SEADE
Fundação Sistema Estadual de Análise de Dados

GOVERNO DO ESTADO DE SÃO PAULO

# Política de Segurança da Informação – PSI

Segunda Edição 2022

SEADE
Fundação Sistema Estadual de Análise de Dados

GOVERNO DO ESTADO DE SÃO PAULO

## INDICE

## 1. Introdução

Como órgão de pesquisa da administração pública paulista, a Fundação Seade realiza tratamento de dados pessoais e de dados pessoais sensíveis. Esse processo tem como finalidade a produção de estatísticas demográficas, sociais e econômicas sobre o Estado de São Paulo, bem como de informações para subsidiar a formulação, o acompanhamento e a avaliação de programas e políticas públicas, de acordo com as bases legais constantes nos incisos II, III e IV do art. 7º e alíneas “a”, “b” e “c” do art. 11, da Lei nº 13.709/2017, a Lei Geral de Proteção de Dados.

As informações produzidas, coletadas e armazenadas na Fundação Seade durante as etapas de preparação, processamento e divulgação devem ser protegidas por acessos restritos aos profissionais que efetivamente precisam tratá-las e analisá-las, de modo a garantir sua integridade, disponibilidade e sigilo. Além da formalização da responsabilidade de seu corpo funcional e de colaboradores pela observância desses preceitos, objeto da edição, em maio de 2018, dos documentos Termo de Confidencialidade, Instruções sobre a Proteção de Confidencialidade Estatística e Protocolo de Confidencialidade, a segurança da informação requer a elaboração de uma política específica voltada para a regulação da utilização das tecnologias e dos ativos de informação.

A Lei Geral de Proteção de Dados (LGPD), ao estabelecer o direito aos seus titulares da proteção de dados pessoais e dados pessoais sensíveis, tanto os de produção própria como os de terceiros, requer a adoção de uma série de medidas para a garantia desse direito, entre as quais a Política de Segurança da Informação (PSI) ocupa lugar de destaque, ao definir regras e responsabilidades para a instituição e seus funcionários e colaboradores.

Soma-se a isto o fato de que a proteção, segurança e integridade das informações armazenadas na Fundação Seade são condições fundamentais para a credibilidade da instituição junto à sociedade e aos seus parceiros e, por consequência, para a manutenção da continuidade de suas atividades de pesquisas e obtenção de dados de outras fontes. Algo, portanto, essencial para a subsistência da Fundação Seade, uma prioridade estratégica.

Para alcançar êxito, a PSI deverá garantir que todas as informações existentes na Fundação Seade tenham origem certificada (autenticidade), que nenhuma delas seja disponibilizada sem autorização (confidencialidade) ou alterada de forma acidental ou dolosa (integridade) e que atendam aos requisitos legais (legalidade).

As inúmeras ameaças à segurança da informação presentes no mundo digital colocam a necessidade de redobrar cuidados, moldar comportamentos e aperfeiçoar procedimentos. Para tanto, este documento visa estabelecer princípios, diretrizes e controles que constituem a Política de Segurança da Informação da Fundação Seade, além de definir competências e responsabilidades das áreas e empregados/colaboradores envolvidos nas atividades da instituição

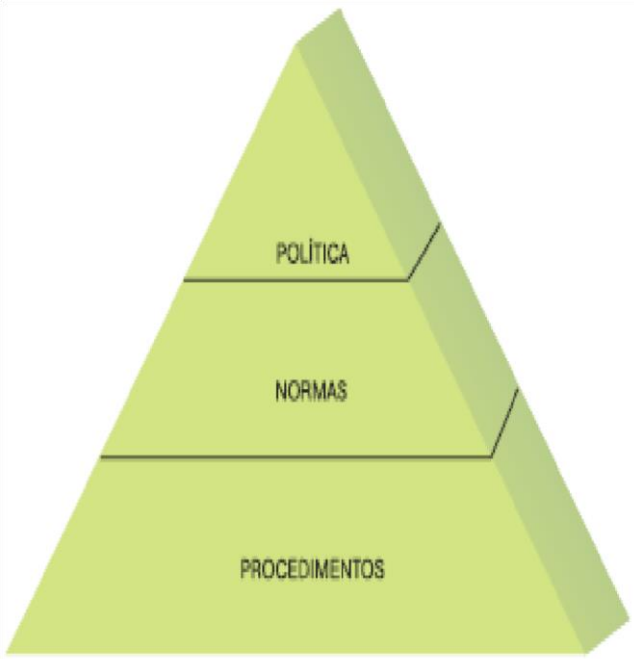
> A segurança da informação é alcançada pela implementação de um conjunto adequado de controles, incluindo políticas, processos, procedimentos, estrutura organizacional e funções de software e hardware. Estes controles precisam ser estabelecidos,

