INTEGRIDADE

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO (PSI) DA FADESP

2025

Fadesp

FUNDAÇÃO DE AMPARO E DESENVOLVIMENTO DA PESQUISA

INTEGRIDADE

Índice

Fadesp

O Conselho Diretor da Fundação de Amparo e Desenvolvimento da Pesquisa – FADESP, no uso de suas atribuições legais, com base no art. 23-D, parágrafo quinto, do Estatuto da FADESP, em sua reunião ordinária, ocorrida em 02 de dezembro de 2025, aprova a Política de Segurança da Informação:

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO (PSI) DA FADESP

1. Introdução

A Fundação de Amparo e Desenvolvimento da Pesquisa - FADESP reconhece a importância da segurança da informação para a proteção de seus ativos, a confidencialidade dos dados e a continuidade de suas operações. Esta Política de Segurança da Informação (PSI) estabelece as diretrizes e os requisitos mínimos para garantir a segurança da informação em todas as atividades da FADESP e de seus colaboradores, parceiros e terceiros.

2. Objetivos

A PSI da FADESP tem como objetivo:

- Declarar o compromisso da FADESP com a proteção de suas informações e das informações sob sua responsabilidade;
- Estabelecer diretrizes que orientem colaboradores, instituições apoiadas, fornecedores, parceiros e prestadores de serviço quanto aos comportamentos esperados no que se refere à segurança da informação;
- Proteger os ativos de informação da FADESP contra ameaças internas e externas, como acessos não autorizados, perdas, roubos, alterações e vazamentos;
- Assegurar a conformidade com as leis e regulamentos aplicáveis;
- Assegurar a confidencialidade, integridade e disponibilidade das informações;
- Estabelecer responsabilidades e procedimentos para o tratamento da informação;
- Promover a conscientização e o treinamento em segurança da informação.

3. Escopo

A presente política se aplica a todos os ativos de informação geridos pela Fundação, incluindo:

- Dados e informações em formato físico ou eletrônico;
- Sistemas de informação, *softwares* e *hardwares*;
- Redes de comunicação e internet;
- Instalações físicas e equipamentos;
- Documentos, contratos e outros registros;
- Informações de propriedade intelectual.

4. Princípios

Os princípios que regem a PSI da FADESP são:

a) Confidencialidade: garantir que as informações sejam acessadas apenas por pessoas autorizadas.
b) Integridade: assegurar que as informações sejam precisas, completas e não sejam alteradas sem autorização.
c) Disponibilidade: garantir que as informações estejam disponíveis para uso quando necessário.
d) Legalidade: cumprir todas as leis e regulamentos aplicáveis à segurança da informação.
e) Responsabilidade: todos os colaboradores são responsáveis pela segurança da informação.
f) Melhoria contínua: a PSI será revisada e atualizada periodicamente para acompanhar as mudanças nas ameaças e tecnologias.

5. Diretrizes

5.1. Segurança Física

• O acesso às instalações da FADESP será controlado por meio de catracas, biometria digital e/ou facial, portarias e sistemas de vigilância, assegurando a integridade patrimonial, a segurança das pessoas que circulam em nossas instalações e a prevenção a fraudes. Tal controle é previsto com base no Art. 11, II, 'g', da LGPD, para garantir a segurança do controlador. Caso o titular não deseje fornecer dado biométrico, será disponibilizada alternativa viável de autenticação, sem prejuízo de acesso.
• Áreas restritas serão monitoradas e controladas por sistemas de segurança e vigilância, sendo acesso principal limitado a pessoas autorizadas.
• Visitantes serão identificados e acompanhados durante a permanência na Fundação.
• Equipamentos e dispositivos devem ser instalados em local com condições ambientais e de segurança adequadas, inclusive com mecanismos de proteção contra roubo ou danos.

5.2. Segurança Lógica

• O acesso aos sistemas de informação será controlado por meio de senhas fortes, autenticação em fatores e outros mecanismos de segurança.
• Os usuários terão acesso apenas às informações necessárias para o desempenho de suas funções.
• *Softwares* e sistemas serão atualizados regularmente para corrigir vulnerabilidades.
• O acesso à internet e ao e-mail corporativo será monitorado e controlado, por meio do registro de *logs* de navegação e análise de tráfego, para garantir o uso adequado e a segurança da informação, respeitando os princípios da legalidade, necessidade e proporcionalidade.
• Dados classificados como confidenciais ou sensíveis, como dados biométricos, informações pessoais, financeiras e/ou estratégicas serão protegidos por meio de técnicas de criptografia.
• Cópias de segurança (*backups*) serão realizadas e testadas regularmente e armazenadas em local seguro.
• Antivírus e *firewalls* serão utilizados para proteger contra *malware*.
• Testes de segurança serão realizados periodicamente para identificar vulnerabilidades.

5.3. Segurança de Recursos Humanos

• Os colaboradores devem assinar um termo de responsabilidade demonstrando ciência das diretrizes da Política de Segurança da informação.
• Todos os colaboradores receberão treinamentos regulares e campanhas educativas em segurança da informação.
• Acordos de confidencialidade serão assinados por colaboradores, parceiros e terceiros.
• O desligamento de um colaborador da FADESP deve ser comunicado imediatamente à Coordenação de Tecnologia da Informação (CTI) para revogação imediata de acessos aos sistemas da Fundação.
• Incidentes de segurança devem ser reportados ao Comitê Gestor de Segurança da Informação, por

e-mail: *cgsi@fadesp.org.br*, ao Encarregado de Dados (*Data Protection Officer* - DPO) e/ou pelo Canal de Comunicação da FADESP, disponível no site institucional.

5.4. Gestão de Riscos

• Uma análise de riscos será realizada periodicamente pelo Comitê Gestor de Segurança da Informação para identificar e avaliar as ameaças à segurança da informação.
• Planos de resposta a incidentes serão desenvolvidos e testados para lidar eficientemente com qual quer violação de segurança da informação, incluindo procedimentos de notificação e mitigação.

5.5. Conformidade Legal

• A FADESP cumprirá todas as leis e regulamentos aplicáveis à segurança da informação, incluindo a Lei Geral de Proteção de Dados (Lei nº 13.709/2018).
• Auditorias de segurança serão realizadas periodicamente pelo Encarregado de Dados (*Data Protection Officer* - DPO) para verificar a conformidade com a PSI.

