POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Companhia Docas de São Sebastião
Avenida Doutor Altino Arantes, 372, Centro –São Sebastião – SP
Tel.: (12) 3892.1899

1. OBJETIVO

Esta norma, Política de Segurança da Informação (PSI), considera as melhores práticas e descreve as condições adequadas para a correta utilização dos Recursos de Informação, conforme as diretrizes definidas na política de segurança da COMPANHIA DOCAS DE SÃO SEBASTIÃO, devendo ser seguida por todos os usuários.

A Política de segurança expressa o compromisso da CDSS com o tratamento de dados pessoais de forma ética e legal, atendendo, especialmente, a Lei Federal nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais - "LGPD").

O princípio da PSI é preservar as informações da COMPANHIA DOCAS DE SÃO SEBASTIÃO quanto a:

- **Confidencialidade**: garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.
- **Integridade:** capacidade de garantir que a informação seja mantida em seu estado original, conforme foi concebida, visando protegê-la contra alterações indevidas, intencionais ou acidentais na guarda ou transmissão.
- **Disponibilidade:** garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

2. ABRANGÊNCIA E VIGÊNCIA

Esta norma aplica-se a todos os empregados, estagiários, aprendizes, parceiros, fornecedores, prestadores de serviço, e em qualquer local onde se encontre informação e equipamentos de informática que pertencem à Companhia Docas de São Sebastião.

Esta norma tem prazo de validade indeterminado, portanto, sua vigência se estenderá até a publicação de uma revisão, que a atualize ou a revogue.

3. TRATAMENTO DE DADOS SENSÍVEIS

Princípios para Tratamento de Dados Sensíveis

O tratamento de dados sensíveis pela COMPANHIA DOCAS DE SÃO SEBASTIÃO (CDSS) seguirá estritamente os requisitos estabelecidos no artigo 11 da Lei Geral de Proteção de Dados Pessoais (LGPD). Os dados sensíveis serão tratados somente nas seguintes condições:

- **Consentimento explícito do titular:** O tratamento de dados sensíveis será realizado somente com o consentimento expresso e inequívoco do titular, coletado por meio de formulários claros e objetivos.
- **Cumprimento de obrigação legal ou regulatória:** Quando necessário para cumprir uma obrigação legal ou regulatória, conforme exigido pela legislação aplicável.
- **Exercício regular de direitos em processos judiciais, administrativos ou arbitrais:** O tratamento de dados sensíveis pode ocorrer para o exercício regular de direitos em processos legais.

Segurança do Tratamento de Dados Sensíveis

Todos os dados sensíveis coletados, processados ou armazenados pela CDSS são protegidos por meio de controles técnicos e organizacionais, como:

- **Criptografia de Dados:** Dados sensíveis serão criptografados em trânsito (utilizando protocolos como HTTPS, TLS) e em repouso (por meio de criptografia de banco de dados e sistemas de armazenamento).
- **Pseudonimização ou Anonimização:** Sempre que possível e solicitado, dados sensíveis serão pseudonimizados ou anonimizados para reduzir os riscos em caso de incidentes.
- **Controle de Acesso:** O acesso a dados sensíveis será restrito com base no princípio de necessidade, e todos os acessos serão monitorados e auditados.

Relatórios de Impacto à Proteção de Dados (DPIA)

A CDSS realizará a análise de impacto à proteção de dados (DPIA) para todas as operações que envolvam o tratamento de dados sensíveis. O DPIA será conduzido da seguinte forma:

- **Identificação de riscos:** Identificação dos riscos para os direitos e liberdades dos titulares de dados.
- **Avaliação de impacto:** Análise do impacto dos riscos para a privacidade e proteção dos dados sensíveis.
- **Mitigação de riscos:** Propostas de medidas para mitigar ou eliminar os riscos identificados, tais como controles adicionais ou ajustes na operação de tratamento.

Plano de Resposta a Incidentes

Objetivos do Plano de Resposta a Incidentes

O plano de resposta a incidentes da CDSS visa garantir a pronta identificação,

contenção, comunicação e mitigação de incidentes de segurança que envolvam dados pessoais ou sensíveis. O plano será executado de acordo com os seguintes passos:

- **Identificação e Contenção do Incidente:**
  - Utilização de sistemas de detecção de intrusões (IDS) e ferramentas de monitoramento para identificar atividades anômalas.
  - Isolamento imediato da área afetada para evitar a propagação do incidente.

- **Análise do Impacto e Determinação das Medidas Corretivas:**
  - Avaliação da gravidade do incidente por meio da análise de logs, registros de acesso e sistemas comprometidos.
  - Implementação de medidas corretivas, incluindo a restauração de backups, correções de falhas e reforço dos controles de segurança.

- **Comunicação do Incidente:**
  - Comunicação formal do incidente à Autoridade Nacional de Proteção de Dados (ANPD) e aos titulares afetados em até 72 horas, conforme exigido pelo artigo 48 da LGPD. A comunicação incluirá detalhes sobre a natureza do incidente, dados afetados, medidas corretivas e riscos potenciais.

- **Registro e Aprendizagem:**
  - Registro completo do incidente e das ações adotadas, incluindo causas, resolução e lições aprendidas.
  - Análise pós-incidente para melhorar as políticas de segurança e prevenir incidentes semelhantes no futuro.

Treinamento Contínuo em Proteção de Dados

Objetivos do Programa de Capacitação

A CDSS executa um programa contínuo de treinamento em proteção de dados, focado na conscientização e capacitação dos colaboradores. O treinamento será estruturado da seguinte forma:

- **Treinamentos Periódicos:**
  - Programas de treinamento obrigatórios sobre boas práticas de segurança, privacidade e conformidade com a LGPD, realizados semestralmente.
  - O treinamento terá o dever de conscientização sobre ameaças à segurança da informação e as melhores práticas de proteção de dados, como senhas fortes, criptografia e proteção de dispositivos móveis. Será de suma importância garantir

que os funcionários estejam cientes das ameaças à segurança da informação e saibam como proteger os seus dados e os dados da Companhia Docas de São Sebastião.

