Secretaria de Saúde do Estado do Paraná – SESA-PR

Política de Segurança da Informação

A Política de Segurança da Informação, também referida como PSI, é o documento que orienta e estabelece as diretrizes corporativas da Secretaria de Saúde do Estado do Paraná – SESA-Pr., para a proteção dos ativos de informação e a prevenção de responsabilidade legal para todos os usuários. Deve, portanto, ser cumprida e aplicada em todas as áreas da instituição.

A informação é um ativo que, como qualquer outro ativo importante para os negócios, tem um valor para a organização e, consequentemente, necessita ser adequadamente protegida. A Política de Segurança da Informação objetiva proteger a informação de diversos tipos de ameaça, para garantir a continuidade dos negócios minimizando os danos e maximizando o retorno dos investimentos e as oportunidades de negócio.

Com a intenção de aumentar a segurança da infraestrutura tecnológica direcionada ao atendimento ao cidadão, Regionais de Saúde, Hemepar, Hospitais, demais Unidades e Secretarias do Governo do Estado do Paraná, foi ELABORADA uma diretriz de Segurança da Informação visando a orientação dos usuários para a utilização dos ativos de tecnologia da informação disponibilizados. Este e outros documentos encontram-se disponíveis na intranet da SESA-Pr.

OBJETIVOS

Estabelecer diretrizes que permitam aos colaboradores e demais utilizadores dos sistemas informatizados da SESA-Pr, seguirem padrões de comportamento relacionados à segurança da informação adequados às necessidades de negócio e de proteção legal da instituição e do indivíduo.

Nortear a definição de diretrizes e procedimentos específicos de segurança da informação, bem como a implementação de controles e processos para seu atendimento.

Preservar as informações da Secretaria de Saúde do Estado do Paraná – SESA-Pr quanto à:

• **Integridade:** garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais.

• **Confidencialidade:** garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.

• **Disponibilidade:** garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

APLICAÇÕES DA PSI

As diretrizes aqui estabelecidas deverão ser seguidas por todos os colaboradores e demais utilizadores dos sistemas informatizados da SESA-Pr, bem como os prestadores de serviço, e se aplicam à informação em qualquer meio ou suporte.

Esta política dá ciência a cada colaborador de que os ambientes, sistemas, computadores e redes da instituição são monitorados e com geração de Log armazenados em área específica podendo ser consultado quando solicitado, com prévia informação, conforme previsto nas leis brasileiras.

É também obrigação de cada colaborador se manter atualizado em relação a esta PSI e aos procedimentos relacionadas, buscando orientação do seu gestor ou do Núcleo de Informática e Informações (NII) sempre que não estiver absolutamente seguro quanto à aquisição, uso e/ou descarte de informações.

PRINCÍPIOS DA PSI

Toda informação produzida ou recebida pelos colaboradores como resultado da atividade profissional contratada pela Secretaria de Saúde do Estado do Paraná – SESA-Pr pertence à referida instituição. As exceções devem ser explícitas e formalizadas em contrato entre as partes.

Os equipamentos de informática e comunicação, sistemas e informações são utilizados pelos colaboradores para a realização das atividades profissionais. O uso pessoal dos recursos não é permitido, salvo, prévia autorização da chefia imediata e desde que não prejudique o desempenho dos sistemas e serviços.

A SESA-Pr, por meio do NII, registra todo o uso dos sistemas e serviços, visando garantir a disponibilidade e a segurança das informações utilizadas.

REQUISITOS DA PSI

Para a uniformidade da informação, a PSI deverá ser comunicada a todos os colaboradores da SESA-Pr a fim de que a política seja cumprida dentro e fora da instituição.

Fica a critério da instituição a criação de um comitê multidisciplinar responsável pela gestão da segurança da informação, doravante designado como Comitê de Segurança da Informação.

Tanto a PSI quanto os procedimentos deverão ser revistos e atualizados periodicamente quando se fizerem necessárias, sempre que algum fato relevante ou evento motive sua revisão antecipada, conforme análise e decisão do Comitê de Segurança.

Deverá constar em todos os contratos da Secretaria de Saúde do Estado do Paraná – SESA-Pr o anexo de Acordo de Confidencialidade ou Cláusula de Confidencialidade, como condição imprescindível para que possa ser concedido o acesso aos ativos de informação disponibilizados pela instituição.

A responsabilidade em relação à segurança da informação deve ser comunicada na fase de contratação dos colaboradores, empresas e ou serviços. Todos os colaboradores devem ser orientados sobre os procedimentos de segurança, bem como o uso correto dos ativos, a fim de reduzir possíveis riscos.
Eles devem assinar um termo de responsabilidade.

Todo incidente que afete a segurança da informação deverá ser comunicado inicialmente ao NII e ele, se julgar necessário, deverá encaminhar posteriormente ao Comitê de Segurança da Informação para análise.

Um plano de contingência e a continuidade dos principais sistemas e serviços deverão ser implantados e testados no mínimo anualmente, visando reduzir riscos de perda de confidencialidade, integridade e disponibilidade dos ativos de informação.

Todos os requisitos de segurança da informação, incluindo a necessidade de planos de contingência, devem ser identificados na fase de levantamento de escopo de um projeto ou sistema, e justificados, acordados, documentados, implantados e testados durante a fase de execução.

