DELIBERAÇÃO

GR-018/2025

Data Início:

Data Fim:

CÓDIGO DE CLASSIFICAÇÃO ARQUIVÍSTICA: 010.01 **CLASSIFICAÇÃO DA INFORMAÇÃO:** Ostensivo

TÍTULO: **POLÍTICA CORPORATIVA DE SEGURANÇA DA INFORMAÇÃO**

PALAVRAS – CHAVE: segurança da informação, segurança cibernética, PCSI, PSS

ANEXO:

1 – Política Corporativa de Segurança da Informação

PROCESSO: 12.09 – Gerenciar Segurança da Informação

O CONSELHO DE ADMINISTRAÇÃO DO SERVIÇO FEDERAL DE PROCESSAMENTO DE DADOS – SERPRO, no uso das competências que lhe atribui o art. 19, inciso II, do Estatuto Social do SERPRO,

DELIBERA

1.0 Alterar a Política Corporativa de Segurança da Informação – PCSI, constante do Anexo 1 desta Deliberação, com o objetivo de fornecer o direcionamento estratégico da segurança da informação para o Serpro.

2.0 Este documento substituirá a Deliberação GR-015/2023 de 17 de agosto de 2023.

NEOSIGNER Assinatura ICP-Brasil
FERNANDO FERREIRA
CPF: 553.***.***-04
28/08/2025
Serpro

FERNANDO FERREIRA
Presidente do Conselho de Administração

NEOSIGNER Assinatura ICP-Brasil
DANIEL DE SABOIA XAVIER
CPF: 051.***.***-55
29/08/2025
Serpro

DANIEL DE SABOIA XAVIER
Conselheiro

NEOSIGNER Assinatura ICP-Brasil
RENAN PINHEIRO DO EGYPTO GUERRA
CPF: 041.***.***-29
27/08/2025
Serpro

RENAN PINHEIRO DO EGYPTO GUERRA
Conselheiro Representante dos Empregados

NEOSIGNER Assinatura ICP-Brasil
ROGERIO SOUZA MASCARENHAS
CPF: 865.***.***-72
27/08/2025
Serpro

ROGÉRIO SOUZA MASCARENHAS
Conselheiro

NEOSIGNER Assinatura ICP-Brasil
IVAN TIAGO MACHADO OLIVEIRA
CPF: 013.***.***-06
27/08/2025
Serpro

IVAN TIAGO MACHADO OLIVEIRA
Conselheiro

NEOSIGNER Assinatura ICP-Brasil
LEONARDO ANDRE PAIXAO
CPF: 125.***.***-80
29/08/2025
Serpro

LEONARDO ANDRÉ PAIXÃO
Conselheiro Independente

ÓRGÃO/REDATOR: DIOPE/SUPSI/SIGSC/SIRSC/rp

1.0 OBJETIVO

Estabelecer o direcionamento estratégico, as responsabilidades e as competências para a gestão da segurança da informação e segurança cibernética.

2.0 ÂMBITO DE APLICAÇÃO

Todos os órgãos da Empresa.

3.0 DEFINIÇÕES

Para efeito desta Política, entende-se por:

a) Ativos de Informação: meios de armazenamento, transmissão e processamento da informação, equipamentos necessários a isso, sistemas utilizados para tal, locais onde se encontram esses meios, recursos humanos que a eles têm acesso e conhecimento ou dado que tem valor para um indivíduo ou organização;

b) Autenticidade: propriedade pela qual se assegura que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, equipamento, sistema, órgão ou entidade;

c) Confidencialidade: propriedade pela qual se assegura que a informação não esteja disponível ou não seja revelada à pessoa, ao sistema, ao órgão ou à entidade não autorizados nem credenciados;

d) Dado Pessoal: informação relacionada à pessoa natural identificada ou identificável;

e) Disponibilidade: propriedade pela qual se assegura que a informação esteja acessível e utilizável, sob demanda, por uma pessoa física ou determinado sistema, órgão ou entidade devidamente autorizados;

f) Integridade: propriedade pela qual se assegura que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

g) Fraude Cibernética: é uma fraude caracterizada como intencional, que envolve a exploração de meios de comunicação, meios digitais, processos e/ou pessoas com objetivo de ludibriar vítimas ou organizações, a fim de obter informações, ganhos financeiros, vantagem competitiva, privilégios ou favorecimento;

h) Gestão de Riscos de Segurança da Informação: processo de natureza permanente, estabelecido, direcionado e monitorado pela alta administração, que contempla as atividades de identificação, avaliação e gerenciamento de potenciais eventos que possam afetar a organização, destinado a fornecer segurança razoável quanto à realização de seus objetivos;

i) Gestão de Segurança da Informação: processo que visa integrar atividades de gestão de riscos, gestão de continuidade do negócio, tratamento de incidentes, tratamento da informação, conformidade, credenciamento, segurança cibernética, segurança física, segurança lógica, segurança orgânica e organizacional, aos processos institucionais estratégicos, operacionais e táticos, não se limitando, portanto, à