5.6. Plano de Continuidade de Negócio (PCN)

• O Plano de Continuidade do Negócio (PCN) deve ser formulado em conjunto com as coordenações/ setores da FADESP, estar sempre atualizado e contemplar os ambientes, processos e recursos críticos da organização.
• O PCN deve incluir ações de gestão de crises e recuperação de desastres, objetivando garantir a retomada das operações em caso de incidentes que comprometam a continuidade dos serviços da FADESP.
• Os colaboradores devem receber treinamento periódico e apropriado sobre suas responsabilidades em caso de acionamento do Plano de Continuidade de Negócios.

6. Responsabilidades

6.1. Alta Administração

A Alta Administração, composta pela Diretoria Executiva, Conselho Diretor e Conselho Fiscal, será responsável por aprovar e apoiar a PSI e ainda:
• Estar alinhada e comprometida com a Política de Segurança da Informação, bem como suas normas e procedimentos.
• Definir responsabilidades e alocar os recursos necessários para a implantação e manutenção dos diversos controles de segurança da informação.
• Promover o desenvolvimento da cultura em segurança da informação conforme estabelecido nas políticas e procedimentos da organização, demonstrando seu apoio às políticas, treinamentos, procedimentos e controles, agindo como tal, de forma exemplar.

6.2. Comitê Gestor de Segurança da Informação (CGSI)

O CGSI será responsável por assessorar a implementação das ações definidas na Política de Segurança da Informação e ainda:
• Realizar avaliações semestrais dos riscos à segurança da informação da Fundação, de modo a identificar áreas de vulnerabilidade e tomar medidas proativas para mitigá-las.
• Implementar medidas e controles de segurança adequados para proteger a infraestrutura tecnológica, sistemas, redes e informações críticas da organização.
• Promover programas de conscientização e treinamento em segurança da informação.
• Realizar monitoramento contínuo dos sistemas e infraestrutura de TI para identificar possíveis ameaças e garantir que os controles de segurança estejam sendo efetivamente aplicados.

6.3. Encarregado de Dados (Data Protection Officer - DPO)

• Acompanhar e revisar as políticas internas de proteção de dados, garantindo que estejam atualizadas e em conformidade com a legislação;
• Supervisionar a implementação e a eficácia das medidas de segurança técnicas e administrativas, como *firewalls*, criptografia, controles de acesso e planos de resposta a incidentes;
• Orientar e treinar colaboradores e terceiros sobre as políticas de proteção de dados, as melhores práticas de segurança da informação e as obrigações legais;
• Fornecer informações sobre os dados pessoais aos titulares, quando solicitado.
• Comunicar a Autoridade Nacional de Proteção de Dados (ANPD) em caso de incidente de segurança envolvendo dados pessoais.
• Promover a cultura de proteção de dados dentro da organização, incentivando a responsabilidade e a atenção aos riscos;
• Elaborar em conjunto com o Comitê Gestor de Segurança da Informação ações periódicas de conscientização e reciclagem do tema aos colaboradores, parceiros e terceiros.
• Realizar auditorias internas para identificar não conformidades e propor melhorias nos processos de proteção de dados.

6.4. Coordenação de Tecnologia da Informação

• Discutir, revisar e aprovar a Política de Segurança da Informação e normas complementares, considerando os interesses, objetivos estratégicos e regulamentações;
• Definir as regras para instalação de *software* e *hardware* na FADESP;
• Homologar os equipamentos pessoais (*smartphones*, *tablets* e *notebooks*) para uso na rede da FADESP;
• Monitorar os acessos às informações e aos ativos de tecnologia (sistemas, bancos de dados, recursos de rede), tendo como referência a política e as normas de segurança da informação;
• Mediante informações da Coordenação de Recursos Humanos, manter registro e controle atualizados de todas as liberações de acesso concedidas, providenciando, sempre que demandado formalmente, a pronta suspensão ou alteração de tais liberações;
• Propor as metodologias, processos e soluções referentes à segurança da informação;
• Analisar criticamente incidentes de segurança em conjunto com o Comitê Gestor de Segurança da Informação e o Encarregado de Dados;
• Buscar alinhamento com as diretrizes da organização.

6.5. Coordenação de Recursos Humanos

• Garantir a assinatura dos termos aplicáveis e endereçar a salvaguarda dos documentos às áreas internas responsáveis;
• Comunicar e solicitar imediatamente às áreas responsáveis o recolhimento de chaves e crachás e revogação de outras concessões que garantam o acesso às instalações físicas;
• Solicitar a revogação do acesso aos sistemas de informação corporativos, conexões remotas, e-mails e quaisquer outros meios de acesso à informação e/ou comunicação corporativa ao departamento de tecnologia da informação;
• Divulgar a relevância do tema segurança da informação durante a contratação de um colaborador, parceiro ou terceiro.

6.6. Colaboradores, parceiros e terceiros

Todos os colaboradores, parceiros e terceiros deverão ser responsáveis por conhecer a Política de Segurança da Informação da FADESP e cumprir com as diretrizes, seguindo os controles e procedimentos

