COMPANHIA DOCAS DO RIO GRANDE DO NORTE – CODERN

PSI - POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Janeiro/2021

SUMÁRIO

1. DISPOSIÇÕES INICIAIS.....2

2. PRINCÍPIOS DA INFORMAÇÃO.....5

3. GESTÃO DA SEGURANÇA.....7

4. SENHAS.....8

5. USO DA INTERNET.....11

6. CORREIO ELETRÔNICO.....16

7. MONITORAMENTO.....22

8. DATACENTER.....23

9. BACKUP.....25

10. COMPUTADORES E RECURSOS TECNOLÓGICOS.....26

11. DA UTILIZAÇÃO DE MÍDIAS REMOVÍVEIS.....27

12. TRANSGREÇÕES E PENALIDADES.....28

13. RESPONSABILIDADES DO USUÁRIO.....29

14. DIREITO À PRIVACIDADE E PROTEÇÃO DE DADOS.....30

15. DISPOSIÇÕES FINAIS.....32

1. DISPOSIÇÕES INICIAIS

"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 somente ao seu propósito, que é o de informar, sem prejudicar quaisquer pessoas ou instituições, é necessário a gestão segura dos recursos disponíveis em tecnologia da informação.

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

- **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;
- **Confidencialidade:** garantia de que o acesso à informação seja obtido somente por pessoas autorizadas; e
- **Disponibilidade:** garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

1.1 APLICAÇÃO

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

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

Diante do exposto, a Política da Segurança da Informação vem propor uma Gestão de Segurança da Informação baseada em controles e procedimentos técnicos, considerando e promovendo

o comportamento dos colaboradores de forma que possa aplicar a tecnologia adequada em todo o processo e atingir efetividade em seu objetivo: entender o negócio e aplicar segurança a ele.

Não adianta a área da Tecnologia da Informação impor controles e medidas técnicas se não existir a participação dos colaboradores, de nada vale a implantação de barreiras e portas de controle de acesso eletrônico se um funcionário, que tem acesso legítimo a determinada área restrita, resolve divulgar informações confidenciais que estavam devidamente protegidas nesta área.

1.2 CLASSIFICAÇÃO DAS INFORMAÇÕES

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.** os seguintes níveis:

1 - ultrassecreta: 25 (vinte e cinco) anos;

2 - secreta: 15 (quinze) anos; e

3 - reservada: 5 (cinco) anos.

1.2.1 Ultrassecreta

Informações 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.

São informações de acesso restrito a um colaborador ou grupo de colaboradores. Sua revelação pode violar a privacidade de indivíduos, violar acordos de confidencialidade, dentre outros.

São exemplos de informações sigilosas:

- Exames e diagnósticos de pacientes;

- Processos judiciais; e

- Dados cadastrais de funcionários.

1.2.2 Secreta

São informações explicitamente aprovadas por seu responsável para consulta irrestrita e cuja divulgação externa não compromete o negócio e que, por isso, não necessitam de proteção efetiva ou tratamento específico.

São exemplos de informação pública:

- Editais de licitação;

- Rotinas e agendas médicas;

- Campanhas de promoção à saúde.

1.2.3 Reservada

São informações disponíveis aos colaboradores da CODERN para a execução de suas tarefas rotineiras, não se destinando, portanto, ao uso do público externo.

São exemplos de informações internas:

- Memorandos, Portarias, Padrões, Políticas e Procedimentos internos;

- E-mails e lista telefônica internos; e

- Avisos e campanhas internas.

2. PRINCÍPIOS DA INFORMAÇÃO

2.1 TRATAMENTO DA INFORMAÇÃO

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

2.1.2 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.

2.1.3 Devem constar nos contratos estabelecidos com terceiros, os documentos “Declaração de Consonância” com as “Normas de Segurança da Informação” devidamente autorizados.

2.1.4 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, através de assinatura da "Declaração de Consonância" com a Política de Segurança da Informação e das Comunicações, devendo ainda os respectivos setores informar à Coordenação de Tecnologia da Informação - COORTI quando do início ou término dos devidos contratos para a gestão correta da informação.

2.2 CONTROLE DE ACESSO

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

2.2.2 Os recursos da informação devem estar disponíveis aos usuários para o desempenho de suas atividades profissionais, segundo critérios estabelecidos pelos gestores destes recursos observando os princípios da economia, eficácia e segurança.

