CODERN
AUTORIDADE PORTUÁRIA

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO – PSI 2025/2028 (PL.1030.01)

Dezembro/2025

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO – PSI 2025/2028

<table>
<tr><td rowspan="4"></td><td colspan="4">COMPANHIA DOCAS DO RIO GRANDE DO NORTE - CODERN</td></tr>
<tr><td colspan="3">Instrumento Normativo (IN)</td><td>Código:
PL.1030.01</td></tr>
<tr><td>Diretoria Responsável/APMC:
DP</td><td colspan="2">Gerência Responsável:
GEDADOS</td><td>URN:
GEDADOS</td></tr>
<tr><td>Data de criação:
10/12/2025</td><td>Início da Vigência:
10/12/2025</td><td>Próxima Revisão:
10/12/2029</td><td>Aprovação:
DIREXE</td></tr>
<tr><td colspan="3">Título: POLÍTICA DE SEGURANÇA DA INFORMAÇÃO – PSI 2025/2028</td><td>Versão:
1.0 - Original</td></tr>
</table>

APROVAÇÃO

Aprovada pela Resolução nº 1137, conforme ATA da 2013ª reunião da Diretoria Executiva da Companhia Docas do Rio Grande do Norte – DIREXE, realizada em 10 de dezembro de 2025.

Aprovada pela Deliberação nº 072/2025, conforme ATA da 768ª reunião da Diretoria Executiva da Companhia Docas do Rio Grande do Norte – DIREXE, realizada em 19 de dezembro de 2025.

SUMÁRIO

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

CAPÍTULO I
DA ABRANGÊNCIA

Art. 1º Este Plano aplica-se a todas as unidades organizacionais da CODERN, abrangendo a Sede em Natal/RN, as administrações portuárias vinculadas, os prestadores de serviços, parceiros institucionais e fornecedores de TIC. Sua execução envolve todos os diretores, gestores e colaboradores, assim como as partes interessadas externas.

CAPÍTULO II
DA FUNDAMENTAÇÃO LEGAL E REFERÊNCIAS

Art. 2º O PSI da CODERN tem amparo legal nos seguintes instrumentos principais:

I - Lei nº 13.303/2016 – Dispõe sobre o estatuto jurídico das empresas públicas e sociedades de economia mista, estabelecendo princípios de governança, controles internos e gestão de riscos;

II - Decreto nº 9.637/2018 – Institui a Política Nacional de Segurança da Informação (PNSI) no âmbito da Administração Pública Federal;

III - Instrução Normativa nº 5, de 30 de agosto de 2021 – GSI/PR – Estabelece diretrizes para a implementação da PNSI e para a gestão da segurança da informação e segurança cibernética nos órgãos e entidades da Administração Pública Federal;

IV - Lei nº 13.709/2018 – Lei Geral de Proteção de Dados (LGPD) – Dispõe sobre o tratamento de dados pessoais e reforça os princípios de segurança e confidencialidade da informação;

V - ABNT NBR ISO/IEC 27001:2006 – Define requisitos para o Sistema de Gestão da Segurança da Informação (SGSI);

VI - ABNT NBR ISO/IEC 27002 (17799:2005) – Estabelece boas práticas e controles de segurança da informação;

VII - ABNT NBR ISO/IEC 27017:2016 – Diretrizes específicas para segurança da informação em serviços de computação em nuvem;

VIII - ABNT NBR ISO/IEC 23894:2023 – Orienta sobre a gestão de riscos relacionados à segurança da informação e à cibersegurança.

CAPÍTULO III
DISPOSIÇÕES INICIAIS

Art. 3º "Segurança da Informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio" (ABNT NBR ISO/IEC 17799:2005). Para que toda a informação que circula possa servir apenas ao seu propósito, que é o de informar, sem prejudicar pessoas ou instituições, é necessária a gestão segura dos recursos disponíveis em tecnologia da informação.

Parágrafo único. Tomando como base os princípios de segurança da informação, a CODERN, por meio deste documento, procura adotar procedimentos padrões, de modo a contribuir de forma positiva com a:

I - Integridade: garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais;

II - Confidencialidade: garantia de que o acesso à informação seja obtido somente por pessoas autorizadas; e

III - Disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

Art. 4º A Tabela de Termos Técnicos e Siglas a seguir é parte integrante desta Política:

Tabela de Termos Técnicos e Siglas

Sigla / Termo	Significado / Definição
ABNT NBR ISO/IEC 17799:2005	Norma brasileira que estabelece diretrizes para a gestão da segurança da informação.
Backup	Cópia de segurança de dados para permitir sua restauração em caso de perda.
Bypass	Técnica ou ação para contornar um controle de segurança (ex.: firewall).
Cloud Computing	Computação em nuvem; modelo de entrega de serviços de TI sob demanda via internet.
CODERN	Companhia Docas do Rio Grande do Norte.
COOREH	Coordenação de Recursos Humanos.
COORTI	Coordenação de Tecnologia da Informação.

CSIC	Comitê de Segurança da Informação e Comunicação
CGD	Comitê de Governança Digital
DATACENTER	Local físico que abriga os equipamentos críticos de processamento e armazenamento de dados.
DDoS	Ataque de Negação de Serviço Distribuído; sobrecarrega um serviço com tráfego de múltiplas fontes.
DPO	Encarregado de Proteção de Dados (Data Protection Officer); responsável pela LGPD na organização.
Download	Transferência de dados de um sistema remoto para o computador local.
EDR	Plataforma de Detecção e Resposta a Endpoints; monitora e responde a ameaças em estações de trabalho e servidores.
ETIR/CODERN	Equipe de Tratamento e Resposta a Incidentes Cibernéticos da CODERN.
Firewall	Dispositivo ou software que controla o tráfego de rede entre redes com diferentes níveis de confiança.
GEDADOS	Gerência de Dados e Apoio à Decisão.
IA	Inteligência Artificial.
LGPD	Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018).
LLM	Modelo de Linguagem de Grande Porte (Large Language Model); tipo de modelo de IA generativa.
MTTR	Tempo Médio para Resolução (Mean Time to Recover/Resolve); métrica de tempo para solucionar um incidente.
NDA	Acordo de Confidencialidade (Non-Disclosure Agreement).
Phishing	Tentativa fraudulenta de obter informações sensíveis se passando por uma comunicação confiável.
PRIC	Plano de Resposta a Incidentes Cibernéticos.
Ransomware	Tipo de software malicioso que bloqueia o acesso aos dados e exige um resgate para liberá-los.
SEI	Sistema Eletrônico de Informações; plataforma de processos administrativos digitais.
SIEM	Sistema de Gerenciamento de Informações e Eventos de Segurança; centraliza e correlaciona logs de segurança.
Upload	Transferência de dados do computador local para um sistema remoto.
USB	Barramento Serial Universal; padrão para conexão, comunicação e alimentação de dispositivos.

VPN	Rede Privada Virtual; cria uma conexão criptografada através de uma rede pública como a internet.
WIRELESS	Tecnologia de comunicação sem fio.

CAPÍTULO IV

DA APLICAÇÃO E CLASSIFICAÇÃO

Art. 5º Entende-se por Política de Segurança da Informação Digital da Companhia Docas do Rio Grande do Norte o conjunto de critérios e procedimentos de segurança, elaborados, implantados, divulgados e em contínuo processo de monitoração, visando a confidencialidade, a integridade e a disponibilidade da informação.

§ 1º As presentes normas aplicam-se a empregados, comissionados, estagiários e terceiros autorizados, e todos aqueles que, uma vez autorizados, venham a ter acesso aos recursos informatizados disponibilizados pela CODERN.

§ 2º A área de Tecnologia da Informação é responsável pela salvaguarda dos dados da organização, mas o processo de segurança da informação deve envolver todos os colaboradores, independentemente do nível hierárquico, posto que, de posse de uma informação específica, qualquer pessoa pode, por descuido e/ou má intenção, tornar-se um agente de divulgação não autorizada.

§ 3º A Política de Segurança da Informação visa propor uma Gestão de Segurança da Informação baseada em controles e procedimentos técnicos, considerando e promovendo o comportamento dos colaboradores de forma a aplicar a tecnologia adequada em todo o processo e atingir efetividade em seu objetivo.