> implementados, monitorados, analisados criticamente e melhorados, quando necessário, para assegurar que os objetivos do negócio e a segurança da informação da organização são atendidos. (ISO 27002-2013 – 0.1 Contexto e histórico)

Segundo o Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança no Brasil (Cert.br), mantido pelo Núcleo de Informação e Coordenação do Ponto BR (NIC.br) do Comitê Gestor da Internet do Brasil (CGI.br), a política de segurança da informação é baseada em três principais propriedades: confidencialidade, integridade e disponibilidade, sendo considerada uma ameaça qualquer ação que abale tais propriedades. A política de segurança é um instrumento com a finalidade de proteger a organização e as informações sob sua responsabilidade contra tais cominações. Ainda segundo o Cert.br, não é papel de uma política de segurança da informação definir quais procedimentos devem ser adotados. Uma boa política deve atribuir claramente os direitos e responsabilidades às pessoas envolvidas, segundo suas posições dentro da organização (administradores da rede, diretores, empregados/colaboradores, etc.). O órgão defende ainda que, anteriormente à definição de uma política, é importante classificar as informações que serão objeto de proteção, analisando os riscos que envolvem:

- recursos protegidos pela política;
- ameaças às quais estes recursos estão sujeitos;
- vulnerabilidades que podem viabilizar a concretização destas ameaças, analisando-as individualmente.

Para Nakamura e Geus (2010), a diretriz para o planejamento de uma política de segurança é manter o seu caráter geral e abrangente em todos os pontos, estabelecendo regras que deverão ser cumpridas por todos. Na visão dos autores, deve-se especificar quem pode acessar cada recurso e em que nível de acesso, destacando-se procedimentos e controles que serão aplicados para proteger cada informação. Portanto, a regulamentação da PSI deve ser complementada por normas e criação de procedimentos específicos.




## 2. Termos e definições

- **Ameaça**: causa potencial de um incidente de segurança que pode trazer danos para sistemas, informações ou para a própria organização.
- **Ativo**: qualquer item (equipamentos, *softwares*, metodologias, informações, por exemplo) que tenha valor para a organização.
- **Ativo de informação**: dados, microdados, informações e conhecimentos obtidos, gerados, tratados e/ou armazenados na Fundação Seade. Exemplos: base de dados, arquivos, documentação de sistema, informações sobre pesquisa, manuais de usuário, materiais de treinamento, procedimentos e planos institucionais, processos de trabalho, entre outros.
- **Ativo de tecnologia da informação**: *softwares* e *hardwares* que permitem armazenamento, transmissão e processamento das informações. Entre os ativos de *software* podem ser citados os aplicativos, sistemas, algoritmos, ferramentas de desenvolvimento e utilitários. Nos ativos físicos estão incluídos os equipamentos computacionais fixos e móveis, equipamentos utilizados para processamento, armazenamento e comunicação de dados e mídias removíveis.
- **Ativos críticos de tecnologia da informação**: são todos os ativos de tecnologia da informação necessários para suportar os processos diretamente relacionados aos objetivos estratégicos da instituição e que, de alguma forma, quando não executados de acordo com seus requisitos, podem causar prejuízo material ou danos significativos à Fundação Seade.
- **Autoridade Nacional de Proteção de Dados – ANPD**: órgão da administração pública indireta responsável por zelar, implementar e fiscalizar o cumprimento da LGPD.

- **Sistemas de informação:** todos os *softwares* desenvolvidos internamente, adquiridos ou obtidos sem custo, utilizados na consecução das atividades da Fundação Seade. Excluem-se *softwares* de prateleira, como o Office 365, SPSS, entre outros.
- **Controle**: forma de gerenciar o risco, incluindo políticas, procedimentos, diretrizes, práticas ou estruturas organizacionais, que podem ser de naturezas administrativa, técnica, de gestão ou legal, também usado como um sinônimo para proteção ou contramedida.
- **Contas de acesso**: identificação única, concedida de forma pessoal e intransferível a um empregado/colaborador, em conjunto com um método de autenticação. As credenciais habilitam o empregado/colaborador que as recebe a acessar equipamentos, sistemas e aplicações e informações específicas, de acordo com o perfil para ele definido.
- **Contas de acesso com perfil de administrador**: contas que, por necessidade de trabalho, possuem acesso irrestrito a todos os servidores, *storages*, sistemas e diretórios e arquivos da rede, tanto em *on-premises* como em nuvem.
- **Controlador**: nos termos da LGPD, pessoa natural ou jurídica, de direito público ou privado, a quem compete as decisões referentes ao tratamento de dados pessoais e a comunicação de incidentes de segurança à ANPD.
- **Diretriz**: orientação sobre o que deve e como ser feito para se alcançarem os objetivos estabelecidos nas políticas.
- Encarregado: nos termos da LGPD, pessoa natural, indicada pelo controlador, que atua como canal de comunicação entre o controlador, os titulares e a ANPD.
- **Gestor de ativos de informação**: empregado responsável por gerenciar determinados conjuntos de informações e todos os ativos da informação a eles relacionados.
- **Gestor de sistemas de informação**: empregado responsável por gerenciar determinado sistema de informação.
- **NBR ISO/IEC 27002**: norma que rege a elaboração da PSI.
- **Nuvem**: infraestrutura, plataformas ou *softwares* hospedados por fornecedores terceirizados e disponibilizados aos usuários via internet.
- **Operador**: nos termos da LGPD, pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.
- **Política**: intenções e diretrizes globais formalmente expressas pela direção.
- **Segurança da informação**: preservação da confidencialidade, integridade e disponibilidade da informação. Adicionalmente, outras propriedades podem também estar envolvidas, tais como autenticidade, responsabilidade, não repúdio e confiabilidade.
- **Teletrabalho**: prestação de serviços preponderantemente fora das dependências do empregador, com a utilização de tecnologias de informação e de comunicação que, por sua natureza, não se constituam como trabalho externo (Lei 13.467/2017).

