Política de Segurança da Informação (PSI) da Fundação de Apoio Científico e Tecnológico do Tocantins - Fapto

FAPTO FUNDAÇÃO DE APOIO CIENTÍFICO E TECNOLÓGICO DO TOCANTINS	**Política de Segurança da Informação**

Sumário

1. Introdução

A informação é um ativo que possui grande valor para a Fundação de Apoio Científico e Tecnológico do Tocantins (Fapto), devendo ser adequadamente utilizada e protegida contra ameaças e riscos. A adoção de políticas e procedimentos que visem garantir a segurança da informação deve ser prioridade constante da instituição, reduzindo os riscos de falhas, os danos e/ou os prejuízos que possam comprometer a imagem e os objetivos da instituição.

A segurança da informação é crucial para a proteção de dados confidenciais, preservação da privacidade dos indivíduos e manutenção da integridade dos dados, sendo essencial para o funcionamento e a continuidade dos negócios.

A informação pode existir e ser manipulada de diversas formas, ou seja, por meio de arquivos eletrônicos, mensagens eletrônicas, internet, bancos de dados, em meio impresso, verbalmente, em mídias de áudio e de vídeo, etc.

Além disso, uma estratégia de segurança da informação bem implementada é vital para a inovação segura, gestão de riscos, e estabelece uma cultura organizacional de responsabilidade e prestação de contas.

Por princípio, a segurança da informação deve abranger três aspectos básicos, destacados a seguir:

I. Confidencialidade: somente pessoas devidamente autorizadas pela Fundação devem ter acesso à informação;
II. Integridade: somente alterações, supressões e adições autorizadas pela Fundação devem ser realizadas nas informações;
III. Disponibilidade: a informação deve estar disponível para as pessoas autorizadas sempre que necessário ou demandado;

Para assegurar esses três itens mencionados, a informação deve ser adequadamente gerenciada e protegida contra roubo, fraude, espionagem, perda não-intencional, acidentes e outras ameaças.

2. Objetivo

A Política de Segurança da Informação (PSI) da Fapto é uma declaração formal da instituição acerca de seu compromisso com a proteção das informações de sua propriedade e/ou sob sua guarda, devendo ser cumprida por todos os seus colaboradores.

Seu propósito é estabelecer as diretrizes a serem seguidas pela Fapto no que diz respeito à adoção de procedimentos e mecanismos relacionados à segurança da informação.

3. Aplicação

As regras e recomendações desta política de segurança da informação são aplicáveis a todos os colaboradores, estagiários, aprendizes, prestadores de serviços e visitantes.

4. Definições

São adotadas as seguintes definições a seguir no contexto desta política de segurança da informação.

4.1. Informação

A informação pode ser a reunião dos dados processados, que são capazes de gerar resultados para um determinado sistema que o recebe.

Serão consideradas informações os dados que, mesmo não sendo processados, for útil para construir modificações no conhecimento dos sistemas, sendo eles informatizados ou não.

4.2. Equipamentos

Todo dispositivo utilizado para processamento, produção, transformação, manipulação, organização ou transmissão de informações no ambiente da Fapto, ou que seja de sua propriedade.

Essa denominação engloba computadores, impressoras, scanners, smartphones, roteadores, switches, servidores, centrais telefônicas, aparelhos telefônicos, câmeras, headset, mouse, teclado, monitores, dentre outros.

4.3. Aplicativos

Qualquer programa ou grupo de programas que instrui o hardware sobre a execução de uma tarefa, sendo também referenciados com sistema, aplicativo, ou software, podendo estar instalados localmente ou disponíveis na internet.

4.4. Recursos de Tecnologia da Informação

Faz referência a todos os equipamentos e aplicativos, internos e externos.