- Acompanhamento de mudanças legislativas e novas ameaças cibernéticas para garantir que os colaboradores estejam sempre atualizados.

- **Simulações de Incidentes:**
  Realização de simulações de incidentes de segurança, como vazamentos de dados e ataques de phishing, para garantir que a equipe saiba como reagir adequadamente.

- **Avaliação e Feedback:**
  Após cada treinamento, será realizada uma avaliação de eficácia e um feedback dos participantes, visando melhorar continuamente o conteúdo e a forma de entrega do treinamento.

Monitoramento e Auditoria

- **Monitoramento Contínuo**
  O ambiente de TI é monitorado 24 horas por dia, 7 dias por semana, por meio de ferramentas de detecção de intrusões e análise de tráfego de rede, com foco na identificação de comportamentos suspeitos e possíveis brechas de segurança. O monitoramento incluirá:

- **Monitoramento de Registros:**
  Análise contínua de logs de servidores, aplicativos e dispositivos de rede para detectar qualquer atividade irregular.

- **Ferramentas de Gestão de Vulnerabilidades:**
  Ferramentas automáticas serão utilizadas para identificar vulnerabilidades nos sistemas e infraestrutura, aplicando correções e atualizações de segurança.

4. Regra para Acesso à Informação

Todos os cidadãos têm o direito de solicitar informações públicas não sigilosas mantidas pela Companhia Docas de São Sebastião, sem qualquer restrição indevida ou tratamento discriminatório.

As solicitações devem ser realizadas exclusivamente pelos seguintes canais:

Do Encarregado Pelo Tratamento De Dados Pessoais

Nos termos da Lei Geral de Proteção de Dados Pessoais, Encarregado é a pessoa indicada para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD). Em ato contínuo, há previsão expressa de que o controlador deverá indicar a identidade e informação de contato do mesmo de forma clara e objetiva, no site do Controlador. Algumas das atribuições do encarregado são: aceitar reclamações e comunicações dos titulares, prestar esclarecimentos, receber comunicações da ANPD e orientar funcionários sobre proteção de dados.

O Encarregado pelo Tratamento de Dados será nomeado pelo Diretor Presidente.

Contatos/Reclamações/Dúvidas

Perguntas, comentários ou reclamações sobre esta Política entre em contato conosco através do Formulário disponível no site da Companhia Docas de São Sebastião, no endereço https://portoss.sp.gov.br/home/fale-conosco/ouvidoria/;

- Sistema Estadual de Ouvidorias, disponível em https://fala.sp.gov.br/;
- Pedido de acesso à informação formalizado conforme a legislação vigente.

A Companhia deve responder às solicitações no prazo máximo de 20 dias úteis, contados a partir da data do protocolo do pedido. Esse prazo pode ser prorrogado por mais 10 dias úteis, mediante justificativa formal e comunicação prévia ao solicitante.

O acesso a informações poderá ser negado nos seguintes casos:

- Quando se tratar de informações classificadas como sigilosas, nos termos da legislação vigente, salvo se solicitadas pelo próprio titular dos dados, mediante comprovação de identidade e seguir os critérios estabelecidos pela **Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018)**;
- Quando o fornecimento da informação puder comprometer a segurança institucional, a privacidade dos usuários, servidores ou terceiros envolvidos;
- Quando o pedido for considerado genérico, desproporcional ou envolver esforços excessivos e injustificados de busca.

Caso o acesso seja negado, o solicitante será informado dos motivos, bem como dos meios disponíveis para apresentar recurso administrativo, conforme previsto na legislação aplicável.

A Companhia Docas de São Sebastião assegurará que todos os dados pessoais sejam tratados em conformidade com os princípios e normas da LGPD, garantindo a privacidade e segurança das informações.

5. Cookies e Categorias de Dados Coletados

5.1. Cookies

Cookies são pequenos arquivos de texto armazenados em dispositivos ao acessar um site. Eles registram ações e preferências do usuário para oferecer uma experiência personalizada. Embora não identifiquem diretamente os usuários, permitem reconhecê-los e adaptar os serviços oferecidos.

5.1.2 Finalidades dos cookies

O Porto de São Sebastião utiliza cookies para:

- Facilitar o uso de seus sites e aplicativos.
- Personalizar a experiência do usuário.
- Compilar dados sobre o uso de seus serviços, aprimorando conteúdos e estruturas.

5.1.3 Tipos de cookies e finalidades específicas:

- **Essenciais:** Garantem segurança, verificação de identidade e funcionalidades de rede. Não podem ser desativados.
- **Funcionais:** Registram preferências do usuário para melhorar a personalização da experiência.
- **Sessão:** Mantêm o usuário logado, lembram preferências e armazenam itens de carrinho de compras.
- **Marketing:** Exibem anúncios personalizados com base no comportamento de navegação, como páginas visitadas ou produtos pesquisados.

5.1.4. Como os dados são coletados pelo Porto de São Sebastião:

- **Dados ativos:** Informações fornecidas diretamente pelo usuário, como no momento do cadastro.
- **Dados automáticos:** Informações coletadas durante o uso da plataforma, como comportamento de navegação.

Essas informações auxiliam na melhoria contínua dos serviços e na adequação às preferências e necessidades dos usuários.

5.1.5. Dados Coletados pelo Porto de São Sebastião

O Porto de São Sebastião coleta dados de duas formas principais, descritas abaixo:

- **Dados fornecidos ativamente pelo usuário:**

o Informações pessoais inseridas durante o cadastro ou preenchimento de formulários, como:
- Nome completo
- E-mail
- Telefone de contato
- Dados profissionais (se aplicável)
- Preferências de comunicação

- **Dados coletados automaticamente durante a navegação na plataforma:**

o Informações técnicas sobre o dispositivo utilizado, incluindo:
- Endereço IP
- Tipo e versão do navegador
- Sistema operacional
- Resolução de tela

o Dados de navegação e comportamento:
- Páginas acessadas e tempo de permanência
- Produtos ou serviços pesquisados
- Cliques, interações e preferências identificadas
- Localização aproximada (se autorizada pelo dispositivo)

5.1.6 Esses dados são utilizados exclusivamente para:

- Personalizar a experiência de navegação.
- Garantir a funcionalidade e segurança da plataforma.
- Melhorar serviços e conteúdos com base em análise de comportamento.
- Comunicações relevantes, alinhados aos interesses do usuário.