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

2.2.4 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 às ações necessárias para assegurar que os recursos sejam preservados quanto à integridade e confidencialidade.

2.3 CAPACITAÇÃO E CONSCIENTIZAÇÃO

2.3.1 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.

2.3.2 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 a importância para o desempenho de suas atividades.

2.3.3 A Coordenação de Tecnologia da Informação - COORTI encaminhará mensalmente dicas sobre a boa utilização dos recursos de informática em uso.

2.4 ESTABILIDADE DO AMBIENTE

2.4.1 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.

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

2.4.3 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 Coordenação de Tecnologia da Informação – COORTI, conforme o processo definido para o respectivo recurso.

2.4.4 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 a autorização para tal, 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 em ações administrativas e penalidades decorrentes de processos civil e criminal, sendo que nesses casos a instituição cooperará ativamente com as autoridades competentes.

3. GESTÃO DA SEGURANÇA

3.1 Cabe à Coordenação de Tecnologia da Informação - COORTI:

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

b) Difundir a cultura de segurança da informação;

c) Propor programas de treinamento em segurança da informação; e

d) Atualizar a instrução normativa conforme o crescimento e desenvolvimento de novas tecnologias.

3.2 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 reportados à Coordenação de Tecnologia da Informação – COORTI, para providências cabíveis, por intermédio da sua Equipe.

3.3 As Normas devem ser revisadas pela Coordenação de TI anualmente ou quando oportuno.

4. SENHAS

4.1 USO ADEQUADO

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

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

4.1.3 Os empregados, comissionados, estagiários e terceiros autorizados devem memorizar as suas senhas, não devendo registrá-las em meio que permitam a sua leitura por terceiros.

4.1.4 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.

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

4.1.6 A alteração da senha será solicitada automaticamente quando da sua expiração. Os empregados, comissionados, estagiários e terceiros autorizados não poderão acessar os recursos de informação caso, não seja realizada a alteração das suas respectivas senhas expiradas.

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

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

4.1.9 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.

4.2 REGRAS DE FORMAÇÃO

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

4.2.1.1 Evitar utilizar como conteúdo das senhas:

a) Caracteres repetidos consecutivamente (aaa,2222, aabbcc etc);

b) Caracteres em ordem ou alfabética (12345, abcdef, aeiou etc);

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

d) Datas de nascimento, casamento, números de telefone;

e) A própria identificação funcional, apelidos, abreviações, iniciais dos nomes etc;

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

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

a. Login: joaosilva

b. Senha: joaosilva123

4.2.1.2 Para os nossos requisitos de autenticação de senha exigem os seguintes critérios de complexidade:

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

Exemplos: Agu@246

14Aao()4

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

4.3 PROCESSOS

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

4.3.2 As senhas dos terceiros autorizados devem ser solicitadas através do formulário "Formulário de Cadastramento de Senhas da Rede", disponível na Intranet, pelos respectivos fiscais dos contratos ou pelos gestores das unidades nas quais estão alocados, a Coordenação de Recursos Humanos, que repassará esse pedido à Coordenação de Tecnologia da Informação – COORTI para sua liberação.

4.3.3 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.

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

5. USO DA INTERNET

Todas as regras atuais da CODERN visam basicamente o desenvolvimento de um comportamento eminentemente ético e profissional do 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.

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

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.

5.1 USO ADEQUADO

5.1.1 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:

a) Desenvolver negócios particulares;

b) Acessar sites com conteúdo incompatíveis com os princípios da CODERN, tais como: pornografia, incitação à violência, preconceitos em geral etc;

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

d) 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;

e) Comprometer a privacidade dos usuários ou o sigilo das informações;

f) Praticar jogos, jogos on-line;

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

h) 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;

i) Efetuar Upload (subida) de qualquer software licenciado à CODERN ou de dados de sua propriedade aos seus parceiros e clientes, sem expressa autorização do responsável pelo software ou pelos dados;

j) Acesso à 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;

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

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

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

5.1.3 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.

5.1.4 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.

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

5.1.6 Não serão permitidos os acessos a softwares peer-to-peer (Kazaa, BitTorrent, µtorrent e afins).

5.1.7 Não serão permitidos os acessos a sites de compartilhamento de arquivos, tais como: mega, uploaded, bitshare, depositfiles, etc.

