SESCOOP/SP

RESOLUÇÃO Nº 089/2022 – CONSELHO ADMINISTRATIVO DO SESCOOP/SP

Dispõe sobre a regulamentação da Política de Segurança da Informação PSI - do Serviço Nacional de Aprendizagem do Cooperativismo no Estado de São Paulo - SESCOOP/SP.

O Presidente do Conselho Administrativo do Serviço Nacional de Aprendizagem do Cooperativismo no Estado de São Paulo – SESCOOP/SP, no uso das atribuições conferidas nos incisos III e IX do artigo 13 do seu Regimento Interno (Resolução nº 71/2019), torna público que o Conselho Administrativo, 206ª (ducentésima sexta) Reunião Ordinária, realizada em 22 de fevereiro de 2022,

CONSIDERANDO a previsão estabelecida no artigo 4º, inciso III, alínea "a" e inciso IV e artigo 17 do Regulamento da Governança Corporativa (Resolução 078/2020 do Conselho Administrativo do SESCOOP/SP), que dispõem respectivamente sobre o Regulamento de natureza estratégica, que as deliberações do Conselho Administrativo serão instrumentalizadas por meio de Resolução e da revisão dos normativos internos,

CONSIDERANDO na necessidade de preservar a integridade, confidencialidade, autenticidade e disponibilidade das informações do SESCOOP/SP,

CONSIDERANDO a necessidade de assegurar o cumprimento das propriedades da informação, otimizando riscos, maximizando a eficácia ao acesso às informações, e, garantindo a continuidade das atividades do SESCOOP/SP,

RESOLVEU

Art. 1º – Aprovar a Política de Segurança da Informação PSI, aplicável a todos usuários de informação do SESCOOP/SP e a todo tipo de informação tanto localizada em ambiente de tecnologia quanto em em ambiente convencional.

Art. 2º – Esta Política, entra em vigor, na data de sua aprovação pelo Conselho Administrativo do SESCOOP/SP, revogando as disposições da Resolução 069 de 13 de setembro de 2018.

São Paulo, 22 de março de 2022.

EDIVALDO DEL GRANDE
Presidente do Conselho Administrativo do SESCOOP/SP

SESCOOP/SP

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO - PSI DO SERVIÇO NACIONAL DE APRENDIZAGEM DO COOPERATIVISMO - SESCOOP/SP

CAPÍTULO I
CONCEITO E OBJETIVO

Art. 1º. A Política de Segurança da Informação – PSI é o conjunto de princípios, regras e ações que norteiam a gestão de segurança das informações, a fim de assegurar o acesso aos recursos computacionais e suas informações.

Art. 2º. A informação é o conjunto de dados, textos, imagens, métodos, sistemas ou qualquer forma de representação dotada de significado em determinado contexto independente do suporte em que resida ou da forma pela qual seja veiculado.

Art. 3º. A PSI objetiva assegurar o cumprimento das propriedades da informação, otimizando riscos, maximizando a eficácia ao acesso às informações, e, portanto, garantindo a continuidade do negócio.

Art. 4º. As propriedades da informação são: integridade, confidencialidade, autenticidade e disponibilidade:

I. **Integridade** — garantir que a informação seja mantida em seu estado original visando protegê-la, na guarda ou transmissão, contra alterações indevidas intencionais ou acidentais;

II. **Confidencialidade** — garantir que o acesso à informação seja obtido somente por pessoas autorizadas;

III. **Autenticidade** — consiste na garantia da veracidade da fonte das informações. Por meio da autenticação é possível confirmar a identidade da pessoa ou entidade que presta as informações.

IV. **Disponibilidade** — garantir que os usuários autorizados obtenham acesso às informações e aos ativos correspondentes sempre que necessário.

CAPÍTULO II
ABRANGÊNCIA

Art. 5º. As diretrizes apresentadas nesta Política se aplicam a todos os usuários de informação do **SESCOOP/SP**: conselheiros, presidente, superintendentes, empregados estagiários, aprendizes, visitantes, alunos, prestadores de serviço, etc., e também, abrange toda informação, independente do meio ou forma em que se apresente, logo, em ambiente de tecnologia ou em ambiente convencional.

Parágrafo 1º. Ambiente de Tecnologia: é o ambiente em que o usuário se relaciona com a informação de maneira indireta, através de equipamentos avançados de tecnologia do tipo

Serviço Nacional de Aprendizagem do Cooperativismo
no Estado de São Paulo
Rua Treze de Maio, 1376 - Bela Vista
01327-002 - São Paulo - SP
www.sescoopsp.coop.br

computadores. Neste ambiente, a informação encontra-se em formato digital e, com a utilização destes equipamentos, os usuários conseguem acessar a informação.

Parágrafo 2º. Ambiente Convencional: é o ambiente em que o usuário se relaciona diretamente com a informação que está armazenada em uma superfície que seja possível ler, tipo papel, ou através da comunicação direta, oral, visual ou tátil de uma informação.

