e não lhe enviar qualquer e-mail;
- É proibido o envio de mensagens de e-mail tipo mala direta, como, por exemplo, publicidade, comercial ou não, anúncios e informativos, ou propaganda política;
- É proibido o envio de e-mails mal-intencionados, sobrecarregar um usuário, site ou servidor com
- e-mail muito extenso ou numerosas partes de e-mail; Caso a empresa julgue necessário haverá bloqueios:
    - De e-mail com arquivos anexos que comprometa o uso de banda ou perturbe o bom andamento dos trabalhos;
    - De e-mail para destinatários ou domínios que comprometa o uso de banda ou perturbe o bom andamento dos trabalhos.
- É proibido o forjar qualquer das informações do cabeçalho do remetente;
- É proibido clicar em links que apareçam no conteúdo das mensagens;
- É obrigatória a manutenção da caixa de e-mail, evitando acúmulo de e-mails e arquivos inúteis;
- Há a obrigatoriedade da utilização de software homologado pelo departamento técnico, para ser o cliente de e-mail (Microsoft Outlook), configurado da seguinte forma:

- Manter sempre a versão mais atualizada; ○ Não abrir arquivos ou executar programas sem antes executar no antivírus; ○ Desabilitar as opções de abrir ou executar automaticamente arquivos ou programas anexados as mensagens;
- Desabilitar o modo de visualização de e-mails no formato HTML;

- É obrigatória a utilização de assinatura nos e-mails com o seguinte formato:
  - Nome do Funcionário; ○ Departamento; ○ Telefone Comercial.

Atualmente, usuários da Internet têm sido bombardeados com e-mails indesejáveis e, principalmente, com mensagens fraudulentas cuja finalidade é a obtenção de vantagens financeiras. Alguns exemplos são: ○ Mensagens alertando sobre pendências financeiras no SPC; ○ Mensagens solicitando a alteração das senhas bancárias;

Mensagens que procuram induzir o usuário a acessar uma determinada página na Internet ou a instalar um programa, abrir um álbum de fotos, ver cartões virtuais, etc., mas cujo verdadeiro intuito é fazer com que o usuário forneça dados pessoais e sensíveis, como contas bancárias, senhas e números de cartões de crédito.

Como identificar: seguem algumas dicas para identificar mensagens fraudulentas:

- Leia atentamente a mensagem. Normalmente, ela conterá diversos erros gramaticais e de ortografia;
- Ao passar o cursor do mouse sobre o link, será possível ver o real endereço do arquivo malicioso na barra de status do programa leitor de e-mails, ou browser. Normalmente, este link será diferente do apresentado na mensagem;
- Qualquer extensão pode ser utilizada nos nomes dos arquivos maliciosos, mas fique particularmente atento aos arquivos com extensões ".exe", ".zip" e ".scr", pois estas são as mais utilizadas. Outras extensões freqüentemente utilizadas por fraudadores são ".com", ".rar" e ".dll";
- Fique atento às mensagens que solicitam a instalação/execução de qualquer tipo de arquivo/programa;
- Acesse a página da instituição que supostamente enviou a mensagem, digitando o endereço da página diretamente no browser, e procure por informações relacionadas com a mensagem que você recebeu. Em muitos casos, você vai observar que não é política da instituição enviar e-mails para usuários da Internet, de forma indiscriminada, principalmente contendo arquivos anexados.
- No caso de mensagem recebida por e-mail, o remetente pode ser facilmente forjado pelos fraudadores, portanto desconfie dos e-mails conhecidos também;
- Se você ainda tiver alguma dúvida e acreditar que a mensagem pode ser verdadeira, entre em contato com a instituição para certificar-se sobre o caso, antes de enviar qualquer dado, principalmente informações sensíveis, como senhas e números de cartões de crédito;
- Sites de comércio eletrônico ou Internet Banking confiáveis ***sempre*** utilizam conexões seguras quando dados pessoais e financeiros de usuários são solicitados. Caso a página não utilize conexão segura, desconfie imediatamente. Caso a página falsificada utilize conexão segura, um novo certificado, que não corresponde ao site verdadeiro, será apresentado.