Todas as informações são tratadas conforme a legislação vigente e com medidas de segurança adequadas para proteger os dados dos usuários.

6. Utilização de Recursos de Informação

É responsabilidade de todos cuidarem da integridade e bom funcionamento dos recursos de informação da COMPANHIA DOCAS DE SÃO SEBASTIÃO.

Todo acesso a recursos de tecnologia da informação (servidores, estações de trabalho, aplicativos e outros) deve ser sempre autenticado por contas de usuários e senhas.

As contas de usuários devem ser individuais.

A senha é de responsabilidade do usuário. A área de TI não possui acesso a senha do usuário, que é pessoal e intransferível.

Caso o usuário esqueça a sua senha, este deverá entrar em contato imediatamente com a área de TI.

O desbloqueio da conta será efetuado apenas pelo administrador do sistema.

Os recursos de tecnologia da informação devem ser utilizados, exclusivamente para as atividades competentes à COMPANHIA DOCAS DE SÃO SEBASTIÃO.

- Não é permitido o uso de recursos de informação de propriedade particular nas instalações da empresa, exceto quando autorizado pelo gestor da área direta.
- Não é permitido o uso de recursos de informação para prestação de serviços a terceiros, exceto quando autorizado pelo gestor da área direto.

A área de TI é responsável por manter atualizado o inventário dos equipamentos e softwares da Empresa.

A área de TI é a responsável pela validação de aplicativos, devendo efetivar a aceitação formal após cumprir os processos de testes e homologação, para que seu uso seja disponibilizado.

Não é permitida a utilização de software não adquirido oficialmente pela Empresa, exceto gratuitos ou livres, bem como cópias destes não licenciados, sem previa autorização e homologação pela área de TI. O usuário responsabilizado pela utilização desses tipos de software será punido conforme previsto na CLT e na legislação em vigor.

- Exceções devem ser comunicadas à área de TI para que sejam tomadas as providências necessárias a fim de que a utilização do recurso esteja dentro do nível de segurança definido pela Empresa;
- A utilização dos softwares da empresa se dará com a análise das reais necessidades dos usuários pela área de TI.

Os equipamentos portáteis são tratados com cuidados adicionais, tais como controle de acesso e cadastramento do dispositivo.

A COMPANHIA DOCAS DE SÃO SEBASTIÃO pode inspecionar todo e qualquer arquivo eletrônico que transita na sua rede ou que está armazenado em qualquer equipamento pertencente à Companhia. Esta medida tem por objetivo assegurar que procedimentos ou informações que possam causar algum prejuízo à empresa ou a terceiros sejam divulgados.

A inspeção de arquivos eletrônicos só poderá ser realizada por pessoa indicada e autorizada para esta atividade, pertencente à Área de TI.

É expressamente proibido:

- O acesso, exibição, edição, cópia, armazenamento e distribuição de material de conteúdo pornográfico e ou que expressem ou promovam algum tipo de discriminação;
- O armazenamento, utilização e distribuição de aplicações e softwares pirateados;
- Acesso remoto de qualquer natureza sem a devida autenticação;
- Utilização de mídias removíveis (Pen Drive, CDROM, DVDROM, CD/DVD, etc.), exceto quando aprovado por escrito pela chefia imediata e encaminhado para área de TI.
- O acesso aos sistemas (Correio eletrônico, Internet, Intranet e Sistemas) será bloqueado durante o período de afastamento do funcionário (Férias e Licenças) e deverá ser comunicado pelo departamento de RH.
- A inserção de dados classificados como confidenciais ou não autorizados em ferramentas de inteligência artificiais publicas, ou que descumpram a legislação vigente (LGPD).

7. Regras Específicas

Regra de Segurança para Acesso aos Ambientes Físicos Restritos do Departamento de TI:

Controle de Acesso

Para garantir a proteção das informações e dos ativos físicos do Departamento de TI, o controle de acesso aos ambientes físicos restritos deve ser implementado conforme as diretrizes a seguir:

Identificação e Autenticação:

- Todo indivíduo, incluindo servidores e visitantes, deve realizar o processo de identificação e autenticação antes de acessar as áreas restritas.
- É obrigatória a utilização de crachás, cartões magnéticos ou dispositivos biométricos faciais para autenticação de acesso.

Gerenciamento de Controle de Acesso:

- O acesso aos ambientes físicos restritos será concedido somente às pessoas autorizadas, com base em suas funções e responsabilidades.
- As permissões de acesso devem ser revisadas periodicamente para garantir que estejam alinhadas às necessidades organizacionais.
- Visitantes devem ser previamente registrados e acompanhados por um responsável autorizado durante sua permanência nas áreas restritas.

Vigilância e Segurança Física:

- Os ambientes restritos devem ser monitorados 24 horas por dia, por meio de sistemas de vigilância como câmeras de segurança e sensores de acesso.
- Portas e janelas dos ambientes restritos devem permanecer trancadas, utilizando sistemas de trancamento automatizados.

Cumprimento da Política de Controle de Acesso:

- Todos os usuários que acessam os ambientes restritos devem seguir as diretrizes estabelecidas na Política de Controle de Acesso da organização.
- Qualquer incidente ou tentativa de violação de segurança deve ser imediatamente relatada à equipe responsável para análise e ação corretiva.

Monitoramento e Medidas Corretivas:

- O controle de acesso será monitorado regularmente por meio de registros de log e auditorias internas.
- A organização reserva-se o direito de aplicar medidas corretivas e disciplinadoras em casos de descumprimento das normas de acesso.

Abertura de Chamados

Todas as solicitações relacionadas à área de TI podem ser encaminhadas diretamente por meio de três canais de atendimento: sistema de Helpdesk, e-mail ou telefone. O sistema de Helpdesk está disponível para o registro e

acompanhamento de chamados, garantindo maior organização e priorização das demandas. Em qualquer um dos canais, o horário de atendimento de chamados será em tempo integral: 24 horas por dia, sete dias por semana, todos os dias do ano, inclusive sábados, domingos e feriados.