Deverão ser criados e instituídos controles apropriados, trilhas de auditoria ou registros de atividades, em todos os pontos e sistemas em que a instituição julgar necessário para reduzir os riscos dos seus ativos de informação como, por exemplo, nas estações de trabalho, notebooks, nos acessos à internet, no correio eletrônico, nos sistemas comerciais e financeiros desenvolvidos pela SESA-Pr ou por terceiros.

Os ambientes de produção devem ser segregados e rigidamente controlados, garantindo o isolamento necessário em relação aos ambientes de desenvolvimento, testes e homologação.

A SESA-Pr exonera-se de toda e qualquer responsabilidade decorrente do uso indevido, negligente ou imprudente dos recursos e serviços concedidos aos seus colaboradores, reservando-se o direito de analisar dados e evidências para obtenção de provas a serem utilizadas nos processos investigatórios, bem como adotar as medidas legais cabíveis.

Esta PSI será implementada na SESA-Pr por meio de procedimentos específicos, obrigatórios para todos os colaboradores, independentemente do nível hierárquico ou função na instituição, bem como de vínculo empregatício ou prestação de serviço.

O não cumprimento dos requisitos previstos nesta PSI e dos requisitos de Segurança da Informação acarretará violação às regras internas da instituição e sujeitará o usuário às medidas administrativas e legais cabíveis.

DAS RESPONSABILIDADES ESPECÍFICAS

1 - Dos Colaboradores em Geral

Entende-se por colaborador toda e qualquer pessoa física, contratada CLT ou prestadora de serviço por intermédio de pessoa jurídica ou não, que exerça alguma atividade dentro ou fora da instituição. Será de inteira responsabilidade de cada colaborador, todo prejuízo ou dano que vier a sofrer ou causar à SESA -Pr e/ou a terceiros, em decorrência da não obediência às diretrizes e regras aqui referidas.

2 - Dos Colaboradores em Regime de Exceção (Temporários)

Devem entender os riscos associados à sua condição especial e cumprir rigorosamente o que está previsto no aceite concedido pelo Comitê de Segurança da Informação. A concessão poderá ser revogada a qualquer tempo se for verificado que a justificativa de motivo de negócio não mais compensa o risco relacionado ao regime de exceção ou se o colaborador que o recebeu não estiver cumprindo as condições definidas no aceite.

3 - Dos Gestores de Pessoas e/ou Processos

Ter postura exemplar em relação à segurança da informação, servindo como modelo de conduta para os colaboradores sob a sua gestão. Atribuir aos colaboradores, na fase de contratação e de formalização dos contratos individuais de trabalho, de prestação de serviços ou de parceria, a responsabilidade do cumprimento da PSI da SESA-Pr. Exigir dos colaboradores a assinatura do Termo de Compromisso e Ciência, assumindo o dever de seguir as diretrizes estabelecidas, bem como se comprometendo a manter sigilo e confidencialidade, mesmo quando desligado, sobre todos os ativos de informações da SESA-Pr. Antes de conceder acesso às informações da instituição, exigir a assinatura do Acordo de Confidencialidade dos colaboradores casuais e prestadores de serviços que não estejam cobertos por um contrato existente, por exemplo, durante a fase de levantamento para apresentação de propostas comerciais. Adaptar as diretrizes, os processos, procedimentos e sistemas sob sua responsabilidade para atender a esta PSI, bem como aos termos das regras e procedimentos que porventura sejam aplicadas a instituição.

4 - Dos Custodiantes da Informação

4.1 - Da Área de Tecnologia da Informação

Testar a eficácia dos controles utilizados e informar aos gestores os riscos residuais.

Acordar com os gestores o nível de serviço que será prestado e os procedimentos de resposta aos incidentes.

Configurar os equipamentos, ferramentas e sistemas concedidos aos colaboradores com todos os controles necessários para cumprir os requerimentos de segurança estabelecidos por esta PSI, e em suas diversas versões quando se aplicarem, pelas diretrizes de Segurança da Informação complementares.

Os administradores dos sistemas informatizados e ativos de rede podem, pela característica de seus privilégios como usuários, acessar os arquivos e dados de outros usuários. No entanto, isso só será permitido quando for necessário para a execução de atividades operacionais e ou solicitados formalmente (chamado, ofício e ou e-mail) sob sua responsabilidade como, por exemplo, a realização de auditorias ou testes no ambiente.

Segregar as funções administrativas, operacionais e terceirizadas a fim de restringir ao mínimo necessário os poderes de cada indivíduo e eliminar, ou ao menos reduzir, a existência de pessoas que possam excluir os logs e trilhas (log) de auditoria das suas próprias ações.

Garantir segurança especial para sistemas com acesso público, incluindo o ambiente terceirizado, Wi-Fi público e todo e qualquer serviço de self-service feito pelo cidadão, fazendo guarda de evidências que permitam a rastreabilidade para fins de auditoria ou investigação.

Gerar e manter as trilhas (log) para auditoria com nível de detalhe suficiente para rastrear possíveis falhas e fraudes. Para as trilhas (log) geradas e/ou mantidas em meio eletrônico, implantar controles de integridade para torná-las juridicamente válidas como evidências.