Art. 6º As informações devem ser classificadas e identificadas por rótulos, considerando o "caput" do Art. 24, parágrafo 1º, da LEI Nº 12.527, DE 18 DE NOVEMBRO DE 2011, nos seguintes níveis:

I - Ultrassecreta: 25 (vinte e cinco) anos;

II - Secreta: 15 (quinze) anos; e

III - Reservada: 5 (cinco) anos.

Art. 7º Consideram-se informações Ultrassecretas as referentes à soberania e à integridade territorial nacionais, a planos e operações militares, às relações internacionais do país, a projetos de pesquisa e desenvolvimento científico e tecnológico de interesse da defesa nacional e a programas econômicos, cujo

conhecimento não autorizado possa acarretar dano excepcionalmente grave à segurança da sociedade e do Estado.

Art. 8º Consideram-se informações Secretas aquelas explicitamente aprovadas por seu responsável para consulta irrestrita e cuja divulgação externa não compromete o negócio.

Art. 9º Consideram-se informações Reservadas as disponíveis aos colaboradores da CODERN para a execução de suas tarefas rotineiras, não se destinando, portanto, ao uso do público externo.

CAPÍTULO V
DOS PRINCÍPIOS DA INFORMAÇÃO

Art. 10. Toda informação gerada internamente, bem como aquela obtida ou adquirida externamente para atender aos interesses da empresa, é considerada patrimônio da CODERN.

Art. 11. Todos os empregados, comissionados, estagiários e terceiros autorizados são responsáveis pela segurança das informações da CODERN e devem atuar em conformidade com estas Normas de Segurança da Informação.

Art. 12. Deve constar nos contratos firmados com terceiros a Declaração de Consonância com as Normas de Segurança da Informação, devidamente autorizada pelos responsáveis competentes.

Art. 13. Compete aos setores de Recursos Humanos, Contratos e Estágio divulgar e cientificar todos os funcionários, terceirizados e estagiários, no ato da formalização de seus Contratos e/ou Convênios e Termos de Compromisso de Estágio, por meio da assinatura da “Declaração de Consonância” com a Política de Segurança da Informação e das Comunicações, devendo ainda os respectivos setores informar à Gerência de Dados e Apoio à Decisão – GEDADOS e à Coordenação de Tecnologia da Informação - COORTI sobre o início ou término dos devidos contratos para a gestão correta da informação.

CAPÍTULO VI
DO CONTROLE DE ACESSO E CAPACITAÇÃO

Art. 14 Os usuários devem possuir identificação pessoal e intransferível, qualificando-os como responsáveis por todas as atividades desenvolvidas por meio dela.

Art. 15 Os recursos da informação devem estar disponíveis aos usuários para o desempenho de suas atividades profissionais, segundo critérios estabelecidos pelos

gestores desses recursos, observando os princípios da economia, eficácia e segurança.

Art. 16 O uso dos recursos da informação deve estar em conformidade com as normas internas, cláusulas contratuais e legislação aplicável.

Art. 17 Cada unidade funcional tem por atribuição zelar pelos recursos de informação utilizados em suas atividades, sendo de responsabilidade dos empregados, comissionados, estagiários e terceiros autorizados as ações necessárias para assegurar que os recursos sejam preservados quanto à integridade e confidencialidade.

CAPÍTULO VII
DA ESTABILIDADE DO AMBIENTE E GESTÃO DA SEGURANÇA

Art. 18 Os empregados, comissionados, estagiários e terceiros autorizados devem possuir capacitação para utilização dos recursos de informação e para a aplicação dos conceitos de segurança, de forma a garantir níveis adequados de confidencialidade, integridade e disponibilidade das informações da CODERN.

Art. 19 Estas Normas de Segurança da Informação e das Comunicações devem ser amplamente divulgadas a fim de conscientizar todos os empregados, comissionados, estagiários e terceiros autorizados sobre sua importância para o desempenho de suas atividades.

Art. 20 A GEDADOS encaminhará mensalmente dicas sobre a boa utilização dos recursos de informática em uso.

Art. 21 Os recursos de informação devem ser inventariados, identificados de forma individual e única, ter documentação atualizada e plano de manutenção preventiva para proteger e garantir sua disponibilidade.

Art. 22 Os recursos de informação devem estar em conformidade com os padrões definidos internamente.

Art. 23 A disponibilidade do recurso de informação para uso deve ser efetivada após a realização de testes em ambiente apropriado, a homologação e o aceite pela COORTI, conforme o processo definido para o respectivo recurso.

Art. 24 A COORTI, ao monitorar a rede interna, pretende garantir a integridade dos dados e programas. Toda tentativa de alteração dos parâmetros de segurança, por qualquer colaborador, sem o devido credenciamento e autorização, será julgada inadequada e os riscos relacionados serão informados ao colaborador e ao respectivo gestor. O uso de qualquer recurso para atividades ilícitas poderá acarretar ações administrativas e penalidades decorrentes de processos civil e

criminal, sendo que, nesses casos, a instituição cooperará ativamente com as autoridades competentes.

Art. 25 Cabe à GEDADOS:

I - Planejar, definir e aplicar o modelo de implementação das Normas de Segurança da Informação e das Comunicações;

II - Difundir a cultura de segurança da informação;

III - Propor programas de treinamento em segurança da informação; e

IV - Atualizar a instrução normativa conforme o crescimento e desenvolvimento de novas tecnologias.

Art. 26 As falhas, vulnerabilidades ou sugestões de aprimoramento na segurança da informação, ou nos seus procedimentos, observadas pelos empregados, comissionados, estagiários e terceiros autorizados, devem ser formalmente reportadas à GEDADOS, que, por sua vez, tomará as providências cabíveis por intermédio de sua equipe.

Art. 27 As Normas devem ser revisadas anualmente ou quando oportuno.

CAPÍTULO VIII

DAS SENHAS

Art. 28 Os empregados, comissionados, estagiários e terceiros autorizados são responsáveis por todas as ações realizadas mediante as senhas que lhes são atribuídas.

Art. 29 As senhas são de uso pessoal e intransferível, sendo vedado ao titular compartilhá-las ou fornecê-las a terceiros.

Art. 30 Os empregados, comissionados, estagiários e terceiros autorizados devem memorizar suas senhas, não devendo registrá-las em meio que permita sua leitura por terceiros.

Art. 31 Os usuários podem alterar a própria senha e devem ser orientados a fazê-lo caso suspeitem que terceiros obtiveram acesso indevido ao seu login/senha.

Art. 32 A periodicidade programada para as trocas de senha não deverá ser superior a 06 (seis) meses.

Art. 33 A alteração da senha será solicitada automaticamente quando de sua expiração. Os empregados, comissionados, estagiários e terceiros autorizados não

poderão acessar os recursos de informação caso não seja realizada a alteração de suas respectivas senhas expiradas.

Art. 34 Os empregados, comissionados, estagiários e terceiros autorizados devem usar senhas diferenciadas de acordo com orientações estabelecidas pela COORTI.

Art. 35 As senhas recebidas pelos empregados, comissionados, estagiários e terceiros autorizados para acesso aos ambientes e aplicativos devem ser alteradas no primeiro acesso.

Art. 36 Após 03 (três) tentativas de acesso, a conta do usuário será bloqueada. Para o desbloqueio, é necessário que o usuário entre em contato com a COORTI. Deverá ser estabelecido um processo para solicitação da renovação de senha.

Art. 37 Os empregados, comissionados, estagiários e terceiros autorizados devem compor suas senhas observando as seguintes regras:

Art. 38 Evitar utilizar como conteúdo das senhas:

I - Caracteres repetidos consecutivamente (aaa, 2222, aabbcc, etc);

II - Caracteres em ordem alfabética (12345, abcdef, aeiou, etc);

III - Nomes próprios em geral (pessoas, empresas, estados, cidades, etc.);

IV - Datas de nascimento, casamento, números de telefone;

V - A própria identificação funcional, apelidos, abreviações, iniciais dos nomes, etc;

VI - Termos óbvios: Brasil, CODERN, GERTAB, TERSAB, SEDE, senha, usuário, password, system, sistema, etc; e

g) Senhas iguais ou semelhantes ao “login”. Exemplo:

* Login: joaosilva

* Senha: joaosilva123

Art. 39 Para os nossos requisitos de autenticação de senha, exigem-se os seguintes critérios de complexidade:

I - Combinação de letras (maiúsculas e minúsculas), números e/ou caracteres especiais (#&%*/[]);

* Exemplos: Agu@246, 14Aao()4

Art. 40 É vedada a reutilização das últimas 10 (dez) senhas ou das senhas utilizadas nos últimos 12 (doze) meses.