aplicáveis às suas atividades. Abaixo, são apresentadas as principais responsabilidades:
• Ler e assinar o termo acordo de confidencialidade;
• Utilizar os recursos tecnológicos e as informações em caráter estritamente profissional, limitado ao âmbito de suas atividades e observando sempre os requisitos de ética;
• Proteger as informações às quais tenha acesso, garantindo que recebam o tratamento adequado de acordo com sua classificação e procedimentos em respeito ao compromisso de sigilo profissional assumido;
• Fazer uso seguro de dispositivos de autenticação corporativos, tais como o crachá, as chaves e suas correspondentes senhas e os certificados digitais, que devem ser usados de forma individual e não podem ser compartilhados.
• Zelar pelos equipamentos de tecnologia e ativos de informação a que tiver acesso, a fim garantir a segurança da informação.
• Reportar ao Comitê Gestor de Segurança da Informação, por e-mail: *cgsi@fadesp.org.br*, ao Encarregado de Dados (*Data Protection Officer* - DPO) ou pelo Canal de Comunicação da FADESP, disponível no site institucional qualquer suspeita de violação de segurança e comportamentos em não conformidade com as diretrizes contidas na Política de Segurança da Informação.
• Participar de treinamentos e ações de conscientização promovidos pela FADESP sobre segurança da informação.
• Observar e respeitar os direitos de propriedade intelectual, sabendo que estes direitos recaem tanto sobre ativos tangíveis quanto intangíveis, incluindo as marcas, as patentes, os códigos-fonte, os contratos de licenciamento, entre outros.
• Garantir que todos os ativos da empresa em posse daquele colaborador (dispositivos, documentos, dados, informações) sejam protegidos quando estiverem em áreas públicas. Em caso de perda, furto ou roubo, deve ser notificada imediatamente o gestor direto e a Coordenação de Tecnologia da Informação.
• Ter ciência que qualquer informação que é acessada, transmitida, recebida ou produzida na FADESP está sujeita a divulgação e auditoria pelas partes relevantes. O colaborador pode sofrer medidas legais e/ou profissionais caso acesse, transmita ou gere informações de conteúdo ilegal, malicioso, impróprio ou que conflite ou contrarie os valores e interesses da FADESP.

7. Gestão da Informação

As informações que circulam ou são produzidas pela FADESP – sejam dados, documentos, itens ou conjuntos informacionais – devem ser tratadas com o devido grau de confidencialidade, salvo nos casos em que houver disposição interna ou exigência legal ou regulamentar que determine sua divulgação. Todos os colaboradores devem zelar pela manutenção de níveis adequados de confidencialidade e, sempre que possível, explicitar a classificação atribuída às informações.

As informações obtidas ou geradas pela FADESP, bem como por terceiros, são classificadas nos seguintes níveis:

a) Confidencial: é o nível mais alto de segurança dentro deste padrão. As informações confidenciais são aquelas que, se divulgadas interna ou externamente, têm potencial para trazer grandes prejuízos financeiros ou à imagem da FADESP. São protegidas por rigorosos controles de acesso.
b) Restrita: é o nível intermediário de confidencialidade. São informações estratégicas que devem estar disponíveis apenas para grupos restritos de colaboradores.
c) Uso interno: representa baixo nível de confidencialidade. Informações de uso interno são aquelas que não podem ser divulgadas a pessoas externas, mas caso aconteça, não causarão grandes impac-

tos. A preocupação nesse nível está relacionada principalmente à integridade da informação.
d) Pública: são dados que não necessitam de proteção contra vazamentos, pois podem ser de conhecimento público.

A classificação da informação será atribuída pelo responsável direto por sua criação ou guarda, conforme orientações do Comitê Gestor de Segurança da Informação. A reclassificação deverá ser avaliada periodicamente. Abaixo uma tabela, não exaustiva, que lista alguns itens de informação em cada categoria:

Categoria de Classificação	Elementos da Informação
Confidencial	Dados bancários e de pagamento de projetos ainda não publicamente divulgados; Estratégias de captação de recursos e negociações em andamento com financiadores; Informações tratadas pelo Comitê de Ética ou no Canal de Comunicação da FADESP; Dados pessoais sensíveis de colaboradores, bolsistas ou parceiros (ex: laudos médicos, biometria, endereço residencial); Relatórios de auditoria interna antes da conclusão e homologação; Documentos sigilosos de processos judiciais envolvendo a Fundação.
Restrita	Propostas de projetos em fase de elaboração ou negociação com instituições parceiras; Minutas de contratos ainda não assinados; Planejamentos estratégicos internos ou análises de riscos não divulgadas; Dados financeiros parciais de projetos em execução; Resultados preliminares de editais/seleções internas; Atas de reuniões de diretoria ou comitês internos que tratam de decisões estratégicas não divulgadas.
Uso Interno	Comunicados internos sobre prazos operacionais ou mudanças administrativas; Manuais internos de procedimentos e fluxos de trabalho; Relatórios consolidados de projetos concluídos, sem informações sensíveis; Dados agregados de desempenho institucional utilizados em apresentações internas.
Pública	Relatórios anuais ou de gestão publicados no site institucional; Resultados finais de editais ou chamadas públicas; Dados institucionais disponíveis em portais de transparência; Campanhas institucionais e materiais de divulgação; Informações sobre eventos promovidos pela Fundação.

7.1. Manutenção do Sigilo da Informação

As seguintes regras devem ser observadas quanto à utilização de informações confidenciais e/ou restritas:

- Os colaboradores devem proteger a confidencialidade de quaisquer informações obtidas durante o exercício de suas funções na FADESP, que não devem ser: a) divulgadas a terceiros; b) divulgadas ou disponibilizadas em domínio público; c) copiadas ou transferidas (mesmo que por foto) a celulares, *tablets*, computadores pessoais ou quaisquer outros dispositivos portáteis.
- A obrigação de sigilo prevista no item anterior, se aplica mesmo após a rescisão do vínculo do colaborador da FADESP, qualquer que seja a razão, permanecendo o colaborador obrigado a manter sigilo e a proteger a confidencialidade das informações obtidas durante o exercício de suas funções na FADESP;
- A divulgação indevida de informações confidenciais poderá ensejar responsabilização civil, adminis-

trativa e/ou criminal, conforme a legislação vigente, mediante apuração interna nos termos do Código de Conduta e do Programa de Integridade da FADESP.

• A FADESP adotará a política de mesas limpas. Todos os colaboradores devem evitar manter papéis e documentos confidenciais expostos em suas mesas de trabalho.

• As informações confidenciais de clientes enviadas ou entregues à FADESP para execução de transações são protegidas por lei. O compartilhamento destas informações com terceiros depende de expressa autorização dos clientes, por escrito.

• A FADESP poderá revelar as informações confidenciais e restritas sempre que estiver obrigada a revelá-las, seja em virtude de dispositivo legal, ato de autoridade competente, ordem ou mandado judicial.

8. Uso Aceitável de Recursos

8.1. Privacidade

A FADESP se reserva o direito de acessar informações armazenadas em seus sistemas eletrônicos, como rede interna, e-mails e nuvem corporativa, bem como nos equipamentos e mobiliários da organização, desde que esse acesso observe os princípios da boa-fé, necessidade, proporcionalidade e os direitos à privacidade e à proteção de dados pessoais previstos na Lei Geral de Proteção de Dados (LGPD). Ainda que seja tolerado o uso pessoal moderado desses recursos, os colaboradores devem estar cientes de que tais informações podem ser acessadas pela FADESP para fins legítimos, como auditoria, segurança da informação ou cumprimento de obrigações legais.

