MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÕES - MCTI
EMPRESA BRASILEIRA DE PESQUISA E INOVAÇÃO INDUSTRIAL - EMBRAPII
POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE - PoSIP

Art. 1° O presente documento tem por objetivo estabelecer a Política de Segurança da Informação e Privacidade - PoSIP no âmbito da Empresa Brasileira de Pesquisa e Inovação - EMBRAPII.

CAPÍTULO I
ESCOPO
Seção I
Dos objetivos e Princípios

Art. 2º A PoSIP objetiva garantir a disponibilidade, integridade, confidencialidade, autenticidade e privacidade das informações produzidas ou custodiadas pela EMBRAPII.
Art. 3° As diretrizes de Segurança da Informação e Privacidade - SIP devem considerar, prioritariamente, objetivos estratégicos, processos, requisitos legais e estrutura da EMBRAPII.
Art. 4° A Gestão de Segurança da Informação e Privacidade - GSIP deve apoiar e orientar a tomada de decisões institucionais e otimizar investimentos em segurança que visem à eficiência, eficácia e efetividade das atividades de SIP.
Art. 5º A Política de Segurança da Informação e Privacidade – PoSIP da EMBRAPII é guiada pelos princípios da legalidade, segurança, publicidade, privacidade e ética, seguindo os princípios constitucionais, administrativos e das demais normas vigentes que regem a Administração Pública Federal.

Seção II
Da abrangência

Art. 6° As diretrizes, normas complementares e manuais de procedimentos da PoSIP da EMBRAPII aplicam-se a colaboradores, Unidades, parceiros, prestadores de serviço e a quem, de alguma forma, execute atividades vinculadas a EMBRAPII.
Parágrafo único. Todos são responsáveis e devem estar comprometidos com a segurança da informação e privacidade.
Art. 7º Os contratos, convênios, acordos, termos e outros instrumentos congêneres celebrados pela EMBRAPII devem atender a esta PoSIP.
Parágrafo único. Se houver conflito entre normas, o Comitê de Segurança da Informação e Privacidade – COSIP deliberará sobre o tema.

CAPÍTULO II
CONCEITOS E DEFINIÇÕES

Art. 8º Os termos e definições da PoSIP estão definidos em Glossário, anexo a este documento.
Parágrafo único. Os termos e definições deverão ser utilizados, no âmbito desta PoSIP, em todos as normas, procedimentos, documentos, atividades, correspondências e manuais a serem elaborados com o objetivo de manter o entendimento único e guardar relacionamento e integração com a PoSIP.

CAPÍTULO III
DIRETRIZES
Seção I
Das Diretrizes Gerais

Art. 9º O cumprimento desta política de segurança e privacidade e suas normas complementares deverá ser avaliado periodicamente por meio de verificações de conformidade, realizadas por grupo de trabalho formalmente constituído pelo Comitê de Segurança da Informação e Privacidade – COSIP, buscando a certificação do cumprimento dos requisitos de segurança da informação e privacidade;
Art. 10º As áreas e unidades da EMBRAPII devem adotar ou utilizar esta PoSIP e suas normas complementares como modelos de referência para elaboração dos seus documentos.

Seção II
Das Diretrizes Específicas

Art. 11º O Comitê de Segurança da Informação e Privacidade – COSIP estabelecerá normas e procedimentos destinados a disciplinar e proteger o uso da informação no âmbito da EMBRAPII, complementando os controles de Gestão de SIP contidos na PoSIP, sobre os temas julgados relevantes para a atuação da EMPRAPII, tais como:

I. arquivamento de documentos convertidos para o formato digital;
II. arquivamento de documentos em formato físico;
III. ativos de infraestrutura;
IV. contratação, permanência e desligamento de pessoas;
V. controle de acesso físico;
VI. controle de acesso lógico;
VII. correio eletrônico;
VIII. descarte de mídias;
IX. dispositivos móveis pessoais e da EMBRAPII;
X. gestão de riscos de informação;
XI. impressão;
XII. privacidade de proteção de dados pessoais;
XIII. redes sociais;
XIV. segurança física e de ambiente;
XV. serviços de conectividade e acessos à internet;
XVI. uso de computadores.