Art. 41 As senhas dos empregados, comissionados e estagiários que ingressarem na Empresa devem ser solicitadas pela Coordenação de Recursos Humanos – COOREH à COORTI.

Art. 42 As senhas de acesso destinadas a terceiros autorizados devem ser solicitadas por meio do Formulário de Cadastramento de Senhas da Rede, disponível na Intranet. O pedido deve ser realizado pelos fiscais dos contratos ou pelos gestores das unidades onde os terceiros estiverem alocados e encaminhado à Coordenação de Recursos Humanos, que o repassará à COORTI para a devida liberação.

Art. 43 As senhas dos empregados, comissionados, estagiários e terceiros autorizados desligados da CODERN serão bloqueadas mediante solicitação da Coordenação de Recursos Humanos, dos fiscais do contrato ou dos gestores das unidades nas quais estão alocados.

Art. 44 As senhas dos empregados licenciados ou cedidos devem ser bloqueadas e desbloqueadas mediante solicitação da Coordenação de Recursos Humanos.

CAPÍTULO IX
DO USO DA INTERNET E CORREIO ELETRÔNICO

Art. 45 Todas as regras atuais da CODERN visam basicamente ao desenvolvimento de um comportamento eminentemente ético e profissional no uso da internet. Embora a conexão direta e permanente da rede corporativa da instituição com a internet ofereça um grande potencial de benefícios, ela abre a porta para riscos significativos para os ativos de informação.

Art. 46 Qualquer informação que é acessada, transmitida, recebida ou produzida na internet está sujeita a divulgação e auditoria. Portanto, a GEDADOS da CODERN, em total conformidade legal, reserva-se o direito de monitorar e registrar todos os acessos a ela.

Art. 47 Os equipamentos, tecnologias e serviços fornecidos para o acesso à internet são de propriedade da instituição, que pode analisar e, se necessário, bloquear qualquer arquivo, site, correio eletrônico, domínio ou aplicação armazenados na rede/internet, estejam eles em disco local, na estação ou em áreas privadas da rede, visando assegurar o cumprimento das Normas de Segurança da Informação e das Comunicações.

Art. 48 A internet é um recurso corporativo colocado à disposição dos empregados, comissionados, estagiários e terceiros autorizados para o desenvolvimento das

atividades profissionais, sendo vedados usos com finalidades pessoais diversas, tais como:

I. Desenvolver negócios particulares;

II. Acessar sites com conteúdo incompatível com os princípios da CODERN, tais como: pornografia, incitação à violência, preconceitos em geral, etc.;

III. Como regra geral, materiais de cunho sexual não poderão ser expostos, armazenados, distribuídos, editados, impressos ou gravados por meio de qualquer recurso;

IV. Documentos digitais de condutas consideradas ilícitas, como, por exemplo, apologia ao tráfico de drogas e pedofilia, são expressamente proibidos e não devem ser acessados, expostos, armazenados, distribuídos, editados, impressos ou gravados por meio de qualquer recurso;

V. Comprometer a privacidade dos usuários ou o sigilo das informações;

VI. Praticar jogos, jogos on-line;

VII. Acesso a salas de conversação (chat), salvo exceções para uso corporativo, devidamente autorizado pela Diretoria Executiva da CODERN;

VIII. O uso, a instalação, a cópia ou a distribuição não autorizada de softwares que tenham direitos autorais, marca registrada ou patente na internet são expressamente proibidos. Qualquer software não autorizado baixado será excluído pela COORTI;

IX. Efetuar upload (subida) de qualquer software licenciado à CODERN ou de dados de sua propriedade a seus parceiros e clientes, sem expressa autorização do responsável pelo software ou pelos dados;

X. Acesso a sites de relacionamento existentes e que venham a existir, tais como Facebook, WhatsApp, Google+, etc., salvo exceções para uso institucional, devidamente autorizado pela Diretoria Executiva da CODERN;

XI. Praticar qualquer tipo de hostilidade eletrônica. Exemplo: alterar ou destruir a integridade de informações armazenadas em computadores sem a devida autorização; e

XII. Fazer download (baixa de arquivos/programas) ou distribuição de softwares ou dados pirateados, atividade considerada delituosa de acordo com a legislação nacional.

Art. 49 Os serviços da internet autorizados pela CODERN são os de acesso às páginas World Wide Web (www) e o correio eletrônico.

Art. 50 Não é permitida a utilização de acesso à internet (modem 3G e linhas ADSL) em equipamento conectado à rede nas dependências da Sede e nas Unidades Operacionais da CODERN.

Art. 51 A critério da CODERN, e em conformidade com seus princípios, será vedado o acesso a sites que não sejam considerados de interesse da instituição ou que possam comprometer sua imagem ou a segurança da informação.

Art. 52 Aos empregados, comissionados, estagiários e terceiros autorizados não é permitido o download, tampouco a instalação de softwares, exceto se devidamente autorizado pela Diretoria Executiva da CODERN.

Art. 53 Não serão permitidos os acessos a softwares peer-to-peer (Kazaa, BitTorrent, µTorrent e afins).

Art. 54 Não serão permitidos os acessos a sites de compartilhamento de arquivos, tais como: Mega, Uploaded, Bitshare, Depositfiles, etc.

Art. 55 Não serão permitidas tentativas de burlar os controles de acesso à rede, tais como utilização de proxies anônimos e estratégias de bypass de firewall.

Art. 56 Não será permitido o uso de aplicativos de reconhecimento de vulnerabilidades, análise de tráfego, ou qualquer outro que possa causar sobrecarga ou prejudicar o bom funcionamento e a segurança da rede interna, salvo os casos em que o objetivo for realizar auditorias de segurança, quando a COORTI deverá estar devidamente ciente e ter concedido autorização para tal.

Formatos proibidos:

I. Arquivos executáveis:

- .exe;
- .com;
- .bat;
- .pif;
- Plugins;
- .scr;
- Dentro de arquivo compactado; e
- Novos formatos de executáveis que venham a surgir.

II. Arquivos de música:

- .mp3;
- .cda;
- .wav;
- .wma;
- .ram;
- .rm;
- .midi;
- Dentro de arquivo compactado;
- Outros formatos de áudio; e
- Novos formatos de áudio que venham a surgir.

III. Vídeos:

- .avi;
- .mpg;
- .mpeg;
- .asf;
- .wmf;
- .wmp;
- .3gp;
- Outros formatos de vídeo;
- Dentro de arquivo compactado; e
- Novos formatos de vídeos que venham a surgir.

IV. Imagens em geral.

Art. 57 Os empregados, comissionados, estagiários e terceiros autorizados, quando da utilização da internet, devem adotar linguagem e postura em concordância com os princípios da CODERN.

Art. 58 Os empregados, comissionados, estagiários e terceiros autorizados devem respeitar as políticas vigentes nos sites visitados.

Art. 59 A solicitação de uso de qualquer serviço diferente dos descritos no Item 5.1 deve ser encaminhada formalmente, com justificativa da necessidade de liberação do acesso, à COORTI, com cópia para GEDADOS.

Art. 60 O correio eletrônico é um recurso corporativo colocado à disposição dos empregados, comissionados, estagiários e terceiros autorizados para o desenvolvimento de suas atividades profissionais, de acordo com as necessidades e interesses da CODERN.

Art. 61 O uso de correio eletrônico interno será disponibilizado aos empregados, comissionados, estagiários e terceiros de acordo com os interesses da CODERN;

Art. 62. Os empregados, comissionados, estagiários e terceiros autorizados somente podem utilizar o correio eletrônico sob a sua própria identificação ou endereço organizacional sob sua responsabilidade, sem prejuízo do disposto no art. 60.

