Política de Segurança da Informação

Pré-Sal Petróleo S.A. (PPSA)

Sumário

1. Introdução

A Pré-Sal Petróleo S.A. – PPSA (“PPSA”) é uma empresa pública vinculada ao Ministério de Minas e Energia (“MME”), cuja criação foi autorizada pela Lei nº 12.304/2010, de 2 de agosto de 2010 e com a publicação do Decreto nº 8.063/2013, em 1º de agosto de 2013.

A PPSA tem por objetivo a gestão dos contratos de Partilha de Produção celebrados pelo MME e de comercialização de Petróleo, de Gás Natural e de outros hidrocarbonetos fluidos da União. Ademais, incumbe à estatal representar a União nos procedimentos de Individualização da Produção e nos acordos deles decorrentes, quando as Jazidas Compartilhadas se estendam para Áreas não Contratadas no interior do polígono do pré-sal, assim como nos Acordos de Coparticipação envolvendo os Volumes Excedentes da Cessão Onerosa.

A atuação da PPSA pauta-se pela qualidade na prestação dos seus serviços e pela transparência. Para isso, investe constantemente na capacitação de seus Colaboradores, e também em tecnologias que garantam a inovação dos seus serviços e proteção das Informações necessárias ao desenvolvimento do negócio.

A Informação manipulada de maneira indevida ou compartilhada em ambientes sem autorização pode gerar danos irreparáveis à PPSA, além de afetar a sua imagem perante ao mercado. Desse modo, a preservação de seus Ativos como a Informação, o banco de dados e a reputação, por meio da adoção de um Sistema de Gestão de Segurança da Informação (“SGSI”) é essencial para a proteção e o crescimento da PPSA.

O primeiro passo do SGSI foi a implementação desta Política de Segurança da Informação (“PSI”), ora revisada, documento que trouxe a combinação de requisitos do negócio, de estrutura de processos e do uso de tecnologias e, o mais relevante, do comportamento dos Colaboradores, independentemente do nível hierárquico ou da atividade desenvolvida.

Sendo assim, a PPSA estabelece neste documento a sua PSI, pautada nas legislações e regulamentações nacionais e nos princípios da ética e da transparência.

2. Objetivo e Alcance

2.1. Esta PSI tem como objetivos:

Declarar formalmente o comprometimento da alta administração da PPSA na promoção de diretrizes estratégicas, responsabilidades, competências e apoio ao SGSI, a fim de garantir a proteção dos seus Ativos tangíveis e intangíveis;

Viabilizar e assegurar a Confidencialidade, Integridade, Disponibilidade, Autenticidade e Legalidade da Informação;

Estabelecer as responsabilidades e os limites de atuação dos Colaboradores da PPSA em relação à Segurança da Informação, reforçando a cultura interna e priorizando as ações necessárias conforme o negócio.

2.2. Esta PSI é um documento interno, com valor jurídico e aplicação imediata indistintamente a todos os Colaboradores da PPSA.

3. Referências Legais e Normativas

3.1. Constituição Federal de 1988, em especial o artigo 5º, incisos IV, V, X, XII, XIV;

3.2. Lei nº 10.406/2002, de 10 de janeiro de 2002, Código Civil, em seus artigos 186, 187, 538, 927, 932, 933 e 1016;

3.3. Decreto-lei nº 2.848/1940, de 7 de dezembro de 1940, Código Penal, artigos 138, 139, 140, 151, 152, 154-A, 184, 297, 299, 305, 307, 308 e 325;

3.4. Decreto-lei nº 3.689, de 3 de outubro de 1941, Código de Processo Penal, artigos 231, 232 e 233;

3.5. Lei nº 12.304/2010, de 2 de agosto de 2010 – Autoriza o Poder Executivo a criar a empresa pública denominada Empresa Brasileira de Administração de Petróleo e Gás Natural S.A. – Pré-Sal Petróleo S.A. (PPSA) e dá outras providências;

3.6. Decreto nº 8.063/2013, de 1º de agosto de 2013 - Cria a empresa pública denominada Empresa Brasileira de Administração de Petróleo e Gás Natural S.A. - Pré-Sal Petróleo S.A. - PPSA, aprova o seu Estatuto Social, e dá outras providências;

3.7. Lei nº 9.279/1996, de 14 de maio de 1996 - Lei de Propriedade Industrial (Marcas e Patentes);

3.8. Lei nº 7.232/1984, de 29 de outubro de 1984 - Dispõe sobre a Política Nacional de Informática, e dá outras providências;

3.9. Lei nº 8.027/1990, de 12 de abril de 1990 - Dispõe sobre normas de conduta dos servidores públicos civis da União, das Autarquias e das Fundações Públicas, e dá outras providências;

3.10. Lei nº 13.303, de 30 de junho de 2016;

3.11. Lei nº 9.296/1996, de 24 de julho de 1996 - Lei de Interceptação;

3.12. Lei nº 9.609/1998, de 19 de fevereiro de 1998 - Lei de Software - Dispõe sobre a proteção da propriedade intelectual de programa de computador, sua comercialização no País, e dá outras providências;

3.13. Lei nº 9.610/1998, de 19 de fevereiro de 1998 - Lei de Direitos Autorais;

3.14. Leis nº 12.735/2012 e 12.737/2012, ambas de 30 de novembro de 2012, Leis de Delitos Informáticos;

3.15. Lei nº 12.846/2013, de 1º de agosto de 2013 - Lei Anticorrupção;

3.16. Decreto nº 11.129, de 11 de julho de 2022 – Regulamenta a Lei nº 12.846, de 1º de agosto de 2013, que dispõe sobre a responsabilização administrativa e civil de pessoas jurídicas pela prática de atos contra a administração pública, nacional ou estrangeira;