Alguns exemplos de temas e respectivas descrições dos textos encontrados em mensagens deste tipo são apresentados na tabela:

Exemplos de temas de mensagens fraudulentas

Tema	Texto da mensagem
Bancos	Comprovante bancário, atualize seu cadastro
SERASA e SPC	débitos, restrições ou pendências financeiras.
Serviços de governo eletrônico	CPF/CNPJ pendente ou cancelado, Imposto de Renda (nova versão ou correção para o programa de declaração, consulta da restituição, dados incorretos ou incompletos na declaração), eleições (título eleitoral cancelado, simulação da urna eletrônica).
Álbuns de fotos	pessoa supostamente conhecida, celebridades, relacionado a algum fato noticiado (em jornais, revistas, televisão), traição, nudez ou pornografia, serviço de acompanhantes.
Serviço de telefonia	pendências de débito, aviso de bloqueio de serviços, detalhamento de fatura, créditos gratuitos para o celular.
Antivírus	a melhor opção do mercado, nova versão, atualização de vacinas, novas funcionalidades, eliminação de vírus do seu computador.
Notícias/boatos	fatos amplamente noticiados (ataques terroristas, *tsunami*, terremotos, etc.), boatos envolvendo pessoas conhecidas (morte, acidentes ou outras situações chocantes).
Reality shows	BigBrother, A fazenda, etc. -- fotos ou vídeos envolvendo cenas de nudez ou eróticas, discadores.
Programas ou arquivos diversos	novas versões de *softwares*, correções para o sistema operacional Windows, músicas, vídeos, jogos, acesso gratuito a canais de TV a cabo no computador, cadastro ou atualização de currículos, recorra das multas de trânsito.
Pedidos	orçamento, cotação de preços, lista de produtos.
Sites de comércio eletrônico	atualização de cadastro, devolução de produtos, cobrança de débitos, confirmação de compra
Prêmios	E-mails informando sobre prêmios
Dinheiro fácil	descubra como ganhar dinheiro na Internet.
Promoções	diversos.
Prêmios	loterias, instituições financeiras.
Propaganda	produtos, cursos, treinamentos, concursos.
FEBRABAN	cartilha de segurança, avisos de fraude.
IBGE	censo.

4. Internet

A Internet é indiscutivelmente nossa mais poderosa ferramenta de trabalho. O uso recreativo da Internet está proibido.

Existem diversos riscos envolvidos no acesso aos sites da internet:

- Execução de programas não confiáveis;
- Acesso a sites falsos, se fazendo passar por instituições bancárias ou de comércio eletrônico;
- Realização de transações comerciais ou bancárias via Web, sem qualquer mecanismo de segurança.

O uso e acesso à Internet não é permitido aos seguintes tópicos:

- Acesso a sites com conteúdo pornográfico, jogos, bate-papo, apostas e assemelhados estará bloqueado e monitorado;
- É proibido o uso de ferramentas P2P (emule, torrent, etc.);
- É proibido o uso de Instant messengers para fins pessoais;
- Não será permitida a utilização de serviços de streaming, tais como Rádios On-Line, Youtube, Netflix, Spotify e afins.
- Bloquear pop-up nos navegadores e permiti-las apenas para sites conhecidos e confiáveis, onde forem realmente necessárias;
- É proibido utilizar os recursos da UNISEPE–UNIÃO DAS INSTITUIÇÕES DE SERVIÇOS,ENSINO E PESQUISA LTDA para fazer o download ou distribuição de software ou dados não legalizados;
- É proibido a divulgação de informações confidenciais da UNISEPE–UNIÃO DAS INSTITUIÇÕES DE SERVIÇOS, ENSINO E PESQUISA de discussão, listas ou batepapo, não importando se a divulgação foi deliberada ou inadvertida, sendo possível sofrer as penalidades previstas nas políticas e procedimentos internos e/ou na forma da lei;

- Os funcionários com acesso à Internet podem baixar somente programas ligados diretamente às atividades da UNISEPE–UNIÃO DAS INSTITUIÇÕES DE SERVIÇOS, ENSINO E PESQUISA LTDA e devem providenciar o que for necessário para regularizar a licença e o registro desses programas;
- É proibido efetuar upload (envio) de qualquer software licenciado da empresa ou de dados de propriedade da ou de seus clientes, sem expressa autorização do gerente responsável pelo software ou pelos dados;

Caso a UNISEPE–UNIÃO DAS INSTITUIÇÕES DE SERVIÇOS, ENSINO E PESQUISA LTDA julgue necessário haverá bloqueios de acesso à:

- Arquivos que comprometa o uso de banda ou perturbe o bom andamento dos trabalhos;
- Domínios que comprometa o uso de banda ou perturbe o bom andamento dos trabalhos;

Haverá geração de relatórios dos sites acessados por usuário e se necessário a publicação desse relatório.