- **Titular de dados**: nos termos da LGPD, pessoa natural a quem se referem os dados pessoais e pessoais sensíveis que são objeto de tratamento pela Fundação Seade.
- **Tratamento de ativo de informação**: toda operação realizada com dados, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.
- **Vulnerabilidade**: fragilidade de um ativo ou grupo de ativos que pode colocar em risco a segurança das informações ao serem exploradas por agentes mal intencionados.

## 3. Aspectos preliminares

### 3.1. Abrangência e escopo de atuação da política

A PSI se aplica a todos os ativos de informação produzidos ou obtidos pela instituição, ativos de tecnologia de informação que fazem parte do seu patrimônio e sistemas de informações. Esta política se estende ainda a todos os empregados/colaboradores, abrangendo:

- recursos humanos;
- recursos de *software*;
- recursos de *hardware*;
- recursos de rede;
- recursos de dados e informações;
- armazenamento de dados e informações;
- controles de desempenho dos sistemas;
- entrada de dados e informações;
- processamento de dados e informações;
- disseminação de informações;
- bases de conhecimentos.

### 3.2. Utilização de contas de acesso

- As contas de acesso são individuais e seu compartilhamento é proibido.
- O empregado/colaborador titular da conta de acesso é responsável por toda e qualquer ação (inclusive na internet) realizada mediante a utilização da sua conta.
- Cada conta deve ter apenas acesso a informações e recursos no mínimo necessário ao desempenho de suas atribuições profissionais.
- Se o empregado/colaborador possuir acessos adicionais, como no caso das chefias e usuários com perfil de administrador, estes devem ser utilizados somente se houver necessidade para o pleno desempenho das suas atribuições.
- Quando o empregado/colaborador mudar ou afastar-se de uma área de trabalho, os gestores de ativos e sistemas de informação daquela área devem

informar à Sutin, para que a respectiva conta seja recriada com novas definições de acesso.

- As contas com perfil de administrador devem ser sempre individuais.
- Contas com perfil de administrator devem ser usadas com princípio ético e somente quando indispensáveis para execução de tarefas relacionadas à sustentação de ativos de tecnologia da informação, ativos de informação ou para o estrito cumprimento de tarefas formalmente atribuídas.
- Os desenvolvedores de sistemas devem consultar, prévia e formalmente, os gestores de ativos de informação para acessar suas bases de dados. Estes últimos poderão negar ou adiar o acesso.
- Contas de desenvolvedores de sistemas que possuam acessos privilegiados a ambientes de tratamento e produção de informações pessoais serão objeto de registro por meio de *logs*.
- Contas de acesso para utilização de automação de serviços que necessitem autenticação devem ser criadas exclusivamente para este fim, sendo proibida sua utilização por qualquer empregado/colaborador.

## 4. Política de senhas

### 4.1. Requisitos para formação e utilização de senhas

- A composição das senhas (quantidade e tipo de caracteres) será definida pela Sutin, que ainda fornecerá recomendações adicionais aos usuários.
- As senhas serão trocadas periodicamente, mediante solicitação automática do sistema de acesso.
- A solicitação de troca da senha (individual ou coletiva) pode ocorrer a qualquer momento, tantas vezes quanto for necessário, em função dos requisitos de segurança das informações.
- Não será permitido o reúso de senhas.
- A senha será bloqueada após cinco tentativas mal sucedidas de acesso.
- A senha é individual e secreta e não deve ser compartilhada ou divulgada.
- A senha não deve ser anotada, apenas memorizada.
- Senhas coletivas serão toleradas apenas em casos específicos, como no acesso a *e-mails* de respostas de pesquisas realizadas pela Fundação Seade e no acesso ao servidor de *uploads* dos Cartórios de Registro Civil.
- A senha para acesso à rede Wi-fi “VISITANTES”, que possibilita acesso eventual à internet para visitantes da Fundação Seade, deve ser solicitada à Sutin pela área que está recebendo o(s) visitante(s).
- A senha para acesso à rede Wi-fi “VISITANTES” perderá a validade imediatamente após a comunicação _à Sutin, pela área solicitante, do término da utilização pelos visitantes.

### 4.2. Senhas default (padrão)

- A senha inicial e o nome de usuário da conta de acesso serão definidos pela Gerho.
- Para qualquer nova conta de acesso, a senha deve ser substituída imediatamente na sua primeira utilização, mesmo que o sistema eventualmente não solicite.

### 4.3. Outros cuidados com a senha de acesso

- Nenhuma pessoa, e-mail ou sistema pode solicitar que o empregado/colaborador divulgue sua senha das contas de acesso, nem mesmo empregados/colaboradores com nível hierárquico superior.
- A Fundação Seade jamais solicitará a divulgação das senhas das contas de acesso.
- O empregado/colaborador que solicitar senhas alheias ou divulgar senhas de contas de acesso incorrerá em falta grave.
- Respeitadas as políticas de senhas, cada empregado/colaborador tem autonomia para trocar sua senha, sem necessitar da intervenção da Sutin.
- Administradores de redes e sistemas não devem ter acesso a qualquer tipo de senha de terceiros. Esta sempre deve estar criptografada.
- Cabe exceção para a senha da rede sem fio para visitantes, a qual é compartilhada sob demanda da área solicitante.

## 5. Direitos e responsabilidades

### 5.1. Direitos e responsabilidades dos empregados/colaboradores

- Receber, ler, dar ciência formalmente e cumprir a política de segurança da informação – PSI.
- Receber somente da Gerho contas de acesso compostas por um nome de usuário, endereço de e-mail corporativo (nome_de_usuário@seade.gov.br) e senha de acesso.
- Guardar e zelar pelo uso de sua(s) conta(s) de acesso.
- Ter os devidos direitos de acessos implementados em sua conta.
- Acessar os ativos de informação exclusivamente por meio da infraestrutura fornecida pela Fundação Seade ou homologados pela Sutin, inclusive para teletrabalho.
- Os ativos de informação contendo dados pessoais ou sigilosos não devem ser copiados a não ser por estrita necessidade de trabalho dos operadores dessas informações. Uma vez cumprida sua função, essas cópias devem eliminadas.
- Da mesma forma, cópias ou extratos de bancos de dados contendo dados pessoais ou sigilosos para desenvolvimento, homologação ou manutenção de sistemas devem ser eliminadas após o término dessas atividades. Nesse caso o gestor do ativo de informação deve ser avisado com antecedência dessa cópia e deve anuir

formalmente com esse procedimento e, posteriormente, ser informado de sua eliminação.

- Os recursos, ativos de informação e de tecnologia da informação aos quais o empregado/colaborador possuir direito de acesso devem permanecer disponíveis para utilização plena pelo empregado/colaborador detentor de contas de acesso.
- Somente na utilização da rede Wi-fi, provida pela Fundação Seade, é permitida a utilização de equipamentos particulares e portáteis, desde que o empregado/colaborador se autentique utilizando sua conta de acesso.
- Os equipamentos particulares utilizados no domicílio dos empregados/colaboradores para acessar a rede da Fundação Seade em teletrabalho devem atender aos requisitos de hardware e sistema operacional estabelecidos pela Sutin.
- Ao utilizar os recursos corporativos de acesso à internet, o empregado/colaborador não deve violar aspectos éticos, legais ou administrativos.
- O empregado/colaborador deve zelar pela segurança da rede e dos sistemas de informação da Fundação Seade, usando-os de forma segura e somente para fins institucionais.
- Os acessos de cada conta podem ser monitorados e registrados, sendo as ações de cada empregado/colaborador de sua inteira responsabilidade.
- A utilização dos equipamentos, programas e informações da Fundação Seade deve se enquadrar ao estabelecido no Termo de Confidencialidade, Instruções sobre a Proteção de Confidencialidade Estatística e Protocolo de Confidencialidade.
- Ao se ausentar de seu posto de trabalho, o empregado/colaborador deve realizar o bloqueio de tela em seu equipamento, para evitar que pessoas não autorizadas tenham acesso a informações pessoais ou sigilosas.
- O empregado/colaborador deve notificar qualquer incidente ou fragilidade de segurança percebida, comunicando o mais rapidamente possível à Sutin, pessoalmente, por telefone ou pelo e-mail incidente@seade.gov.br.
- Não é aceitável nenhuma prática que possa ser considerada contrária a requisitos legais, causando a violação de qualquer lei criminal ou civil, estatutos, regulamentações ou obrigações contratuais.
- É vedado o armazenamento de arquivos pessoais na rede de informática da Fundação Seade.
- Os sistemas de monitoramento e relatórios das contas de acesso devem ser empregados com ética e para finalidades unicamente voltadas à segurança e eficiente utilização dos recursos providos pela Fundação Seade.
- Contas de acesso com perfil de administrador devem ser passíveis de auditoria pela Diretoria.
- Nenhuma conta com perfil de administrador poderá ser criada ou excluída sem autorização da Diretoria.