Art. 63. As mensagens eletrônicas dos empregados, comissionados, estagiários e terceiros autorizados serão identificadas com nome, cargo ou função, unidade na qual estão alocados ou prestando serviços, e telefone para contato.

Art. 64. As mensagens do correio eletrônico enviadas sob a identificação do empregado, comissionado, estagiário ou terceiro autorizado são de sua responsabilidade perante a CODERN, devendo ser observado, especialmente, o conteúdo daquelas endereçadas ao ambiente externo, pois a elas estará associado o nome da CODERN, uma vez que a origem institucional da mensagem é registrada no próprio endereço do remetente (nome.sobrenome@codern.com.br).

Art. 65. Os empregados, comissionados, estagiários e terceiros autorizados, quando da utilização do correio eletrônico, devem adotar linguagem e postura em concordância com os princípios da CODERN.

Art. 66. Aos empregados, comissionados, estagiários e terceiros autorizados é permitida delegação de direito de leitura e envio de mensagens, através do uso do recurso específico para este fim existente no correio eletrônico.

Art. 67. Entre as mensagens e anexos não autorizados para envio, destacam-se os seguintes:

I. Relativos a negócios particulares;

II. Assinaturas de newsletter que não condizem com o Sistema, por exemplo: Sites de e-commerce e compras coletivas, promoções, propagandas, etc. Para estes sites, o colaborador não está proibido de utilizar seu e-mail pessoal;

III. Propagandas comerciais, políticas partidárias e/ou religiosas;

IV. Correntes e boatos;

V. Com conteúdos incompatíveis com os princípios da CODERN, tais como: pornografia, incitação à violência e preconceitos em geral;

VI. Com informações que impliquem violação de direito autoral; e

VII. Com conteúdos que possam comprometer a privacidade dos usuários ou o sigilo das informações.

Art. 68. É permitido anexar a mensagens de correio eletrônico arquivos de documentos, apresentações, planilhas eletrônicas e de banco de dados. É

recomendável que este conteúdo seja compactado antes do envio. São exemplos destes arquivos as extensões descritas abaixo:

I – Documento:

- .txt;
- .doc e .docx;
- .odf e .odt;
- .pdf; e
- .rtf.

II – Apresentação:

- .ppt, .pps, .pptx, .ppsx; e
- .odp.

III – Planilha eletrônica:

- .xls, .xlsx; e
- .ods.

IV – Banco de dados:

- .mdb, .mdbx e .dbf.

V – Exemplo dos arquivos supracitados quando compactados:

- .7Z, .ZIP, .RAR, .TAR e .GZ.

Art. 69 Os empregados, comissionados, estagiários e terceiros autorizados podem anexar a mensagens de correio eletrônico arquivos de documentos, apresentações, planilhas eletrônicas e de banco de dados. É recomendável que este conteúdo seja compactado antes do envio. São exemplos destes arquivos os do art. 68, acrescidos das páginas Web (.htm e .html).

Art. 71. Os empregados, comissionados, estagiários e terceiros autorizados não devem abrir e devem excluir ou, a seu critério, encaminhar à COORTI mensagens recebidas que possam representar ameaça à segurança da informação da CODERN em função da possibilidade de contaminação por vírus de computador. São características dessas mensagens, dentre outras:

- Remetente desconhecido;
- Assunto não aderente aos interesses de trabalho; e
- Notificações do SERASA, cobranças desconhecidas, Policiais, Ministério Público — estas instituições não notificam seus clientes por meio de mensagens eletrônicas.

Art. 72. Os empregados, comissionados, estagiários e terceiros autorizados devem encerrar ou bloquear sua estação de trabalho sempre que se ausentarem da sala.

Art. 73. As estações de trabalho serão bloqueadas automaticamente após 30 (trinta) minutos de inatividade por parte do usuário, sendo necessário autenticar-se novamente para dar continuidade às atividades.

Art. 74. As mensagens de correio eletrônico sempre deverão incluir assinatura com o seguinte formato:

- Nome do Colaborador;
- Cargo ou Função do Colaborador;
- Nome da Gerência ou Setor onde trabalha;
- Nome da Empresa;
- Telefone(s); e
- Correio Eletrônico.

Art. 75. Para garantir o desempenho e a disponibilidade do ambiente computacional da CODERN, a COORTI delimitará e divulgará:

- O tamanho das mensagens enviadas e recebidas pelos empregados, comissionados, estagiários e terceiros autorizados;
- A quantidade de destinatários no envio de mensagens internas e externas; e
- O tamanho das caixas postais dos empregados, comissionados, estagiários e terceiros autorizados.

Art. 76. As mensagens que estiverem em desacordo com os limites estabelecidos serão automaticamente bloqueadas, gerando o envio de notificação para o remetente.

Art. 77. Algumas destas mensagens são também bloqueadas diretamente no servidor, entre elas destacam-se: problemas com o servidor do remetente, SPAMs e anexos não permitidos.

Art. 78. É proibido produzir, transmitir ou divulgar mensagem que:

I – vise obter acesso não autorizado a outro computador, servidor ou rede;

II – vise interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;

III – vise burlar qualquer sistema de segurança;

IV – vise vigiar secretamente ou assediar outro usuário;

V – vise acessar informações confidenciais sem explícita autorização do proprietário;

VI – tenha conteúdo considerado impróprio, obsceno ou ilegal;

VII – seja de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico, entre outros;

VIII – inclua material protegido por direitos autorais sem a permissão do detentor dos direitos;

IX – o uso de e-mails pessoais é aceitável, se usado com moderação, em caso de necessidade e quando:

a) não contrariar as normas aqui estabelecidas;

b) não interferir negativamente nas atividades profissionais individuais ou na de outros colaboradores;

c) não interferir negativamente na CODERN e na sua imagem.

Art. 79. Para garantir o desempenho e a disponibilidade do ambiente computacional da CODERN, a COORTI delimitará e divulgarará:

- I – o tamanho das mensagens enviadas e recebidas pelos empregados, comissionados, estagiários e terceiros autorizados;

- II – a quantidade de destinatários no envio de mensagens internas e externas; e

- III – o tamanho das caixas postais dos empregados, comissionados, estagiários e terceiros autorizados.

Art. 80. As mensagens que estiverem em desacordo com os limites estabelecidos serão automaticamente bloqueadas, gerando o envio de notificação para o remetente.

Art. 81. Algumas destas mensagens são também bloqueadas diretamente no servidor, entre elas destacam-se: problemas com o servidor do remetente, SPAMs e anexos não permitidos.

Art. 82. É proibido produzir, transmitir ou divulgar mensagem que:

- I – vise obter acesso não autorizado a outro computador, servidor ou rede;
- II – vise interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;

- III – vise burlar qualquer sistema de segurança;
- IV – vise vigiar secretamente ou assediar outro usuário;
- V – vise acessar informações confidenciais sem explícita autorização do proprietário;
- VI – tenha conteúdo considerado impróprio, obsceno ou ilegal;
- VII – seja de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico, entre outros;
- VIII – inclua material protegido por direitos autorais sem a permissão do detentor dos direitos;
- IX – o uso de e-mails pessoais é aceitável, se usado com moderação, em caso de necessidade e quando:

- a) não contrariar as normas aqui estabelecidas;

- b) não interferir negativamente nas atividades profissionais individuais ou na de outros colaboradores;

- c) não interferir negativamente na CODERN e na sua imagem.

Art. 83. O cadastramento de terceiros autorizados e estagiários no correio eletrônico interno e externo deve ser solicitado à Coordenação de Recursos Humanos pelas unidades gestoras dos respectivos contratos, que repassará esses pedidos à COORTI para sua liberação.

Art. 84. A criação e atualização de listas públicas de distribuição devem ser solicitadas pelo gestor da unidade interessada à COORTI.

Art. 85. Quando do desligamento ou suspensão do contrato de trabalho de empregados, comissionados e estagiários, a Coordenação de Recursos Humanos deve solicitar à COORTI o bloqueio e a exclusão de acesso aos recursos de rede corporativa de forma imediata.

Art. 86. Quando do encerramento do contrato de prestação de serviços de terceiros autorizados, os fiscais dos respectivos contratos deverão solicitar imediatamente à COORTI, com cópia para a GEDADOS, a exclusão do acesso ao correio eletrônico e demais recursos da rede corporativa.