Há a obrigatoriedade da utilização de software homologado pelo departamento técnico, para ser o cliente de navegação (Chrome e Firefox) que deve manter-se atualizado;

Lembrando novamente que o uso da internet estará sendo auditado constantemente e o usuário poderá vir a prestar contas de seu uso.

5. Internet Banking

Cuidados que um usuário deve ter ao acessar sites de comércio eletrônico ou Internet Banking:

- Realizar transações somente em sites de instituições que você considere confiáveis;
- Procurar sempre digitar em seu *browser* o endereço desejado. Não utilize *links* em páginas de terceiros ou recebidos por *e-mail*;
- Certificar-se de que o endereço apresentado em seu *browser* corresponde ao *site* que você realmente quer acessar, antes de realizar qualquer ação;
- Certificar-se que o *site* faz uso de conexão segura;
- Não acessar *sites* de comércio eletrônico ou *Internet Banking* através de computadores de terceiros;
- Desligar sua *Webcam* (caso você possua alguma), ao acessar um *site* de comércio eletrônico ou *Internet Banking;*
- Manter o seu *browser* sempre atualizado e com todas as correções (*patches*) aplicadas;
- Alterar a configuração do seu *browser* para restringir a execução de *JavaScript* e de programas *Java*, exceto para casos específicos;
- Configurar seu *browser* para bloquear *pop-up Windows* e permiti-las apenas para *sites* conhecidos e confiáveis, onde forem realmente necessárias;
- Configurar seu programa leitor de *e-mails* para não abrir arquivos ou executar programas automaticamente;
- Não executar programas obtidos pela Internet, ou recebidos por *e-mail*.

Como verificar se a conexão é segura (criptografada)?

Existem pelo menos dois itens que podem ser visualizados na janela do seu browser, e que significam que as informações transmitidas entre o browser e o site visitado estão sendo criptografadas.

O primeiro pode ser visualizado no local onde o endereço do site é digitado. O endereço deve começar com https:// (diferente do http:// nas conexões normais), onde o s antes do sinal de dois-pontos indica que o endereço em questão é de um site com conexão segura e, portanto, os dados serão criptografados antes de serem enviados. A figura abaixo apresenta o protocolo https, indicando uma conexão segura.

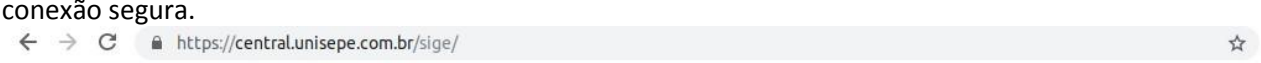

Figura 1: protocolo https e cadeado indicando uma conexão segura.

O segundo item a ser visualizado corresponde a algum desenho ou sinal, indicando que a conexão é segura. Normalmente, o desenho mais adotado nos browsers recentes é de um "cadeado fechado", apresentado antes do endereço do site.

Ao clicar sobre o cadeado, será exibida uma tela que permite verificar as informações referentes ao certificado emitido para a instituição que mantém o site, bem como informações sobre o tamanho da chave utilizada para criptografar os dados.

É muito importante que você verifique se a chave utilizada para criptografar as informações a serem transmitidas entre seu browser e o site é de no mínimo 128 bits. Chaves menores podem comprometer a segurança dos dados a serem transmitidos.

Outro fator muito importante é que a verificação das informações do certificado deve ser feita clicando única e exclusivamente no cadeado exibido. Atacantes podem tentar forjar certificados, incluindo o desenho de um cadeado fechado no conteúdo da página.

Checar se o endereço digitado permanece inalterado no momento em que o conteúdo do site é apresentado no browser do usuário. Existem algumas situações onde o acesso a um site pode ser redirecionado para uma página falsificada, mas normalmente nestes casos o endereço apresentado pelo browser é diferente daquele que o usuário quer realmente acessar.

Como saber se o certificado emitido para o site é legítimo?

Um exemplo de um certificado, emitido para um site de uma instituição é mostrado abaixo.