3.17. Portaria CGU nº 909, de 7 de abril de 2015 - Dispõe sobre a avaliação de programas de integridade de pessoas jurídicas;

3.18. Portaria CGU nº 910, de 7 de abril de 2015 - Define os procedimentos para apuração da responsabilidade administrativa e para celebração do acordo de leniência de que trata a Lei nº 12.846, de 1º de agosto de 2013;

3.19. Instrução CGU Normativa nº 1, de 7 de abril de 2015 - Estabelece metodologia para a apuração do faturamento bruto e dos tributos a serem excluídos para fins de cálculo da multa a que se refere o art. 6º da Lei nº 12.846, de 1º de agosto de 2013;

3.20. Instrução CGU Normativa nº 2, de 7 de abril de 2015 - Regula o registro de informações no Cadastro Nacional de Empresas Inidôneas e Suspensas – CEIS e no Cadastro Nacional de Empresas Punidas – CNEP;

3.21. Instrução Normativa CGU nº 4, de 11 de setembro de 2014 - Dispõe sobre o processo de contratação de Soluções de Tecnologia da Informação pelos órgãos integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal;

3.22. Decreto nº 1.171/1994, de 22 de junho de 1994 - Código de Ética do Servidor Público;

3.23. Lei nº 12.850/2013, de 2 de agosto de 2013 - Lei de Provas Eletrônicas - Define organização criminosa e dispõe sobre a investigação criminal, os meios de obtenção da prova, infrações penais correlatas e o procedimento criminal; altera o Decreto-Lei nº 2.848/1940, de 7 de dezembro de 1940 (Código Penal); revoga a Lei nº 9.034, de 3 de maio de 1995; e dá outras providências;

3.24. Lei nº 12.965/2014, de 23 de abril de 2014 – Marco Civil da Internet;

3.25. Lei nº 13.709/2018, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais (LGPD);

3.26. Decreto nº 9.637, de 26 de dezembro de 2018 - Institui a Política Nacional de Segurança da Informação;

3.27. Lei nº 12.527/2011, de 18 de novembro de 2011 – Lei de Acesso à Informação;

3.28. Decreto nº 7.724/2012, de 16 de maio de 2012 - Regulamenta a Lei nº 12.527/2011, de 18 de novembro de 2011, que dispõe sobre o acesso a informações previsto no inciso XXXIII do *caput* do art. 5º, no inciso II do §3º do art. 37 e no §2º do art. 216 da Constituição;

3.29. Decreto nº 7.845/2012, de 14 de novembro de 2012 - Regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento;

3.30. Portaria GSI/PR nº 93, de 26 de setembro de 2019 - Glossário de Segurança da Informação;

3.31. Instrução Normativa Nº 1, de 27 de maio de 2020 do GSI que dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal;

3.32. Norma Complementar nº 04/IN01/DSIC/GSIPR, de 25 de fevereiro de 2013 - Diretrizes para o processo de Gestão de Riscos de Segurança da Informação e Comunicações - GRSIC nos órgãos e entidades da Administração Pública Federal;

3.33. Norma Complementar nº 05/IN01/DSIC/GSIPR, de 17 de agosto de 2009 - Disciplina a criação de Equipes de Tratamento e Respostas a Incidentes em Redes Computacionais - ETIR nos órgãos e entidades da Administração Pública Federal;

3.34. Norma Complementar nº 06/IN01/DSIC/GSIPR, de 23 de novembro de 2009 - Estabelece Diretrizes para Gestão de Continuidade de Negócios, nos aspectos relacionados à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF;

3.35. Norma Complementar nº 07/IN01/DSIC/GSIPR, de 16 de julho de 2014 - Estabelece as Diretrizes para Implementação de Controles de Acesso Relativos à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta;

3.36. Norma Complementar nº 08/IN01/DSIC/GSIPR, de 24 de agosto de 2010 - Estabelece as Diretrizes para Gerenciamento de Incidentes em Redes Computacionais nos órgãos e entidades da Administração Pública Federal;

3.37. Norma Complementar nº 09/IN01/DSIC/GSIPR, de 16 de julho de 2014 - Estabelece orientações específicas para o uso de recursos criptográficos em Segurança da Informação e Comunicações, nos órgãos ou entidades da Administração Pública Federal (APF), direta e indireta;

3.38. Norma Complementar nº 10/IN01/DSIC/GSIPR, de 10 de fevereiro de 2012 - Estabelece diretrizes para o processo de Inventário e Mapeamento de Ativos de Informação, para apoiar a Segurança da Informação e Comunicações (SIC), dos órgãos e entidades da Administração Pública Federal, direta e indireta – APF;

3.39. Norma Complementar nº 11/IN01/DSIC/GSIPR, de 10 de fevereiro de 2012 - Estabelece diretrizes para avaliação de conformidade nos aspectos relativos à Segurança da Informação e Comunicações (SIC) nos órgãos ou entidades da Administração Pública Federal, direta e indireta – APF;

3.40. Norma Complementar nº 12/IN01/DSIC/GSIPR, de 10 de fevereiro de 2012 - Estabelece diretrizes e orientações básicas para o uso de dispositivos móveis nos aspectos referentes à Segurança da Informação e Comunicações (SIC) nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta;

3.41. Norma Complementar nº 13/IN01/DSIC/GSIPR, de 10 de fevereiro de 2012 - Estabelece diretrizes para a Gestão de Mudanças nos aspectos relativos à Segurança da Informação e Comunicações (SIC) nos órgãos e entidades da Administração Pública Federal, direta e indireta (APF);

3.42. Norma Complementar nº 15/IN01/DSIC/GSIPR, de 21 de junho de 2012 - Estabelece diretrizes de Segurança da Informação e Comunicações para o uso de redes sociais, nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta;

3.43. Norma Complementar nº 16/IN01/DSIC/GSIPR, de 21 de novembro de 2012 - Estabelece as Diretrizes para o Desenvolvimento e Obtenção de Software Seguro nos Órgãos e Entidades da Administração Pública Federal, direta e indireta;

3.44. Norma Complementar nº 17/IN01/DSIC/GSIPR, de 10 de abril de 2013 - Estabelece Diretrizes nos contextos de atuação e adequações para Profissionais da Área de Segurança da Informação e Comunicações (SIC) nos Órgãos e Entidades da Administração Pública Federal (APF);

3.45. Norma Complementar nº 18/IN01/DSIC/GSIPR, de 10 de abril de 2013 - Estabelece as Diretrizes para as Atividades de Ensino em Segurança da Informação e Comunicações (SIC) nos Órgãos e Entidades da Administração Pública Federal (APF);

3.46. Norma Complementar nº 19/IN01/DSIC/GSIPR, de 16 de julho de 2014 - Estabelece Padrões Mínimos de Segurança da Informação e Comunicações para os Sistemas Estruturantes da Administração Pública Federal (APF), direta e indireta;

3.47. Norma Complementar nº 20/IN01/DSIC/GSIPR, de 15 de dezembro de 2014 - Estabelece as Diretrizes de Segurança da Informação e Comunicações para Instituição do Processo de Tratamento da Informação nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta;

3.48. Norma Complementar nº 21/IN01/DSIC/GSIPR, de 10 de outubro de 2014 - Estabelece as Diretrizes para o Registro de Eventos, Coleta e Preservação de Evidências de Incidentes de Segurança em Redes nos órgãos e entidades da Administração Pública Federal, direta e indireta;

3.49. Súmula 341 do Supremo Tribunal Federal;

3.50. Súmula 428 do Tribunal Superior do Trabalho;

3.51. Norma NBR ISO/IEC 27001:2013 – Tecnologia da Informação – Técnicas de Segurança – Sistemas de gestão da segurança da informação – Requisitos (https://www.abntcatalogo.com.br/);

3.52. Norma NBR ISO/IEC 27002:2013 – Tecnologia da Informação – Técnicas de Segurança – Código de prática para a gestão da segurança da informação (https://www.abntcatalogo.com.br/);

3.53. Norma NBR 16167 – Segurança da Informação – Diretrizes para classificação, rotulação e tratamento da informação (https://www.abntcatalogo.com.br/);

3.54. Norma ISO/IEC 27014– Tecnologia da Informação – Técnicas de Segurança – Governança de Segurança da Informação (https://www.iso.org/standards.html);

3.55. COBIT 5 – Control Objectives for Information and related Technology. ISACA, ITGI, 2012.

3.56. Procedimento de Gestão de Classificação da Informação (PG.DAFC.006/2023), documento interno PPSA.

3.57. Procedimento de Gerenciamento de Riscos (PG.PRE.001/2018), documento interno PPSA.

3.58. Política de Gestão de Riscos (PO.PRE.001/2021), documento interno PPSA.

3.59. Procedimento de Gestão de Incidente de Segurança da Informação (PG.DAFC.009/2023), documento interno PPSA.

3.60. Política de Tratamento de Dados Pessoais (PO.DAFC.001/2023), documento interno PPSA.

3.61. Uso de Ativos e Recursos da Tecnologia da Informação (PG.DAFC.011/2023), documento interno PPSA.

3.62. Procedimento de Gestão de Apuração de infração Disciplinar (PG.DAF.003/2020), documento interno PPSA.

4. Definições e Siglas

4.1. A Instrução Normativa Nº 1, de 27 de maio de 2020 do GSI que dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal estabelece que:

"Art. 6º Os órgãos e as entidades da administração pública federal deverão utilizar o Glossário de Segurança da Informação, aprovado pelo Gabinete de Segurança Institucional da Presidência da República por meio da Portaria GSI/PR nº 93, de 26 de setembro de 2019, como referência na elaboração de normativos internos afetos à segurança da informação e de trabalhos correlatos."

Neste sentido todas a siglas e definições desta política de segurança estão de acordo com a Portaria GSI/PR nº 93 de 26 de setembro de 2019.

4.2. **Ameaça** - Conjunto de fatores externos com o potencial de causar em dano para um sistema ou organização;

4.3. **Ativo –** Tudo que tenha valor para a organização, material ou não;

4.4. **Ativo Intangível –** Referem-se a bens que não possuem uma existência física, mas possuem valor econômico para PPSA. Isso inclui direitos de propriedade intelectual, marcas registradas, softwares, licenças de uso de softwares, websites, banco de dados, informações confidenciais, processos de negócios e know-how técnico.

4.5. **Autenticidade - P**ropriedade pela qual se assegura que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, equipamento, sistema, órgão ou entidade;

4.6. ***Backup*** **-** Conjunto de procedimentos que permitem salvaguardar os dados de um sistema computacional, garantindo guarda, proteção e recuperação. Tem a fidelidade ao original assegurada. Esse termo também é utilizado para identificar a mídia em que a cópia é realizada;

4.7. **Colaborador -** Todo e qualquer empregado, estagiário, servidor cedido, requisitado ou movimentado, diretor, conselheiro, membro de comitê, fornecedor, prestador de serviço terceirizado e qualquer outra pessoa que preste serviços para PPSA;

4.8. **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;

4.9. **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;

4.10. **Dispositivos Móveis - E**quipamentos portáteis, dotados de capacidade de processamento, ou dispositivos removíveis de memória para armazenamento, entre os quais se incluem, não limitando a estes: e-books, notebooks, netbooks, smartphones, tablets, pendrives, USB drives, HD externo, e cartões de memória;

4.11. **Dispositivos Removíveis de Armazenamento de Informação -** Dispositivos capazes de armazenar Informação que pode ser removida de um equipamento, possibilitando a portabilidade dos dados, como CD, DVD, pen drive e disco externo;

4.12. Identidade Digital - Representação unívoca de um indivíduo dentro do espaço cibernético;

4.13. Incidente de Segurança da Informação - Qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;

4.14. Informação - Dados, processados ou não, que podem ser utilizados para produção e para transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

4.15. Integridade - Propriedade pela qual se assegura que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

4.16. Legalidade - Garantia de que a Informação seja criada e gerenciada de acordo com as disposições do ordenamento jurídico em vigor;

4.17. Quebra de Segurança - Ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação;

4.18. Recursos de Tecnologia da Informação (Recursos de TI) - 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;

4.19. Repositórios Digitais (cyberlockers) - Plataformas de armazenamento de Informação na *internet*, por exemplo: Google Drive, OneDrive, Dropbox, iCloud, Box, SugarSync, Slideshare e Scribd, entre outros;

4.20. Segurança da Informação - É a preservação da Confidencialidade, Integridade, Disponibilidade, Legalidade e Autenticidade da Informação e da comunicação. Visa proteger a Informação dos diversos tipos de Ameaças para garantir a continuidade dos negócios;

4.21. Violação - Qualquer atividade que desrespeite as regras estabelecidas nos procedimentos de Segurança da Informação da PPSA.

5. Princípios de Segurança da Informação

5.1. Preservar e proteger a Informação da PPSA ou sob sua responsabilidade, em todo o seu ciclo de vida, contida em qualquer suporte ou formato, dos diversos tipos de Ameaça;

5.2. Prevenir e reduzir impactos gerados por Incidentes de Segurança da Informação, assegurando a Confidencialidade, Integridade, Disponibilidade, Autenticidade e Legalidade no desenvolvimento das atividades profissionais;

5.3. Cumprir a legislação brasileira e os demais instrumentos regulamentares relacionados ao negócio no que diz respeito à Segurança da Informação.

6. Diretrizes Gerais

6.1. **Interpretação:** Esta PSI e seus documentos complementares devem ser interpretados de forma restritiva, ou seja, as atividades que não estão tratadas nos procedimentos internos só devem ser realizadas após prévia e formal autorização do superior hierárquico do Colaborador.

6.2. **Publicidade:** Esta PSI e seus documentos complementares devem ser divulgados aos Colaboradores pela Gerência de Tecnologia de Informação (“GTI”), visando dar publicidade para todos que se relacionam profissionalmente com a PPSA.

6.3. **Propriedade:** As Informações geradas, acessadas, manuseadas, armazenadas ou descartadas no exercício das atividades realizadas pelos Colaboradores, bem como os demais Ativos, tangíveis e Intangíveis disponibilizados, são de propriedade ou estão sob a responsabilidade e direito de uso exclusivo da PPSA, devendo ser utilizados unicamente para fins profissionais.

6.4. **Propriedade Intelectual:** É vedado o uso das marcas, identidade visual e qualquer outro sinal distintivo, atual ou futuro da PPSA, em qualquer forma ou mídia, inclusive na *internet* e nas mídias sociais, sem a prévia e formal autorização da Assessoria Especial de Comunicação e Ouvidoria (AC).

6.5. **Classificação da Informação:** Toda a Informação de propriedade ou sob a responsabilidade da PPSA devem ser classificadas e protegidas com controles específicos em todo o seu ciclo de vida, nos termos do Procedimento de Gestão de Classificação da Informação (PG.DAFC.006/2023).

6.6. Anonimização de dados pessoais: A anonimização é a técnica de processamento de dados pessoais que remove ou modifica Informações que possam identificar uma pessoa. Essa técnica resulta em dados anonimizados, que não podem ser associados a nenhum indivíduo específico. Os sistemas na PPSA que irão receber anonimização de dados serão indicados pelo *Data Protection Officer* (DPO), seguindo-se o disposto no art. 12, da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais - LGPD), e quando houver um registro estatístico após o período estabelecido na tabela de temporalidade.

6.7. Bloqueio de dados pessoais: Previsto no art. 5º, inciso XIII, da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais - LGPD), e consiste na suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou banco de dados. Tem como finalidade a imposição de um limite temporal ou circunstancial para não ocorrência de tratamento. A solicitação de bloqueio de dados pessoais poderá ser feita pelo titular de dados, a qualquer tempo, conforme a necessidade, e poderá ser analisada pelo DPO. Em caso de solicitação de bloqueio dos dados pessoais, a PPSA nada poderá fazer qualquer tratamento com os dados, salvo mantê-los em seus bancos de dados. A restrição somente poderá ser levantada, mediante comunicação e autorização do titular de dados pessoais. Para tanto, caberá à GTI definir as ferramentas necessárias para o bloqueio de dados pessoais, sem exclusão deles de sua base de dados.

6.8. Eliminação dos dados pessoais: A eliminação dos dados pessoais está consagrada no art. 5º, inciso XIV, da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais - LGPD), e configura a exclusão completa de um dado ou conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado. A exclusão dos dados tem por finalidade o apagamento completo dos dados pessoais do titular junto ao banco de dados da PPSA, sendo que o único critério para eliminação dos dados é que o processo seja definitivo, não importando os procedimentos utilizados.

6.9. Sigilo: É vedada, a qualquer tempo, a revelação de Informação de propriedade ou sob a responsabilidade da PPSA sem a prévia e formal autorização do responsável pela Informação, excetuando-se a informação pública.

6.10. Uso dos Ativos: Os Ativos de propriedade ou sob responsabilidade da PPSA devem ser utilizados somente para fins profissionais e de acordo com as orientações dos fabricantes e da PPSA.

6.11. Uso dos recursos operacionais e de comunicações: Todo o uso dos recursos encontra-se no PG.DAFC.011/2023 - Uso de Ativos e Recursos da Tecnologia da Informação.

6.12. Recursos de Tecnologia da Informação Particulares: O uso de Recursos de Tecnologia da Informação particulares na execução de qualquer atividade profissional deve ocorrer somente após solicitação formal e fundamentada do Colaborador, autorização do superior hierárquico e aprovação da GTI.

6.13. Manutenção dos Recursos de Tecnologia da Informação: A gestão dos Recursos de Tecnologia da Informação da PPSA deve atender as recomendações dos fabricantes e desenvolvedores, sendo que qualquer necessidade de manutenção, atualização ou correção de falhas técnicas somente podem ser realizadas pela GTI**.**

6.14. Repositórios Digitais e Dispositivos Removíveis: É vedado aos Colaboradores o uso de Repositórios Digitais e dispositivos removíveis não homologados pela GTI para armazenar ou transmitir informações de propriedade ou sob a responsabilidade da PPSA.

6.15. *Softwares* de Comunicação Instantânea: É vedado aos Colaboradores a instalação ou uso de *softwares* de comunicação instantânea não homologados pela GTI nos Recursos de Tecnologia da Informação da PPSA para compartilhamento de Informações de propriedade ou sob a responsabilidade da empresa.

6.16. Mídias Sociais: A participação dos Colaboradores nas mídias sociais por meio dos Recursos de Tecnologia de Informação da PPSA é permitida e deve ser realizada com cautela e parcimônia, não afetando o rendimento e a atenção dos Colaboradores.

6.16.1. Conduta do Colaborador no Uso das Mídias Sociais: Os Colaboradores devem ser cautelosos e éticos em relação ao excesso de exposição de sua vida particular, a exemplo de rotinas, trajetos, contatos e intimidades, além do dever de preservar o sigilo profissional nas mídias sociais.

6.17. Auditoria e Conformidade: O uso dos recursos de tecnologia da informação e comunicação (TIC) disponibilizados pela PPSA é passível de monitoramento e auditoria, serão mantidos procedimentos, tais como: trilhas de auditoria, rastreamento, acompanhamento, controle e verificação de acessos para todos os sistemas corporativos e rede interna da PPSA.

6.18. Controle de Acesso: A PPSA controla o acesso físico e lógico aos seus ambientes e Informações. Desse modo, cada Colaborador deve possuir uma Identidade Digital de uso individual, intransferível e de conhecimento exclusivo.

6.18.1. Os Colaboradores são responsáveis pelo uso e sigilo de sua Identidade Digital, não sendo permitido, compartilhar, revelar, salvar, publicar ou fazer uso não autorizado de credenciais de terceiros.

6.19. Ambientes Lógicos: Os sistemas e Recursos de Tecnologia da Informação que suportam os processos e as Informações da PPSA devem ser confiáveis, íntegros, seguros e disponíveis.

6.19.1. Senhas: Os sistemas, serviços e dispositivos da PPSA devem ser configurados para que os padrões mínimos de senha forte sejam exigidos na criação, como: conter pelo menos uma letra maiúscula; conter pelo menos uma letra minúscula; conter números (0 a 9); conter símbolos, incluindo: ! @ # $ % ^ & * - _ + = [ ] { } | \ : ‘ , . ? / ` ~ “ < > ( ), contendo, no mínimo, 6 (seis) caracteres. Deve-se evitar a utilização de nomes, sobrenomes, nomes de contas de usuários e dados de membros da família, números de documentos, números de telefone, placa de carros e datas comemorativas, bem como sequência do teclado (ex.: asdfg123). Recomenda-se que as senhas sejam compostas por números aleatórios, por vários e diferentes tipos de elementos e caracteres especiais.

6.20. Ambientes Físicos: A PPSA deve estabelecer perímetros de segurança para proteção de seus Ativos tangíveis, especialmente aqueles que processam Informações críticas e sigilosas para o negócio, além de implementar controles de identificação e registro antes do acesso aos seus ambientes físicos.

6.21. Áudio, Vídeos e Fotos: É vedada qualquer atividade relacionada a gravação de áudio, vídeo ou foto dentro das dependências da PPSA por seus Colaboradores sem a prévia e formal autorização da Assessoria de Comunicação (AC).

6.22. Contratação de Pessoal, Bens e Serviços: As contratações em que ocorra o compartilhamento de Informações de propriedade ou sob a responsabilidade da PPSA ou a concessão de acesso aos seus ambientes e Recursos de Tecnologia da Informação devem ser precedidas por termos de confidencialidade e cláusulas contratuais relacionadas à Segurança da Informação.

6.23. Desenvolvimento ou Aquisição de *Software*: O desenvolvimento ou aquisição de *softwares* deve garantir os controles de Segurança da Informação e ser homologado pela GTI.

6.24. ***Backup*****:** A PPSA deve manter um processo de salvaguarda das Informações e dos dados necessários para completa recuperação dos seus sistemas, visando à continuidade do negócio em caso de falhas ou Incidentes.

6.25. Análise dos Processos e Recursos de Tecnologia da Informação: A GTI deve analisar, em intervalos regulares, seus processos e Recursos de Tecnologia da Informação, visando assegurar que estejam devidamente inventariados e com seus gestores identificados e cientes, assim como suas vulnerabilidades e Ameaças de segurança mapeadas.

6.26. Monitoramento: A PPSA monitora seus ambientes físicos e lógicos, visando à eficácia dos controles implantados, a proteção de seu patrimônio e sua reputação, possibilitando ainda a identificação de eventos ou alertas de Incidentes referente a segurança da informação.

6.26.1. Inspeção dos Recursos de Tecnologia da Informação: A GTI, sempre que considerar necessário, pode auditar ou inspecionar os Recursos de Tecnologia da Informação corporativos ou particulares dos Colaboradores que interagem com seus ambientes físicos ou lógicos ou com suas Informações, quando autorizada a entrada em suas dependências.

6.27. Gestão de Risco: A GTI deve identificar e avaliar os riscos relacionados à Segurança da Informação e adotar as melhores práticas para o seu gerenciamento, conforme disposto na Política de Gestão de Riscos (PO.PRE.001/2021) e no Procedimento de Gerenciamento de Riscos (PG.PRE.001/2018).

6.28. Gestão de Mudança: O andamento e o resultado de uma mudança, principalmente nos sistemas e na infraestrutura tecnológica da PPSA, devem preservar os controles relacionados a Disponibilidade, Integridade, sigilo e Autenticidade das Informações, e realizada somente após aprovação da GTI.

6.29. Continuidade do Negócio: Os procedimentos de Continuidade do Negócio devem ser executados em conformidade com os requisitos de Segurança da Informação da PPSA.

6.30. Investimentos: Os investimentos em Segurança da Informação na PPSA devem ser estudados pela GTI e deliberados no Comitê de Tecnologia e Segurança da Informação (CTSI), considerando a viabilidade dos investimentos (custo x benefício) e os impactos de sua aplicação à qualidade dos processos de negócio.

6.31. Comitê de Tecnologia e Segurança da Informação ("CTSI"): A PPSA deve estabelecer o CTSI, que será responsável por assessorar e gerenciar a implementação dos

controles estabelecidos pelo SGSI, analisar questões específicas ao tema e auxiliar com a melhoria constante e observância dos procedimentos de Segurança da Informação.

6.31.1. Composição do CTSI: O CTSI deve ser composto por uma equipe multidisciplinar, com atuação permanente, reunindo-se periodicamente para tratar de pautas relacionadas à Segurança da Informação.

6.32. Tratamento e Resposta a Incidentes: A GTI é responsável por tratar os Incidentes de Segurança da Informação.

6.33. Comunicação de Incidentes: A PPSA deve possuir um canal de comunicação divulgado aos seus Colaboradores para reportar possíveis casos de Incidentes de Segurança da Informação, conforme disposto no Procedimento de Gestão de Incidente de Segurança da Informação (PG.DAFC.009/2023).

6.34. Capacitação: A PPSA deve possuir um programa de conscientização em Segurança da Informação para capacitação e disseminação dessa cultura junto aos seus Colaboradores.

6.35. Alterações: As alterações desta PSI e de seus documentos complementares devem ser comunicadas aos Colaboradores.

6.36. Exceções: As exceções a essa PSI devem ser formalizadas e fundamentadas pela GTI, que pode, a qualquer tempo e por mera liberalidade, revogá-las.

6.37. Dúvidas: Qualquer dúvida relativa a esta PSI deve ser encaminhada à GTI por meio do endereço eletrônico: seginfo@ppsa.gov.br.

7. Autoridades e Competências

7.1. Conselho de Administração da PPSA

7.1.1 Analisar e aprovar esta PSI.

7.2. Diretoria Executiva da PPSA

7.2.1. Analisar e aprovar esta PSI e, posteriormente, submetê-la à deliberação do Conselho de Administração da PPSA;

7.2.2. Cumprir e fazer cumprir esta PSI e demais documentos complementares por todos os Colaboradores da PPSA.

7.3. Comitê de Tecnologia e Segurança da Informação – CTSI

7.3.1. Cumprir e fazer cumprir esta PSI e demais documentos complementares por todos os Colaboradores da PPSA;

7.3.2. Assessorar na implementação dos controles de Segurança da Informação estabelecidos na PPSA;

7.3.3. Analisar e aprovar esta PSI, e, posteriormente, submetê-la à Diretoria Executiva da PPSA;

7.3.4. Aprovar os documentos complementares a esta PSI;

7.3.5. Aprovar os investimentos em Segurança da Informação na PPSA, considerando a viabilidade e os impactos de sua aplicação à qualidade dos processos de negócio;

7.3.6. Constituir, sempre que necessário, grupos de trabalho para tratar de temas e propor soluções específicas sobre Segurança da Informação;

7.3.7. Orientar para que as atividades desempenhadas pela GTI estejam adequadas ao negócio da PPSA;

7.3.8. Instaurar, quando couber, procedimento administrativo interno, apurar a responsabilidades dos envolvidos em Violações ou Quebras de Segurança e dar andamento nas medidas que devam ser adotadas;

7.3.9. Propor procedimentos internos relativos à Segurança da Informação, em conformidade com as legislações existentes sobre o tema.