tecnologia da informação;

j) Log: registro de eventos relevantes em um dispositivo ou sistema computacional;

k) Necessidade de Conhecer: condição segundo a qual o conhecimento da informação classificada é indispensável para o adequado exercício de cargo, função, emprego ou atividade. O termo "necessidade de conhecer" descreve a restrição de dados que sejam considerados extremamente sigilosos. Sob restrições do tipo "necessidade de conhecer", mesmo que um indivíduo tenha as credenciais necessárias para acessar uma determinada informação, ele só terá acesso a essa informação caso ela seja estritamente necessária para a condução de suas atividades oficiais;

l) Privilégio Mínimo: permissão de acesso limitada apenas aos recursos ou sistemas necessários para a condução de tarefas específicas em conformidade com a necessidade de conhecer;

m) Resiliência Organizacional: é a capacidade de uma organização antecipar, preparar, responder e adaptar-se a mudanças incrementais e interrupções súbitas para sobreviver e prosperar;

n) Segregação de Funções: a segregação de funções refere-se à prática em que o conhecimento e/ou privilégios necessários para completar um processo são divididos entre vários usuários, de modo que nenhum deles seja capaz de executá-lo ou controlá-lo sozinho;

o) Segurança Cibernética: ações voltadas para a segurança de operações, visando garantir que os sistemas de informação sejam capazes de resistir a eventos no espaço cibernético, capazes de comprometer a disponibilidade, a integridade, a confidencialidade e a autenticidade dos dados armazenados, processados ou transmitidos e dos serviços que esses sistemas ofereçam ou tornem acessíveis; e

p) Segurança da Informação: ações que visam viabilizar e assegurar a confidencialidade, integridade, disponibilidade e autenticidade das informações.

4.0 PREMISSAS

4.1 A segurança da informação abrange processos, procedimentos, serviços e ações que visam assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade dos dados e das informações, do Serpro ou sob sua guarda, incluindo a segurança cibernética, contemplando ações voltadas para a segurança de operações, bem como a proteção de dados pessoais.

4.2 A segurança da informação adota os seguintes princípios:

a) privilégios mínimos;

b) necessidade de conhecer / necessidade de trabalho; e

c) segregação de funções.

4.3 A segurança da informação está alinhada ao planejamento estratégico do Serpro, visando fomentar e viabilizar novos negócios e a evolução tecnológica de soluções íntegras e confiáveis.

4.4 A segurança da informação garante condições para que os empregados sejam orientados sobre a existência e a utilização dos instrumentos normativos, procedimentos e controles de segurança adotados pela empresa.

4.5 A segurança da informação assegura a adequação e a evolução das soluções de segurança para atender as necessidades dos clientes, os requisitos do negócio, legais e contratuais, assim como a inovação em soluções digitais.

4.6 A segurança da informação e segurança cibernética adota princípios, aspectos e requisitos, a fim de assegurar a estratégia de antifraude cibernética.

5.0 DETERMINAÇÕES

5.1 Os dados, informações e ativos de informação do Serpro, ou sob sua guarda, de acordo com natureza, classificação, sensibilidade e exposição a riscos de segurança da informação, devem ser protegidos de forma a garantir a confidencialidade, a integridade, a disponibilidade e a autenticidade, em alinhamento com as necessidades do negócio, requisitos legais, regulamentares, estatutários e contratuais.

5.2 A organização da segurança da informação deve ser estabelecida, implementada, mantida e melhorada em ciclos contínuos, por meio dos processos e ações coordenadas de governança e gestão, visando atender as necessidades do Serpro.

5.3 Os dados, as informações e os ativos de informação do Serpro ou sob sua guarda devem receber o mesmo nível de proteção, independente do meio em que estejam sendo tratados.

5.4 As instalações do Serpro devem ser protegidas contra acessos não autorizados, danos e interferência nos recursos de tratamento de dados.

5.5 Equipamentos, materiais e documentos do Serpro ou sob sua guarda devem estar protegidos contra perda, danos, roubo ou comprometimento, bem como a interrupção das operações, tanto em trabalho remoto ou em trânsito.

5.6 O Serpro deve assegurar processos eficientes para gerir o ciclo de vida dos registros de eventos (logs) em ativos de informação, garantindo o adequado tratamento e monitoramento, em conformidade com os requisitos de segurança e proteção dos dados, a fim de prover a rastreabilidade.

5.7 A monitoração da segurança deve ser realizada de forma permanente e proativa para identificar eventos adversos e fraudes cibernéticas.

5.7.1 Os desvios e as falhas de segurança identificados não devem ser explorados ou utilizados indevidamente e devem ser reportados às áreas responsáveis.

5.7.2 As violações de segurança devem ser registradas, e as evidências devem ser protegidas de forma adequada, visando subsidiar o tratamento de incidentes, prevenção e combate à fraude cibernética, e a análise forense computacional, e suprir as necessidades de comunicação sobre fragilidades e eventos de segurança da informação.

