SEADE

Fundação Sistema Estadual de Análise de Dados

Política de Segurança da Informação

São Paulo

2018

Política de Segurança da Informação

Sumário

Introdução

A Fundação Seade, como agência de estatística, produz e coleta dados socioeconômicos sobre o Estado de São Paulo. Essas informações, durante as etapas de preparação, processamento e divulgação, devem ser protegidas por meio de acessos restritos àqueles que efetivamente precisam trabalhar com elas, de modo a garantir sua integridade, disponibilidade e sigilo. Além da responsabilidade de seu corpo funcional e de colaboradores, 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.

Preservar a integridade, a precisão e o sigilo das informações próprias e de terceiros armazenadas na Fundação Seade é prioridade estratégica, fundamental para a credibilidade da instituição e manutenção da sua capacidade de fazer pesquisas e obter dados de outras fontes, ou seja, crucial para sua própria subsistência.

Para alcançar êxito, a política de segurança da informação (PSI) deverá garantir que todas as informações existentes na Fundação Seade tenham origem certificada (autenticidade) e que nenhuma delas seja disponibilizada sem autorização (confidencialidade) ou alterada de forma acidental ou indevida (integridade).

As inúmeras ameaças à segurança da informação presentes no momento atual colocam a necessidade de aumentar os cuidados, moldar comportamentos e aperfeiçoar procedimentos. Para tanto, este documento visa estabelecer princípios, diretrizes e controles para implantação de uma política de segurança da informação, além de definir competências e responsabilidades das áreas e empregados/colaboradores envolvidos nas atividades da instituição

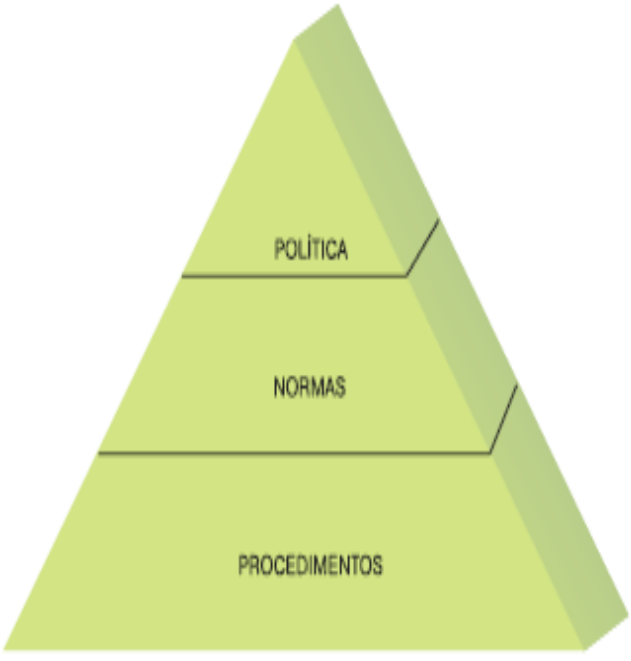
> A segurança da informação é alcançada pela implementação de um conjunto adequado de controles, incluindo políticas, processos, procedimentos, estrutura organizacional e funções de software e hardware. Estes controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e 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 ameaças**.** 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 compreendidos em:

- 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.



Ainda sugerem os autores que, para o desenvolvimento da política de segurança da informação, devem-se considerar e compreender os diversos aspectos de segurança – tecnológicos, jurídicos, humanos, de negócio e processuais, além de questões culturais, sociais e pessoais.

Termos e definições

- **Ameaça**: causa potencial de um incidente de segurança que pode trazer danos para sistemas, informações ou à própria organização.
- **Ativo**: qualquer coisa 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.
- **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 MS Office, 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 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 diretórios e arquivos da rede.
- **Diretriz**: descrição que orienta o que deve ser feito e como, para se alcançarem os objetivos estabelecidos nas políticas.

