IEPTB-PSI
Política de Segurança da Informação do Instituto de Estudos de Protesto de Títulos do Brasil

I Ficha técnica deste documento

Documento	PSI IEPTB
Versão	1.1
Data da Versão	24/novembro/2020
Criado Por:	Márcio Bordignon (Multip)
Revisado Por:	Cida Rosa (IEPTB)
Aprovado Por:	Léo Barros Almada (IEPTB)
Vigência:	A partir de 25/11/2020
Nível de Confidencialidade	Público
Número de Páginas	**Este documento contém 11 paginas**

Histórico de Alterações e Aprovações

Data	Versão	Editado por	Descrição da Alteração / Aprovação
30/09/20	Draft 1.0	Márcio Bordignon	Esboço do documento
24/11/20	Versão 1.1	Rodrigo Fontoura	Emissão da versão 1.1

II Controle de impressão

A versão digital deste documento é a versão mais recente. É responsabilidade de cada indivíduo garantir que qualquer versão impressa seja a versão mais recente. A versão impressa deste documento não é controlada e não pode ser invocada, exceto quando formalmente emitido e assinado pelo Controlador de Documentos e fornecido com indicação de controle de cópia, conforme indicado nos campos abaixo:

Versão:	*1.1*
Data da Emissão:	*24/11/2020*
Cópia Controlada	**X**
Cópia não Controlada	

III Resumo Executivo

Esta política apresenta as diretrizes gerais para a gestão de segurança da informação no IEPTB, visando a proteção dos seus ativos de informação.

Tais orientações devem ser devidamente compreendidas e adotadas em todos os ambientes e níveis do Instituto.

Tem como objetivo a preservação dos aspectos de disponibilidade, integridade, confidencialidade e autenticidade das informações, bem como contribuir para que a missão do IEPTB seja cumprida.

Este documento disserta sobre o propósito, diretrizes, funções e responsabilidades, violações e sanções, revisões e atualizações, contatos e referencias.

1 Introdução

Todo dado e informação criada, armazenada, tratada, processada e descartada por qualquer Agente do IEPTB é considerada patrimônio valioso.

A informação pode ser gerada e manipulada de diversas formas: mensagens e arquivos eletrônicos, internet, meio impresso, verbal e outros. Independentemente da forma, três aspectos da informação norteiam sua segurança:

- Confidencialidade: a informação só deve ser acessível a quem tem a devida autorização
- Integridade: a informação deve manter-se inalterada desde sua geração ou alteração autorizada
- Disponibilidade: a informação deve estar sempre disponível às pessoas autorizadas.

O presente documento constitui a Política de Segurança da Informação do IEPTB.

Toda informação deve ser protegida conforme as regras definidas nesta Política. A adoção de procedimentos que promovam a segurança da informação deve ser parte cotidiana das atividades, a fim de reduzir falhas e danos que possam comprometer a operação do negócio ou trazer prejuízos a outrem.

De modo geral, esta política resume os princípios da Segurança da Informação que o IEPTB reconhece como importantes, e demonstra o comprometimento do IEPTB com sua aplicação, por meio do apoio de todos os servidores, colaboradores, prestadores de serviço, e todos aqueles que estão diretamente envolvidos na sua aplicação.

2 Finalidade, aplicabilidade, escopo e usuários

O objetivo desta Política de Segurança de Informação (PSI) de alto nível é definir os propósitos e finalidades, as diretrizes, os princípios e as regras básicas de gestão da segurança da informação.

Esta política aplica-se ao IEPTB em todos os ambientes e processos deste.

Os usuários deste documento são os servidores, colaboradores, prestadores de serviço do IEPTB, assim como as partes externas relevantes.

Faz parte do escopo desta PSI:

- Declarar formalmente o compromisso do IEPTB com a Segurança da Informação;
- Prover orientação e apresentar diretrizes sobre a segurança da informação para todos os colaboradores e partes a quem se aplica;
- Definir funções e responsabilidades relacionadas à Segurança da Informação;

- Prover diretrizes para preservar a confidencialidade, a integridade e a disponibilidade das informações em todos os níveis de atividades, proporcionar a segurança física e lógica das informações, reduzir riscos, alcançar as conformidades legais, minimizar problemas causados por indisponibilidades dos serviços e proteger a imagem e a operação do IEPTB.