7.1. Antivírus

A área de TI é a responsável pela divulgação de informações sobre vírus de computador. Qualquer outra informação desta natureza, enviada por entidade externa ou funcionários deve ser comunicada a ela para análise e diagnóstico.

Deve ser utilizado somente o software de proteção antivírus homologado pela área de TI da Empresa.

O sistema antivírus utilizado na estação deve permanecer sempre atualizado e ativo sem modificações na sua configuração, sendo padronizada e protegendo assim arquivos compartilhados via rede local ou Web.

Todo meio de armazenamento (discos flexíveis, zip disk, CD-ROM´s, fitas, Pen Drive e outros) deve ser verificado pelo software antivírus antes de ser acessado, e em caso de gravação, deverá ter a devida autorização da área de TI.

7.2. Contas e Senhas

A regra de composição de senhas deve obedecer aos seguintes pontos:

- Manter confidencialidade sobre a senha. A senha deve ser do conhecimento exclusivo do próprio usuário, não devendo ser divulgada.
- Após cinco tentativas de identificação de usuário, consecutivas e malsucedidas, será bloqueado de acesso do usuário à rede ou ao sistema. Sua senha deverá ser recadastrada, o que deve ser feito seguindo-se os procedimentos vigentes de cadastramento de senha, através de solicitação à área de TI.
- Recomenda-se mudar a senha a cada 45 (quarenta e cinco) dias. Havendo a qualquer momento indicação ou suspeita de comprometimento a senha deverá ser substituída imediatamente.
- Senhas totalmente alfabéticas não serão permitidas. As senhas precisam seguir os seguintes critérios:

  - **Complexidade:**
    As senhas devem ser complexas e difíceis de prever, contendo no mínimo **12 caracteres**. Devem incluir:

- Letras maiúsculas (A-Z);
- Letras minúsculas (a-z);
- Números (0-9);
- Caracteres especiais (ex.: @, #, $, %).

- **Troca Periódica:**

- As senhas deverão ser substituídas a cada 60 dias, sendo o acesso bloqueado automaticamente até que a nova senha seja criada e registrada no sistema. O sistema notificará os usuários da proximidade do prazo de troca para evitar bloqueios;

- Reutilização de Senhas:

- Não será permitido reutilizar as últimas quatro senhas utilizadas. Cada sistema e conta deve possuir uma senha única e distinta, de forma a minimizar riscos associados ao comprometimento de múltiplos acessos.

- Não se recomenda uso de triviais, por ser de fácil identificação, não devem ser utilizadas. Itens que não podem fazer parte da senha: meses do ano, dias da semana ou qualquer outro dado relativo a datas, nomes de familiares, iniciais, placas de carro, nomes comuns à empresa, números de telefone, identificação de usuário (userid), nome do usuário, grupo do usuário, sequência numérica com mais de dois caracteres idênticos consecutivos, etc.
- Práticas Aceitáveis

- **Armazenamento:**

- Utilize um gerenciador de senhas seguro, quando necessário, para guardar informações adicionais;
- Não armazene senhas em locais de fácil acesso ou em texto simples;
- Não compartilhe suas senhas com outras pessoas.

- C**ompartilhamento:**

- O compartilhamento de senhas entre usuários é **proibido**, exceto em situações excepcionais e com **autorização prévia de um superior**.

- **Proteção:**

- As senhas devem ser protegidas contra acesso não autorizado;
- Bloqueie a tela do computador sempre que se afastar de sua estação de trabalho;
- Evite digitar senhas em dispositivos ou redes não confiáveis.

- **Responsabilidades**

- **Usuários:**
  É responsabilidade dos usuários criar senhas fortes e seguras, além de notificar **imediatamente o departamento de TI** caso haja suspeita de comprometimento de suas senhas.

- **Departamento de TI:**

O departamento de TI será responsável por gerenciar o **Active Directory do Windows Server**, garantindo que as senhas estejam armazenadas de forma segura e em conformidade com os requisitos estabelecidos, além de fornecer suporte aos usuários em caso de incidentes relacionados à segurança.

7.3. Compartilhamento

Não é permitido o compartilhamento de unidades físicas e/ou lógicas (unidades de disco flexível, CD-ROM's, pastas, diretórios, arquivos) de estações de trabalho. A transferência de arquivos entre estações deve ser realizada através de um diretório de área de transferência na rede.

7.4. Aquisição e Desenvolvimento de Software

O objetivo desta norma é definir os padrões e procedimentos para a aquisição, desenvolvimento e manutenção de sistemas de informação, para garantir a disponibilidade contínua dos serviços oferecidos por esses sistemas. Visa minimizar os riscos para a Companhia Docas de São Sebastião, garantindo a confidencialidade, integridade e disponibilidade dos dados. É fundamental que os sistemas de informação a serem utilizados estejam de acordo com os padrões estabelecidos, a fim de proporcionar uma base sólida para a operação eficiente e segura das atividades da Companhia.

Diretrizes para aquisição, desenvolvimento e manutenção de sistemas :

Os procedimentos de aquisição, desenvolvimento e manutenção dos sistemas de informação devem aderir a uma metodologia formal, que seja fundamentada em

uma análise crítica abrangente. Essa análise deve considerar aspectos relacionados às exigências legais em vigor e aos padrões de segurança da informação.

O sistema de informação deve passar por uma validação de segurança visando minimizar os riscos, possíveis vulnerabilidades, normas de segurança de informações. Será obrigatória a assinatura de Termo de Compromisso ou Acordo de Confidencialidade por parte da prestadora de serviços, conforme contrato assinado entre as partes, garantindo que os dados disponíveis na aplicação só possam ser acessados pelos usuários autorizados.

Os contratos assinados com prestadores de serviços terceirizados devem conter termos de sigilo, e as regras de contratação e desenvolvimento seguem sempre as diretrizes estabelecidas. As regras de contratação seguem os critérios da Lei de Licitações Públicas nº 13.303, visando sempre a economia e a ampla concorrência.