CAPÍTULO III
PRINCÍPIOS E REGRAS
Seção I – Propriedade da Informação do SESCOOP/SP

Art. 6º. Toda informação produzida ou recebida pelos usuários, que resulte da atividade profissional contratada ou prestada ao **SESCOOP/SP**, pertence ao **SESCOOP/SP**. As exceções deverão ser explicitadas e formalizadas em contrato entre as partes.

Seção II – Uso da informação pelos usuários

Art. 7º. Os equipamentos de informática, comunicação, sistemas, informações autorizadas e disponibilizadas deverão ser utilizados pelos usuários, única e exclusivamente, para o desempenho de suas atividades profissionais no **SESCOOP/SP**.

Parágrafo único: É proibida qualquer atividade dos usuários na utilização dos recursos de tecnologia do **SESCOOP/SP** que viole esta política. A entidade poderá verificar e auditar qualquer ação sobre informação ou recurso disponibilizado para o usuário.

Seção III – Computação pessoal e móvel

Art. 8º. As informações estruturadas e sistemas da entidade, somente serão utilizados, em recursos (dispositivos) da entidade. É proibido o uso de equipamentos pessoais para acessar informações estruturadas e sistemas corporativos do **SESCOOP/SP**.

Seção IV – Correio Eletrônico (E-mail)

Art. 9º. O uso do correio eletrônico (e-mail) do **SESCOOP/SP** é para fim corporativo e relacionado às atividades do usuário na entidade.

Parágrafo 1º. Cada usuário é responsável pela conta de e-mail disponibilizada pela entidade, tendo ciência que o conteúdo do correio eletrônico poderá ser acessado e monitorado pelo **SESCOOP/SP**.

Parágrafo 2º. As mensagens do correio eletrônico devem ser escritas com linguagem profissional e cordial, não comprometendo a imagem do **SESCOOP/SP.**

Parágrafo 3º. É proibido: enviar spam, mensagem usando nome de outra pessoa ou do departamento sem autorização; mensagens que tornem o remetente ou o **SESCOOP/SP** vulnerável à ação civil ou criminal; falsificar ou alterar endereçamento ou cabeçalho, apagar mensagens quando a pessoa ou o **SESCOOP/SP** estiver sujeito a investigações; e enviar

Serviço Nacional de Aprendizagem do Cooperativismo
no Estado de São Paulo
Rua Treze de Maio, 1376 - Bela Vista
01327-002 - São Paulo - SP

e-mails com anexo(s) superior(es) ao tamanho máximo permitido, divulgado internamente pela Área de Tecnologia da Informação. Havendo necessidade de envio de arquivo acima do tamanho permitido (25 Mb) deverá ser solicitado orientação junto a Área de Tecnologia da Informação.

Seção V – Ambiente da Internet: Rede Social

Art. 10º. O ambiente da internet deve ser usado para o desempenho das atividades profissionais do usuário. Sites que não, contenham informações que agreguem conhecimento para os serviços prestados não devem ser acessados.

Parágrafo 1º. O usuário deverá observar, no uso da internet, um comportamento eminentemente ético e profissional de forma a não expor o **SESCOOP/SP** ou torná-lo vulnerável à ação civil ou criminal. 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.

Parágrafo 2º. Qualquer informação que é acessada, transmitida, recebida ou produzida na internet está sujeita a divulgação e auditoria. Portanto, o **SESCOOP/SP**, em total conformidade legal, reserva-se o direito de monitorar e registrar todos os acessos a ela.

Parágrafo 3º. É proibida a divulgação e/ou o compartilhamento indevido de informações em listas de discussão, sites ou comunidades de relacionamento, sala de bate-papo ou chat, comunicadores instantâneos ou qualquer outra tecnologia correlata que venha surgir na internet.

Seção VI – Acesso à informação: Nível de sigilo e confiabilidade

Art. 11. À informação, com relação ao nível de sigilo e confidencialidade, deverá ser classificada pelo Gestor da Informação, que é o responsável pela autorização de acesso às informações sob a sua responsabilidade e área de atuação. A definição do gestor da informação se dará por meio do Termo de Responsabilidade - PSI, Anexo I.

Parágrafo 1º. A autorização de acesso. aos sistemas informatizados e respectivos documentos em papel deverá ser concedida apenas para os usuários que necessitem da informação para o desempenho de suas atividades profissionais.

Parágrafo 2º. A autorização de acesso (leitura, atualização, criação, remoção) poderá ocorrer de forma discreta (individual), via perfil de acesso, por meio de grupo de acesso ou outra forma definida pelo gestor da informação ou normativo específico.

Parágrafo 3º. O acesso da informação também engloba aquelas hospedadas em ambiente fora do **SESCOOP/SP**, tais como sistemas de informação (**SESCOOP/SP** ou não) hospedados em "nuvem" e/ou sites da Internet.