5.8 Os ativos de informação relevantes devem ser identificados e protegidos. Cabe a cada empregado atender as necessidades de proteção e observar as regras para uso seguro e

apropriado.

5.9 O uso de dados, informações e recursos operacionais e de comunicações do Serpro deve estar em consonância com esta política e com as normas e padrões da Empresa.

5.10 O acesso a dados, informações e aos recursos de processamento do Serpro ou sob sua guarda devem ser limitados e garantidos apenas aos acessos autorizados, observando os princípios de necessidade de conhecer e privilégio mínimo. Os empregados são responsáveis pelo cumprimento das regras de uso e proteção.

5.10.1 Informações e processos de negócios de Clientes devem ser tratados de acordo com os requisitos de segurança e proteção dos dados estabelecidos em contrato.

5.11 A gestão de riscos de segurança da informação do Serpro deve ser um processo contínuo e parte das atividades de gestão de segurança da informação.

5.11.1 A gestão de riscos de segurança da informação deve resultar na identificação de requisitos de segurança da informação e na seleção de controles de segurança, com o objetivo de redução do risco ao nível aceitável.

5.12 O Serpro deve adotar procedimentos para evitar a violação de quaisquer obrigações legais, estatutárias, regulamentares ou contratuais relacionadas à segurança da informação e de quaisquer requisitos de segurança considerados necessários.

5.12.1 A análise crítica da segurança da informação deve ser realizada para assegurar sua implementação em conformidade com as políticas e procedimentos corporativos.

5.13 A cultura de segurança da informação deve ser permanentemente fortalecida com objetivo de proteger os interesses do Serpro e dos seus clientes, considerando os aspectos de educação, treinamento e conscientização de forma a assegurar que empregados e partes externas cumpram suas obrigações e responsabilidades, relacionadas à segurança da informação.

5.14 A segurança da informação e a privacidade devem estar contempladas em todas as etapas do ciclo de vida das soluções digitais.

5.15 Os empregados do Serpro e partes externas são obrigados a guardar sigilo quanto aos dados, informações e ativos de informação que tiverem acesso, por força de suas atividades, em conformidade com sua classificação, termos de confidencialidade e/ou sigilo, contratos e demais legislações aplicáveis.

5.16 O Serpro deve garantir a proteção dos ativos da organização acessados pelos fornecedores, estabelecidos em contratos, em consonância aos requisitos de segurança da informação e proteção dos dados, e o tratamento dos riscos associados à cadeia de suprimentos de produtos e serviços de tecnologia da informação e comunicação.

5.17 A resiliência organizacional do Serpro deve contemplar a continuidade do negócio, de forma a assegurar a disponibilidade dos recursos, responder efetivamente e salvaguardar os interesses das partes interessadas, a reputação, a marca da organização, bem como assegurar o atendimento das necessidades dos clientes, expressos em contratos e aplicados na prestação de serviços e produtos.

5.18 A adoção e a construção de tecnologias de Inteligência Artificial devem contemplar o

gerenciamento de riscos de segurança da informação, segurança cibernética e de proteção de dados pessoais.

5.19 O Serpro deve garantir que funções conflitantes e áreas de responsabilidade pelas suas ações e decisões sejam segregadas, a fim de mitigar riscos de fraude, erros e/ou desvios em medidas e processos relativos à segurança da informação e cibernética.

6.0 RESPONSÁVEIS

6.1 O Comitê Estratégico de Governança de TI – COGTI é o órgão colegiado de pronúncia, atualização e proteção desta Política.

6.2 A Superintendência de Segurança da Informação – SUPSI é responsável pela divulgação, gestão e pela supervisão da implementação da PCSI.

6.3 A Superintendência de Segurança da Informação – SUPSI é responsável por coordenar os aspectos de segurança nos processos de mapeamento de ativos de informação e gestão de mudanças, assim como a integração com os processos de gestão de segurança da informação e gestão de continuidade de negócios.

6.4 As Unidades são responsáveis pela implementação da PCSI no seu respectivo segmento de atuação, de acordo com o modelo de gestão e o processo de segurança da informação adotado.

7.0 DISPOSIÇÕES FINAIS

7.1 A presente Política Corporativa de Segurança da Informação – PCSI alinha-se institucionalmente à Política Serpro de Privacidade e Proteção de Dados – PPPD e à Política de Governança de Dados.

7.2 A contratação de serviços deve considerar os critérios de segurança da informação e de segurança cibernética definidas nesta PCSI.

7.3 A PCSI deve ser de conhecimento dos empregados, dos terceirizados e das empresas prestadoras de serviço.

7.4 O Programa de Segurança do Serpro – PSS contempla o modelo de governança e de gestão da segurança da informação e tem como objetivo atender as orientações da PCSI.

7.5 A PCSI deve ser revisada a cada dois anos ou nas situações que representem alterações significativas nos processos ou estrutura do Serpro.

7.6 A não observância da PCSI e seus desdobramentos normativos implicará a aplicação das sanções previstas nas normas disciplinares do Serpro.