Todo e qualquer evento de segurança detectado deve ser reportado para área responsável onde será categorizado, priorizado e tratado por uma equipe designada pelo responsável do departamento de Tecnologia da Informação, definindo-se um procedimento para gerenciar incidentes.

Aquisição de Softwares de Prateleira

- Nenhum software poderá ser adquirido sem prévia avaliação da área de Tecnologia da Informação (TI).
- Caso o software seja destinado a um departamento específico, a área demandante será responsável por:

  - Elaborar um estudo de viabilidade;
  - Justificar a necessidade da aquisição.

- A área técnica solicitante também será responsável pela avaliação dos critérios técnicos, enquanto à área de TI caberá validar questões de segurança e instalação.
- Todos os softwares e programas utilizados pela Companhia devem ser previamente homologados pela área de TI.

Desenvolvimento de Sistemas

- O desenvolvimento de sistemas deverá seguir uma metodologia formal, incluindo documentação adequada, uso de ferramentas de gestão apropriadas e controle rigoroso de mudanças e versões.

- Testes de segurança, homologação e validação são obrigatórios antes da implantação de qualquer nova versão em ambiente de produção.
- O acesso ao ambiente de produção será restrito a usuários autorizados formalmente pelo gestor da área responsável.
- A base de dados utilizada no ambiente de homologação deve ser exclusivamente destinada a testes.
- Antes de disponibilizar uma nova versão de qualquer aplicação no ambiente de produção, o usuário deverá:

  - Realizar testes de validação;
  - Formalizar a homologação;
  - Autorizar a liberação da nova versão para produção.

- O ambiente de produção terá acesso restrito a usuários autorizados pelo gestor responsável, minimizando riscos e acessos indevidos.
- O departamento de TI deverá garantir a efetividade do processo de gestão de mudanças, analisando o impacto e minimizando os riscos associados a alterações em diferentes ambientes.
- A atualização de códigos-fonte somente será realizada mediante autorização formal, em conformidade com os procedimentos de controle de mudanças e versões.
- Para garantir continuidade, segurança e evitar alterações não registradas ou autorizadas:

  - Os acessos aos códigos-fonte serão restritos e controlados, incluindo restrições específicas para a área de infraestrutura.
  - Sempre que possível, será priorizado o uso de licenças que não exijam o compartilhamento do código-fonte.
  - Todo código fonte gerado deve ser armazenado em local seguro restritos e controlados, indicado pela equipe de infraestrutura.

- Informações sensíveis em códigos gerados (como em HTML) deverão ser suprimidos para evitar exposição de dados.

Senhas, Armazenamento, Acesso, Comunicação, Segurança da Informação e Backups

- Estes aspectos devem seguir rigorosamente os critérios definidos na Política de Segurança da Informação da Companhia Docas de São Sebastião.

- São exigidos padrões elevados de segurança, como autenticação forte, restrição de acessos, uso de criptografia e monitoramento contínuo para evitar vulnerabilidades.
- A política inclui controle de senhas, segurança na comunicação (como uso de HTTPS e VPNs), além de diretrizes para backups e restauração de dados.

Contratação de serviços em nuvem (cloud computing)

Diretrizes para o uso de serviços em nuvem pela Companhia Docas de São Sebastião, em conformidade com a LGPD. Ele aborda os benefícios da nuvem, como escalabilidade e redução de custos, e enfatiza a importância de garantir a segurança e privacidade das informações.

Os principais modelos de nuvem destacados são:

- **IaaS**: Recursos de TI virtualizados, como servidores e armazenamento, oferecidos por provedores como AWS, Azure e GCP.
- **PaaS**: Plataformas para desenvolvimento e gerenciamento de aplicativos.
- **SaaS**: Aplicativos prontos para uso via internet, sem necessidade de instalação local.

Diretrizes para contratação de serviços em nuvem

Avaliação da necessidade

- Identificar benefícios esperados e riscos associados à migração para a nuvem, com ênfase em segurança e conformidade regulatória.
- Avaliar deficiências e necessidades de melhoria dos sistemas existentes.
- Definir claramente os requisitos técnicos e de negócio que os serviços em nuvem devem atender.

Seleção do provedor

- Garantir que o provedor esteja em conformidade com a LGPD e outras regulamentações aplicáveis.
- Avaliar detalhadamente as políticas de segurança e privacidade do provedor, como criptografia de dados, controle de acesso e práticas de gerenciamento de incidentes.
- Exigir contratos detalhados que estabeleçam:
  - Responsabilidades de ambas as partes.
  - Termos de serviço, níveis de serviço (SLAs) e políticas de segurança.
  - Procedimentos claros para encerramento de contratos, com migração segura e destruição de dados, evitando acessos não autorizados.

- Garantir cláusulas contratuais que permitam auditorias periódicas para verificar conformidade com as políticas acordadas.
- Avaliar a reputação e a capacidade técnica do provedor em oferecer serviços confiáveis e de alta disponibilidade.

Monitoramento e gestão

- O provedor deve fornecer ferramentas robustas para que a Companhia monitore a segurança e a conformidade dos serviços em nuvem.
- Implementar mecanismos para identificar e responder rapidamente a incidentes de segurança.
- Realizar revisões periódicas das práticas de gestão de dados e conformidade com a LGPD, ajustando políticas e procedimentos conforme necessário.
- Garantir análise contínua de logs e eventos, em conformidade com os procedimentos internos de registro e monitoramento.
- Promover treinamento contínuo para os funcionários sobre o uso seguro da nuvem e a proteção de dados.

Backup

- O provedor contratado será responsável por executar os procedimentos de backup definidos pela Companhia Docas de São Sebastião.
- Backups devem ser realizados regularmente, respeitando cronogramas predefinidos e cobrindo todos os dados críticos, como bancos de dados, sistemas de arquivos e configurações.
- O provedor deve apresentar relatórios periódicos com evidências documentadas da realização dos backups.
- Os backups devem ser armazenados em locais seguros, protegidos contra acessos não autorizados e desastres.
- Em caso de perda ou corrupção de dados, o provedor deve iniciar imediatamente os procedimentos de restauração para minimizar o tempo de inatividade.
- Testes regulares de restauração devem ser realizados para garantir a integridade e eficácia dos backups.

