GOVERNO DO ESTADO
DO ESPÍRITO SANTO
Secretaria de Estado da Saúde

Política de Uso dos Recursos de TIC da Secretaria de Estado da Saúde

Este documento estabelece diretrizes claras e objetivas para os usuários dos ativos de informação quanto à sua utilização, descrevendo seus papéis e responsabilidades para com a Segurança da Informação.

O não-cumprimento desta determinação será considerado violação da Política de uso dos Recursos de TIC da SESA e estará sujeito a sanções legais.

Sumário

	Tipo de Documento: Política de Uso dos Recursos de TIC	Código: XXX–

Título do Documento: **POLÍTICA DE USO DOS RECURSOS DE TIC DA SECRETARIA DE ESTADO DA SAÚDE**		Homologação:
Número total de páginas:	Vigorar a partir de:	Revisão atual:

1 - OBJETIVO:

Essa Norma estabelece critérios e princípios para uma utilização ética e responsável dos recursos de TIC da SESA, os quais devem ser cumpridos por todos os seus colaboradores, objetivando um comportamento responsável e a aplicação de boas práticas para utilização desses recursos, contribuindo para a garantia e a maximização dos indicadores do nível de segurança e de estabilidade, bem como dos benefícios oferecidos aos usuários dos recursos de TIC da SESA.

Orientada pela PETI, essa Norma define regras, parâmetros e boas práticas de uso dos recursos de TIC, a serem cumpridas por todos os servidores e colaboradores a serviço da SESA dentro das responsabilidades e particularidades de suas áreas de atuação.

2 - REFERÊNCIA:

- Política Estadual de Tecnologia da Informação do Governo do Estado do Espírito Santo;

3 - ABRANGÊNCIA:

Essa Norma aplica-se a:

- Todas as unidades da SESA;
- Todo o funcionalismo público e colaboradores a serviço ou em uso da estrutura da SESA;
- Todos os ativos pertencentes ou usados pela estrutura da SESA;
- Todos os ambientes sejam eles informatizados ou apenas locais convencionais de processamento, comunicação e armazenamento de informações.

4 - NORMAS GERAIS DE USO DOS RECURSOS:

4.1 - PROPRIEDADE E RESPONSABILIDADE

O cidadão, através da SESA, é o único proprietário de todas as informações adquiridas, geradas, custodiadas ou tramitadas por meio da sua infraestrutura de processos, sistemas de informações e ambientes físicos, sob quaisquer meios de processamento, comunicação e armazenamento, incluindo além desses os ativos tecnológicos, suporte desses processos e sistemas.

Os recursos de TIC existentes no âmbito da SESA têm sua utilização sujeita a presente Instrução Normativa, independentemente da respectiva propriedade.

Os recursos de TIC de propriedade da SESA devem ser utilizados para o desempenho de atividades administrativas, não configurando quebra de sigilo a realização de auditorias e inspeções, manutenções preventivas e corretivas que vierem a ser executadas pela GTI, setor responsável pela infraestrutura tecnológica da SESA.

Os softwares e hardwares disponibilizados por empresas prestadoras de serviços e demais colaboradores são de inteira responsabilidade dos mesmos, que estão sujeitos a comprovação da legalidade e procedência desses recursos, bem como de autorização prévia da GTI para sua utilização nas dependências da SESA.

É dever de todo o servidor público e demais colaboradores da SESA:

a) cumprir os termos descritos nessa Norma assim como a PETI;
b) assumir a responsabilidade pelos ativos e informações que estejam sob sua custódia, não podendo em qualquer tempo ou sob qualquer propósito, apropriar-se dessas informações, limitando-se aos direitos e permissões concedidos para execução de suas atividades;
c) reportar Incidentes de Segurança da Informação, sejam supostos ou evidenciados, devendo os mesmos serem comunicados imediatamente a GTI;
d) não interferir, obstruir ou dissuadir outros servidores e/ou colaboradores a agir de forma segura ou reportar incidentes de segurança da informação;
e) ter ciência de que a GTI está autorizada a resolver ou fazer reportes externos dos incidentes de segurança da informação ocorridos nas áreas sob a responsabilidade da SESA;
f) ter ciência de que suas solicitações, relativas a incidentes, novas instalações, manutenções ou configurações físicas ou lógicas em ambientes computacionais nas áreas sob a responsabilidade da SESA, devem ser submetidas exclusivamente a área

responsável (GTI), cuja implementação e/ou resolução é de exclusiva responsabilidade dessa mesma área competente.