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

5.1.9 Não serão permitidos 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 concedido autorização para tal.

Formatos proibidos:

a) Arquivos executáveis:

- exe;
- com;
- bat;

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

b) Arquivo 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.

c) Vídeo:

- Avi;
- Mpg;
- Mpeg;
- Asf;
- Wmf;
- Wmp;

- 3gp;
- Outros formatos de vídeo;
- Dentro de arquivo compactado; e
- Novos formatos de vídeos que venham a surgir.

d) Imagens em geral

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

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

5.1.8 A solicitação de uso de qualquer serviço, diferente dos descritos no Item 5.1, deve ser encaminhado formalmente com justificativa da necessidade de liberação ao acesso, à Coordenação de Tecnologia da Informação da Companhia.

6. CORREIO ELETRÔNICO

O objetivo destas normas é informar aos colaboradores da CODERN quais são as atividades permitidas e proibidas quanto ao uso do correio eletrônico corporativo.

6.1 USO ADEQUADO

6.1.1 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 de interesses da CODERN.

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

6.1.3 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 item 6.1.1.

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

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

6.1.6 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.

6.1.7 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.

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

a) Relativos a negócios particulares;

b) 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;

c) Propagandas comerciais, políticas partidárias e/ou religiosas;

d) Correntes e boatos;

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

f) Com informações que impliquem em violação de direito autoral; e

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

6.1.9 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 exemplo destes arquivos as extensões descritas abaixo:

a) Documento

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

b) Apresentação

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

c) Planilha eletrônica

- xls, xlsx; e
- ods.

d) Banco de dados

- mdb, mdbx e dbf.

e) Exemplo dos arquivos supracitados quando compactados

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

6.1.10 Os empregados, comissionados, estagiários e terceiros autorizados não devem abrir arquivos anexados às mensagens diferentes daqueles constantes no item 6.1.9 acrescidos das páginas Web (htm e html).

6.1.11 Os empregados, comissionados, estagiários e terceiros autorizados não devem abrir, devem excluir ou a seu critério, encaminhar à Coordenação de Tecnologias da Informação, 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 através de mensagens eletrônicas.

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

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

6.1.14. 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.

6.2 RESTRIÇÕES DE USO

6.2.1 Para garantir o desempenho e a disponibilidade do ambiente computacional da CODERN, a Coordenação de Tecnologia da Informação 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.

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

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

6.2.4 É proibido produzir, transmitir ou divulgar mensagem que:

- Vise obter acesso não autorizado a outro computador, servidor ou rede;
- Vise interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;
- Vise burlar qualquer sistema de segurança;
- Vise vigiar secretamente ou assediar outro usuário;
- Vise acessar informações confidenciais sem explícita autorização do proprietário;
- Tenha conteúdo considerado impróprio, obsceno ou ilegal;
- Seja de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico entre outros;
- Inclua material protegido por direitos autorais sem a permissão do detentor dos direitos;
- O uso de e-mails pessoais é aceitável, se usado com moderação, em caso de necessidade e quando:
- Não contrariar as normas aqui estabelecidas;
- Não interferir, negativamente, nas atividades profissionais individuais ou na de outros colaboradores;
- Não interferir, negativamente, na CODERN e na sua imagem.

6.3 PROCESSOS

6.3.1 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 Coordenação de Tecnologia da Informação para sua liberação.

6.3.2 A criação e atualização de listas públicas de distribuição devem ser solicitadas pelo gestor da unidade interessada à Coordenação de Tecnologia da Informação.

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

6.3.4 Quando do encerramento do contrato de prestação de serviços de terceiros autorizados, os ficais dos respectivos contratos deverão solicitar imediatamente, à Coordenação de Tecnologias da Informação, a exclusão do acesso ao correio eletrônico/demais recursos da rede corporativa.

7. MONITORAMENTO

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:

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

7.2 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;

7.3 A CODERN, por meio da Coordenação de Tecnologia da Informação, reserva-se o direito de realizar testes eletrônicos a fim de detectar:

a) Senhas frágeis;

b) No uso da internet na instituição, vulnerabilidade e falhas de seguranças a fim de preservar a integridade das informações; e

c) Uso adequado pelos empregados, estagiários e terceiros autorizados no correio eletrônico.