3 Documentos de Referência

- Resolução BACEN 4.658/2018
- Lei 13.709/2018 (LGPD)
- Marco Civil da Internet
- RISI (Regulamento Interno de Segurança da Informação do IEPTB) e respectivos teros de ciência
- Acordo Padrão de Confidencialidade (NDA) do IEPTB
- Programa de Conscientização da Segurança da Informação do IEPTB (PCSI)
- Procedimento de Gestão de Usuários do IEPTB (PGU)
- Procedimento de Inventário e Propriedade de ativos de TI do IEPTB (PIP)
- Procedimento de Organização da Segurança da Informação do IEPTB (POSI)
- Procedimento de Gestão de Incidentes do IEPTB (PGI)
- Procedimento de Mesa Limpa e Tela Limpa do IEPTB (PTL)
- Procedimento de Segregação de Redes e Dados do IEPTB (PSR)
- Procedimento de Gestão de Operações Seguras do IEPTB (POS)
- Planilha de inventário de Ativos
- Organograma do IEPTB

4 Termos e Definições

Termos, expressões e definições utilizados nesta Política estão conceituados no Anexo 1

5 Diretrizes para a Gestão da Segurança da Informação no IEPTB

As diretrizes orientam a elaboração das normas e procedimentos para instituir e manter o Sistema de Gestão da Segurança da Informação no IEPTB. São elas:

Considerar informação como patrimônio
Assegurar que toda a informação, coletada, gerada, adquirida, utilizada, em trânsito e armazenada; própria, pessoal ou custodiada; por meio de tecnologias, procedimentos, pessoas e ambientes do IEPTB, deve ser tratada como parte do seu patrimônio e deve ser protegida quanto aos aspectos de confidencialidade, integridade e disponibilidade, bem como de proteção de dados pessoais, privacidade e conformidade legal.

Proteção da informação
Assegurar que essas diretrizes sejam aplicáveis aos ambientes, sistemas, pessoas e processos do IEPTB, tanto no meio digital quanto nos meios analógicos de processamento, comunicação e armazenamento de informações.

Responsabilizar proprietário dos ativos
Considerar o colaborador ou terceirizado, proprietário dos ativos de informação sob sua responsabilidade, como responsável pela liberação e cancelamento do acesso, classificação de segurança e medidas de proteção de informação e dados.

Segregar funções
Segregar a administração e a execução de funções conflitantes ou áreas de responsabilidade críticas para que ninguém detenha controle de um processo na sua totalidade, visando reduzir os riscos de mau uso, acidental ou deliberado, dos ativos do IEPTB.

Responsabilizar uso da credencial de acesso
Liberar o acesso e uso de ativos por meio de credencial de acesso, pessoal e intransferível, qualificando o titular como responsável por todas as atividades desenvolvidas por meio dela.

Restringir acesso e uso de ativos
Assegurar que o acesso e o uso dos ativos sejam controlados e limitados às atribuições necessárias para cumprimento das atividades de usuários autorizados e utilizados no estrito interesse do IEPTB, apenas para as finalidades profissionais, lícitas, éticas, administrativamente aprovadas e devidamente autorizadas. Qualquer outra forma de acesso e uso necessitará de prévia autorização do proprietário do ativo de informação.

Usar ativos seguros
Permitir somente o uso de ativos homologados e autorizados pelo IEPTB, desde que sejam identificados de forma individual, inventariados, protegidos e tenham um proprietário responsável. Sua operação deve estar de acordo com a Política de Segurança da Informação do IEPTB, cláusulas contratuais e legislação em vigor.

Promover a proteção de dados pessoais e a privacidade
Proteger dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito que possa afetar a privacidade do titular (ref. Lei Federal 13709/2018).

Monitorar e auditar permanentemente
Monitorar e auditar periodicamente o cumprimento da Política de Segurança da Informação, pelas áreas competentes, respeitando-se os princípios legais e normativos.

Conscientizar de forma contínua
Assegurar que usuários sejam continuamente capacitados e conscientizados sobre os procedimentos de proteção e uso correto dos ativos do IEPTB quando da realização de suas atividades, bem como estejam conscientes e cumpram suas responsabilidades, de forma a minimizar riscos.

Implantar e manter em operação um Sistema de Gestão da Segurança da Informação no IEPTB
Implantar o Comitê Gestor de Segurança da Informação multidisciplinar – CGSI – que será responsável pela aprovação das Normas, Regulamentos e procedimentos de Segurança da Informação do IEPTB, dele fazendo parte representantes das principais áreas do IEPTB que tratam com ativos de informação. O Comitê também dará o suporte às ações estratégicas para a gestão da Política de Segurança da Informação, entre elas:

- Definição de Normas e Procedimentos de Segurança da Informação a serem aprovadas pelo CGSI.
- Implantação de um Sistema de Gestão de Segurança da Informação – SGSI – que permita:
  - Avaliação contínua dos riscos de segurança da informação através de análise sistemática e periódica.
  - Gestão de acesso a sistemas de informação de forma que o acesso seja controlado e esteja de acordo com as Normas e os Procedimentos definidos.
  - Implantação do processo para inventário e gestão dos ativos de Tecnologia da Informação.
  - Implantação de uma equipe de resposta a incidentes de Segurança da Informação de forma que as fragilidades e eventos de segurança associados a sistemas de informação sejam comunicadas e permitindo a tomada de ação corretiva em tempo hábil.
- Definição de processo de validação das evidências de cumprimento da política de segurança da informação.
- Definição e utilização de Regulamentos e Termos de Responsabilidade para acesso às informações classificadas.
- Estabelecimento de um programa de capacitação e conscientização de todos os usuários em relação à adoção de comportamento seguro na utilização das informações.

6 Funções e Responsabilidades

Direção Geral
Cabe à Direção Geral do IEPTB:

- Aprovar e Publicar 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 pelo Comitê Gestor de Segurança da Informação
- Autorizar o CGSI, quando necessário e para finalidade específica de auditoria e/ou produção de provas, a realizar monitoramento de conteúdo das informações armazenadas, tratadas ou trafegadas em rede nos dispositivos do IEPTB
- Divulgar ao público resumo desta PSI contendo as suas linhas gerais, em conformidade com o Art. 5º. da Resolução BACEN 4.658/2018.
- Designar Diretor do IEPTB como responsável por esta PSI, em conformidade com o Art. 7º. Da Resolução BACEN 4.658/2018

Comitê Gestor de Segurança da Informação (CGSI)
Cabe ao Comitê Gestor de Segurança da Informação:

- Propor alterações nesta Política
- Aprovar a estrutura, os processos e procedimentos do Sistema de Gestão de Segurança da Informação
- Propor alterações e aprovar as Normas, Regulamentos e Procedimentos de Segurança da Informação
- Definir a classificação das informações pertencentes ou sob a guarda do IEPTB
- Analisar os casos de violação desta Política e das Normas de Segurança da Informação, encaminhando-os à Direção Geral, quando for o caso
- Propor medidas relacionadas à melhoria da segurança da informação do IEPTB
- Propor o planejamento e a alocação de recursos no que tange à segurança da informação
- Determinar a elaboração de relatórios, levantamentos e análises que dêem suporte à gestão de segurança da informação e à tomada de decisão
- Acompanhar o andamento dos principais projetos e iniciativas relacionados à segurança da informação
- Aprovar a relação de “proprietários” das informações do IEPTB
- Elaborar e emitir o Relatório Anual (01/janeiro a 31/dezembro) sobre a implementação e sustentação desta PSI, conforme o Art. 8º. Da Resolução BACEN 4.658/2018, e apresenta-lo à Direção Geral até no máximo 31 de março do ano subsequente
- Convocar reuniões ordinárias e extra-ordinárias do CGSI

Serão membros do Comitê Gestor de Segurança da Informação:

- Representantes da área de Informática, tecnologia e Segurança da Informação
- Gerencia de Tecnologia da Informação
- Secretaria de Gestão de Pessoas
- Representantes da Direção Geral
- Controlador de Documentos

O responsável pela Área de TI (Gerente de TI) coordenará os trabalhos do Comitê e suas atribuições abrangerão a convocação das reuniões e a realização de outras atividades de suporte.
As reuniões ordinárias do Comitê:
(a) Serão realizadas trimestralmente, podendo haver convocação extraordinária, sempre que necessário;
(b) Serão instaladas com a presença de, no mínimo, 2/3 (dois terços) dos membros do Comitê; e
(c) Serão registradas em ata.

As deliberações do Comitê serão pela maioria dos votos presentes.

Sempre que necessário outros profissionais do órgão e também convidados externos poderão participar das reuniões.

Proprietário da Informação
O(a) Proprietário(a) da Informação é o(a) líder (gerente, coordenador) da área responsável pela concessão de acesso à informação a ele relacionada ou sob sua guarda. A ele(a) cabe:

- Elaborar matriz de cargos e funções e respectivos direitos de acesso para todas as informações sob sua guarda
- Autorizar e desautorizar acesso às informações sob sua guarda, observada a matriz definida no item anterior. Sempre que necessário apoio técnico para operacionalização, o Proprietário da Informação deverá solicitar a concessão e/ou remoção de privilégios de acesso ao Suporte Técnico, conforme procedimentos aplicáveis
- Analisar relatórios de acesso fornecidos pela área de segurança da informação corrigindo desvios porventura observados
- Participar das reuniões do Comitê quando convocado

Assessoria Jurídica
À Assessoria Jurídica do IEPTB cabe:

- Informar ao Comitê alterações legais ou regulatórias que impliquem responsabilidade ou ação que envolvam a gestão da segurança da informação
- Avaliar, sempre que solicitada, as Normas, os Procedimentos e os Termos de Sigilo referentes à gestão da segurança da informação
- Auxiliar o Comitê nas demais questões legais.