A GTI terá autonomia para notificar infratores em casos de uso indevido dos recursos de TIC e dar ciência ao superior hierárquico responsável pelos mesmos.

A realização de inspeções mais detalhadas, no sentido de avaliar uma situação de uso indevido dos recursos, depende de autorização expressa do superior hierárquico dos envolvidos, e em casos de reincidência, do Secretário de Estado da Saúde, aos quais será dada a ciência dos resultados obtidos pelo procedimento.

4.2 - ACESSO FÍSICO

As áreas físicas, restritas ou protegidas de todas as unidades que compõem a SESA devem ser:

a) divididas em perímetros de segurança e o acesso às áreas consideradas como restritas ou protegidas sejam controladas por sistema de acesso, registradas, monitoradas e sujeitas a auditoria;

b) frequentadas por servidores públicos e colaboradores, exclusivamente providos de identificação funcional oficial (crachá) utilizada em local visível, não podendo nem mesmo ser compartilhada, cabendo ressaltar que a mesma é pessoal e intransferível e seu uso e ações são de inteira responsabilidade do titular da credencial;

c) providas de registro para todos os acessos físicos, inclusive fora do horário comercial, conforme perfil de acesso, privilégios atribuídos e autorizado pelo gestor funcional do servidor público e/ou colaborador e o gestor das áreas físicas a que o mesmo terá acesso;

d) consultadas com antecedência através de seus gestores para solicitações de acesso físico realizadas pelos colaboradores, informando prazo de vigência e aprovadas pelo gestor das áreas físicas a que os mesmos terão acesso, além da permissão ser concedida somente quando os colaboradores estiverem acompanhados por um funcionário responsável autorizado a acessar tais áreas, delegando ao mesmo funcionário a responsabilidade pelo colaborador, a partir da liberação do acesso, e durante o período em que esse aí permanecer;

e) monitoradas para que nenhum equipamento possa ingressar nas áreas da SESA, sem o devido controle e registro, incluindo-se equipamentos pessoais de fornecedores, terceiros, visitantes ou quaisquer outros;

f) controladas de maneira que qualquer pessoa fique impedida de sair das instalações das áreas restritas e protegidas da SESA com equipamentos ou objetos de propriedade da mesma, sem autorização expressa e escrita dos gestores desses ativos, assim como registro e controle devidamente documentados;

4.3 - ACESSO LÓGICO

O acesso lógico aos sistemas, recursos, serviços e informações:

a) é definido nessa Norma como autenticação e login/logon;
b) deve ser concedido, apenas, sob autorização do gestor das informações pertinentes;
c) deve ser controlado, registrado, monitorado e sujeito a auditoria e bloqueio, a qualquer momento, sem prévio consentimento, conforme definições e interesses exclusivos da SESA;
d) é vedado quando não autorizado, nos casos de tentativa de fraudar autenticação de usuário, segurança de qualquer equipamento de TIC ou sistema da rede corporativa;
e) devem ser compatíveis com as reais necessidades de cada usuário, restringindo qualquer outro acesso compreendido como desnecessário para a realização de suas atividades profissionais;
f) deve possuir um processo oficial para registro da concessão de acesso, a qual deve ser obtida através de autorização formal do gestor e em seguida encaminhada para área responsável;
g) devem ser conectados ou instalados na infraestrutura tecnológica das unidades que compõem a SESA, equipamentos ou sistemas devidamente homologados e autorizados pela GTI, não sendo permitida a utilização de software ou hardware não adquirido oficialmente ou sem autorização expressa, inclusive os que desrespeitarem os direitos legais de propriedade e uso;
h) é vedado tentar e obter acesso não autorizado, tais como tentativa de fraudar autenticação de usuário ou segurança de qualquer equipamento de TIC da rede corporativa;
i) deve ser revisto, periodicamente, pelo gestor do setor, quanto às permissões, retificando ou descontinuando quando do desligamento ou realocação de funções de servidores e/ou colaboradores.
j) deve ser informado, mensalmente, pela Gerência de Recursos Humanos da SESA à GTI todos os desligamentos e transferências de servidores da SESA.