This Certificate belongs to: This Certificate was issued by: **www.example.org**
www.examplesign.com/CPS Incorp.by Ref. Terms of use at LIABILITY
LTD.(c)97 ExampleSign
www.examplesign.com/dir (c)00 **ExampleSign International Server CA** - UF Tecno Class 3 Example
Associados, Inc. ExampleSign, Inc. Cidade, Estado, BR

Serial Number:
70:DE:ED:0A:05:20:9C:3D:A0:A2:51:AA:CA:81:95:1A
This Certificate is valid from Sat Aug 20, 2005 to Sun Aug 20, 2006 Certificate
Fingerprint:
92:48:09:A1:70:7A:AF:E1:30:55:EC:15:A3:0C:09:F0

Informações que devem ser checadas:

- o endereço do site;
- o nome da instituição (dona do certificado);
- o prazo de validade do certificado.

6. Rede

O objetivo é prestar aos funcionários da UNISEPE–UNIÃO DAS INSTITUIÇÕES DE SERVIÇOS, ENSINO E PESQUISA, serviços de rede de alta qualidade e ao mesmo tempo desenvolver um comportamento extremamente ético e profissional. Nos termos da Política de
Utilização da Rede, a UNISEPE–UNIÃO DAS INSTITUIÇÕES DE SERVIÇOS, ENSINO E PESQUISA procederá ao bloqueio do acesso ou o cancelamento do usuário caso seja detectado uso em desconformidade com o aqui estabelecido ou de forma prejudicial à Rede.

Normas de utilização da rede que engloba desde o login, manutenção de arquivos no servidor e tentativas não autorizadas de acesso.

- Não é permitido tentativas de obter acesso não autorizado, tais como tentativas de fraudar autenticação de usuário ou segurança de qualquer servidor, rede ou conta (também conhecido como "cracking"). Isso inclui acesso aos dados não disponíveis para o usuário, conectar-se ao servidor ou conta cujo acesso não seja expressamente autorizado ao usuário ou colocar à prova a segurança de outras redes;
- Não é permitido tentativas de interferir nos serviços de qualquer outro usuário, servidor ou rede. Isso inclui ataques do tipo "negativa de acesso", provocar congestionamento em redes,

tentativas deliberadas de sobrecarregar um servidor e tentativas de "quebrar" (invadir) um servidor;

- Não é permitido o uso de qualquer tipo de programa ou comando designado a interferir com sessão de usuários;
- Antes de ausentar-se do seu local de trabalho, o usuário deverá fechar todos os programas
- Acessados, evitando, desta maneira, o acesso por pessoas não autorizadas e se possível efetuar o logout/logoff da rede ou bloqueio do desktop através de senha (CTRL+ALT+DEL + bloquear computador);
- Falta de manutenção no diretório pessoal, evitando acúmulo de arquivos inúteis;
- Material de natureza pornográfica e racista não pode ser exposto, armazenado, distribuído, editado ou gravado através do uso dos recursos computacionais da rede;
- Não é permitido criar e/ou remover arquivos fora da área alocada ao usuário e/ou que venham a comprometer o desempenho e funcionamento dos sistemas. As áreas de armazenamento de arquivos são designadas conforme abaixo (modelo):

Compartilhamento	Utilização
Diretório U: (usuário)	Arquivos Pessoais inerentes a empresa
Diretório H:\Dados (público)	Arquivos de compartilhamento geral (PASTA PUBLICA)

Em alguns casos pode haver mais de um compartilhamento referente aos arquivos do departamento em qual faz parte.

- A pasta PÚBLICA ou similar, não deverá ser utilizada para armazenamento de arquivos que contenham assuntos sigilosos ou de natureza sensível. Está pasta deverá ser utilizada apenas para transferências de arquivos entre departamentos, qualquer usuário poderá alterar, deletar e incluir, não será realizado backups nesta pasta. O conteúdo desta pasta será excluído periodicamente;
- É obrigatório armazenar os arquivos inerentes a empresa na pasta do usuário ou departamento no servidor de arquivos para garantir o backup dos mesmos;
- É proibido a instalação ou remoção de softwares que não forem devidamente acompanhadas pelo departamento técnico;
- É vedado a abertura de computadores para qualquer tipo de reparo, caso seja necessário o reparo deverá ocorrer pelo departamento técnico;
- Não será permitido a alteração das configurações de rede e inicialização das máquinas bem como modificações que possam trazer algum problema futuro.