Administrar, proteger e testar as cópias de segurança dos programas e dados relacionados aos processos críticos e relevantes para A Secretaria de Saúde do Estado do Paraná.

Implantar controles que gerem registros auditáveis para retirada e transporte de mídias das informações custodiadas pela TI quando for aplicável, nos ambientes totalmente controlados por ela.

O gestor da informação deve ser previamente informado sobre o fim do prazo de retenção, para que tenha a alternativa de alterá-lo antes que a informação seja definitivamente descartada pelo custodiante.

Quando ocorrer movimentação interna dos ativos de TI, garantir que as informações de um usuário não serão removidas de forma irrecuperável antes de disponibilizar o ativo para outro usuário. Quando porventura o usuário informar da existência de informações relevantes e ou importantes para o andamento das atividades da SESA -Pr.

Planejar, implantar, fornecer e monitorar a capacidade de armazenagem, processamento e transmissão necessários para garantir a segurança requerida pelas áreas de negócio. Atribuir cada conta ou dispositivo de acesso a computadores, sistemas, bases de dados e qualquer outro ativo de informação a um responsável identificável como pessoa física, sendo que:

• os usuários (logins) individuais de funcionários serão de responsabilidade do próprio funcionário.

• os usuários (logins) de terceiros serão de responsabilidade do gestor da área contratante.

Proteger continuamente todos os ativos de informação da empresa contra código malicioso, e garantir que todos os novos ativos só entrem para o ambiente de produção após estarem livres de código malicioso e/ou indesejado.

Garantir que não sejam introduzidas vulnerabilidades ou fragilidades no ambiente de produção da empresa em processos de mudança, sendo ideal a auditoria de código e a proteção contratual para controle e responsabilização no caso de uso de terceiros.

Definir as regras formais para instalação de software e hardware em ambiente de produção institucionais, bem como em ambientes administrados e operados por terceiros, exigindo o seu cumprimento dentro da instituição.

Realizar auditorias periódicas de configurações técnicas e análise de riscos.

Responsabilizar-se pelo uso, manuseio, guarda de assinatura e certificados digitais quando a instituição fizer uso.

Garantir, da forma mais rápida possível, com solicitação formal, o bloqueio de acesso de usuários por motivo de desligamento da instituição, incidente, investigação ou outra situação que exija medida restritiva para fins de salvaguardar os ativos da instituição.

Garantir que todos os servidores, estações e demais dispositivos com acesso à rede da instituição operem com o relógio sincronizado com os servidores de tempo oficiais do governo brasileiro.

Monitorar o ambiente de TI, gerando indicadores e históricos de:

• uso da capacidade instalada da rede e dos equipamentos;

• tempo de resposta no acesso à internet e aos sistemas críticos da SESA-Pr;

• períodos de indisponibilidade no acesso à internet e aos sistemas críticos da SESA-Pr;

• incidentes de segurança (vírus, trojans, furtos, acessos indevidos, e assim por diante) está atividade pode ser conjunta com outros setores e ou empresas prestadoras de serviços;

• atividade de todos os colaboradores durante os acessos às redes externas, inclusive internet (por exemplo: sites visitados, e-mails recebidos/enviados, upload/download de arquivos, entre outros);

4.2 - Da Área de Segurança da Informação

Propor as metodologias e os processos específicos para a segurança da informação, como avaliação de risco e sistema de classificação da informação.

Propor e apoiar iniciativas que visem à segurança dos ativos de informação da SESA-Pr.

Publicar e promover as versões da PSI e das diretrizes de Segurança da Informação aprovadas pelo Comitê de Segurança da Informação.

Promover a conscientização dos colaboradores em relação à relevância da segurança da informação para o negócio da SESA-Pr, mediante campanhas internas e externas, palestras, treinamentos e outros meios de endomarketing.

Apoiar a avaliação e a adequação de controles específicos de segurança da informação para novos sistemas ou serviços.

Analisar criticamente incidentes em conjunto com o Comitê de Segurança da Informação.

Apresentar as atas e os resumos das reuniões do Comitê de Segurança da Informação, destacando os assuntos que exijam intervenção do próprio comitê ou de outros membros da diretoria.

Manter comunicação efetiva com o Comitê de Segurança da Informação sobre assuntos relacionados ao tema que afetem ou tenham potencial para afetar a SESA-Pr.

Buscar alinhamento com as diretrizes corporativas da instituição.

4.3 - Do Comitê de Segurança da Informação

Deve ser formalmente constituído por colaboradores com nível hierárquico mínimo gerencial, nomeados para participar do grupo pelo período de um ano.

A composição mínima deve incluir um colaborador de cada uma das áreas da instituição bem como de suas regionais:

Deverá o Comitê de Segurança da Informação reunir-se formalmente pelo menos uma vez a cada seis meses. Reuniões adicionais devem ser realizadas sempre que for necessário deliberar sobre algum incidente grave ou definição relevante para o SESA-Pr.

O Comitê de Segurança da Informação poderá utilizar especialistas, internos ou externos, para apoiarem nos assuntos que exijam conhecimento técnico específico.