7.4 Os empregados, comissionados, estagiários e terceiros autorizados que possuírem senhas consideradas frágeis serão notificados pela Coordenação de Tecnologia da Informação para alteração das suas respectivas senhas; e

7.5 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.

8 – DATACENTER

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.

8.1 O acesso ao DATACENTER somente deverá ser feito por sistema de autenticação. Por exemplo: biometria, cartão magnético, entre outros.

8.2 Todo acesso ao DATACENTER, pelo sistema de autenticação, deverá ser registrado (usuário, data e hora) mediante software próprio ou comprado.

8.3 Deverá ser executada mensalmente uma auditoria nos acessos ao DATACENTER por meio do relatório do sistema de registro.

8.4 O usuário "administrador" do sistema de autenticação ficará sob a responsabilidade da Coordenação de Tecnologia da Informação, de acordo com o Procedimento de Controle de Contas Administrativas.

8.5 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.

8.6 Nas localidades em que não existam colaboradores da área de tecnologia da informação, 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.

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

8.8 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.

8.9 Caso haja necessidade do 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.

8.10 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.

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

8.12 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 Coordenação de TI da Companhia, de acordo com os termos do Procedimento de Controle e Transferência Patrimonial.

8.13 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.

9. BACKUP

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.

9.1 É de responsabilidade da Coordenação de Tecnologia da Informação 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 Coordenação de Tecnologia da Informação.

9.2 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.

9.3 Os dados armazenados nas estações de trabalho são de total responsabilidade do usuário que deverá solicitar orientações quanto ao procedimento a Coordenação de Tecnologia da Informação.

9.4 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.

9.5 São realizadas 02 (duas) Cópias dos backups, o armazenamento é feito na própria sede em locais distintos.

9.6 O Tempo de Retenção das Cópias é de 90 (noventa) dias.

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

9.8 O backup e restore dos dados na infraestrutura em nuvem pública (cloud computing) são de reponsabilidade da empresa contratada pelo serviço.

10. COMPUTADORES E RECURSOS TECNOLÓGICOS

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.

10.1 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 Coordenação de Tecnologia da Informação, ou de quem este determinar.

10.2 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.

10.3 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 Coordenação de Tecnologia da Informação ou por terceiros devidamente contratados para o serviço.

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

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

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

11. DA UTILIZAÇÃO DE MÍDIAS REMOVÍVEIS

11.1 É vedado a utilização de dispositivos removíveis com conexão USB ou WIRELESS nas estações de trabalho da CODERN.

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

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

11.4 Cabe à Coordenadoria de TI analisar e deliberar sobre os casos necessários de permissões de uso de dispositivos externos nas estações de trabalho, conforme o fluxo a seguir:

11.5 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;

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

11.7 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;

11.8 A Coordenadoria de TI 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;

11.9 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;

11.10 Revogam-se as disposições em contrário; e

11.11 Os casos omissos nesta Instrução serão dirimidos pela Coordenadoria de Tecnologia da Informação ou pelo Comitê de Segurança da Informação;

12. TRANSGREÇÕES E PENALIDADES

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:

12.1 A não observância por parte dos empregados, comissionados e estagiários da CODERN, do disposto nas presentes Normas, serão consideradas como falta grave, estando o infrator sujeito às penalidades previstas na Consolidação da Legislação Trabalhista – CLT;

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

a) 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;

b) 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.

13. RESPONSABILIDADES DO USUÁRIO

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

13.2 Além disso, o usuário é responsável por:

a) 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

b) Os arquivos e pastas pessoais, deverão estar separadas dos arquivos/pastas de âmbito institucional.

13.2.1 Nenhum software pode ser instalado nos computadores. Apenas os técnicos da Coordenação de Tecnologia da Informação 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;

13.2.2 Não é permitido utilização de computadores pessoais e nenhum outro dispositivo conectado à rede corporativa; e

13.2.3 Os equipamentos a serem liberados, deverão ser encaminhados à Coordenação de Tecnologia da Informação para análise e configuração dos mesmos, conforme padrões estabelecidos.

14. DIREITO À PRIVACIDADE E PROTEÇÃO DE DADOS

14.1 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, obtêm, trata, usa e armazena dados pessoais à medida que são necessários à gestão administrativa e dos negócios.