7.4. Gerência de Tecnologia de Informação – GTI

7.4.1. Cumprir e fazer cumprir esta PSI e demais documentos complementares por todos os Colaboradores da PPSA;

7.4.2. Realizar a gestão, manutenção e administração dos Recursos de Tecnologia da Informação de propriedade ou sob a responsabilidade da PPSA;

7.4.3. Promover e realizar a gestão do SGSI, garantindo a implementação de controles, modelos, padrões e recursos necessários para a proteção da Informação;

7.4.4. Promover a cultura de Segurança da Informação na PPSA;

7.4.5. Prover a Segurança da Informação e da comunicação;

7.4.6. Identificar possíveis riscos relacionados à Segurança da Informação nos Recursos de Tecnologia da Informação e reportar ao CTSI e à Assessoria de Planejamento Estratégico, responsável pelo Gerenciamento de Riscos na PPSA;

7.4.7. Garantir que todos os Recursos de Tecnologia da Informação utilizados na PPSA atendam as recomendações de seus fabricantes ou desenvolvedores;

7.4.8. Identificar e avaliar os riscos relacionados à Segurança da Informação, propondo melhorias e provendo recursos necessários às ações mitigadoras dos riscos mapeados;

7.4.9. Realizar e acompanhar estudos de tecnologias quanto a possíveis impactos sobre a Segurança da Informação;

7.4.10. Definir, analisar e priorizar ações necessárias, balanceando custo e benefício, de forma a mitigar os riscos de segurança da informação;

7.4.11. Manter contato permanente e estreito com o Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República para o trato de assuntos relativos à Segurança da Informação;

7.4.12. Realizar o registro e o monitoramento dos acessos aos ambientes lógicos da PPSA;

7.4.13. Avaliar, em conjunto com o CTSI, se os requisitos de Segurança da Informação estão presentes antes da aquisição, manutenção ou desenvolvimento de *softwares*;

7.4.14. Garantir que o andamento e o resultado de uma mudança, principalmente nos sistemas e infraestrutura tecnológica da PPSA, preservem os controles relacionados a Disponibilidade, Integridade, sigilo e Autenticidade das Informações;

7.4.15. Elaborar e manter mecanismos adequados para garantir a rápida recuperação em situações de contingência de seus sistemas e processos que envolvam os Recursos de Tecnologia da Informação da PPSA;

7.4.16. Elaborar e manter procedimentos de *Backup* para completa recuperação dos sistemas da PPSA;

7.4.17. Assegurar que os procedimentos de Continuidade de Negócios sejam executados em conformidade com os requisitos de Segurança da Informação;

7.4.18. Aplicar esta PSI e seus documentos complementares relacionados às atividades de tecnologia da informação na PPSA;

7.4.19. Promover a capacitação dos Colaboradores em Segurança de Informação, com o auxílio da Gerência de Recursos Humanos e Suporte Corporativo (“GRHSC”);

7.4.20. Analisar os documentos complementares a esta PSI;

7.4.21. Garantir a publicidade e Disponibilidade dos documentos que compõem o SGSI na PPSA;

7.4.22. Elaborar e manter atualizados os documentos que compõem o SGSI, além de submetê-los à aprovação da CTSI, da DAFC ou da Presidência;

7.4.23. Propor procedimentos internos relativos à Segurança da Informação na PPSA.

7.5. Gerência de Recursos Humanos e Suporte Corporativo – GRHSC

7.5.1. Apoiar o CTSI nas campanhas de capacitação e divulgação da Segurança da Informação;

7.5.2. Estipular controles de segurança especificamente relacionados aos processos de contratação, encerramento e modificação das atividades dos Colaboradores no que couber;

7.5.3. Disponibilizar os procedimentos da PPSA, além de custodiar e colher assinatura do "Termo de Ciência e Responsabilidade" na admissão de novos Colaboradores e, no caso dos prestadores de serviços, de acordo com o contrato de prestação de serviços.

7.6. Assessoria de Comunicação (AC)

7.6.1. Autorizar, ou não, o uso das marcas, identidade visual e qualquer outro sinal distintivo atual ou futuro da PPSA;

7.6.2. Autorizar, ou não, a gravação de áudio, vídeo ou foto das dependências da PPSA.

7.7. Responsável pela Informação

7.7.1. Autorizar, ou não, a revelação de qualquer Informação de propriedade ou sob a responsabilidade da PPSA.

7.8. Responsável pelo Empregado ou pelo Prestador de Serviços

7.8.1. O responsável pelo empregado será seu superior imediato e no caso de um prestador de serviço será o fiscal designado do contrato;

7.8.2. Zelar pelo cumprimento desta PSI e demais documentos complementares pelos seus Colaboradores

7.8.3. Identificar e medir as vulnerabilidades e Ameaças nos processos e atividades de sua responsabilidade, as quais devem ser tratadas diligentemente de modo a reduzir os impactos ao negócio;

7.8.4. Garantir que os Ativos de propriedade ou sob a responsabilidade da PPSA sejam utilizados com cuidado e de acordo com as orientações do fabricante e da empresa;

7.8.5. Identificar Violações, Quebra de Segurança ou qualquer ação duvidosa praticada por seus Colaboradores, comunicando à GTI imediatamente.