Serviço Nacional de Aprendizagem do Cooperativismo
no Estado de São Paulo
Rua Treze de Maio, 1376 - Bela Vista
01327-002 - São Paulo - SP
www.sescoopsp.coop.br

Parágrafo 4º. É proibida a divulgação de informações, imagens de tela, sistemas, documentos ou qualquer outro meio sem autorização expressa do gestor da informação, inclusive após o desligamento do **SESCOOP/SP**.

Parágrafo 5º. Cada usuário deverá acessar apenas as informações e os ambientes previamente autorizados. E qualquer tentativa de acesso consciente a ambientes não autorizados será considerada falta grave.

Seção VII – Identificação, autenticação e autorização de acesso

Art. 12. O acesso à informação e aos seus diversos recursos tecnológicos, pelo usuário deverá ser pessoal e intransferível.

Art. 13. A forma de autenticação do usuário será definida pela Área de Tecnologia da Informação, que informará o usuário dos procedimentos a serem adotados.

Art. 14. Este acesso acontecerá através da identificação e da autenticação do usuário. Os dados para autenticação devem ser mantidos em segredo e possuem o mais alto nível de classificação da informação. Na autorização de acesso à informação deverá ser considerado:

I. As atividades profissionais relacionadas ao usuário, perfil ou grupo;

II. O sigilo da informação e o poder decorrente da utilização da informação;

III. A necessidade de segregação de função do usuário;

IV. A regra de mínimo acesso para o usuário.

Art. 15. Para acesso a rede interna do **SESCOOP/SP** e sistemas, cada usuário receberá para primeiro acesso, login e senha disponibilizada pela Área de Tecnologia da Informação, no entanto, após seu primeiro acesso, deverá cadastrar nova senha, memorizando-a, para Uso pessoal e intransferível, ou seja, não sendo compartilhada com colegas ou outros usuários.

Parágrafo único. É de inteira responsabilidade do usuário a guarda e a utilização da(s) senha(s) fornecida(s), devendo trocá-la(s) nos períodos definidos pela área de Tecnologia da Informação.

Art. 16. A estação de trabalho deverá ser bloqueada sempre que o usuário se afastar do seu posto de trabalho, a fim de não permitir o acesso de informações sob sua responsabilidade.

Art. 17. Os usuários deverão armazenar os arquivos de trabalho na pasta de rede exclusiva de cada área, para que todos os usuários da área possam utilizá-los; e armazenar os arquivos individuais de trabalho na pasta (U:\) ou no serviço corporativo disponibilizado em nuvem, para que haja garantia de integridade confidencialidade, autenticidade e disponibilidade.

Serviço Nacional de Aprendizagem do Cooperativismo
no Estado de São Paulo
Rua Treze de Maio, 1376 - Bela Vista
01327-002 - São Paulo - SP

Parágrafo único. Os arquivos de trabalho a serem compartilhados entre áreas distintas poderão ser armazenados temporariamente na pasta pública da rede (P:\), porém, não terão garantia de integridade, confidencialidade, autenticidade e disponibilidade, por se tratar de um diretório para uso temporário.

CAPÍTULO IV
MONITORAMENTO E GRAVAÇÃO DA INFORMAÇÃO

Art. 18. Esta política dá ciência aos usuários que os ambientes, sistemas de informação estações de trabalho, servidores, correio eletrônico, conexões com a internet, dispositivos móveis, wireless e outros componentes da rede serão monitorados e gravados.

Parágrafo 1º. O **SESCOOP/SP**, por meio da área de Tecnologia da Informação, monitorará o uso dos sistemas e serviços (estações de trabalho, servidores, correio eletrônico conexões com a internet, dispositivos móveis ou wireless e demais componentes da rede) visando garantir a segurança, integridade, confiabilidade, autenticidade e disponibilidade das informações. A informação gerada por esses sistemas será utilizada para identificar usuários e respectivos acessos efetuados, bem como material manipulado.

Parágrafo 2º. O **SESCOOP/SP**, ao monitorar a rede interna, pretende garantira integridade dos dados e programas.

Parágrafo 3º. Toda tentativa de alteração dos parâmetros de segurança, por qualquer usuário, sem o devido credenciamento e autorização para tal, será julgada inadequada e os riscos relacionados serão informados ao usuário e respectivo gestor. O uso de qualquer recurso, para atividades ilícitas poderá acarretar às ações administrativas e as penalidades decorrentes de processos civil e criminal, sendo que nesses casos a instituição cooperará com as autoridades competentes.

CAPÍTULO V
GESTÃO DA CONTINUIDADE DO NEGÓCIO E CONTINGÊNCIAS

Art.19. Toda informação deve ser protegida para que não seja alterada, acessada e destruída indevidamente.

Art. 20. Toda informação utilizada pela entidade deverá possuir, pelo menos, uma cópia de segurança atualizada e guardada em local com proteção equivalente ao local principal.