- Os empregadores/colaboradores devem estar cientes de que informações armazenadas nos discos rígidos das estações de trabalho não são cobertas pelas cópias de segurança.

### 5.2. Responsabilidades do gestor de ativos de informação

- Analisar e catalogar previamente todos os ativos de informação sob sua responsabilidade antes da ação de qualquer operador.
- Enviar imediatamente para o encarregado qualquer atualização do Catálogo dos Ativos de Informação com necessidade de tratamento especial em função de conter dados pessoais de cidadãos, conforme definições da LGPD.
- Identificar todos os ativos de informação que contiverem dados pessoais, conforme definições e orientações da LGPD. Identificados dados pessoais ou dados pessoais sensíveis, o respectivo ativo de informação somente deverá ser acessado por operador(es) e receber tratamento após orientação formal do seu gestor.
- Seguir as orientações no tratamento do ativo de informação estabelecidas pelo controlador, nos termos da LGPD.
- Definir os controles adicionais que devem ser aplicados sobre os ativos de informação sob sua responsabilidade para garantir sua segurança, sigilo e tratamento correto.
- Avaliar continuamente se os requisitos de segurança da informação estão adequados, especialmente os dos dados pessoais.
- Definir quais contas podem acessar os ativos de informação sob sua custódia. Todas as permissões de acesso deverão ser revistas periodicamente.
- Solicitar à Sutin a adequada liberação ou bloqueio de acessos para os ativos de informação sob sua custódia.
- Informar à Sutin, em até três dias, qualquer mudança ou afastamento de empregado/colaborador da área sob sua gestão, para que a respectiva conta de acesso seja recriada com permissões de acesso redefinidas.
- Garantir que a concessão de acesso aos ativos de informação seja a mínima possível, necessária somente para que os empregados/colaboradores possam executar suas funções.
- Assegurar que os ativos de informação sob sua responsabilidade estejam conforme o estabelecido nos procedimentos de Sigilo e Proteção Estatística da Fundação Seade e na LGPD.
- Quando os ativos de informação deixarem de ser do interesse da área, solicitar sua remoção, caso sejam físicos, ou o seu arquivamento em mídias específicas, se estiverem em meio magnético.
- O compartilhamento de ativos de informação contendo dados pessoais para parceiros externos, por qualquer meio, deve ser registrado e observar rigorosamente as premissas de segurança contra vazamentos.

- Orientar todos os empregados/colaboradores da sua respectiva área para que documentos sensíveis não fiquem expostos em impressoras, mídias digitais ou telas de microcomputadores.
- Autorizar acessos externos de não empregados/colaboradores a serviços e sistemas que exijam autenticação. Exemplos: Cartórios de Registro Civil para upload de informações; acesso de empregados/colaboradores lotados em outros órgãos; acesso a sites hospedados pela Fundação Seade.
- No caso de colaboradores de empresas que prestam serviço à Fundação Seade, os pedidos à Sutin para inclusão, bloqueio ou remoção de contas de acesso são de responsabilidade do gerente da área que recebe a prestação dos serviços.

### 5.3. Responsabilidades do gestor de sistemas de informação

- Desenvolver e manter os sistemas segundo as melhores práticas, garantindo a integridade, disponibilidade, confidencialidade e segurança das informações.
- Implantar em ambiente de produção os sistemas desenvolvidos internamente.
- Obter autorização prévia e formal do gestor de ativos de informação para acesso a dados pessoais necessários para desenvolvimento, homologação e manutenção do sistema.
- Assegurar que os sistemas desenvolvidos por terceiros atendam ao escopo da contratação e que os códigos-fonte e demais documentações sejam entregues à Fundação Seade.
- Supervisionar a implantação dos sistemas desenvolvidos por terceiros nos ambientes de produção e homologação.

### 5.4. Responsabilidades da Sutin

- Operar, manter e monitorar o Datacenter da Fundação Seade, avaliando aspectos de segurança.
- Operar, manter, monitorar e auditar o ambiente de computação em nuvem, avaliando aspectos de segurança e a restrição da localização geográfica do provedor.
- Instalar e desinstalar física ou logicamente quaisquer ativos de tecnologia da informação.
- Criar e ativar contas de acesso e e-mail conforme solicitação da Gerho e gestores de ativos de informação.
- Definir a composição das senhas das contas de acesso.
- Instalar, remover e/ou modificar qualquer software nos ativos de tecnologia da informação.
- Os empregadores/colaboradores podem solicitar à Sutin a instalação de softwares, livres ou proprietários, com custos ou gratuitos. A instalação só será efetivada, no entanto, após análise da Sutin sobre a disponibilidade de licenças e segurança do software.