Todos os servidores e colaboradores devem zelar pela integridade e segurança das informações que estejam sob sua custódia.

4.4 - CLASSIFICAÇÃO DA INFORMAÇÃO

Toda informação gerada ou sob a responsabilidade da SESA, deve:

a) por padrão, seguir os critérios de propriedade e responsabilidade adotados no item 4.1 dessa política;

b) ser classificada de forma clara quanto ao seu grau de sigilo, para determinar as medidas de proteção necessárias, visando agilizar o processo de tratamento das informações e otimizar os custos com a sua proteção;

c) receber o tratamento (armazenamento, cópia, remoção, descarte, troca, transmissão, manuseio, entre outros) e identificação adequados;

d) estar coerente com a importância estratégica e em conformidade com o negócio da SESA;

e) considerar as implicações que um determinado nível de criticidade trará para os usuários, e caso haja conflito entre a necessidade de controle de segurança e um requisito do negócio, prevalecerá esse último;

f) ser avaliada mediante uma estimativa dos prejuízos que a divulgação não autorizada possa causar aos interesses do negócio da SESA;

g) ser classificada no momento em que for gerada ou adquirida pelo proprietário; na impossibilidade do mesmo ser o gerador, esse, deve designar um substituto e instruí-lo previamente sobre como classificá-la e/ou reclassificá-la. Na ausência do proprietário, o superior hierárquico será o responsável;

h) ser preservada pelos custodiantes e seus usuários (servidores públicos e/ou colaboradores) durante todo o seu processo de uso;

i) ser classificada de maneira explícita, sem eximir o proprietário, o custodiante, os funcionários e/ou os colaboradores das suas responsabilidades quanto a ausência referente ao nível de sensibilidade da informação;

j) estar autorizada antes que sejam disponibilizadas e/ou divulgadas, para qualquer finalidade e, deve assegurar que os mesmos tenham condições de manter o grau de sigilo conforme exigências;

k) ser cuidada e tratada quando sensível, e mantida de acordo com o grau de sigilo, ainda que tenha sido cedida à SESA, independente de possuir classificação ou não;

l) ter a sua classificação e/ou reclassificações registradas, quando aplicável, enfatizando a responsabilidade específica dos servidores e/ou dos colaboradores autorizados.

4.5 - UTILIZAÇÃO DA SENHA

A criação e a utilização da senha devem seguir os critérios de:

a) tamanho de 8 (oito) a 14 (quatorze) caracteres;
b) composição de letras maiúsculas, minúsculas, caracteres especiais (ex.: #, &, ?, etc.) e números (ex.: 1, 2, 3, etc.);
c) não escolher composições óbvias baseadas em: datas de aniversário e nascimento, nomes (carro, animais de estimação, grau de parentesco), apelidos, palavras contidas em dicionários, dentre outros;
d) não escolher caracteres idênticos consecutivos, todos numéricos ou todos alfabéticos sucessivos;
e) não reutilizar as últimas 04 (quatro) senhas;
f) memorização e nunca registradas em papel ou digitalmente ou em qualquer outro meio que coloque em risco a descoberta da senha por outro usuário;
g) expiração periódica e quando requisitada deverá ser renovada;
h) não compartilhar e proteger o sigilo de suas credenciais de acesso (identificações/senhas);
i) assumir a responsabilidade por todas as transações efetuadas com sua senha.

4.6 - PROTEÇÃO CONTRA VÍRUS

Para manter a rede e a estação de trabalho com riscos mínimos, os usuários:

a) devem certificar-se de que há um software de antivírus instalado;
b) não podem alterar e/ou desativar a configuração do antivírus;
c) devem comunicar todo e qualquer problema relativo ao antivírus à GTI;
d) antes de abrir qualquer arquivo em mídias removíveis, devem executar o antivírus para evitar danos.

4.7 - UTILIZAÇÃO DO CORREIO ELETRÔNICO

4.7.1. Dispõe sobre a padronização, disponibilização e utilização dos Serviços de Correio Eletrônico Oficial da SESA, visando disciplinar a troca de mensagens eletrônicas e estabelecer critérios para formação de nomes para composição dos endereços eletrônicos oficiais e:

a) seu sigilo é inviolável e somente será quebrado mediante ordem judicial ou legislações cabíveis;
b) seu uso está sujeito à monitoração e auditoria pela área responsável;

c) concessões e revogações de acesso devem ser autorizadas pelo gestor da área do servidor e ou colaborador por meio de uma solicitação formal desse serviço à área responsável;

d) nos casos em que for comprovada a inatividade de acesso por um período superior a 180 (cento e oitenta) dias, a GTI terá autonomia para revogar o acesso do servidor e ou colaborador, e excluí-lo quando o período for superior 210 (duzentos e dez) dias;

e) o endereço de e-mail a ser disponibilizado, é de uso pessoal, intransferível e para o desenvolvimento das atividades profissionais;

f) os usuários devem excluir de suas caixas postais as mensagens recebidas e/ou enviadas que não tenham mais utilidade para o desenvolvimento de suas atividades profissionais;

g) a utilização do correio eletrônico será limitada por quota de utilização, de acordo com as definições do Órgão provedor desse serviço.

4.7.2. É vedado:

a) enviar mensagens com o conteúdo e/ou remetente alterado ou falsificado;

b) enviar, transmitir, disseminar indiscriminadamente informações sigilosas, segredos de negócios da SESA;

c) enviar, transmitir ou disseminar conteúdo relacionado a correntes, preconceito, pedofilia, pornográfico e/ou boatos, que possam caracterizar a mensagem eletrônica (e-mail) ou o domínio de origem como Spammer;

d) enviar, disseminar, armazenar ou manusear anúncios pessoais e comerciais, promoções e propagandas;

e) invadir a privacidade de usuários através do acesso não autorizado a sua caixa postal ou sem respaldo legal;

f) enviar, disseminar e/ou armazenar sistemas (*softwares*, programas, aplicativos ou códigos) ou arquivos de imagem, som, ou quaisquer outros que se contraponham aos direitos de uso e/ou propriedade, explorem ou verifiquem vulnerabilidades na infraestrutura tecnológica, ou possam prejudicar a manutenção da confidencialidade, integridade e disponibilidade das informações;

g) cadastrar contas de correio eletrônico corporativo (@saude.es.gov.br) em quaisquer sites, sobretudo para fins pessoais;

4.8 - UTILIZAÇÃO DA INTERNET

A Internet é um recurso corporativo de propriedade da SESA e:

a) o usuário deve conduzir adequadamente o uso da Internet, respeitando direitos autorais, regras de licenciamento de softwares, direitos de propriedade, privacidade e proteção de propriedade intelectual;
b) o acesso à Internet, por meio da rede corporativa, deve ser efetuado somente por equipamentos autorizados pela GTI;
c) a utilização de softwares de comunicação instantânea para uso externo tais como ICQ, Microsoft Messenger e afins, é permitida somente em casos excepcionais, mediante solicitação formal, informando os motivos e o período necessário, aprovada pelo Gestor da Unidade Administrativa e encaminha a GTI;
d) a utilização de softwares de comunicação instantânea para uso interno é permitida somente através de ferramenta padronizada e controlada pela GTI;
e) não é permitido acessar, armazenar, divulgar e repassar qualquer material ligado à pornografia, pedofilia, jogos e de conteúdo ilícito ou preconceituoso, tais como racismo, homofobia, religião entre outros;
f) não é permitido, premeditadamente, efetuar download/upload ou propagar qualquer tipo de conteúdo malicioso (Malware, Vírus, Worm, Trojan, Keylogger, Screenlogger, Spyware, Adware, Backdoor, Exploit, Sniffer, Port Scanner, Bot, Rootkit) bem como spam e conteúdos similares;
g) não é permitido utilizar programas ou acessar páginas de bate-papo (chat) de qualquer natureza, exceto para desempenho de sua atividade profissional;
h) não é permitido utilizar programas para download/upload de arquivos como Peer-to-peer e Streaming de qualquer natureza, exceto para desempenho de sua atividade profissional;
i) deve ser utilizado somente para o desenvolvimento e capacitação profissional.

4.9 - ARMAZENAMENTO DAS INFORMAÇÕES NA REDE / BACKUP

4.9.1. Toda a informação digital que pertença ou tenha sido criada com os recursos tecnológicos da SESA deve:

a) ser armazenada de acordo com as políticas adotadas pela GTI. Essas devem estar em constante atualização, estando sujeitas às melhores práticas de mercado e aos métodos e rotinas de backup;
b) ser zelada por todos os servidores e colaboradores da SESA, objetivando sua integridade e segurança, enquanto estejam sob sua custódia.

4.9.2. A GTI não será responsabilizada pela perda dos dados armazenados em mídias removíveis ou no disco rígido (HD) local da estação de trabalho.

4.10 - MESA LIMPA

Materiais utilizados durante o trabalho que contenham informações sensíveis, com ou sem classificação, quando não estiverem em uso, devem:

a) ser mantidos em locais seguros (idealmente em armário, cofre, gavetas ou outras formas de mobília segura que possam ser trancadas com chave ou segredo) de modo a impedir acesso não autorizado, perda, furto ou alteração das informações;
b) estar sempre organizados de maneira adequada;
c) considerar também o conceito de tela e mesa limpas, pois quando o usuário não estiver utilizando a informação, a mesma não deve ficar exposta.

4.11 - AQUISIÇÃO DE EQUIPAMENTOS E CONTRATAÇÃO DE SERVIÇOS

Todas as solicitações para aquisição de equipamentos, contratação de serviços e demais recursos de TIC, ou de substituição dos existentes, devem ser encaminhadas à GTI para análise prévia sujeita aos critérios de razoabilidade e padronização adotados pela SESA. Após os devidos ajustes que se fizerem necessários, devem seguir para análise financeira e demais trâmites legais.

5 - PROIBIÇÕES

É estritamente proibido a todos servidores e colaboradores da SESA:

a) armazenar arquivos que não estejam relacionados às rotinas de trabalho;
b) conectar qualquer dispositivo não autorizado pela GTI às estações de trabalho;
c) conectar qualquer dispositivo na rede corporativa da SESA sem autorização da GTI;
d) violar os lacres dos dispositivos;
e) alterar a configuração de hardware e de software dos dispositivos sem autorização da GTI;
f) deixar dispositivos portáteis da SESA, tais como notebooks, tablets e similares, desprotegidos em locais de alto risco de furto e roubo, como por exemplo, locais públicos, eventos, hotéis, carros, entre outros;

g) utilizar qualquer dispositivo para jogos ou outras atividades estranhas às rotinas de trabalho.

Toda movimentação de dispositivos, quando ainda não autorizada, deve ser comunicada aos setores responsáveis, principalmente à GTI para que suas permissões sejam revistas.

6 - PENALIDADES

O descumprimento das disposições contidas nessa Norma caracteriza infração funcional, a ser apurada em Processo Administrativo Disciplinar;

A autoridade que determinar a instauração de Processo Administrativo Disciplinar contra servidor ou colaborador da SESA pode requisitar a GTI a suspensão cautelar ou bloqueio da correspondente autorização de uso dos recursos de TIC dos envolvidos;

7 - RESPONSABILIDADES

7.1 - USUÁRIOS

Utilizar adequadamente os recursos de TIC disponibilizados pela SESA, respeitando as normas e regulamentos vigentes;

Armazenar arquivos e informações conforme as políticas adotadas pela GTI;

Reportar incidentes de segurança da informação à GTI;

Zelar pela integridade física dos equipamentos colocados à sua disposição, evitando submetê-los a condições de risco e mantendo-os afastados de líquidos, alimentos ou qualquer material ou utensílio que possa danificá-los;

Devolver todos os dispositivos da SESA que estiverem sob sua responsabilidade, quando do desligamento da instituição.

7.2 - GERENTES E DEMAIS CHEFIAS

Orientar os usuários sob sua coordenação para o uso adequado dos recursos de TIC disponibilizados pela SESA;

Monitorar as atividades de colaboradores e contratados sob sua responsabilidade;

Monitorar a utilização de mídias particulares para armazenamento de informações da SESA;

Reportar imediatamente à GTI qualquer incidente ou hipótese de incidente de segurança da informação que venham a tomar ciência.

7.3 - GTI

Instalar, configurar, corrigir e manter atualizados os recursos de TIC disponibilizados pela SESA;

Analisar os incidentes de segurança da informação e recomendar ações corretivas e preventivas, executando-as quando necessário;

Permitir, quando necessário e autorizado pela autoridade competente, o uso de mídias particulares para armazenar dados da SESA;

Verificar a conformidade com o estabelecido nesta norma e recomendar as ações necessárias.