7.5. Correio eletrônico

O correio eletrônico deve ser utilizado exclusivamente para troca de mensagens que atendam funções operacionais da Empresa.

Todo conteúdo veiculado pelo correio eletrônico deve respeitar os padrões estabelecidos pela empresa, conforme procedimentos específicos estabelecidos pela área de TI.

A COMPANHIA DOCAS DE SÃO SEBASTIÃO pode inspecionar todo e qualquer arquivo eletrônico ou e-mails institucionais. Esta medida tem por objetivo assegurar que procedimentos ou informações que possam causar algum prejuízo à empresa ou a terceiros sejam divulgados.

Utilização de e-mail institucionais são de uso único e exclusivo de funcionários, estagiários, menores aprendizes e departamentais da Empresa, sendo:

- Funcionários: Funcionários contratados em regime CLT.
- Estagiários e menores aprendizes: Estagiários com contrato assinado e ativo.
- Departamentais: Utilizado para departamentos enviarem comunicados ou solicitarem informações externas (o chefe do departamento ficará responsável por esse correio).

Prestadores de serviços deverão utilizar correios eletrônicos disponibilizados pela empresa CONTRATADA, ou seja, não terão e-mail corporativo da COMPANHIA DOCAS DE SÃO SEBASTIÃO, as exceções devem ser autorizadas e o chefe da área ficará responsável por esse correio.

O tamanho máximo de mensagem dos e-mails é:

Utilização via Webmail:
- Limite de 10 MB para envio
- Limite de 10 MB para recebimento

Utilização via Outlook
- Limite de 10 MB para envio
- Limite de 10 MB para recebimento

Obs: Ao enviar uma mensagem com um arquivo anexado, esse arquivo é convertido para texto e isso pode aumentar o tamanho da mensagem, em alguns tipos de arquivos chega a dobrar o tamanho do arquivo original, o que pode influenciar no envio ou recebimento de mensagens.

O e-mail receptor da mensagem poderá ter capacidade menor do que a utilizada na COMPANHIA DOCAS DE SÃO SEBASTIÃO. Como parâmetro de mercado, há um bloqueio de anexo(s) superior(es) a: 2 à 10 MB para ENVIO e 2 à 10Mb para RECEBIMENTO. Portanto, sugerimos pedir confirmação do recebimento de e-mail entre 2 à 10 MB enviado para endereços externos.

É expressamente proibido:

- O envio de mensagens sem identificar a origem ou utilizando-se de conta de correio eletrônico de outras pessoas sem autorização destas;
- O envio de mensagens com vírus, arquivos do tipo “Cavalo de Tróia” e mensagens não solicitadas, como “spam”, “junk mail” e correntes;
- O acesso ao conteúdo das mensagens enviadas por correio eletrônico por pessoa não indicada e autorizada.
- Enviar mensagens não solicitadas para múltiplos destinatários, exceto se a mesma for relacionada a uso legítimo da empresa (ex. correntes, casos interessantes, piadas);
- Enviar qualquer mensagem através dos meios eletrônicos que torne seu remetente e/ou a COMPANHIA DOCAS DE SÃO SEBASTIÃO vulneráveis a ações civis ou criminais;
- Divulgar informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização expressa e formal concedida pelo proprietário deste ativo de informação;
- Falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários;
- Produzir, transmitir ou divulgar mensagem que:

a) Contenha qualquer ato ou forneça orientação que conflite ou contrarie os interesses da COMPANHIA DOCAS DE SÃO SEBASTIÃO;

b) Inclua imagens criptografadas ou de qualquer forma mascaradas;

c) Tenha conteúdo considerado impróprio, obsceno ou ilegal;

d) Seja de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico etc.;

e) Contenha perseguição preconceituosa baseada em sexo, raça, incapacidade física ou mental ou outras situações protegidas;

f) Tenha fins políticos locais ou do país (propaganda política) e religiosos;

g) Inclua material protegido por direitos autorais sem a permissão do detentor dos direitos.

h) Que contenham dados pessoais não autorizados, de acordo com as diretrizes da LGPD.

7.6. Internet

A Internet é um recurso de informação fornecido pela empresa com o objetivo de aumentar a produtividade dos processos de trabalho. Seu uso deve ser exclusivo para atividades da Empresa.

Os funcionários e terceiros não poderão alterar as configurações do navegador web, principalmente as configurações de segurança. Estas configurações são feitas e mantidas pela equipe de TI (Help Desk).

Todos os sites estarão liberados para o acesso ao usuário (não haverá restrições), e todos os sites visitados serão monitorados e caso necessário será gerado um relatório com o nome do usuário e a lista dos sites que ele visitou e encaminhado para a chefia Direta das áreas.

É expressamente proibida:

- A participação em salas de bate-papo (chat-rooms) em nome da empresa, sem a devida autorização;
- O uso de recursos da empresa para participar de jogos pela Internet ou descarregar arquivos (download) de entretenimento.
- A utilização de redes sociais para fins particulares, exceto quando autorizado pelo gestor da área.

O uso de redes sociais será permitido exclusivamente para finalidades relacionadas ao trabalho, desde que realizado em dispositivos corporativos fornecidos pela organização, exceto nos casos em que houver autorização expressa do gestor da área.

Utilização de redes sociais:

- **Finalidade:** O uso de redes sociais é permitido exclusivamente para atividades relacionadas ao trabalho.
- **Exceções:** Situações fora dessa finalidade devem ser previamente autorizadas pelo gestor responsável.
- **Dispositivos:** O acesso deve ser feito unicamente por meio de aparelhos corporativos fornecidos pela organização.

7.7. Acesso à Rede e Sistemas

A criação de acesso ao ambiente de rede e Sistema ORACLE (ERP), Sistema gestão portuário (Sisport) e sistema de monitoramento (CFTV) (ISS) deverá ser autorizada pela chefia imediata.