- **Gestor de ativos de informação**: empregado, nomeado pela Diretoria, pertencente a uma unidade administrativa, responsável por gerenciar determinados segmentos de informações e todos os ativos da informação a eles relacionados.
- **Gestor de sistemas de informação**: empregado, nomeado pela Diretoria, pertencente a uma unidade administrativa, responsável por gerenciar determinado sistema de informação.
- **Segurança da informação**: preservação da confidencialidade, integridade e disponibilidade da informação. Adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade, podem também estar envolvidas.
- **Política**: intenções e diretrizes globais formalmente expressas pela direção.
- **Vulnerabilidade**: fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças.
- **Normas e regulamentos aos quais a política está subordinada**: NBR ISO/IEC 27002.

Aspectos preliminares

Abrangência e escopo de atuação da política

A PSI se aplica a todos os ativos de informação produzidos ou obtidos pela instituição, os ativos de tecnologia de informação que fazem parte do patrimônio e os sistemas de informações. Está 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**.**

Comissão de Sigilo – CS

A implantação e coordenação da PSI ficará a cargo da Comissão de Sigilo com as seguintes atribuições:

- zelar pela aplicação e efetividade da PSI na Fundação Seade;
- avaliar permanentemente a atualidade, aplicabilidade e clareza da PSI;
- dirimir dúvidas e estabelecer diretrizes para casos que a PSI tenha se omitido;
- assegurar que todos os ativos e sistemas de informação da Fundação Seade tenham um gestor;
- coordenar e orientar os gestores de ativos e sistemas de informação nomeados pela Diretoria;
- autorizar exclusivamente a criação/exclusão de contas de acesso com perfil de administrador;
- examinar os incidentes de segurança ocorridos na Fundação Seade e avaliar o tratamento dado a eles, fazendo recomendações e, se for o caso, sugerindo a aplicação de medidas administrativas aos envolvidos;
- solicitar, se necessário, auditoria interna em procedimentos realizados pelos administradores de rede e empregados/colaboradores.

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 suficiente para o desempenho de suas atribuições profissionais.
- Ainda que o empregado/colaborador possua acessos adicionais, estes devem ser utilizados somente se houver necessidade para o pleno desempenho das suas atribuições.
- Caso o empregado/colaborador mude ou afaste-se de determinada área, os gestores de ativos e sistemas de informação devem informar a 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 ou para 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 produção podem ser monitoradas.
- 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.

Política de senhas

Requisitos para formação e utilização de senhas

- A composição das senhas (quantidade e tipo de caracteres) será definida pela Sutin, que ainda fornecerá as recomendações adicionais aos usuários.
- As senhas serão trocadas periodicamente, mediante solicitação automática do sistema de acesso.
- Por motivos de segurança, a solicitação de troca da senha (individual ou coletivamente) pode ocorrer a qualquer momento, tantas vezes quanto for necessário para garantir a segurança.
- Não será permitido o reuso da senha.
- 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, pela área solicitante à Sutin, do término da utilização pelos visitantes.

Senhas default (padrão)

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

Outros cuidados com a senha de acesso

- Nenhuma pessoa, *e-mail* ou sistema pode solicitar a divulgação da senha, nem mesmo empregados/colaboradores com nível hierárquico superior.
- A Fundação Seade jamais solicitará a divulgação da senha 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. Estas sempre devem estar criptografadas.
- Cabe exceção para a senha da rede sem fio para visitantes, a qual é compartilhada sob demanda da área solicitante.

Direitos e responsabilidades dos empregados/colaboradores e áreas da Fundação Seade

Responsabilidades e direitos 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.
- 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.
- Ao utilizar os recursos corporativos de acesso à Internet, o empregado/colaborador não deve violar aspectos éticos, legais ou administrativos.
- Zelar pela segurança da rede e dos sistemas de informação da Fundação Seade, usando-os de forma segura.
- Os acessos de cada conta podem ser monitorados e registrados, sendo as ações de cada empregado/colaborador de sua inteira responsabilidade.