- Avaliar e especificar hardwares, softwares e serviços de TI adquiridos, em aquisição ou obtidos sem custo pela Fundação Seade.
- Garantir, sempre que possível, que o tráfego de dados pessoais ou sigilosos entre a Fundação Seade e outras instituições se dê em ambiente protegido por criptografia.
- Até que um empregado/colaborador tenha sido designado formalmente como gestor de um ativo da informação, a custódia dos ativos será responsabilidade da Sutin, que negará o acesso a todas as contas, com exceção daquelas com perfil de administrador da rede.
- Gerir os softwares utilizados na Fundação Seade, bem como as respectivas licenças de utilização, para garantir os direitos autorais dos fabricantes.
- Assegurar que os ativos de tecnologia da informação descartados por defeito ou obsolescência não contenham informações ou softwares de propriedade da Fundação Seade.
- Em casos de ameaças ou riscos à segurança da informação, a Sutin poderá, sem prévio aviso, retirar ou bloquear quaisquer acessos que utilizem recursos dos sistemas de informação da Fundação Seade, comunicando e justificando posteriormente seus atos ao gestor dos ativos de informação e ao encarregado.
- Manter e configurar os ativos de tecnologia de informação.
- Fazer as especificações dos novos ativos de tecnologia de informação para fins de aquisição, aluguel ou compra como serviço.
- Avaliar as medidas de segurança existentes em ambientes externos de armazenamento de informações de parceiros da Fundação Seade, em casos de cessão, por esta última, de dados pessoais ou sigilosos.
- Fornecer todos os meios e suportes possíveis requisitados pela equipe de resposta a incidentes − ERI.
- Responder e comunicar imediatamente à ERI os incidentes ou fragilidades de segurança da informação.
- No caso de detecção de ameaças ou incidentes de segurança, bloquear automaticamente, por sistemas, acessos ou requisições de acesso.
- Reduzir os danos e eliminar, o mais rápido possível, os efeitos dos incidentes de segurança.
- Apurar causas, danos e responsáveis pelos incidentes de segurança por solicitação da ERI.
- Desenvolvimento e manutenção de sistemas:
  - ✓ garantir que o processo de desenvolvimento de sistemas seja aderente às políticas de segurança da informação;
  - ✓ criar, quando necessário, mecanismos de registro e consulta de eventos e acessos (*logs*) para sistemas utilizados pela Fundação Seade, objetivando sua rastreabilidade, identificação e origem;

- ✓ disponibilizar ambientes de desenvolvimento e homologação, segregados de produção, para o desenvolvimento e manutenção de sistemas;
- ✓ garantir que todo material gerado durante o desenvolvimento de sistemas esteja contido em repositórios sujeitos a mecanismos de controle de acesso, seguindo as regras desta política no que tange às diretrizes de segurança da informação;
- ✓ providenciar que os códigos-fonte dos sistemas desenvolvidos na Fundação Seade sejam armazenados utilizando sistemas de controle de versões;
- ✓ assegurar que a homologação dos sistemas e sua implantação em ambiente de produção sejam efetuadas apenas com autorização do gestor dos ativos de informação;
- ✓ providenciar que os sistemas desenvolvidos na Fundação Seade sejam devidamente documentados;
- ✓ garantir que as alterações de sistemas implantados, que impliquem mudanças significativas nos mesmos e/ou no ambiente de execução, incluam a análise dos riscos envolvidos na segurança;
- ✓ supervisionar o desenvolvimento de sistemas por terceiros, visando resguardar esses ativos de tecnologia quanto à sua segurança;
- ✓ realizar cópias de segurança (*backups*) com o objetivo de recuperar arquivos e sistemas armazenados na rede da Fundação Seade, em caso de falhas de *hardware* ou *software*, incidentes de segurança ou desastres;
- ✓ assegurar que todos os ativos de informação da Fundação Seade possuam cópias de segurança, na frequência adequada para garantir a recuperação, nos menores lapsos de tempo e índice de perda de dados possíveis;
- ✓ definir a frequência dos *backups* e o tempo de guarda das cópias de segurança;
- ✓ restaurar informações por meio das cópias de segurança mediante solicitação das demais áreas da instituição ou em casos de incidentes de segurança;
- ✓ providenciar a guarda externa de cópias de segurança recentes, em empresa especializada;
- ✓ assegurar que o armazenamento externo e o descarte das cópias de segurança sejam realizados por meio de procedimentos adequados, para preservar o sigilo das informações.

### 5.5. Responsabilidades da Gerho

- Definir os nomes da conta dos empregados/colaboradores e respectiva senha inicial.
- Solicitar formalmente à Sutin as devidas providências para ativação do usuário e senha como conta válida.
- Após validação da Sutin, encaminhar formalmente as credenciais das contas aos respectivos empregados/colaboradores.