5. Regras

5.1. Proibições:

- Todo tipo de acesso à informação referente a Fapto, que não for explicitamente autorizado, é proibido;
- Informações confidenciais, não devem ser transportadas em qualquer meio (CD, DVD, disquete, pen-drive, HD externo, papel, e-mail, etc.) sem as devidas autorizações e proteções;
- Todos os equipamentos (computadores, notebook, celular) devem ser protegidos por senha;
- As senhas de usuário são pessoais e intransferíveis, não podendo ser compartilhadas, divulgadas a terceiros (inclusive colaboradores da própria fundação), anotadas em papel ou em sistema visível, ou de acesso não protegido;
- Somente softwares homologados previamente pela Fundação, poderão ser instalados nas estações de trabalho, o que deve ser feito, com exclusividade, pela equipe de Tecnologia da Fundação;
- As políticas para uso de internet e correios eletrônicos devem ser rigorosamente seguidas, e arquivos de origem desconhecida nunca devem ser abertos ou executados;
- Documentos impressos e arquivos contendo informações confidenciais devem ser adequadamente armazenados e protegidos;
- Salvar e manter arquivos da instituição em equipamentos pessoais (tais como: contatos de telefone, arquivos em notebook ou HD pessoal);
- Acessar remotamente os servidores da Fapto (em casos de trabalho no modelo home office) fora do horário de trabalho, salvo casos formalmente autorizados pelo superior hierárquico;
- Utilizar a infraestrutura (computadores, internet, celular, impressora, HD externo) para fins pessoais;

- Utilizar e-mail pessoal para tratativas relacionadas ao desempenho do trabalho junto à Fapto.

5.2. Proibição de Uso de Mídias Removíveis

É estritamente proibida a conexão e o uso de quaisquer mídias removíveis (incluindo, mas não se limitando a, pen drives, HDs externos, cartões de memória, CDs/DVDs e smartphones conectados como dispositivo de armazenamento) em equipamentos da instituição, sejam eles computadores, notebooks ou outros dispositivos eletrônicos.

5.2.1. Exceções e Procedimentos

- **Exceções:** Qualquer exceção a esta política deve ser formalmente solicitada e previamente **aprovada pela área de Tecnologia da Informação (TI)**, mediante justificativa técnica e/ou de negócio. A TI avaliará a necessidade, os riscos e definirá os procedimentos de segurança específicos para o uso temporário e monitorado.
- **Procedimentos para Exceções Autorizadas:** Em casos de exceção autorizada, o uso de mídias removíveis deverá seguir rigorosamente as orientações da TI, que podem incluir:
    - Uso exclusivo de mídias fornecidas ou homologadas pela instituição;
    - Escaneamento antivírus e de malware obrigatório em estação de trabalho controlada pela TI;
    - Criptografia dos dados armazenados na mídia removível;
    - Monitoramento e auditoria do acesso e dos dados transferidos;
    - Destruição segura dos dados após o uso, conforme orientação da TI.

5.3. Controle e Restrição de Fluxo de Dados Pessoais

Todos os fluxos de dados pessoais em trânsito entre sistemas, colaboradores ou terceiros devem ser previamente avaliados quanto à sua necessidade, finalidade e segurança. As transferências só poderão ocorrer se:

- Houver base legal válida e registrada;
- Estiverem documentadas em contrato ou política interna;
- Usarem canais seguros com criptografia (TLS, VPN);

- Houver autenticação forte no acesso aos sistemas envolvidos;
- Os dados forem minimizados conforme a necessidade do processo;
- O fluxo estiver registrado nos logs corporativos com rastreabilidade.

5.4. Obrigações

- A área de Segurança da Informação deve realizar, de forma sistemática, a avaliação dos riscos de incidentes relacionados à segurança da informação;
- O colaborador que proteger arquivos com senhas precisará disponibilizá-las ao seu superior hierárquico ou substituto para acesso em sua ausência;
- Manter todos os arquivos vinculados à Fapto em formato editável nos servidores/rede disponibilizados pela equipe de TI.

5.5. Boas práticas para utilização do e-mail corporativo

- O e-mail corporativo é criado pela equipe de TI com autorização da gerência executiva/diretoria;
- Excluir periodicamente e-mail's não úteis, tais como: mensagens da agenda, propagandas, recebimentos de newsletter, entre outros;
- O e-mail da Fapto é destinado exclusivamente aos assuntos da Fundação e não é permitido o uso para fins pessoais ou de lazer;
- Só é permitido o acesso ao e-mail durante o horário do trabalho, salvo casos formalmente autorizados pela gerência/diretoria;
- O e-mail deve conter uma assinatura pessoal.

6. Disponibilização e Responsabilidade sobre equipamentos

Os usuários são responsáveis pela segurança dos equipamentos recebidos e devem ser responsabilizados caso haja caracterização de mau uso.