7. Estações de trabalho / Rede

Cada estação de trabalho tem códigos internos que permitem que ela seja identificada na rede, e cada indivíduo possui sua própria estação de trabalho. Isso significa que tudo que venha a ser executado de sua estação acarretará em responsabilidade sua. Por isso sempre que sair da frente de sua estação, tenha certeza que efetuou logoff ou bloqueou o desktop.

- Não instale nenhum tipo de software/hardware sem autorização da equipe técnica ou de segurança;
- Não tenha MP3, filmes, fotos e softwares com direitos autorais ou qualquer outro tipo de pirataria;
- Mantenha na sua estação somente o que for supérfluo ou pessoal. Todos os dados relativos as empresas devem ser mantidas no servidor, onde existe um sistema de backup diário e confiável. Caso não saiba como fazer isso, entre em contato com a equipe técnica.

8. Utilização de impressoras

Esse tópico visa definir as normas de utilização de impressoras disponíveis na rede interna.

- Ao imprimir, verifique na impressora se o que foi solicitado já está impresso. Há várias impressões "sem dono" acumulando-se;
- Se a impressão deu errado e o papel pode ser reaproveitado na sua próxima tentativa, recoloque-o na bandeja de impressão. Se o papel servir para rascunho, leve para sua mesa. Se o papel não servir para mais nada, picote e jogue no lixo. Atentar para o conteúdo a ser reutilizado, não se deve reutilizar ou deixar como rascunho, impressões com informações pessoais, documentos com dados sensíveis devem ser descartados.
- Não é permitido deixar impressões erradas na mesa das impressoras, na mesa das pessoas próximas a ela e tampouco sobre o gaveteiro;
- Se a impressora emitir alguma folha em branco, recoloque-a na bandeja;
- Se você notar que o papel de alguma das impressoras está no final, faça a gentileza de reabastecê-la. Isso evita que você e outras pessoas tenham seus pedidos de impressão prejudicados e evita acúmulo de trabalhos na fila de impressão;
- Utilize a impressora colorida somente para versão final de trabalhos e não para testes ou rascunhos.

9. Social

Como seres humanos, temos a grande vantagem de sermos sociáveis, mas muitas vezes quando decorremos sobre segurança, isso é uma desvantagem. Por isso observe os seguintes tópicos:

- Não fale sobre a política de segurança da UNISEPE–UNIÃO DAS INSTITUIÇÕES DE SERVIÇOS, ENSINO E PESQUISA, com terceiros ou em locais públicos;
- Não diga sua senha para ninguém. Nossa equipe técnica jamais irá pedir sua senha;
- Não digite suas senhas ou usuários em máquinas de terceiros, especialmente fora da UNISEPE–UNIÃO DAS INSTITUIÇÕES DE SERVIÇOS, ENSINO E PESQUISA;
- Somente aceite ajuda técnica de um membro de nossa equipe técnica previamente apresentado e identificado;
- Nunca execute procedimentos técnicos cujas instruções tenham chegado por e-mail;
- Relate a equipe de segurança, pedidos externos ou internos que venham a discordar dos tópicos anteriores.

10. Vírus e códigos maliciosos

São os maiores geradores de problemas de segurança. Alguns procedimentos simples podem evitar grandes transtornos:

- Mantenha seu antivírus atualizado. Provavelmente nossa equipe técnica irá se encarregar disso, mas caso não tenha sido feito ou você perceba que a atualização não está funcional, entre em contato com a mesma para que a situação possa ser corrigida;

- Não traga disquetes, CDs ou pendrives de fora da UNISEPE–UNIÃO DAS INSTITUIÇÕES DE SERVIÇOS, ENSINO E PESQUISA LTDA. Caso isso seja extremamente necessário, encaminhe o mesmo para a equipe técnica, onde passará por uma descontaminação;
- Reporte atitudes suspeitas em seu sistema a equipe técnica, para que possíveis vírus possam ser identificados no menor espaço de tempo possível; Suspeite de softwares que "você clica e não acontece nada".

Um antivírus não é totalmente capaz de impedir que um atacante tente explorar alguma vulnerabilidade existente em um computador. Também não é capaz de evitar o acesso não autorizado em um computador. Por isso, você deve ter cuidado redobrado com os arquivos e programas executados em seu equipamento.