Gerência de TI
Cabe à Gerência de TI:

- Propor a estrutura, os processos e procedimentos do Sistema de Gestão de Segurança da Informação – SGSI – sendo que entre os processos devem estar previstos o planejamento, a execução e operação, o monitoramento, o controle e a auditoria da Segurança da Informação
- Nas reuniões do Comitê: convocar, coordenar os trabalhos, lavrar atas e prover apoio às reuniões
- Disponibilizar as informações de gestão de segurança da informação solicitadas pelo Comitê
- Divulgar amplamente a Política e as Normas de Segurança da Informação para todos os Agentes

- Propiciar orientação e treinamento sobre a Política de Segurança da Informação e suas Normas a todos os Agentes
- Propor ações relacionadas à melhoria da segurança da informação do IEPTB
- Propor procedimentos e realizar a gestão dos sistemas de controle de acesso do IEPTB, incluindo os processos de concessão, manutenção, revisão e suspensão de acessos aos usuários
- Identificar e Analisar os riscos relacionados à Segurança da Informação do IEPTB e apresentar relatórios periódicos sobre tais riscos ao CGSI, acompanhados de proposta de aperfeiçoamento do ambiente, quando for o caso
- Executar trabalhos de análise de vulnerabilidade, com o intuito de aferir o nível de segurança dos sistemas de informação e dos demais ambientes em que circulam as informações do IEPTB;
- Solicitar ou requisitar informações às demais áreas do órgão
- Realizar testes e averiguações em sistemas, equipamentos e outros recursos, com o intuito de verificar o cumprimento da Política e das Normas de Segurança da Informação

Secretaria de Gestão de Pessoas
Cabe à área de Recursos Humanos:

- Obter a assinatura do Termo de Responsabilidade dos Agentes, arquivando-o nos respectivos prontuários
- Comunicar à Área de de Segurança da Informação, de imediato, todos os desligamentos, afastamentos e modificações no quadro funcional do IEPTB.

Agentes do IEPTB
Cabe a todos os Agentes do IEPTB:

- Cumprir as diretrizes definidas nesta Política, além das Normas, Regulamentos e Procedimentos aprovados pelo IEPTB de forma pró-ativa
- Compreender ameaças externas que podem comprometer a segurança das informações do IEPTB tais como: fraudes, grampos telefônicos e interceptação de mensagens, vírus de computador, etc.
- Assegurar que informações confidenciais do IEPTB estejam devidamente protegidas
- Evitar discutir assuntos confidenciais de trabalho em ambientes públicos
- Cumprir as determinações do Regulamento Interno de Segurança da Informação, em especial não divulgar ou compartilhar senhas de acesso que serão sempre pessoais e intransferíveis, utilizar apenas softwares homologados pelo IEPTB, e seguir rigorosamente as normas de uso de Internet e Correio Eletrônico do IEPTB, entre outras
- Alertar a Área de Segurança da Informação sobre violações de Normas, Regulamentos, Procedimentos ou dessa Política
- Buscar orientação do Suporte Técnico em caso de dúvidas relacionadas à segurança da informação
- Proteger as informações contra acesso não autorizado pelo IEPTB
- Assegurar que os todos os recursos tecnológicos à sua disposição sejam utilizados apenas e exclusivamente para as finalidades aprovadas pelo IEPTB

7 Violações e Sanções

Os Agentes do IEPTB deverão conhecer e zelar pelo cumprimento da Política de Segurança da Informação (PSI), do Regulamento Interno de Segurança da Informação (RISI), e dos processos e procedimentos de segurança da informação à eles aplicáveis.

A desobediência à PSI, suas normas, regulamentos e procedimentos estabelecidos implicará nas sanções administrativas previstas em regulamentações internas, e legislação em vigor.

8 Revisões e Atualizações

A Política de Segurança da Informação deverá ser analisada anualmente de forma crítica, visando a sua aderência e concordância aos objetivos do IEPTB e legislação vigente, como forma de melhoria contínua.