Art. 21. Os recursos tecnológicos, de infraestrutura e os ambientes físicos, onde são realizadas as atividades operacionais, devem ser. protegidos contra situações de indisponibilidade, como falta de energia, incêndio e constar no plano de gestão de continuidade do negócio.

Parágrafo único. O Plano de Gestão de Continuidade do negócio deverá ser desenvolvido pela área de Tecnologia da Informação, sendo aprovado pelo Comitê de Segurança Informação.

Serviço Nacional de Aprendizagem do Cooperativismo
no Estado de São Paulo
Rua Treze de Maio, 1376 - Bela Vista
01327-002 - São Paulo - SP

CAPÍTULO VI
CÓPIAS DE SEGURANÇA (BACKUP) E RESTAURAÇÃO (RESTORE) INCLUSIVE DE DADOS HOSPEDADOS EM NUVEM

Art. 22. Deverá ser executado procedimentos de backup e restore dos dados do **SESCOOP/SP**, inclusive dos serviços em nuvem, sendo observadas as disposições deste capítulo.

Art. 23. A política de backup a ser adotada deverá contemplar as seguintes características mínimas:

I. Backup full com as seguintes periodicidades: Semanal, aos sábados e/ou domingos; Mensal, no primeiro sábado e/ou domingo cada mês.

II. Backup incremental ou diferencial com periodicidade diária, executado na janela das 20h às 7h.

Art. 24. Deverá alocar e gerenciar automaticamente o armazenamento de backup.
Art. 25. Deverá realizar a transmissão segura e o armazenamento dos dados criptografados.

Art. 26. Deverá fornecer backups consistentes, garantindo que correções adicionais não sejam necessárias para restaurar os dados.

Art. 27. Deverá permitir retenção dos backups durante a vigência do contrato.

Art. 28. Deverá permitir transferência de dados ilimitada, tanto para backup quanto para restore, dentro da região ou do próprio datacenter do provedor.

Art. 29. Deverá fornecer sistema de alertas para falhas no processo de backup, ou consistência dos arquivos.

Art. 30. Deverá prover o armazenamento em nuvem, de cópias de segurança;

Art. 31. O serviço de armazenamento de backup em nuvem, deve prover escala ilimitada e proporcionar alta disponibilidade, sem necessidade de manutenção ou sobrecarga de monitoramento.

Art. 32. Os dados devem ser persistidos com redundância, em equipamentos de hardware diferentes, de forma a prevenir perda de dados com falhas de hardware.

Art. 33. Deverá permitir retenção de dados limitado ao prazo de vigência do contrato.

Art. 34. Deverá permitir a criptografia dos dados.

Art. 35. Deverá implantar procedimento formal periódico de simulação de restauração (restore) a partir dos backups gerados. Este procedimento deverá contemplar a restauração

Serviço Nacional de Aprendizagem do Cooperativismo
no Estado de São Paulo
Rua Treze de Maio, 1376 - Bela Vista
01327-002 - São Paulo - SP

semestral de, no mínimo, 30% do volume total de dados. A documentação que determinará estas simulações deverá ser previamente aprovada pelo **SESCOOP/SP**, que receberá relatórios consolidados dos resultados.

Art. 36. A tecnologia utilizada para a realização das cópias de segurança deverá permitir a realização do backup de todos os dados, inclusive os que estiverem sendo utilizados dentro do horário de realização das cópias.

Art. 37. As solicitações de exclusão e inclusão de novas áreas de armazenamento nos backups deverão ser avaliadas e efetivamente operacionalizadas, em um prazo máximo de 24 (vinte e quatro) horas.

Art. 38. As solicitações de restauração de dados previamente armazenados nos backups deverão ser avaliadas e efetivamente operacionalizadas, em um prazo máximo de 24 (vinte e quatro) horas, para o caso de dados inclusos nos backups diários, e de 72 (setenta e duas) horas para backups de período de retenção mais longo.

Art. 39. Deverá ser disponibilizado acesso de leitura para que a equipe técnica do **SESCOOP/SP** tenha visibilidade da console da ferramenta de backup a qualquer tempo, além de relatórios gerenciais mensais de disponibilidade para a aferição da prestação de serviços.

Art. 40. Para o backup do ambiente de virtualização:

I. Permitir múltiplos snapshots de uma máquina virtual a quente.

II. Permitir Snapshots ou backups consistentes de máquinas virtuais em execução e seu armazenamento no cluster.

III. O método de realização é o chamado, pela Commvault, de Intellisnap e deve ser implementado pela solução ofertada por tecnologia equivalente, devendo ser possível efetuar operação conhecida como "live mount".

IV. Realizar a geração de snapshots, cópia do estado e configurações dos sistemas virtualizados, com os sistemas ativados, bem como, realizar a reversão para estados anteriores da máquina.

V. Retenção dos snapshots:
   a. Hora em Hora: 6 snapshots
   b. Diário: 2 snapshots
   c. Semanal: 2 snapshots
   d. Retenção: 10 dias

Serviço Nacional de Aprendizagem do Cooperativismo
no Estado de São Paulo
Rua Treze de Maio, 1376 - Bela Vista
01327-002 - São Paulo - SP
www.sescoopsp.coop.br

CAPÍTULO VII
CONTRATAÇÃO DE SERVIÇOS EM NUVEM

Art. 41. Na contratação de Serviço em nuvem deverão ser observadas as disposições seguintes:

I. a realização de análise prévia, visando assegurar as garantias fundamentais no tratamento das informações pessoais, segundo preconizam os incisos e os parágrafos do artigo 31 da Lei 12.527, de 18 de novembro de 2011 – Lei de Acesso à Informação;

II. a adequação da contratada à conformidade com os termos da Lei 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais;

III. a prévia classificação da informação hospedada pelo seu gestor quanto ao sigilo de seu conteúdo;

IV. a definição de critérios de continuidade aceitáveis;

V. a definição de critérios para garantir os princípios de confidencialidade, integridade e disponibilidade;

VI. a definição de critérios para permitir a comunicação tempestiva e o adequado tratamento de incidentes de segurança computacional;

VII. a definição de critérios adequados à realização de auditorias de segurança da informação;

VIII. definição do uso aceitável de dados, metadados, informações e conhecimentos tratados, inclusive sobre a vedação ao provedor ou a terceiros de utilização diversa da prevista em contrato;

IX. definição de critérios de eliminação ou destruição definitiva de dados, metadados, informações e conhecimento, especialmente em momentos de transição contratual;

X. requisitos necessários, para os casos de cancelamento, descontinuidade, portabilidade e renovação do referido instrumento contratual ou similar, bem como substituição de ambiente, que visem à eliminação e/ou à destruição definitiva de dados, metadados, informações e conhecimento.

CAPÍTULO VIII
CONTROLE DE ACESSO AO TELETRABALHO E À VPN

Art. 42. A solicitação de concessão de acesso remoto, para execução do teletrabalho, será formalizada pelo responsável da unidade à área de Infraestrutura.

Serviço Nacional de Aprendizagem do Cooperativismo
no Estado de São Paulo
Rua Treze de Maio, 1376 - Bela Vista
01327-002 - São Paulo - SP

Parágrafo Único. No ambiente de teletrabalho, o usuário contará com o mesmo perfil de acesso que detém na rede de computadores e nos sistemas informatizados do **SESCOOP/SP**.

Art. 43. A área de Infraestrutura deverá disponibilizar ferramental para o teletrabalho que proporcione:

I – Segurança do meio de comunicação;

II – Autenticação dos usuários;

III – Limite de acesso restrito aos recursos computacionais segundo as necessidades de cada usuário.

Art. 44. É recomendável ao usuário em regime de teletrabalho:

I – Manter seu computador com as últimas atualizações e correções de segurança instaladas;

II – Utilizar somente sistema operacional e programas licenciados;

III – Manter programa antivírus atualizado;

IV – Habilitar o firewall do sistema operacional;

V – Não expor dados e informações sensíveis do **SESCOOP/SP** a terceiros;

VI – Não salvar as senhas de acesso ao ambiente de teletrabalho nos navegadores ou outros programas;

VII – Alterar imediatamente suas senhas de rede e sistemas em caso de perda, roubo, descarte ou manutenção do equipamento utilizado para teletrabalho;

VIII – Configurar a rede sem fio doméstica com pelo menos o protocolo WPA2, alterando a senha padrão do roteador.

IX – Armazenar os documentos corporativos exclusivamente nos locais adequados providos no ambiente de teletrabalho;

X – Utilizar equipamento apropriado às atividades de trabalho remoto;

Parágrafo único. O licenciamento do sistema operacional e demais programas instalados na estação de trabalho doméstica do usuário é de sua inteira responsabilidade.

Art. 45. O acesso realizado pelo ambiente de teletrabalho será monitorado e registrado, podendo a qualquer momento ser efetuada auditoria, conforme estabelecido no Capítulo IV desta Política.

Serviço Nacional de Aprendizagem do Cooperativismo
no Estado de São Paulo
Rua Treze de Maio, 1376 - Bela Vista
01327-002 - São Paulo - SP

CAPÍTULO IX
POLÍTICA DE MANUTENÇÃO, REMANEJAMENTO, DOAÇÃO OU DESCARTE DE EQUIPAMENTOS DE TI

Art. 46. Em caso de manutenção de equipamentos de TI, a unidade de Infraestrutura deverá considerar as seguintes recomendações:

I – equipamentos, informações ou softwares não devem ser retirados do local sem autorização prévia;

II – realizar backup e eliminar as informações do equipamento quando a manutenção for realizada por equipe externa ao **SESCOOP/SP**;

III – após a manutenção por equipe externa, inspecionar o equipamento para garantir que não foi alterado indevidamente e que não há mau funcionamento.