8.2. Segurança do Patrimônio Físico e Intangível

Integram o patrimônio físico e intangível da FADESP, seus imóveis, instalações, veículos, equipamentos, estoques, valores, planos, produtos, tecnologia, estratégia de negócio e de comercialização, informações, pesquisas e dados que devem ser protegidos pelos funcionários, não podendo estes serem utilizados para obtenção de vantagens pessoais e nem fornecidos a terceiros, independentemente do fim.

Não podem ser utilizados equipamentos ou outros recursos da FADESP para fins particulares, salvo se previamente autorizado pelo gestor de área, sendo a referida aprovação vedada nos casos em que possa:

• Interferir ou concorrer com os negócios da FADESP;
• Fornecer informações a terceiros;
• Envolver solicitação comercial ou outra solicitação não apropriada ao negócio;
• Envolver custos adicionais para a FADESP.

8.3. Uso de Recursos Tecnológicos

Recursos Tecnológicos são ativos disponibilizados aos colaboradores, autorizados, de modo a auxiliá-los no desempenho de suas funções e na execução das atividades. Em relação ao uso de recursos tecnológicos disponibilizados, deve-se seguir as diretrizes:

• Todos os computadores de uso individual deverão ter a BIOS protegida por senha, com o objetivo de restringir o acesso de pessoas não autorizadas;

• O colaborador ou prestador de serviços deverá manter a configuração do equipamento disponibilizado pela Coordenação de Tecnologia da Informação, seguindo os devidos controles de segurança exigidos pela PSI e pelas normas específicas da FADESP;

• Todos os dispositivos e terminais de computador deverão estar bloqueados (protegidos por senha), quando não estiverem sendo acessados por seu usuário;

• É proibido qualquer procedimento de manutenção física ou lógica, instalação, desinstalação, configuração ou modificação nos equipamentos da FADESP, sem autorização prévia da Coordenação de Tecnologia da Informação;
• É vedada a prática de intencionalmente comprometer a privacidade e/ou segurança da informação;
• É vedada a prática de intencionalmente infringir os direitos de propriedade intelectual de terceiros, no que diz respeito a *softwares*, material audiovisual, publicações e demais informações eletrônicas;
• É vedado o uso de recursos disponibilizados para discriminação ou provocação em razão do sexo, raça, cor, religião, nacionalidade, idade, porte de deficiência física, condição de saúde, estado civil ou qualquer outra condição prevista em lei;
• Não é permitido promover comunicações ilegais, tais como ameaça de violência, injúria e difamação, pornografia infantil, assédio e tráfico de drogas, conforme definido pela lei;
• Não é permitido o armazenamento de vídeos, imagens, músicas e/ou jogos de computador que não estejam relacionados à natureza de suas atividades;
• Não é permitido disponibilizar os recursos tecnológicos para indivíduos sem vínculo algum com a Fundação, sem autorização do pessoal responsável;
• É proibida qualquer utilização não autorizada do nome da FADESP para fins estranhos às suas atividades, inclusive o seu endereço na Internet e domínio de correio eletrônico;
• Não é permitido o "*download*" e instalação, pelos colaboradores, de programas, aplicativos ou *softwares* de qualquer natureza vindos da Internet, e-mail ou qualquer outra fonte. Apenas os aplicativos recomendados e homologados oficialmente são permitidos.

8.4. Uso da Rede e Navegação

O uso da rede corporativa e da Internet deve seguir diretrizes específicas. A seguir, estão listadas as principais orientações:
• A Internet deve ser utilizada para a realização das atividades profissionais, porém o uso para fins pessoais é permitido, desde que não cause impactos na operação da rede corporativa e nas atividades da área.
• Nenhum computador poderá utilizar conexões distintas das disponibilizadas pela FADESP e/ou suas controladas para acesso à Internet ou outros serviços de informação quando conectados à rede corporativa.
• Não é permitido o acesso a sites de conteúdo pornográfico e ilegal.
• Não é permitido o envio, recebimento e obtenção de arquivos de uso pessoal, ofensivo e ilegal, assim como seu armazenamento nos recursos tecnológicos disponibilizados, tais como diretórios de rede e e-mail.
• O controle do acesso à Internet via rede corporativa é feito pela área de Tecnologia da Informação, com o auxílio de software específico. Todas as páginas visitadas são registradas em arquivos de controle para fins de monitoramento e auditoria.
• Para que a permissão de acesso à internet seja concedida, o colaborador deve ter configurado em sua credencial de acesso à rede a devida permissão, que é concedida de forma automática de acordo com sua função ou cargo.
• Documentos imprescindíveis para as atividades dos empregados ou prestadores de serviços na FADESP deverão ser salvos na rede. Tais arquivos, se gravados apenas localmente nos computadores (por exemplo, no *drive* C:), não terão garantia de cópias de segurança (*backup*) e poderão ser perdidos caso ocorra uma falha no computador, sendo, portanto, de responsabilidade do próprio usuário.
• Diretórios ou pastas de acesso público não deverão ser utilizados para armazenamento de arquivos que contenham assuntos sigilosos ou de natureza específica. Devem ser utilizados apenas para armazenar informações de interesses gerais.

8.5. Uso de dispositivos portáteis

O manuseio de notebooks, tablets, pendrives e outros dispositivos móveis deve seguir diretrizes para reduzir riscos de vazamento de dados e garantir seu uso adequado:

• Todo colaborador ou prestador de serviços deverá realizar periodicamente cópia de segurança (*backup*) dos dados do dispositivo móvel pertencente à FADESP sob sua guarda.

• Os dispositivos móveis que permanecerem em qualquer área física da FADESP, deverão estar trancados em local de acesso restrito e seguro, quando não estiverem sendo utilizados pelo usuário.