- Comunicar e solicitar imediatamente à Sutin o bloqueio ou remoção de contas de acesso de empregados/colaboradores desligados, afastados ou em qualquer outra situação que a justifique.
- Identificar e atender aos empregados/colaboradores afastados, intermediando as demandas referentes a fornecimento de novas senhas, troca de senhas, nome de contas de acessos, acessos a recursos, entre outros.

## 6. Utilização de softwares (instalação, licenciamento e copyright)

- Demanda de aquisição de softwares devem ser formalmente solicitada à Sutin.
- É proibida a instalação de programas (software) em ativos de tecnologia da informação da Fundação Seade sem avaliação e consentimento formal da Sutin, independentemente do regime de licenciamento.
- A Sutin fará o gerenciamento de licenças de softwares licenciados, sendo autorizada apenas a instalação de softwares legais, respeitando questões de licenciamento e direitos autorais.

## 7. Proteção e uso de informações e dados de configuração de sistemas

- Não é permitido o acesso a qualquer ativo de informação da Fundação Seade sem as devidas permissões/autorizações dos respectivos gestores, cabendo exceção aos ativos de informação publicados no site da Fundação Seade.
- Informações de configurações de sistemas ou qualquer informação que possa de alguma forma fragilizar a segurança da informação da Fundação Seade não devem ser divulgadas.
- A divulgação de qualquer ativo de informação, inclusive os publicados no site da Fundação Seade, deve obedecer rigorosamente ao estabelecido na LGPD e demais legislações pertinentes ao tema, no Termo de Confidencialidade, nas Instruções sobre a Proteção de Confidencialidade Estatística e no Protocolo de Confidencialidade formalizados pela Fundação Seade.
- Todos os ativos de informação, devidamente analisados e catalogados pelos gestores, que contenham dados pessoais, nos termos da LGPD, não poderão ser tratados pela Fundação Seade sem autorização formal do controlador.

## 8. Uso da internet e recursos providos pela Fundação Seade

- O acesso à internet é disponibilizado como recurso para a consecução das atividades institucionais: consultas, pesquisas e troca de informações e ideias, sempre ligadas aos interesses corporativos.
- Deve-se evitar o uso da internet para fins de entretenimento (filmes, jogos, etc.) para não comprometer a disponibilidade do serviço.
- O acesso à internet pode ser revogado ou bloqueado por desrespeito à PSI, por ameaça a qualquer ativo ou necessidade de serviço.

- Os recursos providos pela Fundação Seade têm como finalidade o cumprimento de suas atribuições, sendo, portanto, proibido qualquer tipo de utilização dos recursos que prejudique esse objetivo.
- Arquivos armazenados na rede da Fundação Seade automaticamente passam a contar com determinados níveis de segurança e consumir recursos. A utilização destes recursos, como por exemplo espaço de armazenamento em servidores de arquivos, serviços de e-mail ou gerenciadores de banco de dados, deve ser feita com bom senso, cautela e com fins institucionais.
- A utilização dos recursos poderá ser registrada. A Sutin poderá gerar relatórios de uso de cada recurso, inclusive com identificação das contas de acesso, mediante solicitação dos respectivos gestores de ativos ou da Diretoria.
- Somente contas de acesso autorizadas pela Diretoria podem enviar mensagens para todos os empregados/colaboradores da Fundação Seade ou em massa para endereços externos à instituição.
- A tentativa de burlar sistemas de monitoramento, auditoria, segurança e/ou controle é considerada ameaça grave à segurança e passível de medidas administrativas cabíveis.
- Todos os recursos de segurança, tais como antivírus, *firewall*, atualizações, entre outros, não podem ser desativados pelos empregados/colaboradores.
- O compartilhamento de equipamentos de tecnologia da informação é permitido desde que cada empregado/colaborador utilize sua respectiva conta de acesso.
- A área em que um equipamento de tecnologia da informação estiver alocado é responsável por comunicar imediatamente à Sutin qualquer anomalia, dano ou ausência do equipamento.
- Não é permitido conectar equipamentos pessoais ou de terceiros à rede corporativa da Fundação Seade, com exceção à rede WiFi “Visitantes”.
- Em teletrabalho, os equipamentos particulares utilizados no domicílio dos empregados/colaboradores para acessar a rede da Fundação Seade devem atender aos requisitos de *hardware* e sistema operacional estabelecidos pela Sutin.
- O acesso à rede da Fundação Seade no teletrabalho deve seguir o padrão estipulado pela Sutin e os trabalhos realizados devem ser armazenados na rede da instituição. Informações pessoais ou sigilosas não devem ser copiadas para o equipamento localizado no domicílio do empregado/colaborador e utilizado para o teletrabalho.
- Não é permitido adicionar, remover ou manipular os componentes físicos (*hardware*) de ativos de tecnologia da informação.
- Os recursos computacionais da organização devem ser utilizados somente para fins corporativos.
- Os ativos de informação armazenados na Fundação Seade são considerados de sua propriedade.
- O uso eventual de ativos de tecnologia da informação e da internet para fins pessoais é tolerado, desde que não conflite com determinações e normas internas da

Fundação Seade e com o Código de Ética dos Funcionários Públicos (Decreto n. 60.428, de 8 de maio de 2014 – Código de Ética da Administração Pública Estadual), nem interfira em suas atribuições.