Cabe ao Comitê de Segurança da Informação:

• propor investimentos relacionados à segurança da informação com o objetivo de reduzir mais os riscos;

• propor alterações nas versões da PSI e a inclusão, a eliminação ou a mudança de regras complementares;

• avaliar os incidentes de segurança e propor ações corretivas;

• definir as medidas cabíveis nos casos de descumprimento da PSI e/ou das diretrizes de Segurança da Informação complementares.

5 - DO MONITORAMENTO E DA AUDITORIA DO AMBIENTE

Para garantir as regras mencionadas nesta PSI, bem como de sua versão especifica quando houver, a SESA-Pr poderá:

• implantar sistemas de monitoramento nas estações de trabalho, servidores, correio eletrônico, conexões com a internet, dispositivos móveis ou wireless e outros componentes da rede – a informação gerada por esses sistemas poderá ser usada para identificar usuários e respectivos acessos efetuados, bem como material manipulado;

• tornar públicas as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de exigência judicial, solicitação dos gestores ou por determinação do Comitê de Segurança da Informação;

• realizar, a qualquer tempo, inspeção física nas máquinas de sua propriedade;

• instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso.

•. Habilitar ou desabilitar o uso de dispositivos moveis nas estações, exemplo: entradas USB, CD-ROM, HD Externo, etc.

6 - BOAS PRÁTICAS DE COMUNICAÇÃO VERBAL DENTRO E FORA DA INSTITUIÇÃO

6.1. Cuidado ao tratar de assuntos da instituição dentro e fora do ambiente de trabalho, em locais públicos, ou próximos a visitantes, seja ao telefone ou com algum colega, ou mesmo fornecedor.

6.2. Evite nomes e tratativas de assuntos confidenciais, nestas situações, fora da empresa ou próximos a pessoas desconhecidas.

6.3. Caso seja extremamente necessária a comunicação de assuntos sigilosos em ambientes públicos, ficar atento as pessoas à sua volta que poderão usar as informações com o intuito de prejudicar a imagem da instituição e ou fazer uso em benefício próprio.

CORREIO ELETRÔNICO

O objetivo desta diretriz é informar aos colaboradores da SESA-Pr quais são as atividades permitidas e proibidas quanto ao uso do correio eletrônico corporativo.

O uso do correio eletrônico do SESA-Pr é para fins corporativos e relacionados às atividades do colaborador usuário dentro da instituição.

A utilização desse serviço para fins pessoais é proibida, para que não prejudique o andamento dos trabalhos da instituição e não cause impacto no tráfego da rede.

Acrescentamos que é proibido aos colaboradores o uso do correio eletrônico da SESA-Pr:

• enviar mensagens não solicitadas para múltiplos destinatários, exceto se relacionadas a uso legítimo da instituição;

• enviar mensagem por correio eletrônico pelo endereço de seu departamento ou usando o nome de usuário de outra pessoa ou endereço de correio eletrônico que não esteja autorizado a utilizar;

• enviar qualquer mensagem por meios eletrônicos que torne seu remetente e/ou a SESA-Pr ou suas unidades vulneráveis a ações civis ou criminais;

• divulgar informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização expressa e formal concedida pelo gestor, superior e ou por ordem judicial desse ativo de informação;

• falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários, com o objetivo de evitar as punições previstas;

• apagar mensagens pertinentes de correio eletrônico quando qualquer uma das unidades da SESA-Pr e ou setores correlatos estiverem sujeitos a algum tipo de investigação.

• produzir, transmitir ou divulgar mensagem que:

- ✓ Contenha qualquer ato ou forneça orientação que conflite ou contrarie os interesses da SESA-Pr;

- ✓ Contenha ameaças eletrônicas, como: spam, mail bombing, vírus de computador e outros;
- ✓ Contenha arquivos com código executável (.exe, .com, .bat, .pif, .js, .vbs, .hta, .src, .cpl, .reg, .dll, .inf) ou qualquer outra extensão que represente um risco à segurança;
- ✓ Vise obter acesso não autorizado a outro computador, servidor ou rede;
- ✓ Vise interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;
- ✓ Vise burlar qualquer sistema de segurança;
- ✓ Vise vigiar secretamente ou assediar outro usuário;
- ✓ Vise acessar informações confidenciais sem explícita autorização do proprietário;
- ✓ Vise acessar indevidamente informações que possam causar prejuízos a qualquer pessoa;
- ✓ Inclua imagens criptografadas ou de qualquer forma mascaradas;
- ✓ Contenha anexo(s) superior(es) a 10 MB para envio (interno e internet) e 10 MB para recebimento (internet)
- ✓ Tenha conteúdo considerado impróprio, obsceno ou ilegal;
- ✓ Seja de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico entre outros;
- ✓ Contenha perseguição preconceituosa baseada em sexo, raça, incapacidade física ou mental ou outras situações protegidas;
- ✓ Tenha fins políticos locais ou do país (propaganda política);
- ✓ Inclua material protegido por direitos autorais sem a permissão do detentor dos direitos.

As mensagens de correio eletrônico sempre deverão incluir assinatura com o seguinte formato:
• Nome do colaborador
• Gerência ou departamento
• Nome da instituição
• Telefone (somente telefone comercial)

INTERNET

Todas as regras atuais da SESA-Pr visam basicamente o desenvolvimento de um comportamento eminentemente ético e profissional do uso da internet. Embora a conexão direta e permanente da rede corporativa da instituição com a internet ofereça um grande potencial de benefícios, ela abre a porta para riscos significativos para os ativos de informação.