CAPÍTULO IV
DAS RESPONSABILIDADES

Art. 12º A estrutura de Gestão de Segurança da Informação e Privacidade – GSIP é composta de:

I. Comitê de Segurança da Informação e Privacidade – COSIP;
II. Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais e Privacidade – ETIRP.
III. Gestor de Segurança da Informação e Privacidade – SIP;

Art. 13º Os membros da estrutura de GSIP devem receber regularmente capacitação nas disciplinas relacionadas à Segurança da Informação e Privacidade.

Art. 14º A Estrutura de GSIP deve auxiliar a alta administração na priorização de ações e investimentos com vistas à correta aplicação de mecanismos de proteção, tendo como base as exigências estratégicas e necessidades operacionais da EMBRAPII e as consequências que os riscos poderão trazer ao cumprimento dessas exigências.

Art. 15º. Cabe ao COSIP:

I. aprovar o plano de investimentos em SIP da EMBRAPII;
II. avaliar, revisar e analisar criticamente a PoSIP e suas normas complementares, visando a sua aderência aos objetivos institucionais da EMBRAPII e às legislações vigentes;
III. constituir grupo de trabalho para realizar verificações de conformidade;
IV. constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre SIP;
V. dirimir eventuais dúvidas e deliberar sobre assuntos relativos à PoSIP da EMBRAPII;
VI. monitorar e avaliar periodicamente o plano de SIP de que trata o item I deste artigo, assim como determinar os ajustes cabíveis;
VII. normatizar e supervisionar a SIP no âmbito da EMBRAPII;
VIII. propor alterações na PoSIP;
IX. propor e manter atualizado o seu Regimento Interno; e
X. solicitar apurações quando da suspeita de ocorrências de quebras de SIP.

Parágrafo único. É de competência privativa do COSIP propor normas e procedimentos complementares a esta PoSIP ao Sr. Diretor-presidente da EMBRAPII.

Art. 16º Cabe ao Gestor de SIP:

I. acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;
II. coordenar o COSIP e a ETIRP;
III. promover cultura de segurança da informação e privacidade;
IV. propor ao COSIP, sempre que necessário, alterações na PoSIP e nas normas vigentes;
V. propor normas relativas à SIP;
VI. propor recursos necessários às ações de SIP;
VII. propor, anualmente ao COSIP revisões na PoSIP e normas vigentes; e
VIII. realizar e acompanhar estudos de novas tecnologias, quanto a possíveis impactos na SIP.

Art. 17º Cabe ao ETIRP:

I. avaliar, selecionar, administrar e monitorar controles apropriados de proteção dos ativos de informação;
II. cooperar com outras equipes de Tratamento e Resposta a Incidentes;
III. disponibilizar, de forma imediata e segura, condições para o restabelecimento dos serviços de infraestrutura de informações, privacidade e comunicações da EMBRAPII;
IV. emitir alertas sobre vulnerabilidades e outras notificações relacionadas à SIP no âmbito da EMBRAPII;
V. executar as atividades de tratamento e resposta a incidentes de segurança da informação, junto as equipes envolvidas; e
VI. obter informações quantitativas acerca dos incidentes ocorridos que descrevam sua natureza, causas, data de ocorrência, frequência e custos resultantes.

Parágrafo único. As atividades específicas da ETIRP serão definidas em Regimento Interno.

Art. 18º As atividades do ETIRP poderão, à critério da administração, ser terceirizadas sob supervisão do Gestor de SIP.

Art. 19º É dever de colaboradores, Unidades, parceiros, prestadores de serviço e a quem, de alguma forma, execute atividades vinculadas a EMBRAPII:

I. comunicar os incidentes que afetam a segurança dos ativos de informação à ETIRP;
II. conhecer e cumprir os princípios, diretrizes e responsabilidades desta PoSIP e demais normas e resoluções relacionados à SIC; e
III. obedecer aos requisitos de controle especificados pelos gestores e custodiantes da informação.