• Ao viajar com um computador tipo portátil, o usuário deve:

  ○ Manter o computador tipo portátil em local seguro;
  ○ Ao utilizar um táxi ou outro meio de deslocamento, é necessário a verificação de que retirou toda a sua bagagem, inclusive o computador, quando chegar a seu destino final.
  ○ É responsabilidade do empregado ou prestador de serviços, no caso de furto ou roubo de um dispositivo móvel fornecido pela FADESP, notificar imediatamente seu gestor direto e a Coordenação de Tecnologia da Informação. Também deverá procurar a ajuda das autoridades policiais, registrando, assim que possível, um boletim de ocorrência (BO).

8.6. Uso do telefone e smartphone corporativo

A utilização de aparelhos telefônicos e smartphones fornecidos pela FADESP deve observar as seguintes normas:

• O uso do telefone fixo deve ser utilizado apenas para fins profissionais. É permitido o uso para fins pessoais com bom senso, para assuntos que não sejam conflitantes com as atividades nem que prejudiquem qualquer lei, regulação ou regulamento e políticas internas.

• O uso de *smartphone* fora das dependências da FADESP para discussão de assuntos confidenciais internos pode ser necessário, porém deve-se sempre priorizar fazer ligações dentro da FADESP, evitando exposição de informações em locais públicos.

8.7. Uso do e-mail corporativo

O e-mail institucional deve ser utilizado com responsabilidade, respeitando as orientações e diretrizes:

• O e-mail corporativo é de propriedade da FADESP e poderá ser monitorado, de forma proporcional e nos limites legais, com o objetivo de garantir a segurança da informação e o cumprimento das normas internas, com a devida ciência do colaborador.

• É proibido o envio de mensagens pelo sistema de correio eletrônico, entre quaisquer usuários ou mesmo externamente, que:

  ○ Tragam ao equipamento ou rede, códigos maliciosos, vírus ou quaisquer outros elementos que possam afetar o desempenho da rede e dos sistemas;
  ○ Contenham conteúdo ofensivo e ilegal;
  ○ Contenham material protegido por leis de propriedade intelectual;
  ○ Contenham músicas, vídeos, ou animações que não sejam de interesse específico do trabalho, bem como SPAM;
  ○ Compartilhar documentos sem autorização.

• O endereço de e-mail fornecido não deve ser utilizado para cadastro em sites de compras, relacionamento pessoal, *blogs*, ou qualquer outra página da internet que não esteja relacionada com as atividades profissionais.

• Deve ser evitada a abertura de mensagens de origem desconhecida, contendo anexos ou conteúdo

duvidoso ou que tenham *links* para sites desconhecidos e solicitem o *download* de arquivos ou dados pessoais.

• A FADESP conta com um sistema de bloqueio de *spam*. Em caso de bloqueio indevido ou caso alguma mensagem não solicitada chegue na caixa postal de qualquer colaborador, a área de Tecnologia da Informação deve ser informada para que os ajustes de configuração sejam realizados.

8.8. Uso de Redes Sociais

Em relação à utilização de redes sociais para fins pessoais e para interação em nome da FADESP:

• É permitido o uso de redes sociais de forma moderada, sem que impacte nas atividades da Fundação, devendo este ser realizado nos intervalos de almoço ou antes/após o horário do expediente.

• É expressamente proibido divulgar informações em comunidades virtuais e redes sociais em nome da organização, portanto, não se deve:

- Divulgar informações sobre novas tecnologias, serviços e sistemas;
- Conceder opinião pessoal em resposta a publicações na internet relacionadas a qualquer assunto das áreas internas da Fundação;
- Divulgar informações sobre a rotina profissional, atividades e projetos em andamento;
- Comunicar brechas de segurança ou incidentes ocorridos na Fundação;
- Publicar um documento interno.

• Em caso de necessidade de publicação ou divulgação de informações ao público, devem ser utilizados os canais corporativos nas redes sociais, gerenciados pela Assessoria de Comunicação da FADESP.

8.9. Mesa Limpa

A política de mesa limpa consiste em não deixar informações confidenciais ou bens da FADESP, incluindo, mas não se limitando a papéis, pen-drives ou quaisquer outros tipos de mídias removíveis, acessíveis a outras pessoas sem a devida proteção, quando o colaborador estiver fora de sua estação de trabalho. Logo, ao final do dia de trabalho, documentos confidenciais devem ser guardados em local apropriado e com chave para evitar o acesso de terceiros não autorizados.

8.10. Tela Limpa

Computadores, *notebooks* e outros dispositivos devem estar protegidos por senha quando não estiverem sendo utilizados. Todos os computadores devem ter proteção de tela automática com senha habilitada para acionamento no tempo máximo de 10 minutos de inativação.

8.11. Uso de Impressora

Devem ser observadas por todos os colaboradores quanto à sua utilização:

• Quaisquer impressões, sobretudo as que contêm informações confidenciais, devem ser imediatamente retiradas da impressora;

• Esta ferramenta deve ser utilizada apenas quando o documento físico se fizer imprescindível, evitando desperdícios ou gastos desnecessários;

• As impressoras são ferramentas para fins profissionais, objetivando aumentar a produtividade nas atividades desenvolvidas pela FADESP. Impressões para finalidade pessoal devem ser limitadas e com bom senso, nunca com finalidades conflitantes com os interesses da FADESP, bem como nunca infringindo nenhuma lei, norma, regulamentação e políticas internas da FADESP.

9. Monitoramento e Auditoria do Ambiente

Com o objetivo de proteger os dados institucionais, prevenir incidentes de segurança e cumprir as diretrizes desta Política, a FADESP poderá adotar mecanismos de monitoramento e auditoria do ambiente tecnológico, de forma limitada e proporcional, respeitando os direitos dos colaboradores. As medidas incluem:

• Adoção de sistemas que possibilitem o acompanhamento de acessos às estações de trabalho, servidores, e-mail corporativo, navegação na internet e demais recursos tecnológicos da Fundação, sempre com foco na segurança da informação e na prevenção a fraudes;
• Implantação de sistemas de proteção e detecção de invasões, para garantir a integridade dos dados e da rede institucional;
• Uso de câmeras de segurança nas dependências da FADESP, voltado à proteção patrimonial e das pessoas.

Todas essas ações são conduzidas com responsabilidade, exclusivamente para fins legítimos, em conformidade com a legislação vigente, especialmente a Lei Geral de Proteção de Dados Pessoais (LGPD), e com ciência prévia dos colaboradores nos termos das políticas internas.