Qualquer informação que é acessada, transmitida, recebida ou produzida na internet está sujeita a divulgação e auditoria. Portanto, a SESA-Pr, em total conformidade legal, reserva-se o direito de monitorar e registrar todos os acessos a ela.

Os equipamentos, tecnologia e serviços fornecidos para o acesso à internet são de propriedade da instituição, que pode analisar e, se necessário, bloquear qualquer arquivo, site, correio eletrônico, domínio ou aplicação armazenados na rede/internet, estejam eles em disco local, na estação ou em áreas privativa da rede, visando assegurar o cumprimento de sua Política de Segurança da Informação.

A SESA-Pr, ao monitorar a rede interna, pretende garantir a integridade dos dados e programas. Toda tentativa de alteração dos parâmetros de segurança, por qualquer colaborador, sem o devido credenciamento e a autorização para tal, será julgada inadequada e os riscos relacionados serão informados ao colaborador e ao respectivo gestor. O uso de qualquer recurso para atividades ilícitas poderá acarretar as ações administrativas e as penalidades decorrentes de processos civil e criminal, sendo que nesses casos a instituição cooperará ativamente com as autoridades competentes.

A internet disponibilizada pela instituição aos seus colaboradores, independentemente de sua relação contratual, não pode ser utilizada para fins pessoais, para que não prejudique o andamento dos trabalhos nas unidades.

Como é do interesse da SESA-Pr que seus colaboradores estejam bem informados, o uso de sites de notícias ou de serviços, por exemplo, é aceitável, desde que não comprometa a banda da rede em horários estritamente comerciais, não perturbe o bom andamento dos trabalhos nem implique conflitos de interesse com os seus objetivos de negócio.

Somente os colaboradores que estão devidamente autorizados a falar em nome da SESA-Pr para os meios de comunicação poderão manifestar-se, seja por e-mail, entrevista on-line, podcast, seja por documento físico, entre outros.

Apenas os colaboradores autorizados pela instituição poderão copiar, captar, imprimir ou enviar imagens da tela para terceiros, devendo atender à diretriz interna de uso de imagens, à Lei de Direitos Autorais, à proteção da imagem garantida pela Constituição Federal e demais dispositivos legais.

É proibida a divulgação e/ou o compartilhamento indevido de informações de qualquer área e ou departamento da SESA-Pr em listas de discussão, sites ou comunidades de relacionamento, salas de bate-papo ou chat, comunicadores instantâneos ou qualquer outra tecnologia correlata que venha surgir na internet.

Os colaboradores com acesso à internet não podem fazer o download (baixar) programas de qualquer tipo sem providenciar e regularizar a licença e o registro desses programas, desde que autorizados pelo NII e o Comitê de Segurança da Informação.

O uso, a instalação, a cópia ou a distribuição não autorizada de softwares que tenham direitos autorais, marca registrada ou patente na internet são expressamente proibidos.

Qualquer software não autorizado baixado será excluído e ou removido pela equipe do NII sem a prévia comunicação.

Os colaboradores não poderão em hipótese alguma utilizar os recursos da SESA-Pr para fazer o download ou distribuição de software ou dados pirateados, atividade considerada delituosa de acordo com a legislação nacional.

O download e a utilização de programas de entretenimento, jogos ou músicas (em qualquer formato) não poderão ser realizados por usuários ou profissionais relacionadas a essas categorias. Para tal, será necessário a autorização bem como aquisição e pagamento de taxas que se fizerem necessárias para utilização no ambiente da instituição.

Mediante solicitação e aprovação da área técnica responsável, o uso de jogos será passível de concessão, em regime de exceção, quando eles tiverem natureza intrínseca às atividades de cursos relacionados ao desenvolvimento das atividades da SESA-Pr. Para tal, será necessário aquisição e pagamento das taxas que se fizerem necessárias.

Como regra geral, materiais de cunho sexual não poderão ser expostos, armazenados, distribuídos, editados, impressos ou gravados por meio de qualquer recurso. Caso seja necessário, grupos de segurança deverão ser criados para viabilizar esse perfil de usuário especial e seus integrantes definidos pelos respectivos gestores.

Colaboradores com acesso à internet não poderão efetuar upload (subida) de qualquer software licenciado à SESA-Pr ou de dados de sua propriedade aos seus parceiros e clientes, sem expressa autorização do responsável pelo software ou pelos dados.

Os colaboradores não poderão utilizar os recursos do SESA-Pr para deliberadamente propagar qualquer tipo de vírus, worm, cavalo de troia, spam, assédio, perturbação ou programas de controle de outros computadores.

O acesso a softwares peer-to-peer (Kazaa, BitTorrent e afins) não serão permitidos. Já os serviços de streaming (rádios on-line, canais de podcast e afins) serão permitidos a grupos específicos desde que autorizados pelos gestores e após análise de impacto do tráfego de dados na rede interna da SESA-Pr. Porém, os serviços de comunicação instantânea (MSN, ICQ e afins) não serão permitidos para nem um colaborador da SESA-Pr.

Não é permitido acesso a sites de proxy e ou Web Proxy ou outra URL destinada a burlar as regras de segurança do ambiente informatizado do SESA-Pr.