CAPÍTULO X

DO MONITORAMENTO, DATACENTER E BACKUP

Art. 87.O cumprimento e a eficácia das Normas de Segurança da Informação devem ser objeto de avaliação periódica. Para garantir as regras mencionadas neste documento, a CODERN deverá seguir as seguintes recomendações:

Art. 88. Periodicamente, a GEDADOS encaminhará relatório da utilização dos recursos de tecnologia da informação à Diretoria Executiva, ao Comitê de Tecnologia da Informação e/ou Gerentes, Coordenadores e Supervisores das Unidades Operacionais da CODERN.

Art. 89. Haverá registros dos acessos realizados pelos empregados, comissionados, estagiários e terceiros autorizados para auditorias periódicas. Tais informações ficam disponíveis pelo tempo máximo de 90 (noventa) dias.

Art. 90. A CODERN, por meio da COORTI, reserva-se o direito de realizar testes eletrônicos a fim de detectar:

- I – senhas frágeis;
- II – no uso da internet na instituição, vulnerabilidade e falhas de segurança a fim de preservar a integridade das informações; e

- III – uso adequado pelos empregados, estagiários e terceiros autorizados no correio eletrônico.

Art. 91. Os empregados, comissionados, estagiários e terceiros autorizados que possuírem senhas consideradas frágeis serão notificados pela COORTI para alteração de suas respectivas senhas.

Art. 92. Os serviços da internet, de correio eletrônico e demais serviços de rede corporativa podem ser temporariamente desativados caso haja indício de tentativa de quebra de segurança e outras ações que ponham em risco a integridade das informações.

Art. 93. Define-se *Datacenter* como o local onde são concentrados os equipamentos de processamento e armazenamento de dados de uma empresa ou organização. Normalmente projetados para serem extremamente seguros, abrigam servidores e bancos de dados, processando grande quantidade de informação. Os itens descritos a seguir definem regras de uso e acesso ao *Datacenter* da CODERN, situado no prédio da Sede e em suas filiais.

Art. 94. O acesso ao *Datacenter* somente deverá ser feito por sistema de autenticação. Por exemplo: biometria, cartão magnético, entre outros.

Art. 95. Todo acesso ao *Datacenter*, pelo sistema de autenticação, deverá ser registrado (usuário, data e hora) mediante software próprio ou adquirido.

Art. 96. Deverá ser executada mensalmente uma auditoria nos acessos ao *Datacenter* por meio do relatório do sistema de registro.

Art. 97. O usuário “administrador” do sistema de autenticação ficará sob a responsabilidade da GEDADOS/COORTI, de acordo com o Procedimento de Controle de Contas Administrativas.

Art. 98. A lista de funções com direito de acesso ao *Datacenter* deverá ser constantemente atualizada, de acordo com os termos do Procedimento de Controle de Acesso ao *Datacenter*, e salva no diretório de rede.

Art. 99. Nas localidades em que não existam colaboradores da área de TI, pessoas de outros departamentos deverão ser cadastradas no sistema de acesso para que possam exercer as atividades operacionais dentro do *Datacenter*, como: manutenção da refrigeração e da energia elétrica da sala e suporte em eventuais problemas.

Art. 100. O acesso de visitantes ou terceiros somente poderá ser realizado com acompanhamento de um colaborador autorizado.

Art. 101. O acesso ao *Datacenter* por meio de chave apenas poderá ocorrer em situações de emergência, quando a segurança física do *Datacenter* for comprometida, como incêndio, inundação, abalo da estrutura predial ou quando o sistema de autenticação não estiver funcionando.

Art. 102. Caso haja necessidade de acesso não emergencial, a área requisitante deve solicitar autorização com antecedência a qualquer colaborador responsável pela administração de liberação de acesso, conforme lista salva em Procedimento de Controle de Acesso ao *Datacenter*.

Art. 103. O *Datacenter* deverá ser mantido limpo e organizado. Qualquer procedimento que gere lixo ou sujeira nesse ambiente somente poderá ser realizado com a colaboração da prestadora de Serviços Gerais.

Art. 104. Não é permitida a entrada de nenhum tipo de alimento, bebida, produto fumígeno ou inflamável.

Art. 105. A entrada ou retirada de qualquer equipamento do *Datacenter* somente se dará com o preenchimento da solicitação de liberação pelo colaborador solicitante e a autorização formal desse instrumento pela GEDADOS da Companhia, de acordo com os termos do Procedimento de Controle e Transferência Patrimonial.

Art. 106. No caso de desligamento de empregados, comissionados ou colaboradores que possuam acesso ao *Datacenter*, imediatamente deverá ser providenciada a sua exclusão do sistema de autenticação da lista de colaboradores autorizados, de acordo com o processo definido no Procedimento de Controle de Acesso ao *Datacenter*.

Art. 107. Define-se *Backup* (termo em inglês) como cópia de dados de um dispositivo de armazenamento para que possam ser restaurados em caso da perda dos dados originais. Os itens abaixo definem as normas de segurança no que diz respeito à cópia dos sistemas e arquivos armazenados nos computadores e servidores da CODERN.

Art. 108. É de responsabilidade da COORTI todos os *backups* dos Sistemas de Informações e Banco de Dados armazenados no *Datacenter* instalado no prédio da Sede, filiais e nos *Datacenters* terceirizados. Os *backups* devem ser automatizados por sistemas de agendamento para que sejam preferencialmente executados fora do horário normal do expediente e em conformidade com a Política de *Backup* adotada pela GEDADOS.

Art. 109. Os técnicos responsáveis pela gestão dos sistemas de *backup* deverão realizar pesquisas frequentes para identificar atualizações de correção, novas versões do produto, ciclo de vida (quando o software não terá mais garantia do fabricante), sugestões de melhorias, entre outros.

Art. 110. Os dados armazenados nas estações de trabalho são de total responsabilidade do usuário, que deverá solicitar orientações quanto ao procedimento à COORTI.

Art. 111. A COORTI deve preparar semestralmente um plano para execução de testes de restauração de dados, que deve ter escopo definido em conjunto com as áreas de negócio. Por se tratar de uma simulação, o executor deve restaurar os arquivos em local diferente do original, para que assim não sobreponha os arquivos válidos.

Art. 112. São realizadas duas cópias dos *backups*, cujo armazenamento é feito na própria sede em locais distintos.

Art. 113. O tempo de retenção das cópias é de 90 (noventa) dias.

Art. 114. O acesso aos locais do armazenamento das cópias dos *backups* é restrito à equipe de TI. Utiliza-se o crachá funcional, previamente cadastrado, para ter acesso aos locais através do equipamento de leitura (*Inner*).

Art. 115. O *backup* e *restore* dos dados na infraestrutura em nuvem pública (*cloud computing*) são de responsabilidade da empresa contratada pelo serviço.

CAPÍTULO XI

DOS COMPUTADORES, RECURSOS TECNOLÓGICOS E MÍDIAS REMOVÍVEIS

Art. 116. Os equipamentos disponíveis aos colaboradores são de propriedade da CODERN, cabendo a cada um utilizá-los e manuseá-los corretamente para as

atividades de interesse da Empresa, bem como cumprir as recomendações constantes nos procedimentos operacionais fornecidos pelas gerências, coordenações e supervisões responsáveis. As normas a seguir definem o uso adequado dos recursos computacionais existentes na Companhia.

Art. 117. É proibido todo procedimento de manutenção física ou lógica, instalação, desinstalação, configuração ou modificação, sem o conhecimento prévio e o acompanhamento de um técnico da GEDADOS, ou de quem este determinar.

Art. 118. Todas as atualizações e correções de segurança do sistema operacional ou aplicativos somente poderão ser feitas após a devida validação no respectivo ambiente de homologação, e depois de sua disponibilização pelo fabricante ou fornecedor.

Art. 119. É vedada a abertura ou o manuseio de computadores ou outros equipamentos de informática para qualquer tipo de reparo que não seja realizado por um técnico da GEDADOS ou por terceiros devidamente contratados para o serviço.

Art. 120. É expressamente proibido o consumo de alimentos, bebidas ou fumo na mesa de trabalho e próximo aos equipamentos.