9.1. Política de Senha

O uso de senhas fortes e a sua correta gestão são fundamentais para proteger os sistemas e dados da Fundação. Abaixo, seguem os critérios e práticas obrigatórias:

• A FADESP adota política de troca obrigatória de senhas com período de uso contínuo de no máximo 365 dias. Os sistemas críticos e sensíveis para a instituição e os usuários com privilégios administrativos devem exigir a troca de senhas a cada 180 dias. Os sistemas devem forçar a troca das senhas dentro desse prazo máximo.
• Usuários e senhas são pessoais e intransferíveis. Os colaboradores devem zelar pela proteção dos seus dados de acesso, sendo vedada a divulgação de senhas a terceiros.
• A Coordenação de Recursos Humanos da FADESP é responsável pela emissão e pelo controle dos documentos físicos de identidade dos empregados e prestadores de serviços. A Coordenação de Tecnologia da Informação responde pela criação da identidade lógica dos colaboradores e prestadores de serviços na Fundação.
• Devem ser distintamente identificados os visitantes, estagiários, colaboradores temporários, colaboradores regulares e prestadores de serviços, sejam eles pessoas físicas ou jurídicas. Ao realizar o primeiro acesso ao ambiente de rede local, o usuário deverá trocar imediatamente a sua senha, conforme as orientações apresentadas.
• Os usuários devem alterar sua senha em caso de suspeita de que terceiros tenham obtido acesso à sua conta.
• Todos os acessos devem ser imediatamente bloqueados quando se tornarem desnecessários. Em caso de demissão, a Coordenação de Recursos Humanos deverá, imediatamente, comunicar tal fato à Coordenação de Tecnologia da Informação, permitindo que essa providência seja tomada. A mesma conduta se aplica aos usuários cujo contrato ou prestação de serviços tenha se encerrado, bem como aos usuários de testes e outras situações similares.
• Caso o empregado ou prestador de serviços esqueça sua senha, ele deverá requisitar formalmente a troca por meio de chamado técnico.

9.2. Controle de acesso aos sistemas

O controle aos sistemas visa prevenir o acesso de indivíduos não autorizados ao ambiente e aos sistemas da FADESP, garantindo assim a confidencialidade das informações. Para garantir um nível aceitável de controle são executados os seguintes processos:

•Controle de acessos por meio da matriz de segregação de função. Na matriz estão listadas todas as equipes, colaboradores e acessos liberados;
• Execução de procedimentos formalizados para a concessão, alteração, revogação e gerenciamento de acessos, sendo que para todos os procedimentos citados acima, é respeitado o princípio de menor privilégio e perfil mínimo restrito de acesso, conforme a matriz de segregação de função;
• Todos os usuários são orientados a possuírem acesso apenas à informação de acordo com as necessidades das suas respectivas atividades;
• É de responsabilidade do gestor da equipe o informe do nível de acessos para novos colaboradores. Os acessos são limitados aos ativos de informação sob domínio da equipe;
• Existem casos específicos de colaboradores que necessitam de acesso aos ativos de informação pertencentes a outras equipes. Para estes casos, todos os procedimentos de concessão e alteração são aprovados pelo gestor responsável da equipe do colaborador, gestor da equipe detentora dos ativos de informação, Diretoria Executiva e Controladoria;
• A FADESP realiza revisão de acessos, no mínimo anualmente, conforme política, que tem como objetivo a atualização dos acessos e permissões, procedimento este que é realizado pela Coordenação de Tecnologia da Informação.

9.3. Acesso ao Datacenter

O acesso físico ao datacenter é controlado e restrito a profissionais autorizados, conforme as normas de segurança da informação:

• O acesso ao *Datacenter* somente deverá ser feito por sistema de autenticação (biometria, cartão magnético, entre outros);
• Todo acesso ao *Datacenter*, pelo sistema de autenticação, deverá ser registrado (usuário, data e hora) mediante *software* próprio;
• O acesso ao *Datacenter*, por meio de chave, apenas poderá ocorrer em situações de emergência, quando a segurança física do *Datacenter* estiver comprometida, como incêndio, inundação, abalo da estrutura predial ou quando o sistema de autenticação não estiver funcionando;
• Deverão existir duas cópias de chaves da porta do *Datacenter*. Uma das cópias deverá ficar de posse do coordenador responsável pelo *Datacenter*, e a outra, de posse da Diretoria Executiva.
• O *Datacenter* deverá ser mantido limpo e organizado. Qualquer procedimento de limpeza no ambiente deverá ser acompanhado pela Coordenação de Tecnologia da Informação.
• No caso de desligamento, transferência de setor ou departamento de colaboração ou prestadores de serviços que possuam acesso ao *Datacenter*, imediatamente deverá ser providenciada a sua exclusão do sistema de autenticação e da lista de colaboradores autorizados.

9.4. Engenharia Social

A Engenharia Social é qualquer método usado para enganar ou explorar a confiança das pessoas para a obtenção de informações sigilosas e importantes, tanto da empresa como do colaborador ou prestador de serviços em questão. Para isso, alguém pode se passar por outra pessoa, assumir outra personalidade, fingir que é um profissional de determinada área, entre outros.

Para evitar esse método, todos os colaboradores ou prestadores de serviços devem estar cientes das seguintes regras:

• Nenhum colaborador ou prestador de serviços está autorizado a passar informação às pessoas ou agentes estranhos à Fundação;
• O suporte técnico em hipótese alguma encaminhará, por e-mail, solicitações de senhas ou qualquer outra informação do usuário do sistema ou colaborador ou prestador de serviços que o opera;
• Caso alguém entre em contato por telefone, e-mail ou *softwares* de comunicações solicitando informações sigilosas da empresa ou do usuário, o colaborador ou prestador de serviços abordado deverá entrar em contato com o responsável pela rede interna, ou diretamente com a Coordenação de Tecnologia da Informação, informando tais ações.

9.5. Acesso Remoto

O acesso remoto aos serviços corporativos somente deve ser disponibilizado aos colaboradores ou prestadores de serviços que, oficialmente, execute atividade vinculada à atuação institucional da FADESP e que necessitam desse serviço para execução de suas atividades, desde que autorizados. A liberação de acesso remoto, só será efetivada após a aprovação da Diretoria Executiva e análise técnica de viabilidade da Coordenação de Tecnologia da Informação.