7.9. Colaboradores

7.9.1. Estar ciente e manter-se atualizado com esta PSI e demais documentos complementares;

7.9.2. Conhecer e assinar o "Termo de Ciência e Responsabilidade";

7.9.3. Utilizar os Ativos de propriedade da PPSA ou sob sua responsabilidade de acordo com as orientações do fabricante, do desenvolvedor e da empresa, com cuidado e zelo;

7.9.4. Utilizar de forma profissional, ética e legal as Informações e os Recursos de Tecnologia da Informação da PPSA, respeitando os direitos e as permissões de uso concedidas;

7.9.5. Utilizar todos os Ativos, tangíveis e Intangíveis da PPSA, quando autorizados, somente para fins profissionais;

7.9.6. Preservar a Integridade, a Disponibilidade, a Confidencialidade, Autenticidade e a Legalidade das Informações acessadas ou manipuladas, não as utilizando, enviando, transmitindo ou compartilhando indevidamente, em qualquer local ou mídia, inclusive na i*nternet*;

7.9.7. Não revelar qualquer Informação de propriedade ou sob a responsabilidade da PPSA sem a prévia e formal autorização da GTI;

7.9.8. Não utilizar as marcas, a identidade visual ou qualquer outro sinal distintivo, atual e futuro, da PPSA em qualquer forma ou mídia, inclusive na *internet* e nas mídias sociais, sem a prévia e formal autorização da Comunicação;

7.9.9. Responder por toda e qualquer atividade realizada nos Recursos de Tecnologia da Informação da PPSA realizada mediante o uso de suas credenciais de acesso;

7.9.10. Cumprir a legislação nacional vigente e demais instrumentos regulamentares relacionados às atividades profissionais;

7.9.11. Reportar formalmente à GTI quaisquer eventos relativos à Violação, Quebra de Segurança ou possibilidade de Violação de segurança ou atividades suspeitas.

7.9.12. Conhecer e atuar de acordo com a Política de Tratamento de Dados Pessoais - PO.DAFC.001/2023.

8. Penalidades

8.1. O não cumprimento das disposições constantes nesta Política de Segurança da Informação e Comunicações, suas normas e procedimentos agregados caracteriza infração, a ser apurada de acordo com o procedimento de Gestão de Apuração de infração Disciplinar (PG.DAF.003/2020), sujeitando o infrator às penalidades previstas em lei e nos Procedimentos de Gestão da PPSA.

9. Política de Atualização

9.1. A PPSA deve possuir e manter um programa de revisão/atualização desta PSI e de seus documentos complementares sempre que se fizer necessário, desde que não exceda o período máximo de 03 (três) anos, visando à garantia que todos os requisitos de segurança técnicos e legais implementados estejam sendo cumpridos e atualizados.

10. Disposições Finais

10.1. Esta PSI deve ser lida e interpretada sob a égide das leis brasileiras, no idioma português, em conjunto com os procedimentos aplicáveis pela PPSA.

10.2. Esta PSI, bem como os demais procedimentos da PPSA, encontra-se disponíveis no *OneDrive* ou, em caso de indisponibilidade, podem ser solicitados à GTI.

10.3. Esta PSI entra em vigor na data de sua publicação.

11. Anexos

11.1. TERMO DE CIÊNCIA E RESPONSABILIDADE: *Disclaimer* para ciência eletrônica, eve ser coletado o de acordo de cada Colaborador (usar como barreira de navegação no *login* da rede, ou publicar na intranet com envio para o *e-mail* de todos com a frase abaixo acompanhando ou em local de acesso obrigatório).

Termo de Ciência e Responsabilidade

Formato para assinatura digital:

Eu, _____, pelo presente confirmo que estou ciente do conteúdo da Política de Segurança da Informação da PPSA e reafirmo meu dever de cumprir, disseminar e manter-me sempre atualizado com as regras lá estabelecidas.

Rio de Janeiro, (data constante na assinatura digital)

_____
Assinatura do Empregado
Matrícula do Empregado, ou, na ausência, documento de identificação

Formato Impresso (para assinatura autografa):

Eu, _____, pelo presente, confirmo que estou ciente do conteúdo da **Política de Segurança da Informação** da **PPSA**, e reafirmo meu dever de cumprir, disseminar e manter-me sempre atualizado com as regras lá estabelecidas.

_____, __/___/_____
Local, Data

Índice de Revisões

ÍNDICE DE REVISÕES	
REV.	DESCRIÇÃO
0	Original – Política revisada a partir da Instrução Normativa 2/2016.
0	Aprovada na 123ª Reunião Ordinária do Conselho de Administração em 19/04/2024

	ORIGINAL	REV. 1	REV. 2	REV. 3	REV. 4	REV. 5	REV.61	REV. 7	REV. 8
DATA	05/04/2024								
ELABORADO POR:	GUSTAVO MACABU								
REVISADO POR:	ANDERSON SANTOS								
APROVADO POR:	SAMIR PASSOS/DE								

Elaborado por:	**Revisado por:**	**Aprovado por:**
ANDERSON DE ALMEIDA SANTOS:12546997750 Assinado de forma digital por ANDERSON DE ALMEIDA SANTOS:12546997750 Dados: 2024.04.11 09:15:41 -03'00'	GUSTAVO FALQUER MACABU:08071494704 Assinado de forma digital por GUSTAVO FALQUER MACABU:08071494704 Dados: 2024.04.11 09:04:14 -03'00'	SAMIR PASSOS AWAD:59915315791 Assinado de forma digital por SAMIR PASSOS AWAD:59915315791 Dados: 2024.04.10 19:28:35 -03'00'
Anderson de Almeida Santos Assessor Especial de TI	Gustavo Falquer Macabú Gerente de Tecnologia da Informação	Samir Passos Awad Diretor de Administração, Finanças e Comercialização