Nos casos de mau uso, o usuário deverá assumir os custos de reparo ou, na impossibilidade de conserto, de nova aquisição de equipamento de mesma marca e modelo.

7. Segurança e Monitoramento das informações

Os sistemas, as informações e os serviços utilizados pelos usuários são de exclusiva propriedade da Fapto, não podendo ser interpretados como de uso pessoal.

Todos os profissionais e colaboradores da Fapto devem ter ciência de que o uso das informações e dos sistemas de informação da Fapto pode ser monitorado, e que os registros assim obtidos poderão ser utilizados para detecção de violações da Política de Segurança da Informação e, conforme o caso, servir como evidência em processos administrativos e/ou legais.

8. Acesso aos Sistemas e Equipamentos

Todos os acessos dos usuários aos sistemas utilizados pela Fapto devem estar atrelados a perfis específicos condizentes com sua função e cargo, no caso de funcionários, estagiários e aprendizes, ou ao uso específico, no caso de terceiros, proibido o acúmulo de perfis.

- Os perfis de acesso aos sistemas são criados pela equipe de TI e autorizados pela Gerência Executiva/diretoria;
- Sem necessidade de prévia autorização, a equipe de TI pode restringir o acesso dos usuários que forem detectados, exaurindo ou prejudicando algum recurso tecnológico;
- A restrição imposta ao usuário deve ser comunicada formalmente à Gerência Executiva e/ou Diretoria Executiva;
- Os acessos serão revisados semestralmente;
- Além das revisões periódicas, ocorrerá a revisão imediata de acessos, com:
    - Mudança de função do colaborador;
    - Desligamento do colaborador;
    - Reestruturação de equipes ou departamentos;
    - Projeto finalizado;
    - Incidentes de segurança.

9. Responsabilidade sobre equipamentos pessoais

9.1. Perda ou Furto de Equipamentos Pessoais

Os equipamentos pessoais trazidos e/ou utilizados nas dependências da Fapto são de responsabilidade apenas do proprietário, não cabendo à Fapto qualquer obrigatoriedade de reposição ou indenização.

10. Identificação de pessoas e acesso às informações

Todos os dispositivos de reconhecimento de pessoas utilizados na Fapto, como o número de registro do colaborador, do crachá, das identificações de acessos aos sistemas, dos certificados, das assinaturas digitais e dos dados biométricos têm de estar associados a uma pessoa física e atrelados inequivocamente aos seus documentos oficiais reconhecidos pela legislação brasileira.

10.1. Criação e Controle das Identidades Lógicas

A equipe de TI é responsável pela criação de usuários dos diretores, empregados, estagiários, aprendizes e prestadores de serviços na instituição.

10.2. Desligamento ou Remanejamento de colaboradores, Estagiários e Aprendizes

Nos casos de desligamento ou remanejamento de colaboradores da Fapto, Coordenação de Gestão de Pessoas (RH) deverá comunicar o fato imediatamente à equipe de TI.

10.3. Bloqueio de Acesso do Usuário nos Casos de Desligamento

Quando algum usuário se desligar da Fapto, a equipe de TI deverá bloquear imediatamente o acesso aos sistemas, e-mail’s e equipamentos aos quais ele tinha acesso.

11. Classificação da informação

Todos os usuários são responsáveis pelas informações da Fapto que circulam em diferentes formatos e meios de comunicação, dentro e fora da instituição.
Toda informação deve ser protegida e mantida sob sigilo conforme a sua importância e criticidade para a Fapto. Quanto mais crítica ou sigilosa, maiores cuidados devem ser dedicados ao manuseio, arquivamento e eventual descarte.

A Fapto trabalha com documentos físicos e eletrônicos criados internamente ou recebidos de terceiros. Todos os documentos são de propriedade da Fapto e, portanto, devem ser protegidos, pois podem conter informações corporativas críticas.

12. Proteção contra ameaças digitais

Os hábitos seguros contra ameaças digitais são de responsabilidade de todos os usuários, que devem seguir as recomendações da equipe de TI divulgadas pelos instrumentos de comunicação disponíveis na Fapto.

12.1. Dispositivo de Acesso Externo

É proibido o uso de quaisquer dispositivos externos de acesso à rede que ultrapassem ou anulem intencionalmente os controles de segurança da Fapto.