Art. 20º O não cumprimento das regras desta PoSIP, normas e procedimentos complementares implicará em medida disciplinar, na forma dos regulamentos internos da EMBRAPII.

CAPÍTULO V
DAS DISPOSIÇÕES FINAIS

Art. 21º A PoSIP e seus anexos, normas e procedimentos complementares da EMBRAPII deverão ser revisados sempre que se fizer necessário, não excedendo o prazo máximo de dois anos.

Art.º 22º O COSIP e o ETIRP serão instituídos por meio de regimento interno.

Art.º 23º A PoSIP, normas e procedimentos deverão observar o prazo de adequação à Lei Geral de Proteção de Dados – LGPD conforme legislação vigente.

Art. 24º Esta PoSIP entra em vigor a partir da data de sua publicação.

MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÕES - MCTI
EMPRESA BRASILEIRA DE PESQUISA E INOVAÇÃO INDUSTRIAL - EMBRAPII
POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE - PoSIP

ANEXO I

Glossário de Termos da PoSIP

No âmbito da PoSIP, normas, procedimentos, atividades, correspondências e manuais a serem elaborados, é recomendada a aplicação do glossário a seguir:

1. Ativos de informação: os meios de produção, armazenamento, transmissão e processamento de informações, os sistemas de informação, além das informações em si, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;
2. Autenticidade: propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade;
3. Comitê de Segurança da Informação e Privacidade – COSIP: colegiado de caráter deliberativo responsável pela normatização e supervisão da segurança da informação e privacidade no âmbito da EMBRAPII;
4. Confidencialidade: propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade autorizados;
5. Controle de acesso: conjunto de normas, procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso;
6. Custodiante da informação: é aquele que, de alguma forma, zela pelo armazenamento, operação, administração e preservação de ativos de informação que lhe pertencem ou não, mas que estão sob sua custódia;
7. Dados pessoais: informações relacionadas a pessoa natural identificada ou identificável;
8. Disponibilidade: propriedade de que a informação esteja acessível e utilizável, sob demanda, por uma pessoa física ou determinado sistema, órgão ou entidade;
9. Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais e Privacidade - ETIRP: colegiado com a responsabilidade de receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança e privacidade em redes de computadores no âmbito da EMBRAPII;
10. Estrutura de GSIP: conjunto das equipes responsáveis pela gestão e execução da política de segurança da informação e privacidade - PoSIP;
11. Gestão da Segurança da Informação e Privacidade - GSIP: ações e métodos que visam à integração das atividades de gestão de riscos, gestão da privacidade, gestão de continuidade do negócio, tratamento de incidentes de SIP, tratamento da informação e privacidade, conformidade, credenciamento, segurança cibernética, segurança física, segurança lógica, segurança orgânica e segurança organizacional aos processos institucionais estratégicos, operacionais e táticos, não se limitando, portanto, ao âmbito da tecnologia da informação e privacidade;
12. Gestor de SIP: colaborador nomeado pela diretoria colegiada como responsável pela gestão de segurança da informação e privacidade no âmbito da EMBRAPII;
13. Incidente de SIP: evento que tenha causado algum dano, colocado em risco algum ativo de informação crítico ou interrompido a execução de alguma atividade crítica por um período inferior ao tempo objetivo de recuperação;
14. Informação: conjunto de dados, textos, imagens, métodos, sistemas ou quaisquer formas de representação dotadas de significado em determinado contexto, independentemente do suporte em que resida ou da forma pela qual seja veiculado;

15. Integridade: propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;
16. Quebra de segurança: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e das comunicações;
17. Segurança física e do ambiente: processo que trata da proteção de todos os ativos físicos da instituição, englobando instalações físicas, internas e externas, em todas as localidades em que a organização está presente;
18. SIP: segurança da informação e privacidade
19. Tratamento de incidentes: é a atividade de receber, filtrar, classificar e responder às solicitações e alertas e realizar as análises dos incidentes de segurança e privacidade; e
20. Vulnerabilidade: fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças.