

Esta Política foi aprovada pelo Conselho de Administração da CDP na reunião extraordinária realizada em 03/06/2022, por meio de Deliberação CONSAD 44/2022.

CAPÍTULO I – DISPOSIÇÕES INICIAIS

Artigo 1º Fica instituída a Política de Segurança da Informação e Comunicação da Autoridade Portuária Companhia Docas do Pará – CDP, como parte integrante do conjunto de instrumentos de governança e de gestão que suportam a concepção, implementação e melhoria contínua na estrutura organizacional da Companhia.

SEÇÃO I – DOS OBJETIVOS

Artigo 2º O Sistema de Gestão de Segurança da Informação e Comunicação (SGSIC) tem como objetivo a mitigação sistemática dos riscos à segurança e à privacidade da informação.

Artigo 3º Os instrumentos normativos e instruções de trabalho derivados desta política são de cumprimento obrigatório, aplicáveis a todos os funcionários (ou empregados), contratados, terceirizados, trabalhadores temporários, ou com acesso a qualquer informação, sistema, computador, rede de computadores, telecomunicação, mensagem ou serviço de informações pertencentes à CDP em todas suas instalações, onde as leis locais, estatutos e regulamentações do governo não se sobreponham a essas políticas e procedimentos e de acordo com o escopo definido.

Artigo 4º A CDP entende que a Informação, desde sua criação e processamento até seu descarte, é um componente indispensável no processo de tomada de decisão dos gestores, com o objetivo de dar cumprimento à Missão, Visão e aos Valores que refletem a estratégia corporativa da Companhia.

Artigo 5º Devido à informação ser um ativo chave, devem ser tomadas todas as precauções razoáveis para sua proteção.

Parágrafo Único - A proteção da informação requer que sejam preservadas sua confidencialidade, integridade e disponibilidade. A correta proteção dessas características permitirá à CDP gerar maior valor para os seus clientes, empregados, fornecedores e parceiros.

Artigo 6º Em particular, os processos de negócio executados pela CDP são

altamente dependentes de ativos de informação, fazendo com que a segurança da informação e a privacidade, onde aplicável, sejam prioridades para a Companhia.

§1º Para ser capaz de atender a todos estes requisitos e, ao mesmo tempo, cumprir com os valores corporativos, foi estabelecida uma arquitetura de segurança, onde a Política de Segurança descreve os princípios que devem ser seguidos para a proteção adequada da informação.

§2º A presente Política de Segurança da Informação e Comunicação contém informações a respeito do modo como a CDP trata, total ou parcialmente, de forma automatizada ou não, os dados pessoais de seus empregados que acessam os sistemas internos e a intranet da CDP. O objetivo é esclarecer acerca dos tipos de dados que são coletados, dos motivos da coleta e da forma como o empregado poderá atualizar, gerenciar ou até excluir algumas destas informações.

Artigo 7º Esta Política estabelece aspectos gerais do Sistema de Gestão de Segurança da Informação e Comunicação, tais como:

- I. Definição de Segurança da Informação e Comunicação, e sua importância para a CDP;
- II. Estabelecimento do comprometimento da Alta Gestão com a Segurança da Informação e Comunicação;
- III. Estrutura para Gerenciamento de Riscos de Segurança da Informação e Comunicação;
- IV. Explicação geral dos princípios e políticas que norteiam o Sistema de Gestão de Segurança da Informação e Comunicação (SGSIC); e
- V. Governança (Papéis e Responsabilidades) dentro do SGSIC, e estrutura organizacional da CDP.

Artigo 8º São partes integrantes do escopo da presente Política, todos os processos que dão suporte à manutenção da integridade, disponibilidade e confidencialidade das informações necessárias à condução das atividades que fazem parte dos processos de negócio.

SEÇÃO II – DECLARAÇÃO DE COMPROMISSO DA ALTA GESTÃO

Artigo 9º O Conselho de Administração e a Diretoria Executiva da CDP, cientes da importância da informação para o desenvolvimento da sua missão, estão comprometidos com a preservação da segurança dessa informação e da privacidade.

Parágrafo Único - Como parte desse compromisso, a CDP praticará os esforços razoáveis e cumprirá com os requerimentos exigidos pela lei para proteger a

confidencialidade, integridade e disponibilidade das informações criadas, processadas, armazenadas e transmitidas como parte das suas atividades, bemcomo à privacidade.

SEÇÃO III – ESTRUTURA ORGANIZACIONAL

Artigo 10 A seguir é apresentado às hierarquias relacionadas com os processos definidos pelo SGSIC. Respectivas responsabilidades quanto à Segurança da Informação e Comunicação estão descritas no Capítulo Responsabilidades:



Figura 1 – Estrutura de Decisão

- a. **Alta Gestão (DIREXE e CONSAD):** Grupo composto pela Diretoria Executiva da CDP e pelo Conselho de Administração.
- b. **Comitê Gestor de Tecnologia da Informação (CGTI):** O Comitê Gestor de Tecnologia da Informação (CGTI) é um órgão colegiado, formado por membros das áreas de planejamento, finalísticas, jurídica, contábil e da área de TI, que tem o objetivo de promover a entrega de valor por meio da TI e do uso estratégico da informação na organização.
- c. **Gestor de Segurança da Informação:** Empregado oficialmente nomeado e responsável pela manutenção do SGSIC. Também conhecido como *Security Officer*.
- d. **Gestores:** Empregados oficialmente nomeados e responsáveis pela gestão das unidades organizacionais da CDP.
- e. **Empregados:** Todos os empregados, terceiros e prestadores de serviço com funções dentro da estrutura da CDP.
- f. **Proprietário da Informação:** Proprietários da Informação são supervisores/Coordenadores e Gerentes e Diretores das unidades organizacionais que possuem responsabilidade primária por ativos de informação, associados com sua autoridade funcional.

SEÇÃO IV – ABRANGÊNCIA

Artigo 11 A presente política é aplicável a todos os indivíduos que, de maneira direta ou indireta, envolvam-se em processos de negócio da CDP. Exemplos: empregados, recursos terceirizados, aprendizes, etc.

SEÇÃO V – FUNDAMENTAÇÃO LEGAL E NORMATIVA

Artigo 12 A Política de Segurança da Informação e Comunicação tem como fundamentação legal e normativa:

- I. Estatuto Social da CDP;
- II. Resolução CGPAR Nº 11, que determina a necessidade das empresas estatais federais em planejar, implementar e manter práticas de governança de TI, incluindo a formalização e execução de Políticas de Segurança da Informação;
- III. ISO/IEC 27001:2013, especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação dentro do contexto da organização. Esta Norma também inclui requisitos para a avaliação e tratamento de riscos de segurança da informação voltados para as necessidades da organização;
- IV. ISO/IEC 27002:2013, fornece diretrizes para práticas de gestão de segurança da informação e normas de segurança da informação para as organizações, incluindo a seleção, a implementação e o gerenciamento de controles, levando em consideração os ambientes de risco da segurança da informação da organização;
- V. ISO/IEC 27701:2019 Versão Corrigida 2020, especifica os requisitos e fornece as diretrizes para o estabelecimento, implementação, manutenção e melhoria contínua de um Sistema de Gestão de Segurança da Informação e Comunicação (SGSIC), na forma de uma extensão das ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para a gestão da privacidade dentro do contexto da organização;
- VI. COBIT 5 (2012), Modelo Corporativo. para Governança e Gestão de TI da Organização;
- VII. Instrução Normativa GSI/PR nº 1, de 13 de junho de 2008, que disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências;
- VIII. Decreto nº 9.637/2018, de 26 de dezembro de 2018, que institui a

Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação;

- IX. Lei Federal n. 12.527, de 18 de novembro de 2011, que regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências;
- X. Lei Federal n. 12.965, de 23 de abril de 2014, que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil (Marco Civil da Internet); e
- XI. Lei Federal n. 13.709, de 14/08/2018, que estabelece a Lei Geral de Proteção de Dados Pessoais (LGPD).

CAPÍTULO II – DEFINIÇÕES

Artigo 13 Para os fins desta Política são adotadas as seguintes definições, que poderão ser utilizadas no singular ou plural, sem prejuízo de significado aqui atribuído, e que estão em conformidade com as definições da legislação, com as adaptações necessárias à realidade da CDP:

- a. **Ativos de Informação:** Qualquer elemento imbuído de valor para o negócio da CDP, como documentos físicos e eletrônicos, sistemas de comunicação, registros audiovisuais, sistemas de informação, papéis profissionais, etc.
- b. **Comitê Gestor de Tecnologia da Informação (CGTI):** O CGTI é um órgão colegiado, formado por membros das áreas de planejamento, finalísticas, jurídica, contábil e da área de TI, que tem o objetivo promover a entrega de valor por meio da TI e do uso estratégico da informação na organização
- c. **Segurança da Informação - SI:** Envolve a aplicação e o gerenciamento de medidas de segurança apropriadas considerando um leque abrangente de ameaças, com o foco em garantir o sucesso e a continuidade do negócio de forma sustentável, minimizando impactos de incidentes de segurança da informação. Inclui três dimensões principais: confidencialidade, disponibilidade e integridade
- d. **Tecnologia da Informação e Comunicação - TIC:** Conjunto de conhecimentos, sistemas, processos e práticas utilizadas na prestação de serviços de suporte aos processos empresariais de quaisquer naturezas, através de captura, processamento, geração, armazenamento, recuperação e

comunicação de dados, informações e conhecimentos.

CAPÍTULO III – PRINCÍPIOS

Artigo 14 As ações e procedimentos relativos à Segurança da Informação e Comunicações da CDP deverão ser norteados pelos seguintes princípios:

- I. **Confidencialidade:** diz respeito à divulgação não autorizada de informação sensível para o negócio;
- II. **Integridade:** propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;
- III. **Disponibilidade:** relaciona-se à informação estar disponível quando requerido pelo processo de negócio agora e no futuro;
- IV. **Privacidade:** diz respeito à proteção dos dados pessoais, incluindo o respeito, liberdade e as garantias constitucionais do cidadão.

CAPÍTULO IV - DIRETRIZES

SEÇÃO I – POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

Artigo 15 São objetivos específicos instituídos por esta política:

- I. Buscar garantir a segurança da informação e privacidade, e padronizar as práticas a serem aplicadas por todo o pessoal com responsabilidade para a segurança da informação e comunicação;
- II. Dar consciência dos riscos que ameaçam o sistema de informação e os meios disponíveis para controlá-los;
- III. Criar uma estrutura geral para projetar e executar medidas de segurança dos sistemas de informação; e
- IV. Promover a cooperação entre os departamentos da CDP para criar, aplicar e verificar as instruções, procedimentos e medidas de segurança relacionadas ao negócio.

SEÇÃO II – CLASSIFICAÇÃO DA INFORMAÇÃO

Artigo 16 A classificação da informação irá ser pautada na Lei de Acesso à Informação e na Lei Geral de Proteção de Dados, bem como nos normativos internos que tratem o tema de forma específica.

SEÇÃO III – REQUISITOS GERAIS DE MANIPULAÇÃO DAS INFORMAÇÕES

Artigo 17 São requisitos gerais de manipulação de uma informação:

- I. **Distribuição:** versões eletrônicas do documento devem ser disponibilizadas em formato não alterável após a liberação (PDF/A).
- II. **Armazenamento e Transporte:**
 - a. as mídias extraíveis que contenham informações com diferentes classificações devem ser protegidas de acordo com a classificação da informação mais sensível; e
 - b. antes do transporte de informações em mídias extraíveis, deve haver verificação da existência de outras informações mais sensíveis no dispositivo que não serão transportadas.
- III. **Rotulagem:** o rótulo dos meios de informação (mídias de backup, e-mail, documento físico etc.) devem identificar a classificação da informação mais sensível.

SEÇÃO IV – CONSIDERAÇÕES GERAIS

Artigo 18 É responsabilidade da organização onde o empregado está lotado, a proteção de seus dados pessoais e corporativos utilizados na execução de suas atividades e tarefas;

Artigo 19 Os sistemas de informação com acesso público devem ser verificados periodicamente pelos Gestores da informação disponibilizada contra eventuais falhas de integridade. A periodicidade deve ser:

- I. no mínimo, de uma vez ao ano; ou
- II. conforme necessidade.

Artigo 20 A Gerência de Tecnologia da Informação deve definir, com o apoio dos Gestores das informações, os controles tecnológicos para identificar fragilidades antes de a informação ser disponibilizada, de acordo com as diretrizes de manipulação das informações apresentadas resumidamente no ANEXO 1.

CAPÍTULO V - TRATAMENTO E PROTEÇÃO DOS DADOS PESSOAIS

SEÇÃO I – DIREITOS DO EMPREGADO

Artigo 21 A CDP, por meio da intranet e dos sistemas internos, se compromete a cumprir as normas previstas na LGPD – Lei Geral de Proteção de Dados, em respeito

aos seguintes princípios:

- a. Os dados pessoais do empregado serão tratados de forma lícita, leal e transparente (licitude, lealdade e transparência);
- b. Os dados pessoais do empregado serão coletados apenas para finalidades determinadas, explícitas e legítimas, não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades (limitação das finalidades);
- c. Os dados pessoais do empregado serão coletados de forma adequada, pertinente e limitada às necessidades do objetivo para os quais eles são processados (minimização dos dados);
- d. Os dados pessoais do empregado serão mantidos exatos, e atualizados sempre que necessário, de maneira que os dados inexatos sejam retificados quando possível e apagados se necessário (exatidão);
- e. Os dados pessoais do empregado serão conservados de uma forma que permita a identificação dos Titulares dos dados (empregado) apenas durante o período necessário para as finalidades para as quais são tratados (limitação da conservação); e
- f. Os dados pessoais do empregado serão tratados de forma segura, protegidos do tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental, adotando as medidas técnicas ou organizacionais adequadas (integridade e confidencialidade).

Artigo 22 O empregado que navega pela intranet ou sistemas internos da CDP possui os seguintes direitos, conferidos pela Lei de Proteção de Dados Pessoais:

- a. Direito de confirmação e acesso: é direito do empregado, da CDP, a confirmação de que os dados pessoais que lhe digam respeito, são ou não objeto de tratamento e, se for esse o caso, o direito de acessar os seus dados pessoais;
- b. Direito de retificação: é direito do empregado de obter, sem demora injustificada, a retificação dos dados pessoais inexatos que lhe digam respeito, constantes da intranet e dos sistemas internos da CDP;
- c. Direito à eliminação dos dados (direito ao esquecimento): é direito do empregado de ter seus dados apagados da intranet ou dos sistemas internos da CDP, ao término da finalidade específica do motivo da retenção;
- d. Direito à limitação do tratamento dos dados: é direito do empregado, de limitar o tratamento de seus dados pessoais, podendo exercê-lo quando contestar a exatidão dos dados, quando o tratamento for ilícito, quando a CDP não precisar

mais dos dados para as finalidades propostas, quando tiver manifestado oposição ao tratamento dos dados e em caso de tratamento de dados desnecessários;

- e. Direito de oposição: é direito do empregado de, a qualquer momento, se opor, por motivos relacionados com a sua situação particular, ao tratamento dos dados pessoais que lhe digam respeito; e
- f. Direito de não ser submetido a decisões automatizadas: é direito do empregado de não ficar sujeito a nenhuma decisão tomada exclusivamente com base no tratamento automatizado, que produza efeitos na sua esfera jurídica ou que o afete significativamente de forma similar.

SEÇÃO II – DEVER DE NÃO FORNECER DADOS DE TERCEIROS

Artigo 23 Durante a navegação pela intranet ou sistemas internos da CDP, a fim de resguardar e de proteger os direitos de terceiros, o empregado da CDP deverá fornecer – quando solicitado – somente seus dados pessoais, e não os de terceiros.

SEÇÃO III – INFORMAÇÕES COLETADAS

Artigo 24 A coleta de dados dos empregados se dará em conformidade com o disposto nesta Política de Segurança da Informação e Comunicação e dependerá do consentimento do empregado, sendo este dispensável somente nas hipóteses previstas no art. 11, inciso II, da Lei de Proteção de Dados Pessoais.

SEÇÃO IV – TIPOS DE DADOS COLETADOS

Artigo 25 A utilização, pelo empregado, de determinadas funcionalidades da intranet ou dos sistemas internos da CDP dependerá de cadastro, sendo que, nestes casos, vários dados do empregado poderão ser coletados e armazenados:

- I. **Dados informados em algum formulário de contato:** Os dados eventualmente informados pelo empregado que utilizar algum formulário de contato disponibilizado na intranet ou sistemas internos da CDP, incluindo o teor da mensagem enviada, serão coletados e armazenados.
- II. **Registros de acesso:** Em atendimento às disposições do art. 15, caput e parágrafos, da Lei Federal n. 12.965/2014 (Marco Civil da Internet), os registros de acesso do empregado serão coletados e armazenados pelo tempo legal para retenção dos mesmos.
- III. **Dados sensíveis:** Será coletado pela intranet ou pelos sistemas internos da CDP, quando necessário, dados sensíveis dos empregados, cuja forma de



POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

tratamento está definida nos termos dos arts. 9º a 11 e demais dispositivos da Lei de Proteção de Dados Pessoais – LGPD. Assim, dentre outros, haverá coleta dos seguintes dados:

- a. Dados que revelem sua origem racial ou étnica, e/ou a filiação sindical do empregado;
 - b. Dados genéticos;
 - c. Dados biométricos para identificar uma pessoa de forma inequívoca;
 - d. Dados relativos à saúde do empregado; e
 - e. Dados relacionados a condenações penais ou a infrações ou com medidas de segurança conexas.
- IV. **Coleta de dados não previstos expressamente:** Eventualmente, outros tipos de dados não previstos expressamente nesta Política de Segurança da Informação e Comunicação poderão ser coletados, desde que seja indicada a finalidade e sejam fornecidos com o consentimento explícito do empregado, ou, ainda, que a coleta seja permitida ou imposta por lei.

SEÇÃO IV – FUNDAMENTO JURÍDICO PARA O TRATAMENTO DOS DADOS PESSOAIS

Artigo 26 Ao utilizar os serviços da intranet ou dos sistemas internos da CDP, o usuário está consentindo com a presente Política de Segurança da Informação e Comunicação;

Artigo 27 Nestes casos específicos e enquanto durar o vínculo profissional entre o empregado e a CDP, o empregado não tem o direito de revogar seu consentimento para acessar a intranet ou os sistemas internos da CDP, não comprometendo a licitude do tratamento de seus dados pessoais;

Artigo 28 O tratamento de dados pessoais sem o consentimento do empregado, apenas será realizado em razão de interesse legítimo da CDP ou para as hipóteses previstas em lei, ou seja, dentre outras, as seguintes:

- I. Para o cumprimento de obrigação legal ou regulatória pelo controlador;
- II. Para a realização de estudos por órgão de pesquisa, sendo garantida ao empregado, sempre que possível, a anonimização dos dados pessoais;
- III. Quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o empregado;
- IV. Para o exercício regular de direitos em processo judicial, administrativo ou

arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);

- V. Para a proteção da vida ou da incolumidade física do titular dos dados ou de terceiros;
- VI. Para a tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias;
- VII. Quando necessário para atender aos interesses legítimos da CDP como controlador ou de terceiros, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular dos dados que exijam a proteção dos dados pessoais; e
- VIII. Para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

SEÇÃO V – FINALIDADES DO TRATAMENTO DOS DADOS PESSOAIS

Artigo 29 Os dados pessoais do empregado coletados pela intranet ou pelos sistemas internos da CDP têm por finalidade facilitar, agilizar e cumprir os compromissos estabelecidos entre a CDP e o empregado, bem como fazer cumprir as solicitações realizadas por meio do preenchimento de formulários diversos;

Artigo 30 Os dados pessoais poderão ser utilizados também para a finalidade de personalizar o conteúdo oferecido ao empregado, bem como para dar subsídio à intranet ou algum sistema interno da CDP visando a otimizar a qualidade e funcionamento de seus serviços;

Artigo 31 Os dados de qualquer cadastro serão utilizados para permitir o acesso do empregado a determinados conteúdos da intranet ou de sistemas internos da CDP, exclusivos para os empregados devidamente cadastrados; e

Artigo 32 O tratamento de dados pessoais para finalidades não previstas nesta Política de Segurança da Informação e Comunicação somente ocorrerá mediante comunicação prévia ao empregado, sendo que, em qualquer caso, os direitos e obrigações aqui previstos permanecerão aplicáveis.

SEÇÃO VI – PRAZO DE CONSERVAÇÃO DOS DADOS PESSOAIS

Artigo 33 Os dados pessoais do empregado serão conservados por um período não superior ao definido por uma “tabela de temporalidade” específica ou, na ausência desta, a legislação pertinente ao assunto, para cumprir os objetivos legais e regulatórios em razão dos quais eles são processados.

Artigo 34 O período de conservação dos dados é definido de acordo com os seguintes critérios:

- I. Os dados serão armazenados pelo tempo necessário para a prestação dos serviços fornecidos pela intranet ou pelos sistemas internos da CDP ao empregado, de acordo com a legislação ou regulação aplicáveis ou pode variar de 1 a 6 meses, em caso de não existir legislação regulatória aplicável;
- II. Os dados pessoais dos empregados apenas poderão ser conservados após o término de seu tratamento nas seguintes hipóteses:
 - a. Para o cumprimento de obrigação legal ou regulatória pelo controlador (CDP);
 - b. Para estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
 - c. Para a transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos na legislação; e
 - d. Para uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que os dados sejam anonimizados.

SEÇÃO VII – DESTINATÁRIOS E TRANSFERÊNCIA DOS DADOS PESSOAIS

Artigo 35 Os dados pessoais dos empregados poderão ser compartilhados com terceiros (que serão identificados como operadores e/ou controladores no âmbito da Lei 13.709/2018) para cumprimento de obrigações legais por parte da CDP em favor dos empregados. Os dados serão, portanto, tratados não só pela CDP como por esses terceiros por instrução da CDP.

TÍTULO II - DO TRATAMENTO DOS DADOS PESSOAIS

CAPÍTULO I - RESPONSÁVEIS

SEÇÃO I - DO RESPONSÁVEL PELO TRATAMENTO DOS DADOS (DATA CONTROLLER)

Artigo 36 A CDP, na condição de controlador, é responsável pelo tratamento dos dados pessoais do empregado, bem como, por determinar as finalidades e os meios de tratamento de dados pessoais.

Artigo 37 Na intranet da CDP e nos sistemas internos da CDP, o responsável pelo tratamento dos dados pessoais coletados é o Encarregado pela Proteção de Dados da Autoridade Portuária da Companhia Docas do Pará.

SEÇÃO II - CONTROLES DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

Artigo 38 Os controles de segurança consistem em um conjunto amplo de medidas de segurança, visando a minimizar os riscos presentes nos ativos de Informação. Os controles devem se basear na norma de segurança aceita internacionalmente (ISO 27001/27002 e a extensão 27701).

SEÇÃO III - IMPLANTAÇÃO E AVALIAÇÃO

Artigo 39 A CDP deve estar em conformidade com os requisitos desta Política. Os requisitos podem ser revisados para atender as necessidades de parceiros e da própria Companhia. O processo de verificação da conformidade desta deve ser conduzido pela Gerência de Gestão Estratégica (GEGEST), obedecendo às políticas, normas e procedimentos vigentes.

SEÇÃO IV - EXCEÇÃO À POLÍTICA

Artigo 40 As exceções serão avaliadas e devem ser reportadas por escrito ao Comitê Gestor de Tecnologia da Informação (CGTI). Este irá avaliar as exceções conforme as justificativas de negócio fornecidas pelo solicitante e definir o tratamento adequado.

CAPITULO II- SISTEMA DE GESTÃO DA PRIVACIDADE DA INFORMAÇÃO E COMUNICAÇÃO - SGPIC

SEÇÃO I – RISCO

Artigo 41 O Sistema de Gestão de Privacidade da Informação e Comunicação da CDP está voltado para a mitigação do risco dos ativos de informação e da privacidade;

Artigo 42 A CDP entende que o gerenciamento dos riscos em segurança da informação e de comunicação é um processo cíclico e dinâmico que requer uma constante participação de todas as pessoas. Devido ao fato de ser um processo cíclico, está em constante evolução e aprimoramento mediante a comparação dos resultados do processo com os resultados esperados e ajuste das entradas para melhorá-los;

Artigo 43 O processo de gerenciamento do risco está baseado nas seguintes etapas e devem ser gerenciados pela área técnica, são eles:

- I. Identificação dos ativos críticos;
- II. Levantamento e avaliação dos riscos associados a esses ativos;
- III. Criação de um plano para o tratamento desses riscos; e
- IV. Execução do plano de tratamento de riscos.



POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

Artigo 44 O processo é cíclico no sentido de que após a execução do plano de tratamento de riscos, o novo nível de risco deve ser comparado (chamado de risco residual) com o nível avaliado inicialmente;

Artigo 45 A informação resultante dessa comparação deve ser utilizada para iniciar novamente o processo; e

Artigo 46 O processo é dinâmico também no sentido de que os ativos críticos de informação mudam ao longo do tempo e, portanto, devem ser avaliados periodicamente para manter a sua identificação atualizada com os processos de negócio.

SEÇÃO II – REQUISITOS

Artigo 47 São requisitos da Organização da Segurança e Privacidade da Informação e Comunicação:

- I. Uma Estrutura Organizacional de gerenciamento deve ser estabelecida para iniciar e controlar a operação da Segurança e Privacidade da Informação na CDP; e
- II. Esta Estrutura Organizacional deve ser responsável por estabelecer os procedimentos de utilização de dispositivos móveis e trabalho remoto.

Artigo 48 São requisitos para a área de recursos humanos a existencia de procedimentos específicos em Segurança e Privacidade da Informação e Comunicação para os processos de contratação do empregado, durante o seu contrato de trabalho, bem como as mudanças e o encerramento do contrato.

Artigo 49 São requisitos para a área gestão de Ativos de Informação:

- I. A implementação de procedimento de responsabilidade pela proteção dos ativos de informação;
- II. Todas as informações devem ser devidamente classificadas quanto ao nível adequado de proteção, de acordo com a sua importância para o negócio; e CONTROLE DE ACESSO.
- III. Deve existir um conjunto de procedimentos que controle o acesso à informação, aos ativos e recursos de processamento da informação e que garanta ao usuário acesso autorizado a sistemas e serviços existentes para o exercício de suas funções ao mesmo tempo que previna o acesso não autorizado aos mesmos sistemas e serviços; e
- IV. Todos os usuários devem ser responsáveis pela proteção das informações

necessárias para a sua autenticação em sistemas e serviços da CDP.

Artigo 50 Procedimentos de criptografia devem ser utilizados de forma efetiva e adequada para proteger a confidencialidade, autenticidade e/ou a integridade da informação.

Artigo 51 Devem existir procedimentos que previnam o acesso físico não autorizado, incluindo danos, furtos, vandalismo e comprometimento de ativos, e interferências aos sistemas, recursos e serviços de processamento das informações que suportam a CDP.

SEÇÃO III – SEGURANÇA DAS OPERAÇÕES

Artigo 52 Devem existir procedimentos que garantam a operação segura e correta dos sistemas, recursos e serviços de processamento da informação, incluindo proteção contra malware, controle de cópias de segurança, Sistemas Operacionais, registros e monitoramento das operações, além de um Sistema de Gestão de Vulnerabilidades Técnicas, visando a prevenção e controle do risco associado com a exploração indevida por parte de hackers, das possíveis vulnerabilidades técnicas encontradas em sistemas operacionais, sistemas e serviços disponíveis para os empregados.

Artigo 53 Todos os sistemas de informação devem ser periodicamente auditados visando a minimizar o impacto do mau uso ou do uso ineficiente de tais sistemas.

SEÇÃO IV – SEGURANÇA DAS COMUNICAÇÕES

Artigo 54 A segurança das redes deve ser assegurada visando a proteção das informações e recursos de processamento das informações que as apoiam; e

Artigo 55 Toda a informação transferida internamente ou de/para terceiros deve ser devidamente protegida em função de sua classificação quanto à confidencialidade.

SEÇÃO V – AQUISIÇÃO, DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMAS

Artigo 56 Devem existir garantias de que a segurança da informação seja parte integrante de todo ciclo de vida dos sistemas de informação, incluindo os requisitos para o desenvolvimento de sistemas e a devida proteção e privacidade dos dados utilizados para teste.

SEÇÃO VI – RELACIONAMENTO COM FORNECEDORES E TERCEIROS

Artigo 57 Devem existir procedimentos que garantam a proteção dos ativos de

informação, sistemas, recursos e serviços da CDP que são acessados por terceiros.

SEÇÃO VII – GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

Artigo 58 Devem existir procedimentos para gerenciar os incidentes de segurança da informação, incluindo a comunicação de vulnerabilidades encontradas e ocorrência de eventos.

SEÇÃO VIII – GESTÃO DA CONTINUIDADE DO NEGÓCIO

Artigo 59 Devem existir procedimentos que garantam a continuidade do negócio em face de incidentes de segurança da informação.

CAPÍTULO III – RESPONSABILIDADES

Artigo 60 No âmbito da presente Política, as instâncias e unidades de gestão abaixo elencadas são responsáveis, além das suas respectivas atribuições previstas no Estatuto Social, Regimento Interno próprio ou Regimento Interno da Companhia, por:

I. CONSELHO DE ADMINISTRAÇÃO (CONSAD), responsável por:

- a. Aprovar a presente Política;
- b. Definir e desenvolver as estratégias de Segurança da Informação e Comunicação em alinhamento com o Plano Estratégico da CDP; e
- c. Acompanhar as ações da Diretoria Executiva relacionadas à Segurança da Informação e Comunicação.

II. DIRETORIA EXECUTIVA (DIREXE), responsável por:

- a. Garantir o atendimento das Políticas de Segurança da Informação e Comunicação e o funcionamento do SGSIC;
- b. Garantir a compatibilidade da segurança da informação com os objetivos estratégicos da Companhia;
- c. Aprovar as iniciativas para a melhoria contínua do SGSIC;
- d. Prover recursos para a gestão, operação e monitoramento adequado das atividades do SGSIC;
- e. Suportar perante toda a Companhia as iniciativas da Área de Segurança da Informação e Comunicação;
- f. Garantir a contínua manutenção das Políticas de Segurança da Informação e Comunicação e desdobramento de seus respectivos objetivos;



POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

- g. Garantir a contínua análise e realimentação dos resultados de gestão de riscos ao SSIC;
- h. Ter conhecimento das auditorias conduzidas nos sistemas para que os planos de ação sejam cumpridos.

III. GESTOR DE SEGURANÇA DA INFORMAÇÃO, responsável por:

- a. Produzir diretivas locais de segurança, regras e padrões a serem usados pelos empregados;
- b. Propor os recursos necessários às ações de segurança da informação e comunicações;
- c. Desenvolver e promover programas de conscientização de segurança;
- d. Garantir que todos os gestores estejam cientes de suas próprias responsabilidades relacionadas à Segurança da Informação;
- e. Certificar-se que o processo de Gestão de Pessoas leva em conta todos os aspectos de Segurança da Informação ao contratar novos empregados, ou durante o vínculo empregatício, ou em rescisão de contratos de trabalho;
- f. Revisar periodicamente o nível de segurança de sistemas internos, emitindo avisos após estas revisões. Analisar criticamente, em intervalos periódicos, o progresso dos planos de melhoria resultantes em conjunto com os gestores envolvidos;
- g. Manter-se atualizado com relação à tecnologia, legislação e novas ameaças;
- h. Analisar criticamente os incidentes de segurança mais significativos e gerenciar e/ou acompanhar as ações relacionadas na solução dos mesmos;
- i. Representar a CDP, interna e externamente, nos assuntos relacionados ao SSIC;
- j. Gerenciar os processos do SGSIC, na busca da melhoria contínua e alinhamento com a Alta Gestão;
- k. Realizar a coleta de dados e informações pertinentes à segurança da informação para a realização de análise crítica pela Diretoria;
- l. Dar retorno dos resultados das análises críticas feitas pela Direção, aos envolvidos visando possíveis providências;
- m. Acompanhar o sistema de ações corretivas e preventivas do SGSIC; e
- n. Garantir a contínua manutenção e atualização dos indicadores de desempenho dos processos do SGSIC, estimulando melhorias e mudanças de



POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

metas.

IV. GESTORES, responsáveis por:

- a. Manter atualizada a definição dos ativos de informação e notificar em qualquer alteração no inventário de ativos de sua área;
- b. Implantar e monitorar a eficácia de procedimentos, instruções de trabalho e documentos quanto a proteção da Segurança da Informação em sua área de atuação;
- c. Informar/comunicar todos os fatos relacionados ao SGSIC às áreas de operação sob sua responsabilidade;
- d. Contribuir para implantação dos objetivos de gestão de Segurança da Informação e efetuar as medições necessárias por processos;
- e. Implantar as oportunidades de melhoria;
- f. Planejar a adoção de procedimentos do SGSIC e monitorar sua eficácia em sua área de atuação; e
- g. Garantir a contínua eficácia dos controles implantados para satisfazer os requisitos do SGSIC.

V. EMPREGADOS E TERCEIRIZADOS DA CDP, responsáveis por:

- a. Notificar seus gestores sobre qualquer alteração no inventário de ativos de sua área;
- b. Conhecer e seguir os procedimentos constantes no SGSIC;
- c. Recomendar melhorias no SGSIC;
- d. Identificar qualquer incidente de segurança e reportá-lo ao seu gestor/contato direto dentro da CDP; e
- e. Cuidar pela proteção dos ativos de informação a que tiverem acesso.

VI. PROPRIETÁRIOS DA INFORMAÇÃO (Supervisores , Gerentes e Diretores da CDP), responsáveis por:

- a. Definir e atualizar os ativos de informação;
- b. Determinar os requerimentos de confidencialidade, integridade e disponibilidade para proteger esses ativos de informação relacionados com os processos de negócio ao seu cargo;
- c. Definir procedimentos que estejam alinhados aos princípios e diretrizes de Segurança da Informação;



POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

- d. Segregar funções e separar recursos de desenvolvimento, teste e produção dentro dos seus processos de negócio;
- e. Os proprietários da informação gerenciarão a correta prestação de serviços por parte de terceiros que afetem/suportem a segurança dos ativos de informação ao seu cargo, fazendo análise crítica do seu desempenho e possíveis oportunidades de melhoria; e
- f. É responsabilidade do proprietário da informação a realização de análise crítica em seus processos de negócio e em particular dos riscos à informação.