12.2. Proteção Contra Aplicativos Mal-Intencionados

A proteção contra aplicativos mal-intencionados deve ser realizada por meio de ações conjuntas dos profissionais de TI, sistemas de proteção, procedimentos de segurança e comportamento dos usuários.

12.3. Instalação de Aplicativos

Todo e qualquer aplicativo deve ser instalado exclusivamente pela equipe de TI.

12.4. Aplicativos Ilegais ou não Homologados

Não são permitidas instalações de aplicativos ilegais ou não homologados pela equipe de TI nos equipamentos da Fapto.

13. Tratamento de Incidentes

Ao tomar conhecimento de uma brecha, incidente e/ou violação desta política de segurança da informação, o usuário deverá comunicar de imediato o fato à equipe de TI.

O usuário não deverá fazer nenhum teste para checar possíveis falhas na segurança. A efetivação de testes de vulnerabilidade ou tentativa para solucionar possíveis brechas pode ser interpretada como tentativa de violação da segurança e o usuário que assim proceder será responsabilizado.

14. Medidas Disciplinares Por Violação da PSI

Nos casos em que houver violação desta Política ou das Normas de Segurança da Informação, sanções administrativas e/ou legais poderão ser adotadas, podendo culminar com o desligamento e eventuais processos criminais, se aplicáveis.

Os casos omissos, não previstos nesta política de segurança, devem ser avaliados e tratados pela Diretoria Executiva, Gerência Executiva em conjunto com a equipe de TI.

15. Responsabilidades

15.1. Responsabilidades gerais de todos os colaboradores da Fapto

Cabe a todos os colaboradores (funcionários, estagiários, prestadores de serviços e visitantes) da Fapto:

- Cumprir fielmente a Política e as normas de Segurança da Informação da Fapto, bem como manter-se informado sobre suas atualizações;
- Buscar orientação do superior hierárquico imediato em caso de dúvidas relacionadas à segurança da informação;
- Assinar Termo de Responsabilidade, formalizando a ciência e o aceite da Política e das Normas de Segurança da Informação, bem como assumindo responsabilidade por seu cumprimento;

- Proteger as informações contra acesso, modificação, destruição ou divulgação não-autorizados pela Fapto;
- Assegurar que os recursos tecnológicos à sua disposição sejam utilizados apenas para as finalidades aprovadas pela Fapto;
- Comunicar imediatamente à área de Tecnologia da Informação qualquer descumprimento ou violação desta Política e/ou de suas Normas.
- Ser ético na aquisição, tratamento e utilização da informação corporativa;

15.2. Responsabilidades Específicas da Diretoria e Equipe de TI,

Com relação à segurança da informação, cabe à Diretoria:

- Aprovar a Política de Segurança da Informação e suas revisões;
- Tomar as decisões administrativas referentes aos casos de descumprimento da Política e/ou de suas Normas encaminhados pela equipe de Tecnologia da Informação;
- Ter postura exemplar em relação à segurança da informação, servindo como modelo de conduta para os colaboradores da Fapto;
- Adequar as normas, os processos, procedimentos e sistemas sob sua responsabilidade para atender à Política de Segurança da Informação da Fapto.

15.3. Responsabilidades específicas da equipe de TI

- Pela característica de seus privilégios, manter sigilo sobre as informações e dados da Fapto e dos usuários, restringindo-se a acessá-los somente quando forem necessários para a execução das atividades operacionais sob sua responsabilidade;
- Planejar, implantar, fornecer e monitorar a capacidade de armazenagem, processamento e transmissão necessários para garantir a segurança requerida pelas áreas de negócio;
- Garantir, no menor prazo possível, o bloqueio de acesso de usuários por motivo de desligamento da instituição, incidente, investigação ou outra situação que exija medida restritiva para fins de salvaguardar os ativos da Fapto;
- Configurar os equipamentos, ferramentas e sistemas concedidos aos usuários com todos os controles necessários, para cumprir os requerimentos de segurança estabelecidos por esta política de segurança da informação.