IDENTIFICAÇÃO

Os dispositivos de identificação e senhas protegem a identidade do colaborador usuário, evitando e prevenindo que uma pessoa se faça passar por outra perante a SESA-Pr e/ou terceiros.

O uso dos dispositivos e/ou senhas de identificação de outra pessoa constitui crime tipificado no Código Penal Brasileiro (art. 307 – falsa identidade).

*"**Art. 307** - Atribuir-se ou atribuir a terceira falsa identidade para obter vantagem, em proveito próprio ou alheio, ou para causar dano a outrem: Pena - detenção, de três meses a um ano, ou multa, se o fato não constitui elemento de crime mais grave."*

Tal diretriz visa estabelecer critérios de responsabilidade sobre o uso dos dispositivos de identificação e deverá ser aplicada a todos os colaboradores da SESA-Pr.

Todos os dispositivos de identificação utilizados na SESA-Pr, como o número de registro do colaborador, o crachá, as identificações de acesso aos sistemas, os certificados e assinaturas digitais e os dados biométricos têm de estar associados a uma pessoa física e atrelados inequivocamente aos seus documentos oficiais reconhecidos pela legislação brasileira.

O usuário, vinculado a tais dispositivos identificadores, será responsável pelo seu uso correto perante a instituição e a legislação (cível e criminal).

Todo e qualquer dispositivo de identificação é pessoal e intransferível, portanto, não poderá ser compartilhado, emprestado, vendido e ou qualquer outra forma de cessão com outras pessoas em nenhuma hipótese.

Se e quando existir o uso de login compartilhado por mais de um colaborador, a responsabilidade perante a SESA-Pr e a legislação (cível e criminal) será dos usuários que dele se utilizarem. Somente se for identificado conhecimento ou solicitação do gestor de uso compartilhado ele deverá ser responsabilizado.

É expressamente proibido o compartilhamento de login para garantir acesso aos sistemas informatizados da SESA-Pr.

É expressamente proibido o uso de login sem estar associado a um indivíduo (pessoa), não devem ser permitidos acessos a sistemas de nem uma espécie com logins associados a setores e ou terceirizados.

O Departamento de Recursos Humanos da SESA-Pr é o responsável pela emissão de login e pelo controle dos documentos físicos de identidade dos colaboradores (crachá). Ficando responsável o Departamento de Recursos Humanos a exclusão do login quando de sua saída da instituição. Bem como informar ao setor do NII solicitando a negação de acesso aos sistemas informatizados da SESA-Pr.

Cada gestor deve solicitar via chamado para o NII respeitando o fluxo já estabelecido as devidas permissões a pastas, sistemas informatizados e internet quando da entrada de um novo colaborador na instituição.

Devem ser distintamente identificados os visitantes, estagiários, empregados temporários, empregados regulares e prestadores de serviços, sejam eles pessoas físicas e/ou jurídicas. Ao realizar o primeiro acesso ao ambiente de rede local, o usuário deverá trocar imediatamente a sua senha conforme as orientações apresentadas.

Todos os usuários deverão ter senha de tamanho variável, possuindo no mínimo 8 (oito) caracteres alfanuméricos, utilizando caracteres especiais (@ # $ %) e variação entre caixa-alta e caixa-baixa (maiúsculo e minúsculo) sempre que possível. Já os usuários que possuem perfil de administrador ou acesso privilegiado deverão utilizar uma senha de no mínimo 15 (quinze) caracteres, alfanumérica, utilizando caracteres especiais (@ # $ %) e variação de caixa-alta e caixa-baixa (maiúsculo e minúsculo) obrigatoriamente.

É de responsabilidade de cada usuário a memorização de sua própria senha, bem como a proteção e a guarda dos dispositivos de identificação que lhe forem designados. Nunca anotar em papel ou “pendurar” no monitor, abaixo do teclado, bancada ou qualquer local visível a todos.

As senhas não devem ser anotadas ou armazenadas em arquivos eletrônicos (Word, Excel, etc.), compreensíveis por linguagem humana (não criptografados); não devem ser baseadas em informações pessoais, como próprio nome, nome de familiares, data de nascimento, endereço, placa de veículo, nome da empresa, nome do departamento; e não devem ser constituídas de combinações óbvias de teclado, como “abcdefgh”, “87654321”, “qwerty”, entre outras.

Após 3 (três) tentativas de acesso, a conta do usuário será bloqueada. Para o desbloqueio é necessário que o usuário entre em contato com o NII (3330-4554) da SESA-Pr. Deverá ser estabelecido um processo para a renovação de senha (confirmar a identidade).

Os usuários podem alterar a própria senha a qualquer momento que desejarem, e devem ser orientados a fazê-lo, ou caso suspeitem que terceiros obtiveram acesso indevido ao seu login/senha.

A periodicidade máxima para troca das senhas é 60 (sessenta) dias, não podendo ser repetidas as 3 (três) últimas senhas. Os sistemas críticos e sensíveis para a instituição e os logins com privilégios administrativos devem exigir a troca de senhas a cada 30 dias. Os sistemas devem forçar quando possível a troca das senhas dentro desse prazo máximo.