8 - DISPOSIÇÕES FINAIS

Os casos excepcionais a essa Norma devem ser submetidos para análise e parecer da GTI. Caso necessário, deverão ser encaminhados ao Secretário de Estado de Saúde para conhecimento e deliberação.

A SESA se reserva o direito de revogar a autorização de uso e outros privilégios de qualquer usuário que viole essa Norma.

9 - GLOSSÁRIO

Para efeito do disposto nesta Instrução Normativa, consideram-se:

Antivírus: Software que permite identificar e eliminar vírus em computadores;

Arquivo: Conjunto de informações concatenadas, passível de armazenamento em meio digital;

Ativo de rede: Equipamentos básicos que mantêm uma rede local em funcionamento. São equipamentos como Switches, Roteadores, Hubs Conversores de Mídia, Cameras IP, Placas de Rede, Modems, access points, dentre outros;

Backup: Cópia de segurança de dados feita para salvaguardar arquivos;

Correio Eletrônico: Serviço de envio e recebimento de mensagens em meio digital, compreendendo softwares e equipamentos centrais de processamento e de manutenção de caixas postais;

Dispositivo de TIC: Qualquer dispositivo de processamento eletrônico de informações, incluindo servidores de rede, ativos de rede, estações de trabalho, computadores ou microcomputadores e seus respectivos componentes e acessórios como: mouse, teclado, monitor, impressora, scanner, etc;

Estação de trabalho: Computadores individuais através dos quais os usuários acessam a rede local. Todos os computadores, notebooks e tablets da SESA, interligados ou não a sua rede local são considerados estações de trabalho ou dispositivos de trabalho;

GTI: Gerência de Tecnologia da Informação, subordinada a Subsecretaria de Estado da Saúde para Assuntos Administrativos e de Financiamento da Atenção à Saúde da SESA;

Hardware: Todo e qualquer dispositivo físico em um equipamento de TIC. Exemplo: monitor, gabinete, impressora, mouse, unidade de CD, unidade de DVD, entre outros;

Incidente de Segurança da Informação: Indicação de eventos, indesejados ou inesperados, que podem ameaçar a Segurança da Informação;

Internet: Conglomerado de redes em escala mundial de milhões de computadores interligados pelo protocolo de comunicação TCP/IP que permite o acesso a informações e todo tipo de transferência de dados. Possui ampla variedade de recursos e serviços, incluindo documentos interligados por meio de hiperligações da World Wide Web (Rede de Alcance Mundial), e a infraestrutura para suporte de correio eletrônico e serviços como comunicação instantânea e compartilhamento de arquivos;

Keylogger: Malware capaz de capturar e armazenar as teclas digitadas pelo usuário no teclado de um computador. Normalmente, a ativação do keylogger é condicionada a uma ação prévia do usuário, como, por exemplo, após o acesso a um site de comércio eletrônico ou Internet Banking, para a captura de senhas bancárias ou números de cartões de crédito;

Login/Logon: Ato de efetuar autenticação para liberação de acesso a sistema computacional;

Malware: Software projetado para atentar contra a segurança de equipamentos de TIC, normalmente por meio de exploração de alguma vulnerabilidade do equipamento ou de algum software nele instalado;

Mídias: Meio físico utilizado para armazenar dados, tais como fitas, discos, CDs, entre outros;

PETI: Política Estadual de Tecnologia da Informação do Governo do Estado do Espírito Santo, instituída pelo Decreto 2991-R de 05 de abril de 2012;

Rede Local: Conjunto de computadores e outros dispositivos interligados entre si, que compartilham informações ou recursos físicos e lógicos da SESA como: dados, impressoras, mensagens (e-mails), entre outros;

Screenlogger: forma avançada de keylogger, capaz de armazenar a posição do cursor e a tela apresentada no monitor, nos momentos em que o mouse é clicado, ou armazenar a região que circunda a posição onde o mouse é clicado;

Segurança da Informação: Proteção dos sistemas de informação contra a negação de serviço a usuários autorizados, assim como contra a intrusão, e a modificação desautorizada de dados ou informações, armazenados, em processamento ou em trânsito, abrangendo, inclusive, a

segurança dos recursos humanos, da documentação e do material, das áreas e instalações das comunicações e computacional, assim como as destinadas a prevenir, detectar, deter e documentar eventuais ameaças a seu desenvolvimento;

SESA: Secretaria de Estado da Saúde;