O chefe imediato deverá enviar um e-mail à área de TI para que seja aprovada a criação dos acessos. Dado o recebimento do e-mail, a TI disponibilizará os acessos conforme solicitado.

7.8. Regra de uso para Redes Wi-Fi

Segregação de Redes Wi-Fi

A infraestrutura de rede Wi-Fi é dividida em duas redes independentes:

- **Rede Corporativa:** Exclusiva para equipamentos pertencentes à Companhia Docas de São Sebastião.
- **Rede de Visitantes:** Destinada a equipamentos de terceiros, como celulares e note books de visitantes, prestadores de serviço e outros equipamentos não corporativos.

Acesso à Rede Corporativa

Apenas computadores corporativos devidamente cadastrados e registrados no domínio da Companhia Docas terão acesso à rede corporativa.

Dispositivos móveis, tablets e quaisquer outros equipamentos não pertencentes à Companhia Docas estão estritamente proibidos de acessar a rede corporativa.

Acesso à Rede de Visitantes

Equipamentos não corporativos, incluindo dispositivos móveis e laptops de visitantes, terão acesso somente à rede de visitantes.

O acesso à rede de visitantes será condicionado à:

- Autorização prévia por um responsável designado da Companhia Docas.

- Registro do dispositivo pelo endereço MAC (Media Access Control Address) na lista de controle de acesso da rede de visitantes.

Isolamento das Redes

A rede de visitantes será totalmente segregada da rede corporativa, com configurações que impeçam qualquer comunicação direta entre as duas redes. A rede de visitantes terá acesso limitado exclusivamente à internet, sem qualquer permissão para acessar servidores, sistemas ou arquivos da Companhia Docas.

Manutenção e Monitoramento

Ferramentas de monitoramento serão utilizadas para identificar tentativas de acesso não autorizado e atividades suspeitas em ambas as redes. Relatórios de acesso e uso da rede serão gerados regularmente para auditoria e análise de segurança.

Conformidade com o Marco Civil da Internet (Lei nº 12.965/2014)

Esta regra está em conformidade com o **Marco Civil da Internet**, assegurando o cumprimento das diretrizes de segurança, privacidade e proteção de dados.

Todas as medidas implementadas visam garantir:

- A segurança dos dados armazenados e transmitidos nas redes da Companhia Docas;
- A proteção da privacidade dos usuários das redes Wi-Fi, em conformidade com as diretrizes legais aplicáveis;
- A responsabilidade na gestão e operação da infraestrutura de rede, conforme os princípios estabelecidos pela legislação.

Essa política reforça a segurança da infraestrutura da Companhia Docas, assegura a proteção das informações sensíveis e mantém total conformidade com os requisitos legais do Marco Civil da Internet.

7.9. Uso de Impressoras

O uso de impressoras da COMPANHIA DOCAS DE SÃO SEBASTIÃO é para fins corporativos e relacionados às atividades do colaborador dentro da empresa.

As impressoras deverão ficar em locais apropriados e seguros.

Para utilização da impressora será registrado o envio da impressão, possibilitando a identificação do usuário e documento.

Caso necessário um relatório por usuário contendo a quantidade de impressões realizadas por área e por colaborador, por períodos previamente cadastrados, podendo ser mensal, quinzenal, mensalmente, ou outros períodos solicitados via sistema.

7.10. Mesa limpa

Os funcionários e terceiros não poderão deixar documentos com informações críticas em mesas de trabalho, quadro branco, flip chart, impressoras, pontos de envio e recepção de correspondências etc. O tratamento das informações em documentos deverá levar em consideração as classificações da segurança da informação.

7.11. Política de BACKUP e RESTAURAÇÃO

Objetivo:

Estabelecer diretrizes e procedimentos para a execução de backups e restaurações, garantindo a integridade, disponibilidade e confidencialidade dos dados críticos da Companhia Docas de São Sebastião, em conformidade com os requisitos operacionais e regulamentares.

Dados Críticos

Os dados críticos que requerem backups regulares incluem:

- Bancos de dados corporativos (financeiros, operacionais, jurídicos etc.).
- Registros financeiros e contábeis.
- Documentos legais e regulatórios.
- Arquivos de configurações de sistemas e equipamentos (firewall, antivírus, Active Directory, EBS(ERP), Sisport, servidores virtuais etc.).
- Dados de aplicações e imagens essenciais para segurança e operação.
- Esses dados serão priorizados pela sua relevância e impacto na continuidade das atividades da Companhia**.**

Frequência e Retenção dos Backups

Os backups serão realizados seguindo o modelo de retenção em múltiplos níveis:

- Diário: Backup completo de todos os dados críticos, executado diariamente.

- Mensal: Backup completo de todos os dados críticos, executado no último dia do mês.

Período de retenção:

- Backups diários: 14 dias.
- Backups mensais: 5 anos (ou conforme exigências regulatórias).

Métodos de Armazenamento

Os backups serão armazenados em diferentes locais para garantir redundância e segurança:

- Local: Infraestrutura interna da Companhia, incluindo servidores dedicados e dispositivos de armazenamento físico (fitas, discos) em ambientes redundantes.
- Externo: Serviços de armazenamento prestados por empresas especializadas na guarda de backups físicos (fitas magnéticas ou discos rígidos).

Os dados armazenados externamente serão criptografados para garantir a confidencialidade.

Testes de Backup e Restauração

- Testes de restauração (restore) serão realizados semanalmente de forma aleatória para garantir a confiabilidade dos backups.
- Os resultados dos testes serão registrados em logs detalhados, com evidências de sucesso ou falha, e armazenados para auditorias futuras.
- Os testes incluirão a verificação de bancos de dados, aplicações, arquivos e sistemas críticos.

Segurança e Controle de Acesso

- O acesso aos backups será restrito a profissionais autorizados e monitorado por meio de controles de acesso (login, senha e logs de atividade).
- Todos os backups devem ser criptografados utilizando algoritmos reconhecidos como seguros pelo mercado (ex.: AES-256).