CAPÍTULO IV – SANÇÕES

Artigo 61 A não observância desta Política e de seus desdobramentos normativos implicará, no que couber, em sanções previstas no Regulamento Interno de Pessoal e/ou no Código de Ética da CDP.

CAPÍTULO V – DISPOSIÇÕES GERAIS

Artigo 62 Compete aos gestores da Companhia difundir a presente Política e seus desdobramentos aos empregados e zelar por seu cumprimento; e

Artigo 63 É dever dos administradores e empregados da Companhia observar os princípios e procedimentos estabelecidos neste documento.

ANEXO 1 – TERMO DE RESPONSABILIDADE INDIVIDUAL

Belém, _____ de _____ de _____

Pelo presente instrumento, eu, _____

(nome/registro), perante a Companhia Docas do Pará, doravante denominada CDP, na qualidade de usuário do ambiente computacional de propriedade da referida Companhia, declaro estar ciente das normas de segurança das informações digitais da CDP, segundo as quais devo:

- a) tratar a informação digital como patrimônio da CDP e como um recurso que deva ter seu sigilo preservado, em consonância com a legislação vigente;
- b) utilizar as informações disponíveis e os sistemas e produtos computacionais, dos quais a CDP é proprietária ou possui o direito de uso, exclusivamente para o interesse do serviço;
- c) preservar o conteúdo das informações sigilosas a que tiver acesso, sem divulgá-las para pessoas não autorizadas;
- d) não tentar obter acesso à informação cujo grau de sigilo não seja compatível com o que possuo na Companhia ou que eu não tenha autorização ou necessidade de conhecer;
- e) não compartilhar o uso de senha com outros usuários;
- f) não me passar por outro usuário usando arditosamente sua identificação de acesso e senha;
- g) não alterar o endereço de rede ou qualquer outro dado de identificação do microcomputador de meu uso;
- h) instalar e utilizar em meu microcomputador somente programas homologados para uso na CDP e que esta possua as respectivas licenças de uso ou, no caso de programas de domínio público, mediante autorização formal da área de informática da CDP;
- i) no caso de exoneração, demissão, licenciamento, término de prestação de serviço ou qualquer tipo de afastamento, preservar o conteúdo das informações e documentos sigilosos a que tive acesso e não os divulgar a pessoas não autorizadas;
- j) guardar segredo das minhas autenticações de acesso (senhas) utilizadas no ambiente computacional da CDP, não cedendo, não transferindo, não divulgando e não permitindo o seu conhecimento por terceiros;
- k) não utilizar senha com sequência fácil ou óbvia de caracteres que facilite a sua descoberta e não escrever a senha em lugares visíveis ou de fácil acesso;
- l) ao me afastar momentaneamente da minha estação de trabalho, utilizar descanso de tela (*screen saver*) protegido por senha, a fim de evitar que alguém possa ver as informações que estejam disponíveis na tela do computador;

- m) ao me ausentar do local de trabalho, momentaneamente ou ao término de minhas atividades diárias, certificar-me de que a sessão aberta no ambiente computacional com minha identificação foi fechada e as informações que exigem sigilo foram adequadamente salvaguardadas;
- n) seguir as orientações da área de informática da CDP relativas à instalação, à manutenção e ao uso adequado dos equipamentos, dos sistemas e dos programas do ambiente computacional;
- o) comunicar imediatamente ao meu superior hierárquico e à área de informática da CDP a ocorrência de qualquer evento que implique ameaça ou impedimento de cumprir os procedimentos de segurança estabelecidos;
- p) responder, perante a CDP, as auditorias e a área de informática da CDP, por acessos, tentativas de acessos ou uso indevido da informação digital realizados com a minha identificação ou autenticação;
- q) não praticar quaisquer atos que possam afetar o sigilo ou a integridade da informação;
- r) estar ciente de que toda informação digital armazenada e processada no ambiente computacional da CDP pode ser auditada, como no caso de páginas informativas (sites) visitadas por mim;
- s) não transmitir, copiar ou reter arquivos contendo textos, fotos, filmes ou quaisquer outros registros que contrariem a moral, os bons costumes e a legislação vigente;
- t) não transferir qualquer tipo de arquivo que pertença à CDP para outro local, seja por meio magnético ou não, exceto no interesse do serviço e mediante autorização da autoridade competente;
- u) estar ciente de que o processamento, o trâmite e o armazenamento de arquivos que não sejam de interesse do serviço são expressamente proibidos no ambiente computacional da CDP;
- v) estar ciente de que a CDP poderá auditar os arquivos em trâmite ou armazenados nos equipamentos do ambiente computacional da CDP sob meu uso ou responsabilidade;
- w) estar ciente de que o correio eletrônico é de uso exclusivo para o interesse do serviço e qualquer correspondência eletrônica originada ou retransmitida no ambiente computacional da CDP deve obedecer a este preceito; e
- x) estar ciente de que a CDP poderá auditar as correspondências eletrônicas originadas ou retransmitidas por mim no ambiente computacional da CDP.

Desta forma, estou ciente da minha responsabilidade pelas consequências decorrentes da não observância do acima exposto e da legislação vigente.

Assinatura
Nome Completo/registro