Sistema Operacional: Software ou conjunto de programas que responde pelo controle da alocação dos recursos do computador, como memória, tempo de processador, espaço em disco e outros dispositivos;

Site/Sítio: Conjunto articulado de informações, identificado por um domínio e como tal acessível por meio da Internet;

Software: Conjunto de comandos lógicos, escritos em linguagem específica, para execução em equipamentos de TIC;

Spyware: Software com o objetivo de monitorar atividades de um sistema e enviar as informações coletadas para terceiros, geralmente são usadas de forma dissimulada, não autorizada e maliciosa;

Tablet: Dispositivo com tela sensível ao toque (touchscreen) em formato de prancheta com recursos de acesso à Internet, visualização de fotos, vídeos, leitura de livros, jornais e revistas dentre outros;

TIC: Tecnologia da Informação e Comunicação;

Trojan: Malware que se passa por um "presente" (por exemplo, cartões virtuais, álbum de fotos, protetor de tela, jogo, etc.) que além de executar funções para as quais foi aparentemente projetado, também executa outras funções normalmente maliciosas e, sem o conhecimento do usuário, captura suas informações e as envia à outra entidade pela Internet;

Usuário: Todo aquele que exerça, ainda que transitoriamente e sem remuneração, por eleição, nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função pública na SESA;

Vírus: Malware que se propaga inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos de um computador. Depende da execução de arquivos hospedeiros para que possa se tornar ativo e continuar o processo de infecção;

Worm: Malware capaz de se propagar automaticamente através de redes, enviando cópias de si mesmo para outros computadores. Diferente do vírus, o worm não embute cópias de si mesmo em outros programas ou arquivos e não necessita ser explicitamente executado para

se propagar. Sua propagação se dá através da exploração de vulnerabilidades existentes ou falhas na configuração de softwares instalados em computadores;

Adware: Software especificamente projetado para apresentar propagandas. Muito comum aparecerem na hora de instalar um programa. Sua inclusão tem como objetivo o lucro através da divulgação;

Backdoor: Malware que permite a um invasor retornar a um computador comprometido. Normalmente este programa é colocado de forma a não ser notado;

Exploit: Malware projetado para explorar uma vulnerabilidade existente em um software de computador;

Sniffer: Software que tem como objetivo capturar e armazenar dados trafegados em uma rede de computadores. Pode ser usado por um invasor para capturar informações sensíveis (como senhas de usuários), em casos onde esteja sendo utilizadas conexões inseguras, ou seja, sem criptografia. Deixa a placa de rede em modo promíscuo;

Port Scanner: Software que efetua varreduras em redes de computadores, com o objetivo de identificar computadores ativos e os serviços disponibilizados por esses. Permite associar possíveis vulnerabilidades aos serviços habilitados em um computador;

Bot: Malware que além de incluir funcionalidades de worms, dispõe de mecanismos de comunicação com o invasor, permitindo que o programa seja controlado remotamente. O invasor, ao se comunicar com o Bot, pode orientá-lo a desferir ataques contra outros computadores, furtar dados, enviar spam, etc;

Rootkit: Conjunto de programas com o objetivo de esconder e assegurar a presença de um invasor em um computador comprometido;

Spam: Termo de origem inglesa cujo significado designa uma mensagem eletrônica recebida mas não solicitada pelo usuário. O conteúdo de um spam é normalmente uma mensagem publicitária que tem o objetivo de divulgar os serviços ou produtos de alguma empresa a uma grande massa de usuários de e-mail;

Sistema Corporativo: Sistema de uso coletivo da organização;

Download: Transferência de dados de um computador remoto para um computador local. Tais arquivos podem danificar o computador, ou até mesmo toda a rede local, caso estejam infectados com malwares;

Upload: Envio de arquivos de um computador local para um computador remoto. Processo inverso a Download;

Peer-to-peer: Software de compartilhamento de arquivos que possibilita sua distribuição em rede, permitindo o acesso de qualquer usuário a este recurso;

Streaming: Forma de distribuir informação multimídia numa rede através de pacotes, freqüentemente utilizada para distribuir conteúdo multimídia através da Internet. Permite que um usuário reproduza mídia protegida por direitos autorais na Internet sem a violação dos direitos, similar ao rádio ou televisão aberta. Consome grande parte da banda de acesso a internet nas redes locais;