Art. 121. O colaborador deverá manter a configuração do equipamento disponibilizado pela CODERN, seguindo os devidos controles de segurança exigidos pela Norma de Segurança da Informação.

Art. 122. É proibido, a qualquer usuário, movimentar equipamentos, tais como gabinetes, monitores, impressoras, etc., sem autorização da COORTI.

Art. 123. É vedada a utilização de dispositivos removíveis com conexão USB ou WIRELESS nas estações de trabalho da CODERN.

Art. 124. É vedado aos usuários das estações de trabalho da CODERN utilizarem aplicações não oficiais da Companhia como meio de armazenamento de informações corporativas.

Art. 125. Nos casos em que for expressamente necessária a utilização de dispositivos com conexão USB ou WIRELESS nas estações de trabalho, os mesmos deverão ser comunicados, de forma prévia e justificada, à COORTI da CODERN.

Art. 126. Cabe à COORTI analisar e deliberar sobre os casos necessários de permissões de uso de dispositivos externos nas estações de trabalho, conforme o fluxo a seguir:

Art. 127. O gestor da unidade do requisitante deverá formalizar o pedido, enviando um e-mail para informatica@codern.com.br ou através de um processo no sistema SEI para unidade COORTI, com cópia para a GEDADOS.

Art. 128. A solicitação deverá ocorrer com antecedência mínima de 24 (vinte e quatro) horas referente à data desejada para o atendimento.

Art. 129. No corpo da solicitação, deverá constar de forma clara e objetiva a justificativa para o uso do dispositivo, bem como o período desejado para a liberação.

Art. 130. A COORTI analisará o pedido com os meios técnicos necessários e responderá no mesmo corpo do e-mail ou processo SEI, informando se o pedido foi deferido ou indeferido.

Art. 131. Aos usuários que tenham a permissão para a utilização de dispositivos removíveis nas estações de trabalho, atribuem-se responsabilidade pelos riscos e impactos que o uso de tais dispositivos possa vir a causar nos ativos de informação da CODERN.

Art. 132. Revogam-se as disposições em contrário.

Art. 133. Os casos omissos nesta Instrução serão dirimidos pela GEDADOS ou pelo Comitê de Segurança da Informação.

Art. 134. As Normas de Segurança da Informação devem ser cumpridas pelos empregados, comissionados e estagiários da CODERN e pelos terceiros autorizados, nos termos dos contratos de fornecimento de bens e prestação de serviços, considerando-se os aspectos abaixo:

Art. 135. A não observância, por parte dos empregados, comissionados e estagiários da CODERN, do disposto nas presentes Normas, será considerada como falta grave, estando o infrator sujeito às penalidades previstas na Consolidação das Leis do Trabalho – CLT.

Art. 136. A não observância, por parte de terceiros e estagiários autorizados, do disposto na presente Norma, poderá ensejar, conforme o caso:

I. O imediato desligamento do prestador de serviços, sem prejuízo da rescisão do contrato de prestação de serviços celebrado com a empresa responsável pela sua alocação nas dependências da CODERN, e da aplicação das penalidades contratualmente previstas;

II. A imediata rescisão do contrato de estágio celebrado com o estagiário em questão, comunicando-se o fato apurado à entidade conveniada responsável pela alocação, na CODERN, dos estagiários.

Art. 137. É de responsabilidade do usuário toda e qualquer informação contida em seu computador ou notebook disponibilizado pela CODERN.

Art. 138. Além disso, o usuário é responsável por:

I. Permitir que o programa de antivírus e sistema operacional seja atualizado automaticamente, não interrompendo o procedimento na sua estação de trabalho durante a atualização; e

II. Manter os arquivos e pastas pessoais separados dos arquivos/pastas de âmbito institucional.

Art. 139. Nenhum software pode ser instalado nos computadores. Apenas os técnicos da GEDADOS podem fazê-lo, observando se os mesmos estão de acordo com as Normas de Segurança da Informação e das Comunicações. Não são permitidos tocadores de mp3, softwares de celular, players de vídeo, etc.

Art. 140. Não é permitida a utilização de computadores pessoais e nenhum outro dispositivo conectado à rede corporativa.

Art. 141. Os equipamentos a serem liberados deverão ser encaminhados à COORTI para análise e configuração dos mesmos, conforme padrões estabelecidos.

CAPÍTULO XII

DA PRIVACIDADE, PROTEÇÃO DE DADOS E GESTÃO DE VULNERABILIDADES

Art. 142. O direito à privacidade dos colaboradores, gestores, fornecedores, clientes da CODERN e demais partes interessadas nas atividades da Companhia é respeitado, mantendo os dados pessoais (sensíveis ou não) protegidos, em conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD). Devido a isso, a Companhia somente requer, obtém, trata, usa e armazena dados pessoais à medida que são necessários à gestão administrativa e dos negócios.
Art. 143. Os dados pessoais (sensíveis ou não) ou um conjunto de informações distintas que possam identificar ou discriminar uma pessoa física são sigilosos.

Art. 144. O tratamento dos dados pessoais é permitido somente nas seguintes situações:

I. Se houver consentimento expresso do titular do dado;

II. Para execução de contratos;

III. Se decorrer de exigências legais e/ou regulatórias;

IV. Para proteção da vida ou da incolumidade física do titular ou de terceiros;

V. Para proteção ao crédito, exceto quando tratar-se de dado pessoal sensível;

VI. Para atender interesse legítimo do controlador do dado ou de terceiros, exceto quando tratar-se de dado pessoal sensível;

VII. Garantia da prevenção à fraude e segurança do titular, quando tratar-se de dado pessoal sensível;

VIII. Realização de estudos por órgão de pesquisa;

IX. Exercício regular de direitos em processos judiciais e administrativos;

X. Tutela da saúde; ou

XI. Pela administração pública, quando da execução de políticas públicas.

Art. 145. Obrigações relativas à proteção de dados pessoais e dados pessoais sensíveis devem ser tratadas com cautela e sigilo por todos os indivíduos no exercício de suas atividades profissionais (independentemente de a quem pertençam, como foram obtidos ou onde são armazenados), em conformidade com os normativos específicos, obrigações contratuais e legislações em vigor.

Art. 146. Para estar em conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD), a Companhia deve:

I. Considerar questões de proteção de dados pessoais (sensíveis ou não) como parte dos projetos (ex. biometria, interoperabilidade, implementação de sistemas de informação, etc.);

II. Tornar a proteção de dados (sensíveis ou não) um componente essencial da funcionalidade principal dos recursos tecnológicos de forma a proteger as informações de propriedade ou sob custódia da Companhia;

III. Antecipar riscos e eventos invasivos de privacidade antes que eles ocorram e tomar medidas para evitar danos aos colaboradores, gestores, fornecedores e clientes;

IV. Solicitar e tratar dados pessoais que sejam estritamente essenciais ao(s) objetivo(s) da Companhia; e

V. Assegurar que os dados pessoais sejam utilizados exclusivamente para os fins informados previamente ao titular.

Art. 147. As principais considerações sobre privacidade de dados pessoais (sensíveis ou não) devem ser incorporadas às ações, metodologias e controles, de acordo com a gestão de riscos de cada área de negócios e/ou projetos, visando:

I. Identificar previamente as vulnerabilidades sistêmicas e os riscos de inconformidades perante à LGPD, através de diagnóstico de inventário de dados, que deve ser atualizado periodicamente pelos gestores das áreas afins;

II. Conscientizar todos os usuários dos recursos tecnológicos sobre as diretrizes da LGPD visando à proteção de dados pessoais (sensíveis ou não);

III. Cumprir com as obrigações legais e diretrizes de segurança da informação e demais normativos corporativos que versem sobre a privacidade de dados; e

IV. Implantar controles eficazes para mitigar os riscos de incidentes de segurança.

Art. 148. Visando dar suporte às áreas de negócios na adequação e avaliação dos impactos relativos à LGPD, foi instituído pela Companhia um Comitê Gestor de Proteção de Dados (CGDP), com a participação das áreas: Jurídica, Controles Internos e Riscos e Segurança da Informação.

Art. 149. Objetivo: estabelecer diretrizes e responsabilidades para identificação, avaliação, tratamento e monitoramento de vulnerabilidades em sistemas, redes e ativos tecnológicos da CODERN, garantindo a integridade, a disponibilidade e a confidencialidade das informações.