9.6. Serviço de Diretório (Servidor de Arquivos)

Serviços de diretório desempenham um papel importante no desenvolvimento de aplicações intranet e Internet, além de arquivos permitindo o compartilhamento de informações sobre usuários, sistemas, redes, serviços e aplicações através da rede.

A FADESP utiliza dois serviços de diretório em paralelo: um para o acesso interno aos equipamentos dos colaboradores e infraestrutura e outro para acesso aos serviços em nuvem. Os diretórios possuem sincronização ativa, logo, compartilham dos mesmos usuários, grupos, senhas e demais informações. Sempre que possível os sistemas adquiridos e desenvolvidos possuirão *login* integrado com o serviço de diretório em nuvem da FADESP, mantendo assim um canal único e centralizado de gestão de acessos.

9.7. Gestão de Senhas e Acesso

A FADESP disponibiliza a todos os colaboradores um serviço de cofre seguro, que é o meio ideal para armazenar e gerenciar informações confidenciais compartilhadas, como senhas, documentos e identidades digitais. O serviço é acessível apenas na rede interna, nas dependências da FADESP ou via Rede virtual privada (VPN).

A ferramenta fornece controles de segurança preventiva e de investigação, através de fluxos para rotinas de aprovação e alertas em tempo real sobre senhas de acesso. Permite ainda auditorias de segurança da reunião e conformidade regulamentar, como SOX, HIPAA e PCI.

9.8. Gestão de risco de software malicioso

Os *malwares* de computador são programas desenhados para causar perda ou alteração de dados do computador, com isso em vista, todo equipamento da FADESP deve ter um programa antivírus instalado. Os *softwares* antivírus devem ser atualizados diariamente e de forma automática.

9.9. Gestão de backup

Cada coordenação/setor/usuário tem acesso a pelo menos uma pasta no servidor e/ou serviço de nuvem de arquivos. Todos os documentos relacionados ao negócio devem ser armazenados nestas pastas. Além disso, cada usuário tem uma pasta individualizada para uso profissional no servidor e/ou serviço de nuvem de arquivos.

Qualquer arquivo armazenado em pastas locais nos computadores não é passível de *backup*, e por isso o armazenamento nesses locais é de total responsabilidade do usuário.

Todos os e-mails, anexos e arquivos armazenados no diretório em nuvem possuem um serviço de *backup* à parte. O serviço monitora o volume de alterações nestes documentos e cria versões automaticamente, podendo gerar até 6 (seis) *backups* por dia. Todas as versões geradas permanecem armazenadas enquanto o serviço estiver contratado, por prazo indefinido.

9.10. Rastreamento de vulnerabilidades

As varreduras das redes internas e externas devem ser executadas periodicamente ou sempre que houver mudança significativa na estrutura tecnológica. As vulnerabilidades identificadas devem ser tratadas e priorizadas de acordo com seu nível de criticidade.

10. Resposta a Incidentes

As respostas aos incidentes de segurança da informação visam assegurar o restabelecimento do nível normal do ambiente tecnológico, após o acontecimento de um sinistro, através do direcionamento na utilização dos recursos e procedimentos fundamentais, no intuito de garantir uma resposta efetiva.

10.1. Planejamento

Esta atividade compreende identificar, prever e descrever situações de possíveis sinistros, bem como suas respectivas ações de mitigação, responsáveis, tempos e registros, de forma que, em situações reais, as atividades já estejam previamente mapeadas e as ações já preestabelecidas. Assim, deve constar no planejamento:

• A definição de uma equipe de planejamento, suas responsabilidades e papéis predefinidos, para prever situações de sinistro e as possíveis respostas, assim como atuar no monitoramento e na resposta aos incidentes.
• A definição do catálogo dos recursos tecnológicos existentes na FADESP, bem como aqueles necessários para possibilitar uma atuação efetiva na resposta aos incidentes.
• O detalhamento das ações necessárias na resposta a incidentes, conforme o tipo e criticidade desses, o tempo mínimo de resposta e a quem os incidentes devem ser reportados, entre outros.
• O Plano de Continuidade do Negócio atualizado, envolvendo os ambientes e processos críticos da FADESP;
• As implementações para o ambiente tecnológico existente deverão ser adequadas a esta política no prazo de um ano, a partir de sua publicação.

10.2. Identificação

O processo de identificação tem por objetivo implementar ações para reconhecer e registrar sinistros relacionados à segurança da informação. Abaixo, estão descritas as principais práticas e responsabilidades envolvidas nessa etapa:

• Podem ser identificados alertas de segurança que configurem incidentes de segurança por meio dos recursos de detecção na rede, no monitoramento dos servidores e recursos de tecnologia ou por meio de problemas reportados pelos usuários. Diante disso, o CGSI poderá ser acionado para que o alerta seja analisado e sejam tomadas as devidas providências, tanto no tratamento do incidente, quanto no encaminhamento do problema para a gestão;
• Eventos, mesmo que apenas suspeitos, devem ser analisados e validados rapidamente. Uma vez confirmada a ocorrência de um incidente, então a análise do escopo daquele incidente deverá ser executada. Essa análise deve prover informações suficientes que permitam identificar e priorizar as atividades subsequentes;

• Todos os usuários são responsáveis por relatar qualquer tipo de eventos e fragilidades, que possam causar danos à segurança da informação. A notificação do evento ou fragilidades por parte do usuário deverá ser registrada por e-mail.