Monitoramento e Auditoria

- O processo de backup será monitorado em tempo real por meio de ferramentas específicas para identificar falhas ou interrupções.
- Auditorias periódicas serão realizadas para avaliar a conformidade da política com os requisitos internos e regulatórios.

Responsabilidades

- Equipe de TI: Responsável pela execução, monitoramento e testes de backups.
- Gestores das Áreas: Identificar e informar alterações nos dados críticos.
- Fornecedor de Armazenamento Externo: Garantir a guarda segura e o acesso aos dados armazenados externamente.

Essa política garante a continuidade dos negócios e a proteção das informações críticas contra eventos adversos, assegurando a eficiência operacional e a conformidade regulatória da Companhia Docas de São Sebastião.

7.12. Monitoramento

Todo o ambiente de TI da nossa organização é monitorado de forma contínua e preventiva. Esse monitoramento abrange todos os sistemas, redes e equipamentos, com o intuito de garantir o funcionamento adequado e identificar qualquer anomalia ou possível falha antes que ela cause impactos significativos. Através ferramentas avançadas de monitoramento para assegurar o pleno funcionamento dos recursos tecnológicos.

O monitoramento constante permite antecipar problemas e agir rapidamente, minimizando riscos e otimizando a resolução de incidentes. O foco está na prevenção de falhas, interrupções e brechas de segurança, proporcionando maior confiabilidade e disponibilidade dos serviços e garantindo que os processos críticos não sejam afetados. Essa vigilância contínua é uma parte essencial da estratégia de gestão de TI.

7.13. Descarte de Equipamentos

Todo material eletrônico de TI a ser descartado, deve ser encaminhado à área de Tecnologia da Informação com a listagem e descrição dos equipamentos a serem descartados.

Todo equipamento a ser descartado passará por uma inspeção pela área de Tecnologia da Informação onde será destruída toda a informação armazenada em seguida é elaborado um laudo técnico descrevendo o descarte.

O material a ser descartado com NP (número patrimonial) deverá ser relacionado e a listagem com a descrição dos equipamentos encaminhada à área da controladoria para que seja feira a baixa patrimonial do bem.

Todo descarte de material eletrônico deverá ser executado por empresas que atendam as normas ambientais e da ISO 14.001.

8. Aderência à Política de Segurança da Informação e Sanções

Todos os usuários devem ter conhecimento dos conceitos de segurança da informação e da Política de Segurança da Informação.

É de responsabilidade do funcionário e/ou terceiro o uso e sigilo das informações digitais ou não, de sua competência conforme concordado no termo de sigilo de informações assinado por todos, onde se comprometem sobre toda e quaisquer informações que venham a ser divulgadas por pessoas ou instituições inadvertidamente.

Os usuários devem informar a sua chefia quando as informações ou aplicações críticas forem encontradas sem o tratamento de segurança correto.

As áreas de Recursos Humanos e TI devem ser comunicadas imediatamente quando for encontrada alguma infração das normas citadas e junto com a área responsável pela inspeção avaliar a situação e tomar as medidas cabíveis em conjunto com a chefia do funcionário.

A área de Recursos Humanos fica responsável por comunicar imediatamente a área de TI, a admissão e o desligamento de funcionários e estagiários da instituição para que possam ser tomadas as ações cabíveis (Bloqueio e criação de e-mail institucional, bloqueio e criação de usuário de rede, e configuração e backup das informações do seu desktop).

Quando houver funcionários terceirizados o gestor do contrato fica responsável por comunicar imediatamente a área de TI, a admissão ou o desligamento destes funcionários da instituição para que possam ser tomadas as ações cabíveis nestas situações como (Bloqueio do e-mail institucional, usuário de rede, e backup das informações do seu desktop).

O não cumprimento desta Norma caberá:

- Na primeira infração uma advertência e anotação no prontuário;

- Na segunda infração, advertência com indicação de reincidência e anotação no prontuário;
- Na terceira infração, o empregado será passível de medida disciplinar.

Nos casos em que a infração corresponder a atividades ilegais, ou ainda incorrer em dano à empresa ou a terceiros, a Companhia Docas de São Sebastião poderá deliberar pela demissão por justa causa, dispensando as advertências, não eximindo o infrator das medidas previstas pela legislação vigente. A COMPANHIA DOCAS DE SÃO SEBASTIÃO cooperará ativamente com as autoridades nesses casos.

No caso de prestadores de serviços, a Companhia Docas de São Sebastião poderá optar pela rescisão de contrato do prestador na ocorrência de tais fatos.

Os funcionários que desrespeitarem as determinações sofrerão ações da empresa com base na CLT e na legislação em vigor.

9. Considerações Finais

A Política de Segurança da Informação (PSI) da Companhia Docas de São Sebastião foi elaborada com o propósito de garantir a proteção dos dados e ativos digitais, promovendo um ambiente seguro, ético e em conformidade com as legislações vigentes, como a Lei Geral de Proteção de Dados Pessoais (LGPD).

O compromisso de todos os colaboradores, fornecedores e parceiros é fundamental para a eficácia das medidas apresentadas neste documento. A observância das diretrizes estabelecidas aqui assegura a confidencialidade, integridade e disponibilidade das informações corporativas, essenciais para o funcionamento seguro e eficiente da Companhia.

Quaisquer exceções ou ajustes a esta política serão submetidos à aprovação da diretoria e comunicados às áreas pertinentes, garantindo a transparência e o alinhamento organizacional.

Por fim, a adesão às normas aqui apresentadas reforça o compromisso da Companhia com a excelência operacional e com a proteção das informações sensíveis, contribuindo para a manutenção de um ambiente de trabalho confiável e sustentável.

SUMÁRIO DE REVISÕES			
Rev.	**RD/CONSAD**	**Data**	**Descrição**
0	140ª Reunião	28/06/2018	Emissão original

	CONSAD		
1ª	DIRETORIA EXECUTIVA	12/01/2021	Revisão geral
2ª	DIRETORIA EXECUTIVA CONSAD	13ª RD, 25/03/2025 245ª CONSAD, 30/04/2025	Revisão geral, com base na Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018);