Art. 150. Diretrizes:

I. Todas as plataformas tecnológicas sob gestão da CODERN deverão ser submetidas a varreduras periódicas de vulnerabilidades;

II. As vulnerabilidades identificadas deverão ser classificadas por nível de risco (crítico, alto, médio e baixo);

III. Deverão ser aplicados patches de segurança e atualizações críticas em sistemas operacionais, aplicativos e equipamentos de rede conforme cronograma previamente estabelecido;

IV. O ambiente tecnológico deverá ser monitorado continuamente visando à defesa cibernética adotada pela Companhia;

V. Deverá ser mantido registro formal das vulnerabilidades detectadas, com evidências das ações corretivas implementadas e prazos de conclusão; e

VI. As informações sobre vulnerabilidades e medidas corretivas serão apresentadas em relatório periódico à Diretoria Executiva e ao Comitê de Segurança da Informação.

CAPÍTULO XIII

DOS INDICADORES E GESTÃO DE INCIDENTES

Art. 151. Definir parâmetros de medição para avaliar o desempenho e a eficácia dos controles de segurança da informação implantados na CODERN.

Art. 152 As diretrizes de gestão de indicadores e incidentes de segurança da informação da CODERN visam garantir a eficácia dos controles implementados, o monitoramento contínuo da conformidade e a pronta resposta a situações que possam comprometer a confidencialidade, integridade ou disponibilidade das informações corporativas.

Art. 153 A GEDADOS deverá manter um painel de indicadores de segurança, contendo métricas quantitativas e qualitativas.

Art. 154 Os indicadores mínimos deverão contemplar:

I. Percentual de usuários capacitados em segurança da informação;

II. Número e gravidade de incidentes registrados;

III. Tempo médio de resposta a incidentes (MTTR);

IV. Percentual de sistemas com backup testado;

V. Percentual de ativos com patches atualizados;

VI. Nível de aderência às auditorias de segurança.

Art. 155 Os resultados deverão ser apresentados trimestralmente à Diretoria Executiva, ao CSIC e CGD.

Art. 156 Os indicadores deverão apoiar a tomada de decisão estratégica, o planejamento de treinamentos e a priorização de investimentos em segurança da informação.

Art. 157 Estabelecer um processo formal de identificação, registro, análise, tratamento e comunicação de incidentes de segurança da informação na CODERN.

Art. 158 – Diretrizes

Art. 159 Todo incidente de segurança deverá ser imediatamente reportado à GEDADOS por meio de canal oficial.

Art. 160 O tratamento seguirá as seguintes etapas:

I. Identificação e registro do incidente;

II. Análise e classificação da gravidade;

III. Ações de contenção imediata;

IV. Erradicação e mitigação das causas;

V. Recuperação dos serviços afetados;

VI. Elaboração de relatório final e lições aprendidas.

VII. **Art. 161** Os incidentes críticos deverão ser reportados à Diretoria Executiva, ao CSIC e CGD.

Art. 162 Deverão ser realizadas simulações periódicas de resposta a incidentes, com foco em melhoria contínua.

Art. 163 O histórico de incidentes deverá ser mantido em registro centralizado e protegido.

Art. 164 – Responsabilidades

I. A COORTI será responsável pela coordenação técnica das ações de contenção e recuperação;

II. As áreas afetadas deverão colaborar com o fornecimento de informações e apoio operacional.

CAPÍTULO XIV

DA SEGURANÇA CIBERNÉTICA E USO DE INTELIGÊNCIA ARTIFICIAL

Art. 165. Estabelecer diretrizes específicas para prevenção, detecção, resposta e recuperação frente a ameaças cibernéticas que possam comprometer os ativos tecnológicos e informações institucionais da CODERN.

Art. 166 A CODERN deverá adotar mecanismos de defesa em múltiplas camadas, contemplando firewall, antivírus corporativo, EDR, SIEM e monitoramento contínuo de tráfego.

Art. 167 Deverão ser implementadas ações de prevenção contra ransomware, phishing, engenharia social e ataques de negação de serviço (DDoS).

Art. 168 A COORTI deverá manter e revisar periodicamente o Plano de Resposta a Incidentes Cibernéticos (PRIC), contendo fluxos de comunicação, níveis de criticidade e responsabilidades.

Art. 169 Deverá ser garantida a comunicação imediata à alta direção e à equipe de prevenção, tratamento e resposta a incidentes cibernéticos – ETIR/CODERN em casos de incidentes graves.

Art. 170 A CODERN deverá promover campanhas de conscientização voltadas a todos os colaboradores, enfatizando boas práticas de segurança cibernética.

Art. 171 A Política de Segurança Cibernética deverá ser revisada a cada 24 (vinte e quatro) meses, ou sempre que houver mudanças significativas no ambiente tecnológico.

Art. 172 – Responsabilidades

I. A GEDADOS/COORTI é responsável pela implementação e monitoramento dos controles de cibersegurança;

II. O ETIR é responsável pela supervisão e governança estratégica das ações;

III. O encarregado de dados, também conhecido como DPO (Data Protection Officer), deverá atuar em conformidade com a LGPD em casos de vazamento de dados pessoais;

IV. Todos os usuários e gestores devem seguir as boas práticas estabelecidas nesta política.

Art. 173 Estabelecer diretrizes e responsabilidades para o uso ético, seguro e responsável de tecnologias de Inteligência Artificial (IA) no âmbito da CODERN, assegurando conformidade com os princípios da Lei Geral de Proteção de Dados (Lei nº 13.709/2018), da ABNT NBR ISO/IEC 23894:2023 e demais normas de segurança da informação e cibernética aplicáveis à Administração Pública Federal.

Art. 174 O uso de ferramentas e sistemas baseados em Inteligência Artificial deverá observar as boas práticas de ética, segurança, transparência, responsabilidade e conformidade legal.

Art. 175 À GEDADOS, com apoio do Comitê de Segurança da Informação, deverá instituir política complementar de Gestão de Riscos e Segurança no Uso de Inteligência Artificial, considerando, no mínimo, os seguintes aspectos:

I. **Avaliação de riscos:** avaliar riscos associados ao uso de sistemas de IA em suas diversas formas — modelos generativos, modelos de linguagem ampla (LLMs), aprendizado de máquina, modelos baseados em regras ou sistemas especialistas —, observando impactos à confidencialidade, integridade, disponibilidade e autenticidade das informações;

II. **Responsabilidade e governança:** definir claramente as responsabilidades pelas ações e decisões automatizadas, bem como pelos resultados decorrentes da aplicação de IA em processos corporativos;

III. **Qualidade e proteção de dados:** adotar critérios rigorosos de qualidade, atualidade, relevância e origem ética dos dados utilizados em treinamentos e execuções de modelos de IA, assegurando a conformidade com a LGPD e demais normas de proteção de dados;

IV. **Transparência e explicabilidade:** assegurar que os sistemas de IA utilizados pela CODERN sejam compreensíveis, auditáveis e explicáveis, permitindo rastreabilidade de suas decisões e a verificação de seu funcionamento;

V. **Atualização e manutenção:** garantir a atualização contínua dos modelos e algoritmos de IA, com revisões periódicas para correção de falhas, mitigação de vieses e adequação a novos requisitos técnicos e legais;

VI. **Treinamento ético e responsável:** assegurar que todos os colaboradores, terceirizados e gestores envolvidos na especificação, desenvolvimento, contratação, uso ou supervisão de soluções de IA recebam capacitação adequada sobre ética, segurança e governança de IA;

VII. **Supervisão humana:** manter supervisão humana contínua sobre decisões críticas automatizadas, garantindo que o uso de IA não substitua o julgamento humano em situações que envolvam riscos éticos, legais ou de segurança institucional;

VIII. **Conformidade e auditoria:** os sistemas de IA deverão estar sujeitos a auditorias internas e externas periódicas, a fim de avaliar sua conformidade com as políticas de segurança da informação, privacidade e proteção de dados da CODERN.