- A Fundação Seade não se responsabiliza por informações de caráter pessoal, que não tenham relação com as finalidades corporativas, armazenadas em seus ativos de tecnologia da informação pelos empregados/colaboradores.

## 9. Direitos e limites à privacidade

- A utilização, por parte dos empregados/colaboradores, dos recursos providos pela Fundação Seade está condicionada ao cumprimento integral do Termo de Confidencialidade, Instruções sobre a Proteção de Confidencialidade Estatística e do Protocolo de Confidencialidade formalizados pela Fundação Seade, e deve ocorrer com respeito à ética e à legalidade.
- A conta de *e-mail* corporativo é de uso exclusivo de seu titular.
- A Fundação Seade reserva-se o direito de acessar quaisquer contas de *e-mail* (@seade.gov.br) com finalidade de recuperar informações relacionadas às atividades institucionais ou para fins de auditoria.
- Empregados/colaboradores que, por atribuição de suas funções, possuam conta de acesso privilegiada (perfil de administrador) não têm direito a acessar ativos de informação ou áreas de trabalho alheias, a não ser no estrito cumprimento de suas funções/atribuições. Se necessário para o desempenho de suas funções, deve ser feito com ciência e autorização do gestor do ativo da informação.
- Dados pessoais serão tratados nos termos da LGPD.

## 10. Segurança física

- Ativos de tecnologia da informação considerados críticos (servidores, *storages*, *nobreaks*, etc.) devem ficar em áreas fechadas, com acesso restrito à Sutin e controladas por dispositivos de identificação física.
- O acesso ao *Data Center* da Fundação Seade será, além de restrito, monitorado por CFTV e controlado por autenticação.
- O acesso ao interior do *Data Center* e outras áreas fechadas com equipamentos como *nobreaks* e estabilizadores é vedado para empregados/colaboradores que não pertençam à Sutin. Visitantes no *Data Center* devem sempre estar acompanhados por funcionários da Sutin.
- Outros ativos de tecnologia da informação também críticos, como gerador e *switches*, que ficam em áreas abertas são igualmente de acesso restrito à Sutin.

## 11. Auditorias

- A critério da Diretoria, quaisquer contas de acesso e e-mail (.seade.gov.br) poderão ser monitorados a partir dos registros de acessos, tentativas de acesso e das ações praticadas nos ativos de tecnologia da informação.

- A Fundação Seade reserva-se o direito de monitorar e registrar todos os dados armazenados ou em trânsito, com especial atenção aos dados pessoais ou cobertos por sigilo.
- A critério da Diretoria, podem ser realizadas auditorias para verificar se os requisitos de segurança da informação estão sendo aplicados corretamente.

## 12. Penalidades

- O não cumprimento da PSI sujeita o infrator a medidas administrativas, cíveis ou penais.

## 13. Disposições finais

- A PSI deverá ser revista a cada dois anos ou em caso de condições obrigatórias de atualização como:
  - ✓ edição ou alteração de leis e regulamentos;
  - ✓ mudanças nas tecnologias de informação da instituição;
  - ✓ a partir de análise de risco que demonstrem a necessidade de sua readequação;
  - ✓ por mudanças de estratégia da instituição.

## 14. Referências

ABNT – Associação Brasileira de Normas Técnicas. *NBR ISO/IEC 27002: 2013*. Tecnologia da informação – Técnicas de segurança – Código de prática para controles de segurança da informação. Rio de Janeiro, 2013.

CERT.br – Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança no Brasil. *Práticas de segurança para administradores de redes internet* – Documento completo. Capítulo 2 – Políticas. Disponível em: https://www.cert.br/docs/seg-adm-redes/seg-adm-redes.html. Acesso em: 7 maio 2018.

IBGE – Instituto Brasileiro de Geografia e Estatística. *Política de Segurança da Informação e Comunicações do IBGE 2017-2018*. Rio de Janeiro: IBGE, 2017.

NAKAMURA, E. T.; GEUS, P. L. de. *Segurança de redes em ambientes cooperativos*. São Paulo: Novatec, 2010.

SÃO PAULO (Estado). Tribunal de Justiça. *Portaria n. 9.908/2020*. Redefine a Política de Segurança da Informação do Tribunal de Justiça do Estado de São Paulo. São Paulo, 2020.