10.3. Resposta

A resposta a incidentes de segurança da informação envolve ações imediatas para conter, minimizar e tratar os impactos causados por ataques ou falhas. A seguir, são descritas as medidas que devem ser adotadas durante essa fase do processo:

• A partir de uma detecção de um incidente de segurança, é importante controlá-lo antes que uma possível extensão comprometa outros recursos. Como exemplo, tem-se uma infecção por vírus em um computador e que, se não for controlado em tempo, pode comprometer outros computadores da rede;
• A estratégia de resposta ao incidente de segurança da informação a ser adotada deve ser baseada no tipo (ex: vírus, perda de arquivo, incêndio etc.) e na criticidade do incidente;
• Após a identificação e a confirmação que o incidente se trata de um evento de segurança da informação, ou seja, que viole a disponibilidade, a confidencialidade ou a integridade da informação, a resposta deverá ser realizada a partir das seguintes ações:

    ○ Preservar, na medida do possível, todas as evidências, para que seja possível identificar o problema, rastrear a possível causa e servir como evidência em eventuais questionamentos;
    ○ Verificar se existem planos de ação em que o sinistro identificado esteja previsto, no intuito de seguir o planejamento;
    ○ Agir para que os serviços afetados sejam disponibilizados em seu estado normal de funcionamento no menor tempo possível;
    ○ Utilizar todos os recursos necessários para a implementação de uma estratégia de reação, seja permanente ou provisória;
    ○ Utilizar atividades de recuperação, tais como: a restauração de *backups* de sistemas, a instalação de *patches*, a alteração de senhas e a revisão da segurança do perímetro da rede da FADESP.

Quando as consequências do incidente estiverem contidas, é necessário que sejam removidos todos os componentes do incidente, como por exemplo: um código malicioso ou desabilitar contas de usuários violadas.

10.4. Vistoria

Após a contenção do incidente, são realizadas ações de vistoria com o objetivo de verificar causas, impactos e vulnerabilidades. As diretrizes abaixo orientam a execução dessa etapa, visando à prevenção de novos eventos e à melhoria contínua da segurança.

• É fundamental assegurar que as atividades envolvidas nas respostas aos incidentes sejam adequadamente registradas para futuras análises. Os registros servirão de banco de conhecimento para resposta em incidentes semelhantes;
• De acordo com o incidente, uma análise mais aprofundada deve ser conduzida para identificar a origem do incidente para que o tratamento das fragilidades e/ou não conformidade encontradas contribuam para a resolução do incidente;
• Periodicamente, a Coordenação de Tecnologia da Informação deve realizar uma análise no ambiente tecnológico com o objetivo de identificar possíveis vulnerabilidades e, de forma antecipada, eliminá-las.

11. Infrações e penalidades aplicáveis

O não cumprimento desta PSI pode resultar em sanções disciplinares, incluindo advertências, suspensões e demissões, além de medidas legais cabíveis. A não observância do disposto neste instrumento caracteriza-se pelas ações descritas a seguir, assim categorizadas.

11.1. Ações leves

• O uso indevido dos servidores de dados, para armazenamento e/ou transferência de conteúdo irrelevante ao ambiente de trabalho às atividades da FADESP.
• O uso indevido da rede e internet, sendo ela cabeada ou sem fio, ou do plano de dados fornecido, para atividades irrelevantes ao ambiente de trabalho às atividades do FADESP.

11.2. Ações graves

• Compartilhamento de credenciais de acesso de qualquer tipo, ainda que seja compartilhada com pessoa que possua as mesmas permissões de acesso que o usuário.
• O acesso a sites ou aplicativos, a partir de estação de trabalho ou dispositivo móvel conectado à internet sem fio da FADESP, com os seguintes conteúdos:

- Erotismo e pornografia;
- Jogos;
- Sites de Relacionamentos.

• A disseminação de mensagens de conteúdo agressivo e boatos.

11.3. Ações gravíssimas

• Acesso a sites ou aplicativos, a partir de estação de trabalho ou dispositivo móvel conectado à internet sem fio da FADESP, com os seguintes conteúdos:

- Pedofilia;
- Armas de Fogo, Bombas ou Violência;
- Drogas;
- Grupos Terroristas;
- Crimes;
- Apostas online;
- Racismo ou qualquer forma de discriminação.

• A disseminação de programas maliciosos.
• A divulgação indevida de informação confidencial, restrita ou interna.
• A ocorrência de danos causados aos ativos por imperícia ou manipulação não autorizada.
• O compartilhamento de credenciais de acesso, a fim de possibilitar que pessoas não autorizadas executem ações ou visualizem informações que não deveriam.

A apuração de responsabilidades e definição de sanções será feita por meio do Comitê Gestor de Segurança da Informação e do Comitê de Ética, nos termos do Programa de Integridade da FADESP.

12. Revisão

A Política de Segurança da Informação será revisada e atualizada anualmente, ou quando necessário, para refletir mudanças nas ameaças, tecnologias e requisitos legais.

13. Disposições Gerais

A Política de Segurança da Informação é um documento público e estará disponível para todos os colaboradores, parceiros e terceiros no Portal da FADESP. A presente política deverá ser aprimorada e agregada com a Política de Proteção de Dados Pessoais.

A aprovação da Política de Segurança da Informação, bem como suas atualizações, é de responsabilidade do Conselho Diretor e da Diretoria-Executiva da FADESP. Cabe à Diretoria-Executiva garantir que seus colaboradores e parceiros conheçam, assimilem, apliquem e compartilhem os preceitos contidos na presente Política. Sugestões de melhorias devem ser encaminhadas Controladoria e Planejamento, que as encaminhará para a Diretoria-Executiva.

Política aprovada em 02 de dezembro de 2025.
Atualização prevista para prazo máximo de 2 (dois) anos.

ANEXO I

TERMO DE RECEBIMENTO E COMPROMISSO

Declaro que recebi o documento que expõe a Política de Segurança da Informação (PSI) da FADESP, estou ciente de suas diretrizes e disposições e, ao assinar este Termo, manifesto meu compromisso em cumpri-las integralmente na condução das minhas atividades na FADESP e também a disseminar seu conteúdo.

Declaro ainda que participei da capacitação e tenho conhecimento de todas as políticas e ações implantadas pela FADESP, manifestando o meu compromisso de cumpri-las.

Local e data: _____

Nome completo: _____

CPF: _____

Assinatura: _____

ASCOM/FADESP

Fadesp
FUNDAÇÃO DE AMPARO E DESENVOLVIMENTO DA PESQUISA

Fundação de Amparo e Desenvolvimento da Pesquisa
Rua Augusto Corrêa s/n • Cidade Universitária Professor José da Silveira Netto / UFPA
Guamá - Belém/PA | Cep 66075-110
Telefone: (91) 4005.7468 • E-mail: assistentecontroladoria@fadesp.org.br