Art. 47. Em caso de remanejamento de equipamentos de TI, a unidade responsável deverá considerar a formatação do equipamento antes de realizar o seu remanejamento para outra unidade.

Art. 48. Em caso de doação ou descarte de equipamentos de TI, a unidade responsável pela Infraestrutura deverá formatar previamente o equipamento.

CAPÍTULO X
BOAS PRÁTICAS DE SEGURANÇA DA INFORMAÇÃO

Art. 49. Durante a execução das suas atividades profissionais, todos os usuários do **SESCOOP/SP**, seja presencialmente, seja em teletrabalho, devem observar as seguintes recomendações:

I – guardar em local seguro informações sensíveis ou críticas que estejam armazenadas em papel, mídia eletrônica ou outro meio, especialmente quando o local de trabalho estiver desocupado;

II – desligar ou hibernar os computadores ao final do expediente;

III – bloquear os computadores com senha no caso de ausências curtas, por exemplo, para almoço, lanche e reuniões;

IV – utilizar somente equipamentos do próprio **SESCOOP/SP** na realização do trabalho presencial

V – triturar documentos a serem descartados que contenham dados pessoais;

VI – arquivar adequadamente os documentos físicos, considerando o uso de armários com chaves e acessos controlados;

Serviço Nacional de Aprendizagem do Cooperativismo
no Estado de São Paulo
Rua Treze de Maio, 1376 - Bela Vista
01327-002 - São Paulo - SP

VII – certificar-se sobre os destinatários de e-mail antes de enviar a mensagem;

VIII – dar preferência a assinaturas digitais;

VIX – evitar encaminhar documentos digitalizados que contenham assinaturas manuscritas.

CAPÍTULO XI
IMPLANTAÇÃO E COMUNICAÇÃO DA PSI

Art. 50. A responsabilidade em relação à segurança da informação deve ser comunicada na fase de contratação dos empregados, ou, em momento oportuno, quando da sua implantação para aqueles contratados anteriores a esta PSI.

Art. 51. Os usuários serão orientados sobre os procedimentos de segurança e uso correto dos ativos de informação, a fim de reduzir possíveis riscos, e ainda, poderão receber treinamento complementar, para assegurar o cumprimento desta política em ambiente interno e externo do **SESCOOP/SP**.

Art. 52. Os usuários tomarão ciência desta política, e deverão assinar o Termo de Responsabilidade - PSI, Anexo I, em conjunto com o Gestor da Informação comprometendo-se a cumprir os princípios, regras e ações que norteiam os procedimentos de segurança da informação.

Parágrafo único. É obrigação dos usuários cumprir e manterem-se atualizados em relação à PSI, buscando orientação do seu gestor ou da área de Tecnologia da Informação, sempre que não estiver absolutamente seguro quanto à aquisição, uso e/ou descarte de informações.

CAPÍTULO XII
PENALIDADES

Art. 53. O não cumprimento das regras (violação da integridade, quebra de sigilo, inserção de dados falsos, modificação ou alteração não autorizada de sistemas e outras condutas não conformes à PSI), acarretará sanções administrativas e/ou contratuais, podendo chegar à demissão do empregado ou rescisão unilateral do contrato de prestação de serviços, bem como estarão sujeitas às penalidades decorrentes de processos nas áreas civil e criminal.

CAPÍTULO XIII
CLÁUSULA DE CONFIDENCIALIDADE E REQUISITOS DE PRIVACIDADE E PROTEÇÃO DE DADOS

Art. 54. Deverá constar em todos os contratos do **SESCOOP/SP** cláusulas e/ou anexo de Acordo de Confidencialidade, como condição imprescindível para que possa ser concedido o acesso aos ativos de informação disponibilizados pela instituição.

Serviço Nacional de Aprendizagem do Cooperativismo
no Estado de São Paulo
Rua Treze de Maio, 1376 - Bela Vista
01327-002 - São Paulo - SP

CAPÍTULO XIV
RESPONSABILIDADES ENVOLVIDAS
Seção I – Usuários

Art. 55. São responsáveis por observar, cumprir e manter-se atualizados com relação à PSI, assinar o Termo de Responsabilidade-PSI, Anexo I, em conjunto com o Gestor da Informação, bem como:

I. Buscar informação junto ao Gestor da Informação sempre que não estiver absolutamente seguro quanto à obtenção, uso e/ou descarte de informações;

II. Utilizar a informação e os recursos tecnológicos disponibilizados pelo **SESCOOP/SP** em conformidade com as determinações desta política;

III. Contribuir para a melhoria contínua desta política comunicando a área de Tecnologia da Informação qualquer atitude ou procedimento não aderente, recomendando os aperfeiçoamentos ao processo.