14.2 Os dados pessoais (sensíveis ou não) ou um conjunto de informações distintas que possam identificar ou discriminar uma pessoa física são sigilosos.

14.3 O tratamento dos dados pessoais é permitido somente nas seguintes situações:

a) se houver consentimento expresso do titular do dado;

b) para execução de contratos;

c) se decorrer de exigências legais e/ou regulatórias;

d) para proteção da vida ou da incolumidade física do titular ou de terceiros;

e) para proteção ao crédito, exceto quando tratar-se de dado pessoal sensível;

f) para atender interesse legítimo do controlador do dado ou de terceiros, exceto quando tratar-se de dado pessoal sensível;

g) garantia da prevenção à fraude e segurança do titular, quando tratar-se de dado pessoal sensível;

h) realização de estudos por órgão de pesquisa;

i) exercício regular de direitos em processos judiciais e administrativos;

j) tutela da saúde; ou

k) pela administração pública, quando da execução de políticas públicas.

14.4 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.

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

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

b) 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; e

c) antecipar riscos e eventos invasivos de privacidade antes que eles ocorram e tomar medidas para evitar danos aos colaboradores, gestores, fornecedores e clientes;

d) solicitar e tratar dados pessoais que sejam estritamente essenciais ao(s) objetivo(s) da Companhia; e

e) assegurar que os dados pessoais sejam utilizados exclusivamente para os fins informados previamente ao titular.

14.6 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:

a) 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;

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

c) cumprir com as obrigações legais e diretrizes de segurança da informação e demais normativos corporativos que versem sobre a privacidade de dados; e

d) implantar controles eficazes para mitigar os riscos de incidentes de segurança.

14.7 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.

15. DISPOSIÇÕES FINAIS

Compete à Coordenação de Tecnologia da Informação, a análise e eventual aprovação de exceções às regras dispostas nesta Norma.

Estas Normas de Segurança da Informação entram em vigor na data de sua publicação.

Diretor Presidente da CODERN

ANEXO I – TERMO DE COMPROMISSO

NOME:
SETOR:
MATRICULA:
E-MAIL:

Comprometo-me a:

1) Executar minhas tarefas de forma a cumprir com as orientações da Política de Segurança e com as Normas e Padrões vigentes;

2) Utilizar adequadamente os equipamentos da empresa, evitando acessos indevidos aos ambientes computacionais aos quais estarei habilitado, que possam comprometer a segurança das informações;

3) Não revelar, fora do âmbito profissional, fatos ou informações de qualquer natureza que tenha conhecimento devido a minhas atribuições, salvo em decorrência de decisão competente do superior hierárquico;

4) Acessar as informações somente por necessidade de serviço e por determinação expressa do superior hierárquico;

5) Manter cautela quanto à exibição de informações sigilosas e confidenciais, em tela, impressoras ou outros meios eletrônicos; e

6) Observar rigorosamente os procedimentos de segurança estabelecidos quanto à confidencialidade de minha senha.

Declaro estar ciente das determinações acima, compreendendo que quaisquer descumprimentos dessas regras podem implicar na aplicação de sanções disciplinares cabíveis.

Local: _____, _____ de _____ de _____.

_____

Assinatura do Colaborador

CODERN
AUTORIDADE PORTUÁRIA

IG SEST
NÍVEL 1

COMPANHIA DOCAS DO RIO GRANDE DO NORTE

RESOLUÇÃO Nº 233

Natal, 25 de março de 2021.

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 novo Estatuto Social da Companhia, **e considerando o deliberado pela Diretoria-Executiva em sua 1696ª reunião ordinária, realizada nesta data;**

R E S O L V E:

I. Aprovar a Norma de Política de Segurança da Informação (PSI), elaborada pela COORTI, nos termos da minuta apresentada por meio da Proposição DP nº 015/2021, Processo SEI 50902.001605/2021-65.

ELIS TREIDLER ÖBERG

Almirante de Esquadra

Diretor-Presidente

Documento assinado eletronicamente por **Elis Treidler Oberg**, **Diretor Presidente**, em 26/03/2021, às 14:32, 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.infraestrutura.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **3904935** e o código CRC **B9FA9404**.

Referência: Processo nº 50902.001667/2021-77 SEI nº 3904935

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