Art. 176 – Responsabilidades

I. À GEDADOS compete coordenar a implementação das diretrizes, realizar as avaliações de risco e propor políticas complementares relacionadas ao uso de IA;

III. Ao Comitê de Segurança da Informação compete supervisionar, validar e recomendar boas práticas no uso de IA, garantindo o alinhamento com os princípios éticos e de segurança da informação da Companhia;

IV. III. Às áreas usuárias compete utilizar as soluções de IA conforme as políticas vigentes, reportando à GEDADOS eventuais riscos, falhas, inconsistências ou comportamentos anômalos identificados.

CAPÍTULO XV

DA DIVULGAÇÃO DE INFORMAÇÕES E DAS DISPOSIÇÕES FINAIS

Art. 177. Estabelecer diretrizes e restrições quanto à divulgação, reprodução, compartilhamento e armazenamento de informações de caráter estrutural, tecnológico ou de segurança, de forma a preservar a integridade, a confidencialidade e a disponibilidade dos ativos institucionais da CODERN.

Art. 178 É expressamente proibida a divulgação, total ou parcial, de informações relacionadas à infraestrutura tecnológica, lógica, operacional ou física da CODERN, sem a devida autorização formal da GEDADOS e da Diretoria Executiva.

Art. 179 Consideram-se informações estruturais e tecnológicas aquelas referentes a:

I. Estrutura de rede, topologia, endereçamento IP, VPNs e conexões seguras;

II. Especificações de servidores, storages, bancos de dados e data centers;

III. Sistemas corporativos, softwares utilizados, versões, senhas e parâmetros de configuração;

IV. Procedimentos de segurança, autenticação, criptografia, backup e controle de acesso;

V. Relatórios técnicos, manuais operacionais e diagramas de infraestrutura;

VI. Equipamentos, instalações, dispositivos e locais estratégicos de operação tecnológica;

VII. Estratégias de contingência, recuperação de desastres e medidas de defesa cibernética.

Art. 180 É vedado o compartilhamento não autorizado dessas informações por qualquer meio, incluindo, mas não se limitando a:

I. Correio eletrônico (interno ou externo);

II. Mensageiros instantâneos (WhatsApp, Telegram, Teams etc.);

III. Plataformas em nuvem, mídias removíveis ou dispositivos pessoais;

IV. Publicações em redes sociais, apresentações, reuniões, palestras ou eventos.

Art. 181 As informações estruturais e tecnológicas devem ser classificadas, no mínimo, como “reservadas”, conforme o item 1.2 desta Política, e tratadas de acordo com seu grau de criticidade.

Art. 182 Em caso de necessidade institucional de compartilhamento com terceiros, deverá haver autorização expressa da GEDADOS, mediante assinatura de Termo de Confidencialidade (NDA) e registro do processo em sistema oficial.

Art. 183 É proibido o uso de informações tecnológicas da CODERN em materiais de divulgação pública, estudos acadêmicos, apresentações, licitações, relatórios ou propostas externas sem autorização formal.

Art. 184 Qualquer indício de divulgação indevida, acidental ou intencional, deverá ser imediatamente comunicado à GEDADOS para análise e adoção das medidas cabíveis.

Art. 185 A infração às regras deste item constitui violação grave às Normas de Segurança da Informação, sujeitando o infrator às sanções administrativas, trabalhistas e legais previstas na legislação e nos normativos internos.

Art. 186 Compete à GEDADOS a análise e eventual aprovação de exceções às regras dispostas nesta Norma.

Art. 187 Todos os colaboradores das unidades da CODERN são responsáveis:

I. Por conhecer os princípios, diretrizes e responsabilidades desta política;

II. Por implementar ações de Segurança da Informação e garantia da Privacidade dos Dados, observando de forma específica as atribuições pertinentes a cada cargo e/ou função;

III. Pela segurança dos ativos, credenciais ou contas de acesso, e processos que estejam sob sua responsabilidade e por todos os atos executados com sua identificação;

IV. É proibida a exploração de falhas ou vulnerabilidades porventura existentes nos ativos de informação da CODERN.

Art. 188. Esta Política será revisada por tempo indeterminado, conforme recomendação dos órgãos de controle, necessidade institucional, alteração normativa ou deliberação da Alta Administração.

Art. 189. Esta Política entra em vigor na data de sua aprovação pelo CONSAD e pela DIREXE.

PAULO HENRIQUE DE MACEDO CARLOS
Diretor-Presidente

COMPANHIA DOCAS DO RIO GRANDE DO NORTE

RESOLUÇÃO Nº 1137 DE 10 DE DEZEMBRO DE 2025

O Diretor-Presidente da COMPANHIA DOCAS DO RIO GRANDE DO NORTE - CODERN, no uso da atribuição que lhe é conferida pelo Art. 60, Inciso VI do Estatuto Social da Companhia, **e considerando o deliberado pela Diretoria-Executiva em sua 2013ª reunião ordinária, realizada nesta data;**

R E S O L V E:

I. Aprovar o Instrumento Normativo denominado POLÍTICA DE SEGURANÇA DA INFORMAÇÃO (PSI 2025/2028), que tem como objetivo estabelecer o conjunto de critérios e procedimentos de segurança, elaborados, implantados, divulgados e em contínuo processo de monitoração, visando a confidencialidade, a integridade e a disponibilidade da informação, nos termos da minuta apresentada por meio da Proposição DP nº 073/2025 (Processo SEI nº 50902.002217/2025-25).

PAULO HENRIQUE DE MACEDO CARLOS

Diretor-Presidente

Documento assinado eletronicamente por **Paulo Henrique de Macedo Carlos**, **Diretor Presidente**, em 11/12/2025, às 10:48, conforme horário oficial de Brasília, com fundamento no art. 3°, inciso V, da Portaria nº 446/2015 do Ministério dos Transportes.

A autenticidade deste documento pode ser conferida no site https://sei.transportes.gov.br/sei/controlador_externo.php?acao=documento_conferir&acao_origem=documento_conferir&lang=pt_BR&id_orgao_acesso_externo=0, informando o código verificador **10643317** e o código CRC **96DE842C**.

Referência: Processo nº 50902.002398/2025-90 SEI nº 10643317

Av. Eng. Hildebrando de Gois, 220 - Bairro Ribeira
Natal/RN, CEP 59010-700
Telefone: 4005-5320

COMPANHIA DOCAS DO RIO GRANDE DO NORTE
CONSELHO DE ADMINISTRAÇÃO

DELIBERAÇÃO DO CONSELHO DE ADMINISTRAÇÃO Nº 072/2025

O CONSELHO DE ADMINISTRAÇÃO DA COMPANHIA DOCAS DO RIO GRANDE DO NORTE - CODERN, no uso das atribuições legais e estatutárias.

Considerando a Resolução nº 1137, de 10/12/2025, da Diretoria-Executiva.

De acordo com o resolvido na **768ª Reunião Ordinária**, realizada nesta data.

D E L I B E R A:

I. Aprovar o Instrumento Normativo denominado POLÍTICA DE SEGURANÇA DA INFORMAÇÃO (PSI 2025/2028), que tem como objetivo estabelecer o conjunto de critérios e procedimentos de segurança, elaborados, implantados, divulgados e em contínuo processo de monitoração, visando a confidencialidade, a integridade e a disponibilidade da informação, nos termos da minuta apresentada por meio da Proposição DP nº 057/2025 (Processo SEI nº 50902.002217/2025-25).

Natal/RN, 19 de dezembro de 2025.

LUÍZA DE AMORIM MOTTA DEUSDARÁ
Presidente do Conselho de Administração
Conselheira representante do MPOR

FELIPE MARTINS MATOS
Conselheiro representante do MPOR

VALBER PAULO MARTINS GOMES
Conselheiro representante do MPOR

OTÁVIO VIEGAS CAIXETA
Conselheiro representante do MGI

DARLAN EMANOEL SILVA DOS SANTOS
Conselheiro representante dos Empresários

JAMES TIBÚRCIO DE SOUZA
Conselheiro representante dos Empregados

Documento assinado eletronicamente por **James Tiburcio de Souza**, **Conselheiro(a) representante da classe dos trabalhadores**, em 21/12/2025, às 16:04, conforme horário oficial de Brasília, com fundamento no art. 3°, inciso V, da Portaria nº 446/2015 do Ministério dos Transportes.