Todos os acessos devem ser imediatamente bloqueados quando se tornarem desnecessários. Portanto, assim que algum usuário for demitido ou solicitar demissão ou por outro motivo precisar ausentar-se da instituição por um período maior que 30 (trinta) dias, o Departamento de Recursos Humanos deverá imediatamente bloquear o seu login e comunicar tal fato ao setor do NII, a fim de que essa providência seja tomada. Esta mesma conduta se aplica aos usuários cujo contrato ou prestação de serviços tenham-se encerrado, bem como aos usuários de testes e outras situações similares.

Caso o colaborador esqueça sua senha, ele deverá requisitar a troca ou comparecer à área técnica responsável para cadastrar uma nova, respeitando o fluxo já estabelecido.

COMPUTADORES E RECURSOS TECNOLÓGICOS

Os equipamentos disponíveis aos colaboradores são de propriedade da SESA-Pr, cabendo a cada um utilizá-los e manuseá-los corretamente para as atividades de interesse da instituição, bem como cumprir as recomendações constantes nos procedimentos operacionais fornecidos pelos gestores imediatos e ou contidos nos termos de responsabilidades de uso.

É proibido todo procedimento de manutenção física ou lógica, instalação, desinstalação, configuração ou modificação, sem o conhecimento prévio e o acompanhamento de um técnico do NII, ou de quem este determinar.

Os setores e ou Regionais, UN, Hospitais, Laboratórios entre outros que necessitarem fazer testes deverão solicitá-los previamente à NII, ficando responsáveis jurídica e tecnicamente pelas ações realizadas.

Todas as atualizações e correções de segurança do sistema operacional ou aplicativos somente poderão ser feitas após a devida validação no respectivo ambiente de homologação, e depois de sua disponibilização pelo fabricante ou fornecedor.

Os sistemas e computadores devem ter versões do software antivírus instaladas, ativadas e atualizadas permanentemente.

O usuário, em caso de suspeita de vírus ou problemas na funcionalidade, deverá acionar o departamento técnico responsável mediante registro de chamado no “Service Desk”.

A transferência e/ou a divulgação de qualquer software, programa ou instruções de computador para terceiros, por qualquer meio de transporte (físico ou lógico), somente poderá ser realizada com a devida identificação do solicitante, se verificada positivamente e estiver de acordo com a classificação de tal informação e com a real necessidade do destinatário.

Arquivos pessoais e/ou não pertinentes ao negócio da SESA-Pr (fotos, músicas, vídeos etc.), não deverão ser copiados/movidos para os drives de rede, pois podem sobrecarregar o armazenamento nos servidores / NAS e por conterem direitos autorais. Caso identificada a existência desses arquivos, eles poderão ser excluídos definitivamente por meio de comunicação prévia ao usuário.

Documentos imprescindíveis para as atividades dos colaboradores da instituição deverão ser salvos em drives de rede. Tais arquivos, se gravados apenas localmente nos computadores (por exemplo, no drive C: D:), não terão garantia de backup e poderão ser perdidos caso ocorra uma falha no computador, sendo, portanto, de responsabilidade do próprio usuário.

Os colaboradores da SESA-Pr e/ou detentores de contas privilegiadas não devem executar nenhum tipo de comando ou programa que venha sobrecarregar os serviços existentes na rede corporativa sem a prévia solicitação e a autorização da Coordenação do NII.

No uso dos computadores, equipamentos e recursos de informática, algumas regras devem ser atendidas.

• nem um dos computadores de uso individual deverão ter senha de BIOS para restringir o acesso de colaboradores não autorizados. Se houver a necessidade de impedir acesso ao equipamento via senha de BIOS deverá ser feito solicitação ao NII e ela definirá e se responsabilizara por esta senha.

• os colaboradores devem informar ao departamento técnico qualquer identificação de dispositivo estranho conectado ao seu computador.

• é vedada a abertura ou o manuseio de computadores ou outros equipamentos de informática para qualquer tipo de reparo que não seja realizado por um técnico do NII da SESA-Pr ou por terceiros devidamente contratados para o serviço.

• não devem existir acessos por modems internos ou externos para impedir a invasão/evasão de informações, programas, vírus. Em alguns casos especiais, conforme regra específica, será considerada a possibilidade de uso para planos de contingência mediante a autorização dos gestores das áreas e da área de informática.

• é expressamente proibido o consumo de alimentos, bebidas ou fumo na mesa de trabalho e próximo aos equipamentos.

• O colaborador deverá manter a configuração do equipamento disponibilizado pelo SESA-Pr, seguindo os devidos controles de segurança exigidos pela Política de Segurança da Informação e pelas diretrizes específicas da instituição, assumindo a responsabilidade como custodiante de informações.

• deverão ser protegidos por senha (bloqueados), nos termos previstos, todos os terminais de computador e impressoras quando não estiverem sendo utilizados.

• Todos os recursos tecnológicos adquiridos pela SESA-Pr devem ter imediatamente suas senhas padrões (default) alteradas.

• os equipamentos deverão manter preservados, de modo seguro, os registros de eventos, constando identificação dos colaboradores, datas e horários de acesso.

Acrescentamos algumas situações em que é proibido o uso de computadores e recursos tecnológicos da SESA-Pr.

• tentar ou obter acesso não autorizado a outro computador, servidor ou rede.