Seção II – Área de Tecnologia da Informação

Art. 56. A área de Tecnologia da informação é a custodiante dos ativos da informação responsabilizando-se também:

I Pelas orientações técnicas e procedimentos estabelecidos nesta política;

II Pela coordenação do Comitê de Segurança da Informação - CSI;

III. Manutenção e melhoria contínua do processo de Segurança de Informação do **SESCOOP/SP**, revisão e atualização desta PSI, proposição das resoluções complementares, treinamento e implantação das mesmas;

IV. Por esclarecer as dúvidas e informações adicionais a esta política, que deverão ser solicitados via "sistema de chamado" da área de Tecnologia da informação.

Seção III - Gestores da Informação

Art. 57. São responsáveis pela atribuição do acesso à informação dos usuários e sistemas de informação sob sua responsabilidade, e, também:

I. Pela atribuição de permissão de acesso via solicitação de login e senha para os usuários dos sistemas de informação sob sua subordinação. Para isso deverão descrever os sistemas e acessos autorizados, e assinar o Anexo |, Termo de Responsabilidade-PSI, em conjunto com o usuário;

Serviço Nacional de Aprendizagem do Cooperativismo
no Estado de São Paulo
Rua Treze de Maio, 1376 - Bela Vista
01327-002 - São Paulo - SP

II. Manter os processos sob sua responsabilidade aderentes às políticas, normas e procedimentos específicos de segurança da informação, tomando as ações necessárias para cumprir tal responsabilidade.

Seção IV — Comitê de Segurança da Informação – CSI

Art. 58. O Comitê de Segurança da Informação — CSI, composto pelos profissionais indicados, será responsável pela análise e tratamento dos incidentes de segurança e não conformidades à PSI: proposição de sanções administrativas e/ou contratuais; orientação quanto a proposta orçamentária para o Plano Diretor de Segurança da Informação e Plano de Continuidade do Negócio; elaboração de novos regulamentos sobre segurança da informação, visando o aprimoramento deste processo de atualização desta política.

Art. 59. O Comitê de Segurança da Informação — CSI será composto por representantes nomeados por portaria.

Art. 60. A convocação para reuniões e atuação do CSI será estabelecido em instrumento próprio.

Art. 61. Toda violação à PSI deverá ser comunicada inicialmente aos componentes do Comitê de Segurança da Informação.

Parágrafo único: São exemplos de incidentes a serem tratados pelo Comitê de Segurança da Informação:

a. Tentativas de obter acesso não autorizado a sistemas ou informação;
b. Ataques de negação de serviços, ransomware e demais malwares;
c. Uso ou acesso não autorizado a um sistema;
d. Modificações em um sistema, sem o conhecimento, instruções ou consentimento prévio;
e. Roubo ou extravio de informações;
f. Perda de informações ou equipamentos que armazenam dados críticos;
g. Desrespeito à política de segurança.

CAPÍTULO XV
CONSIDERAÇÕES FINAIS

Art. 62. A PSI deverá ser revista e atualizada a qualquer tempo sempre que algum fato relevante motive sua revisão.

Parágrafo único: As normas complementares a esta política serão aprovadas conforme alçadas estabelecidas nos normativos internos do **SESCOOP/SP**, sendo previamente comunicadas aos usuários, e quando necessário, disseminadas através de treinamentos específicos.

Art. 63. As dúvidas e casos omissos não abrangidos por esta política serão submetidos para deliberação do Conselho Administrativo do SESCOOP/SP.

Serviço Nacional de Aprendizagem do Cooperativismo
no Estado de São Paulo
Rua Treze de Maio, 1376 - Bela Vista
01327-002 - São Paulo - SP
www.sescoopsp.coop.br

Art. 64. Esta Política, entra em vigor, na data de sua aprovação pelo Conselho Administrativo do SESCOOP/SP, revogando as disposições da Resolução 069 de 13 de setembro de 2018, podendo ser revista sempre que necessário.

São Paulo, 22 de março de 2022.

EDIVALDO DEL GRANDE
Presidente do Conselho Administrativo do SESCOOP/SP

Serviço Nacional de Aprendizagem do Cooperativismo no Estado de São Paulo
Rua Treze de Maio, 1376 - Bela Vista
01327-002 - São Paulo - SP
www.sescoopsp.coop.br

SESCOOP/SP

ANEXO I

TERMO DE RESPONSABILIDADE E ADERÊNCIA À POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DO SESCOOP/SP

SESCOOP/SP	TERMO DE RESPONSABILIDADE - PSI		
I – IDENTIFICAÇÃO DO USUÁRIO			
Nome:			
Detalhamento:	**Tipo de usuário:**	**Cargo:**	**Matrícula:**
		Lotação:	**CPF:**
II – IDENTIFICAÇÃO DO GESTOR			
Nome:		**Cargo:**	
Matrícula:		**CPF:**	
III – IDENTIFICAÇÃO DOS ACESSOS – SISTEMAS			
Sistema	**Módulos/grupo**	**Nível de acesso**	

Pelo presente Termo declaro conhecer o conteúdo da Política de Segurança da Informação – PSI do **SESCOOP/SP**, e na qualidade de usuário comprometendo-me a cumprir suas recomendações e determinações.