11. Verificação da utilização da Política de Utilização da Rede

Para garantir as regras mencionadas acima a UNISEPE–UNIÃO DAS INSTITUIÇÕES DE SERVIÇOS, ENSINO E PESQUISA LTDA se reserva no direito de:

- Implantar softwares e sistemas que podem monitorar e gravar todos os usos de Internet através da rede e das estações de trabalho UNISEPE–UNIÃO DAS INSTITUIÇÕES DE SERVIÇOS, ENSINO E PESQUISA LTDA;
- Inspecionar qualquer arquivo armazenado na rede, estejam no disco local da estação ou nas áreas privadas da rede, visando assegurar o rígido cumprimento desta política;
- Foram instalados uma série de softwares e hardwares para proteger a rede interna e garantir a integridade dos dados e programas, incluindo um firewall, que é a primeira, mas não a única barreira entre a rede interna e a Internet.

12. Sistemas Operacionais e Softwares instituídos

- **Sistemas Operacionais** ○ Windows Server, 2008, 2012, 2017 ○ Windows 7 (prazo final 2022)
  - Windows 8.1
  - Windows 10
  - Slackware 10, 12 e 13, 14, 14.2
  - FreeBsd 6.x ou 7.x ○ PFSense

- **Softwares Aplicativos** ○ Microsoft Office 2013 e 2016. ○ Firefox e Chrome atualizados ○ Adobe Acrobat Reader DC ○ MSSQL Server 2008 e 2012

- **Software para Email** ○ Microsoft Office Outlook 2013 ou 2016 ou superior

 Anti-Virus

  - Symantec (para os servidores e administrativo)

- Salvo equipe técnica - CPD (Centro de Processamento de Dados):

- Que poderá utilizar softwares ou sistemas operacionais que não estão instituídos, para fins de pesquisa e utilização para solucionar problemas pontuais no departamento do CPD, mas em hipótese alguma poderá ser utilizadas em terminais de usuários finais.
- Utilização do Skype só será permitida para fins profissionais, seguindo os seguintes critérios:
  - Não utilizar fotos inadequadas, ofensivas ou preconceituosas ○ Não colocar frases inadequadas, ofensivas ou preconceituosas

- Os softwares acadêmicos apenas poderão ser utilizados com as devidas licenças.

13. O não cumprimento dessa política

VIOLAÇÕES DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E SANÇÕES

Nos casos em que houver violação desta Política ou das Normas de Segurança da Informação, sanções administrativas e/ou legais poderão ser adotadas, podendo culminar com o desligamento e eventuais processos criminais, se aplicáveis.

O não cumprimento, pelo funcionário da UNISEPE–UNIÃO DAS INSTITUIÇÕES DE SERVIÇOS, ENSINO E PESQUISA, das normas estabelecidas neste documento, seja isolada ou acumulativamente, poderá ensejar, de acordo com a infração cometida, as seguintes punições:

COMUNICAÇÃO DE DESCUMPRIMENTO

Será encaminhado ao funcionário, por e-mail, comunicado informando o descumprimento da norma, com a indicação precisa da violação praticada. Cópia desse comunicado permanecerá arquivada junto ao Departamento de Recursos Humanos na respectiva pasta funcional do infrator.

ADVERTÊNCIA OU SUSPENSÃO

A pena de advertência ou suspensão será aplicada, por escrito, somente nos casos de natureza grave ou na hipótese de reincidência na prática de infrações de menor gravidade.

DEMISSÃO POR JUSTA CAUSA

Nas hipóteses previstas no artigo 482 da Consolidação das Leis do Trabalho.

Fica desde já estabelecido que não há progressividade como requisito para a configuração da dispensa por justa causa, podendo a UNISEPE–UNIÃO DAS INSTITUIÇÕES DE SERVIÇOS, ENSINO E ESQUISA, no uso do poder diretivo e disciplinar que lhe é atribuído, aplicar a pena que entender devida quando tipificada a falta grave.

14. Finalidade

Este documento não tem a intenção de estabelecer regras, limites ou controles levianamente, mas sim proteger e salvaguardar as informações e os interesses da UNISEPE – UNIÃO DAS INSTITUIÇÕES DE SERVIÇOS, ENSINO E PESQUISA.

Sabemos que os resultados de segurança são difíceis de ser demonstrados e que trabalhamos sempre com a esperança de não recorrermos a todas as nossas ferramentas, porém os funcionários da UNISEPE – UNIÃO DAS INSTITUIÇÕES DE SERVIÇOS, ENSINO E PESQUISA.
Não devem tentar enganar a política de segurança.