16. Segurança em Recursos Humanos

Na segurança da informação, os recursos humanos (RH) desempenham um papel vital, pois grande parte da segurança depende do comportamento e consciência dos funcionários. A seguir, são apresentadas algumas medidas de segurança em recursos humanos que devem ser adotadas para reforçar a proteção da informação:

Acordos de Confidencialidade: Garantir que os novos contratados assinem acordos de não divulgação ou de confidencialidade;

Programas de Conscientização: Fornecer treinamento regular e atualizações sobre práticas recomendadas de segurança da informação, phishing, engenharia social, e outros riscos relevantes.

Integração: Todos que ingressam no corpo de funcionários deverá receber as políticas, procedimentos e receber treinamento para entender o ambiente digital ao qual integrará. Deverá registrar em documento específico cientificando o recebimento de todos os documentos, treinamento e, ainda, deverá se submeter ao alinhamento de aprendizado para verificação da apreensão do conteúdo, o qual deverá pontuar em, pelo menos 70% (setenta por cento).

Simulações de Segurança: Realizar exercícios e simulações, como testes de phishing, para educar os funcionários sobre ameaças.

Alterações de Acesso: Atualizar prontamente as permissões de acesso quando um funcionário muda de função ou deixa a empresa para garantir que somente as pessoas autorizadas tenham acesso a informações sensíveis.

Avaliação de Risco para Mudanças de Função: Avaliar quaisquer novos riscos de segurança que possam surgir devido a mudanças nas responsabilidades do funcionário.

Avaliações Regulares: Conduzir avaliações periódicas de desempenho que incluam a aderência às políticas de segurança da informação.

Procedimentos de Desligamento: Ter um processo formal de desligamento que inclua a revogação de todos os acessos a sistemas e informações da empresa.

Entrevistas de Saída: Realizar entrevistas de saída para reforçar as obrigações de confidencialidade após o término do emprego.

Os setores envolvidos deverão estar em contato e em contínuo estabelecimento de melhorias quanto a estes pontos e com sugestão de melhorias.

17. Gestão de Incidentes de Segurança da Informação

A gestão de incidentes de segurança da informação é um processo estruturado para identificar, responder, mitigar e aprender com os incidentes de segurança que afetam as informações e sistemas de uma organização. Este processo é crucial para minimizar o impacto dos incidentes e restaurar os serviços normais o mais rápido possível, enquanto preserva as evidências para análises e melhorias futuras. São etapas da gestão de incidentes:

Identificação de Incidentes: O processo começa com a capacidade de detectar rapidamente atividades anormais ou suspeitas que possam indicar uma violação de segurança. Isso geralmente é feito através de sistemas de monitoramento, alertas de segurança, análise de logs e relatórios de usuários;

Resposta a Incidentes: Uma vez identificado o incidente, a resposta deve ser imediata. Equipes de resposta a incidentes (usualmente chamadas de CIRT, Computer Incident Response Team) são mobilizadas para conter a ameaça, avaliar o impacto e começar os esforços de recuperação. Isso pode incluir desligar sistemas afetados, isolar segmentos da rede ou revogar acessos;

Comunicação: Durante e após um incidente, a comunicação eficaz é vital. Isso inclui notificar as partes internas relevantes, como a liderança executiva e departamentos afetados, e, quando necessário, comunicar-se com clientes, parceiros e autoridades regulatórias;

Recuperação: Restaurar os serviços e processos normais é uma prioridade. Isso envolve eliminar a causa raiz do incidente, restaurar dados a partir de backups e implementar medidas para evitar a recorrência do incidente;

Análise e Melhoria: Após a resolução do incidente, é fundamental realizar uma análise pós-incidente para identificar as causas, aprender com os erros e melhorar as medidas de segurança. Isso pode resultar em atualizações de políticas, reforço de infraestruturas de segurança, e treinamento adicional para a equipe;

As informações mais detalhadas, inclusive quanto ao Comitê de gestão de incidentes de segurança da informação e LGPD, serão detalhadas em Política própria.

18. Revisão da Política

Esta política deve ser revisada anualmente, caso necessário ou sempre que houver mudanças significativas nos sistemas de informação, ou na organização, em mesma reunião que verificará o cronograma de treinamento e comunicação, realização de auditorias anuais e melhorias contínuas.

Data da Segunda Revisão	Responsável	Data da Aprovação Segunda Versão	Responsável
26/05/2025	Eduardo/Oziel	04/09/2025	Léo Araújo