Declaro estar ciente do privilégio de acesso ou alteração do(s) sistema(s) informatizado(s), e respectivos documentos em papel, autorizado pelo gestor da informação, descrito neste formulário ou e-mail.

Declaro que concordo em cumprir os princípios, regras e ações apresentadas na Política de Segurança da Informação - PSI, e que estou ciente que o não cumprimento poderá acarretar penalidades administrativas.

Declaro que estou ciente que não devo ter expectativa de privacidade em relação às minhas atividades no ambiente computacional e tecnológico, que serão registradas e poderão ser auditadas ou investigadas pela entidade.

Concordo em notificar a área do Departamento Pessoal sobre quaisquer circunstâncias que possam tornar falsas, imprecisas ou incompletas as declarações aqui prestadas.

Serviço Nacional de Aprendizagem do Cooperativismo no Estado de São Paulo
Rua Treze de Maio, 1376 - Bela Vista
01327-002 - São Paulo - SP
www.sescoopsp.coop.br

SESCOOP/SP

Comprometo-me a comunicar a área de Tecnologia da Informação as não conformidades observadas com relação à Política de Segurança da Informação - PSI, visando o processo de melhoria contínua.

São Paulo XX de XXXXXX de 20XX

_____	_____
Nome do usuário	Nome do Gestor da Informação
Cargo:	Cargo:
Departamento:	Departamento:

Serviço Nacional de Aprendizagem do Cooperativismo no Estado de São Paulo
Rua Treze de Maio, 1376 - Bela Vista
01327-002 - São Paulo - SP

www.sescoopsp.coop.br

sistemaocesp @sistemaocesp Sistema Ocesp

ANEXO II
GLOSSÁRIO DE TERMOS TÉCNICOS

TERMO	SIGNIFICADO
Ativos de informação	São os meios de produção, armazenamento, transmissão e processamento de informações, os sistemas de informação, além das informações em si, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso.
Classificação da informação	Identificação de quais são os níveis de proteção que as informações demandam e estabelecimento de classes e formas de identificá-las, além de determinar os controles de proteção necessários a cada uma delas.
Comitê de Segurança d Informação	Colegiado de caráter deliberativo responsável pela análise dos incidentes, penalidades, orientações e melhorias dos processos de segurança da informação.
Computação em nuver	Utilização da capacidade de armazenamento e processamento de servidores, compartilhados e interligados por meio da Internet.
Controle de acesso	Conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso.
Custodiante do ativo de informação	É aquele que, de alguma forma, zela pelo armazenamento, operação, administração e preservação de ativos de informação que não lhe pertencem, mas que estão sob sua custódia.
Gestão de continuidade do negócio	Processo de gestão que identifica ameaças potenciais para uma organização e os possíveis impactos nas operações de negócio, caso essas ameaças se concretizem.
Gestores da informaçã	Gestores de equipes responsáveis por autorizar acesso a sistemas de informação de seus subordinados.
incidente de segurança	Evento que tenha causado algum dano, colocando em risco algum ativo de informação crítico ou interrompido a execução de alguma atividade; não conformidade à Política de Segurança da Informação.
Informação estruturada	É aquela que já foi tratada, classificada, recebeu valor agregado e obedece a um fluxo, podendo ser recuperada facilmente.
Malware	É um programa de computador destinado a infiltrar-se em um sistema de computador alheio de forma ilícita, com o intuito de causar algum dano, alterações ou roubo de informações.

Serviço Nacional de Aprendizagem do Cooperativismo
no Estado de São Paulo
Rua Treze de Maio, 1376 - Bela Vista
01327-002 - São Paulo - SP

Ransomware	É um tipo de software nocivo que restringe o acesso. ao sistema infectado e cobra um resgate para que o acesso possa ser restabelecido.
Recursos de Tecnologi	Computadores e equipamentos, softwares, redes e telecomunicações, sistemas de armazenamento e recuperação de dados, aplicações computacionais, cabeamento e rede telefônica.
Segurança da Informação	Proteção da informação contra ameaças;
Site	Conjunto de páginas (Web) acessíveis na internet. E alocado num servidor conectado à rede mundial de computadores;
Tratamento de incident	É o processo que consiste em receber, filtrar, classificar e responder às análises dos incidentes, procurando extrair informações que permitam impedir a continuidade.

Serviço Nacional de Aprendizagem do Cooperativismo no Estado de São Paulo
Rua Treze de Maio, 1376 - Bela Vista
01327-002 - São Paulo - SP