- A utilização dos recursos 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 implementar o bloqueio de tela em seu equipamento para evitar que pessoas não autorizadas tenham acesso a informações sigilosas.
- Notificar qualquer incidente ou fragilidade de segurança percebida, comunicando-o diretamente por telefone à Sutin 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.
- A utilização dos sistemas de monitoramento e relatórios de utilização devem acontecer com ética e para finalidades unicamente voltadas à segurança e eficiente utilização dos recursos providos pela Fundação Seade.
- Arquivos de registros de utilização, acessos internos, acessos à Internet, alarmes de sistemas, contas de acessos, etc. poderão ser utilizados e fornecidos a qualquer momento para a CS e/ou Diretoria.
- Contas de acesso com perfil de administrador devem ser passíveis de auditoria pela CS e/ou Diretoria.
- Nenhuma conta com perfil de administrador poderá ser criada ou excluída sem autorização da CS.

Responsabilidades do gestor de ativos de informação

- Definir os controles aplicados sobre os ativos de informação sob sua responsabilidade.
- Avaliar continuamente se os requisitos de segurança da informação estão adequados.
- Classificar os ativos de informação quanto à sua importância e grau de confidencialidade, solicitando à Sutin os recursos compatíveis para garantir o tratamento adequado.
- Definir quais contas podem acessar os ativos de informação sob sua custódia. Todas as permissões de acesso deverão ser revistas em um prazo de até 60 dias após a designação do gestor.
- 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 o estabelecido no Termo de Confidencialidade, Instruções sobre a Proteção de Confidencialidade Estatística e no Protocolo de Confidencialidade formalizados pela Fundação Seade, solicitando à Sutin as adequações necessárias no que diz respeito aos direitos de acessos aos ativos de informação sob sua responsabilidade.
- Informar à Sutin quando os ativos de informação deixarem de ser do interesse da área e solicitar sua remoção, se físicos, ou o arquivamento em mídias específicas, no caso de informações.
- Autorizar o transporte dos ativos de informação em qualquer mídia, com o devido registro e procedimentos adequados.
- Orientar todos os empregados/colaboradores da sua respectiva área para que documentos sensíveis, em impressoras, mídias digitais ou em telas de microcomputadores não fiquem expostos.
- 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 é de responsabilidade do gerente da área que recebe os serviços.

Responsabilidades do gestor de sistemas de informação

- Desenvolver e manter os sistemas segundo as melhores práticas, garantindo a integridade, disponibilidade e confidencialidade das informações.
- Implantar em ambiente de produção os sistemas desenvolvidos internamente.
- Obter autorização prévia e formal do gestor de ativos de informação para acesso aos dados necessários para desenvolvimento 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.

Responsabilidades da Sutin

- Instalação e desinstalação física ou lógica de quaisquer ativos de tecnologia da informação.
- Criar e ativar contas de acesso e *e-mail* conforme solicitação da Gerho e gestores de ativos de informações.
- Definir a composição das senhas das contas de acesso.
- Instalar, remover e/ou modificar qualquer *software* nos ativos de tecnologia da informação. A instalação pelos empregados/colaboradores de qualquer *software* (livre ou não, sem custo ou não) deve sempre ser precedida de consulta e autorização formais da Sutin.
- Avaliar e especificar *hardwares*, *softwares* e serviços relacionados em aquisição, adquiridos ou utilizados pela Fundação Seade.
- Garantir, sempre que possível, que o tráfego de informações entre a Fundação Seade e o mundo exterior se dê em ambiente protegido por criptografia.
- Até que um empregado/colaborador tenha recebido formalmente da Diretoria a designação 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 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 à CS e ao gestor dos ativos de informação.
- 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 de serviços.
- 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 sigilosos.
- Tratamento e resposta de incidentes de segurança:
  - responder imediatamente às notificações de incidente ou fragilidade de segurança da informação comunicada pelos empregados/colaboradores;

- bloquear acessos automaticamente por sistemas ou demanda, após detecção de ameaças;
- reduzir os danos e eliminar, o mais rápido possível, os efeitos dos incidentes ocorridos;
- apurar causas, danos e responsáveis pelos incidentes e informar a CS;
- intermediar as tratativas de segurança da informação com entidades externas que tratam sobre incidentes de segurança da informação;
- restaurar informações por meio das cópias de segurança mediante solicitação das áreas ou em casos de incidentes.