• burlar quaisquer sistemas de segurança.

• acessar informações confidenciais sem explícita autorização do proprietário.

• vigiar secretamente outrem por dispositivos eletrônicos ou softwares, como, por exemplo, analisadores de pacotes (sniffers).

• interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado.

• usar qualquer tipo de recurso tecnológico para cometer ou ser cúmplice de atos de violação, assédio sexual, perturbação, manipulação ou supressão de direitos autorais ou propriedades intelectuais sem a devida autorização legal do titular;

• hospedar pornografia, material racista ou qualquer outro que viole a legislação em vigor no país, a moral, os bons costumes e a ordem pública.

• utilizar software pirata, atividade considerada delituosa de acordo com a legislação nacional.

DISPOSITIVOS MÓVEIS

A SESA-Pr deseja facilitar a mobilidade e o fluxo de informação entre seus colaboradores. Por isso, permite o uso de equipamentos portáteis. Exclui-se notebook particulares, somente terá acesso a rede se passar o equipamento pelo processo de padronização, atualização e instalação de ferramentas de monitoramento.

Quando se descreve “dispositivo móvel” entende-se qualquer equipamento eletrônico com atribuições de mobilidade de propriedade da instituição, ou aprovado e permitido por sua área responsável pela tecnologia, como: Notebooks, Smartphones e “pen drives”.

Essa diretriz visa estabelecer critérios de manuseio, prevenção e responsabilidade sobre o uso de dispositivos móveis e deverá ser aplicada a todos os colaboradores que utilizem tais equipamentos. Bem como a observância ao termo de responsabilidade assinado pelo usuário quando este realizou a solicitação do equipamento.

A SESA -Pr, na qualidade de proprietária dos equipamentos fornecidos, reserva-se o direito de inspecioná-los a qualquer tempo, caso seja necessário realizar uma manutenção de segurança.

O colaborador, portanto, assume o compromisso de não utilizar, revelar ou divulgar a terceiros, de modo algum, direta ou indiretamente, em proveito próprio ou de terceiros, qualquer informação, confidencial ou não, que tenha ou venha a ter conhecimento em razão de suas funções na SESA-Pr, mesmo depois de terminado o vínculo contratual mantido com a instituição.

Todo colaborador deverá realizar periodicamente cópia de segurança (backup) dos dados de seu dispositivo móvel. Deverá, também, manter estes backups separados de seu dispositivo móvel, ou seja, não os carregar juntos.

O suporte técnico aos dispositivos móveis de propriedade da SESA-Pr e aos seus usuários deverá seguir o mesmo fluxo de suporte contratado pela instituição.

Todo colaborador deverá utilizar senhas de bloqueio automático para seu dispositivo móvel.

Não será permitida, em nenhuma hipótese, a alteração da configuração dos sistemas operacionais dos equipamentos, em especial os referentes à segurança e à geração de logs, sem a devida comunicação e a autorização da área responsável e sem a condução, auxílio ou presença de um técnico do NII.

O colaborador deverá responsabilizar-se em não manter ou utilizar quaisquer programas e/ou aplicativos que não tenham sido instalados ou autorizados pelo NII da SESA-Pr.

A reprodução não autorizada dos softwares instalados nos dispositivos móveis fornecidos pela instituição constituirá uso indevido do equipamento e infração legal aos direitos autorais do fabricante.

É permitido o uso de rede banda larga de locais conhecidos pelo colaborador como: sua casa, hotéis, fornecedores e clientes.

É responsabilidade do colaborador, no caso de furto ou roubo de um dispositivo móvel fornecido pela SESA-Pr, notificar imediatamente seu gestor direto e ao NII. Também deverá procurar a ajuda das autoridades policiais registrando, assim que possível, um boletim de ocorrência (BO).

O colaborador deverá estar ciente de que o uso indevido do dispositivo móvel caracterizará a assunção de todos os riscos da sua má utilização, sendo o único responsável por quaisquer danos, diretos ou indiretos, presentes ou futuros, que venha causar à SESA-Pr e/ou a terceiros.

O colaborador que deseje utilizar equipamentos portáteis particulares ou adquirir acessórios e posteriormente conectá-los à rede da SESA-Pr deverá submeter previamente tais equipamentos ao processo de autorização do NII.

Equipamentos portáteis, como smartphones, palmtops, pen drives e players de qualquer espécie, quando não fornecidos ao colaborador pela instituição, não serão validados para uso e conexão em sua rede corporativa.

VIGÊNCIA E VALIDADE

A presente política passa a vigorar a partir da data de sua homologação e publicação em diário oficial, sendo válida por tempo indeterminado. Caberá à SESA-Pr fazer as alterações quando se fizerem necessárias

DAS DISPOSIÇÕES FINAIS

Assim como a ética, a segurança deve ser entendida como parte fundamental da cultura interna da Secretaria de Saúde do Estado do Paraná – SESA-Pr. Ou seja, qualquer incidente de segurança subtende-se como alguém agindo contra a ética e os bons costumes regidos pela instituição.

DOCUMENTOS DE REFERÊNCIA

- ✓ Lei 9.609/98 – Lei do *Software*
  http://www.planalto.gov.br/ccivil_03/leis/l9609.htm