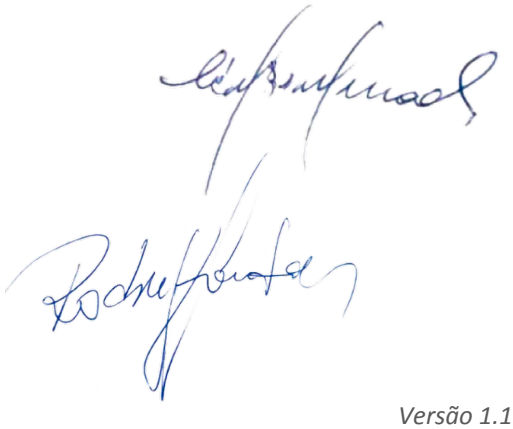
9 Disposições Finais

Os documentos, relatórios, evidências de , dados e informações produzidos para dar sustentação à operacionalização desta PSI, conforme descrito no Art. 23º da Resolução BACEN 4.658, devem ser armazenados pelo IEPTB e ficar à disposição de autoridades competentes pelo período de 5 (cinco) anos.

10 Informações para Contato

Dúvidas e solicitações de informações referentes à esta PSI devem ser encaminhadas ao CGSI (Comitê Gestor de Segurança da Informação), por meio dos contatos abaixo:

Controlador de Documentos do IEPTB-BR:
Rodrigo Fontoura
rodrigo.fontoura@cartoriosdeprotesto.org.br



Versão 1.1
Vigência: a partir de 25/novembro/2020

Anexo 1 Definições e Glossário

- Agentes do IEPTB: são todas as autoridades, membros, servidores, prestadores de serviço e colaboradores que geram, processam e descartam informações no âmbito funcionamento do IEPTB.
- Análise de riscos: uso sistemático da informação para identificar, avaliar e estimar riscos e ameaças.
- Ativo: Qualquer coisa que tenha valor para a organização.
- Ativos de Informação: são dados, documentos, informações, dispositivos e/ou componentes, bens e direitos, utilizados na produção, tratamento, processamento, armazenamento, transmissão e recuperação da informação, incluindo a própria informação.
- Autenticidade: atributo que estabelece a fidedignidade e/ou legitimidade de dado, informação, usuário, identidade da pessoa que solicita acesso à um ativo, aplicada na origem e/ou no destino
- CGSI: Comitê Gestor de Segurança da Informação.
- Confidencialidade: propriedade da informação para que a mesma não seja disponibilizada ou divulgada a indivíduos, entidades ou processos sem autorização. Característica da informação que está disponível somente para acesso exclusivo de pessoas ou sistemas autorizados. Atributo que define o grau de sigilo, permitindo identificar os privilégios necessários para acesso e restrições de uso.
- Disponibilidade: propriedade de ser acessível e utilizável sob demanda por uma entidade autorizada. Característica de informações e/ou sistemas de ser acessado(a) por pessoas e/ou sistemas autorizadas quando for necessário. Atributo que define a capacidade de um usuário ou sistema em obter acesso à informação armazenada mediante os meios de acesso legítimos disponíveis.
- Evento de segurança da informação: ocorrência identificada de um sistema, serviço ou rede que indica uma possível violação da Política de Segurança da Informação ou falha de controles, ou uma situação previamente desconhecida, que possa ser relevante para a segurança da informação.
- Gestão de riscos: atividades coordenadas para dirigir e controlar uma organização, no que se refere aos riscos. Normalmente inclui a avaliação do risco, o tratamento do risco, a aceitação do risco e a comunicação do risco.
- IEPTB: Instituto de Estudos de Protesto de Títulos do Brasil
- Incidente de segurança: evento ou série de eventos adversos, indesejados ou inesperados, confirmado ou sob suspeita, relacionado ao comprometimento da integridade, disponibilidade ou autenticidade de ativos ou ao bom funcionamento do negócio da organização, tais como (mas não limitado a) ataques, uso ou acesso não autorizado, vírus, vazamento de informação ou mesmo violação à Política de Segurança
- Integridade: propriedade ou atributo que define a exatidão da informação e sua capacidade de se manter exata mediante tentativa de modificação legítima ou ilegítima
- Segurança da informação: preservação da disponibilidade, integridade, confidencialidade e autenticidade da informação; adicionalmente, outras propriedades, tais como responsabilidade, não repúdio e confiabilidade podem também estar envolvidas.
- Segurança: estar livre de perigos e incertezas.
- Sistema de gestão da segurança da informação - a parte do sistema de gestão que cuida do planejamento, implementação, manutenção, revisão e aprimoramento da segurança da informação.
- Tratamento de riscos: processo de seleção e implantação de medidas de controle para modificar um risco.
- Valoração do risco: processo de comparar o risco estimado contra critérios de risco estabelecidos para determinar a significância do risco.