- Aquisição, desenvolvimento e manutenção de sistemas:
  - criar, quando necessário, para os sistemas adquiridos ou desenvolvidos internamente, mecanismos de registro e consulta de eventos e acessos (*log* de sistema), objetivando sua rastreabilidade e garantindo sua identificação e origem;
  - criar ambientes de desenvolvimento e homologação, segregados do de produção, para o desenvolvimento e manutenção de sistemas construídos na Fundação Seade;
  - 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;
  - zelar para que os códigos-fonte dos sistemas sejam armazenados utilizando sistemas de controle de versões que garantam acesso e controle das diferentes versões;
  - assegurar que a homologação dos sistemas e sua implantação em ambiente de produção sejam efetuadas apenas com autorização do gestor de sistema de informação responsável e que os mesmos contenham documentação baseada na metodologia de desenvolvimento adotada, que os descreva e que permita seu gerenciamento e suporte;
  - garantir que as manutenções de sistemas já implantados, que impliquem mudanças significativas nos mesmos e/ou no ambiente de execução, incluam a análise dos riscos envolvidos pelo gestor do sistema;
  - efetuar análise crítica dos sistemas após mudanças nas plataformas operacionais para assegurar que não ocorra nenhum impacto adverso nas operações ou na segurança;
  - supervisionar o desenvolvimento de sistemas por terceiros, visando resguardar os ativos quanto à integridade e confidencialidade;
  - garantir que o processo de desenvolvimento de sistemas seja aderente às políticas de segurança da informação.

- Cópias de segurança (*backups*):
  - realizar cópias de segurança com o objetivo de recuperar arquivos e sistemas armazenados na rede da Fundação Seade, em caso de falhas de *hardware*, falhas de *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, com os menores tempo e índice de perda possíveis de dados, configurações e sistemas, em caso de falhas ou perdas nos ativos, tanto físicas como lógicas;
  - definir a frequência e guarda das cópias de segurança.
  - Informações armazenadas nos discos rígidos dos computadores não são cobertas pelas cópias de segurança.
  - providenciar a guarda externa de cópias de segurança recentes, em empresa especializada, contratada para este fim;
  - assegurar que o armazenamento externo ou descartes das cópias de segurança seja realizado por meio de procedimentos adequados, para preservar o sigilo das informações.

Responsabilidades da Gerho

- Definir o nome 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.

Utilização de *softwares* (instalação, licenciamento e *copyright*)

- Necessidades de aquisição de *softwares* devem ser formalmente solicitadas 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.

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 no Termo de Confidencialidade, Instruções sobre a Proteção de Confidencialidade Estatística e no Protocolo de Confidencialidade formalizados pela Fundação Seade.

Uso da Internet e recursos providos pela Fundação Seade

- A Internet é disponibilizada como recurso para a consecução das atividades institucionais, consultas, pesquisas e troca de informações e ideias sempre ligadas aos interesses corporativos.
- O acesso à Internet pode ser revogado ou bloqueado por desrespeito à PSI, por ameaça a qualquer ativo ou necessidade de serviço.
- Deve-se evitar o uso da Internet para fins de entretenimento (filmes, jogos, etc.) para não comprometer a disponibilidade do 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, da CS 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 proibida e 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.
- A utilização de equipamentos de tecnologia da informação é permitida em equipamentos alocados/compartilhados em seu posto de trabalho ou fora dele, em pleno exercício de suas atribuições. A utilização ainda é condicionada pelos direitos de acessos configurados em cada conta.
- 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 permitida a utilização de equipamentos pessoais ou de terceiros na rede corporativa da Fundação Seade.
- 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, 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 pelo empregado/colaborador.

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 devem ser utilizados com ética.

- 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 recuperação de informações relacionadas às atividades da Fundação Seade 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.

Segurança física

- Ativos de tecnologia de 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.

Auditorias

- A critério da CS ou da Diretoria, qualquer conta de acesso e *e-mail* poderá ser monitorada, 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 cobertos pelo sigilo.
- A critério da CS ou da Diretoria, podem ser realizadas auditorias para verificar se os requisitos de segurança da informação estão sendo aplicados corretamente.

Penalidades

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

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: ABNT, 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.

ABNT NBR ISO/IEC 27002 – 2013.