COMPANHIA DOCAS DO RIO DE JANEIRO
DIRETORIA ADMINISTRATIVO FINANCEIRA
SUPERINTENDÊNCIA DE TECNOLOGIA DA INFORMAÇÃO
GERÊNCIA DE ESTRUTURAÇÃO E CONSTRUÇÃO DE SOLUÇÕES

Documento nº 5656820/2022/GERCOS-CDRJ/SUPTIN-CDRJ/DIRAFI-CDRJ

Rio de Janeiro, 27 de maio de 2022.

Processo nº 50905.001042/2022-66

Interessado: CDRJ

1. **INTRODUÇÃO**

O presente documento visa o estabelecimento das diretrizes e competências que garantam a disponibilidade, integridade, confidencialidade e autenticidade dos dados, informações e documentos produzidos, armazenados ou transmitidos no âmbito da Companhia Docas do Rio de Janeiro.

A Política de Segurança da Informação e Comunicação (POSIC) na CDRJ aplica-se a todos os empregados, terceirizados, sistemas e serviços, incluindo trabalhos executados externamente ou por terceiros, que utilizem o ambiente de processamento ou as informações sob responsabilidade da CDRJ.

2. **MISSÃO DA SUPERINTENDÊNCIA DE TECNOLOGIA DA INFORMAÇÃO (SUPTIN)**

Gerir o processo de segurança de TIC e proteger as informações da organização, catalisando, coordenando, desenvolvendo e/ou implementando ações para esta finalidade.

3. **OBJETIVO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO**

Estabelecer e difundir normas, diretrizes e procedimentos que viabilizem o acesso seguro às informações corporativas de modo que não impeçam e/ou dificultem o processo do negócio, mas garantam os aspectos de integridade, confidencialidade e disponibilidade dos dados e informações sob responsabilidade da CDRJ e a participação e cumprimento de todos os colaboradores nesse processo.

4. **DA VIOLAÇÃO DA POLÍTICA DE SEGURANÇA**

O não cumprimento dessas políticas poderá ser considerado uma infração e estará passível às punições administrativas cabíveis.

5. **CONCEITOS E DEFINIÇÕES**

5.1. **Ameaça:** Conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização;

5.2. **Ativos de Informação**: Conjunto de conhecimento organizado e gerenciado como uma

entidade única. Pode ser uma base de dados, arquivos, contratos e acordos, documentação de sistema, informações sobre pesquisa, manuais de usuário, material de treinamento, etc., bem como os sistemas de informação e os equipamentos necessários para a transmissão e processamento de dados (computadores, equipamentos de comunicação e de interconexões);

5.3. **Área de trabalho**: É a principal área exibida na tela quando o computador é ligado;

5.4. **Área digital sensível:** Área considerada vital para o pleno funcionamento da Companhia, em função do material digital existente na mesma ou das atividades digitais ali desenvolvidas;

5.5. **Área digital sigilosa:** São áreas sensíveis que abrigam material digital sigiloso;

5.6. **Autenticidade**: Propriedade que assegura que a informação é realmente da fonte que se declara ser;

5.7. **Backup**: Cópia de segurança de dados e informações realizada em dispositivo de armazenamento secundário, buscando a sua preservação em caso de perda ou indisponibilidade;

5.8. **Compartimentação Digital:** É o resultado eficaz de todas as medidas que visam a restringir o acesso a dados e conhecimentos digitais sigilosos às pessoas que não possuem a necessidade de conhecer;

5.9. **Confidencialidade**: Propriedade de que a informação não esteja disponível ou revelada a indivíduos, entidades ou processos não autorizados;

5.10. **Controle de Acesso:** Conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso;

5.11. **Credencial de acesso:** Um conjunto de informações (usuário e senha, por exemplo) que concede um determinado acesso de um indivíduo pré-cadastrado a um ambiente específico, como um computador ou uma rede corporativa;

5.12. **Diretório ou pasta:** Subdivisão lógica de um sistema de arquivos, que permite o agrupamento de arquivos que se relacionam de alguma forma;

5.13. **Disponibilidade**: Propriedade de estar acessível e utilizável, sob demanda, por uma entidade autorizada;

5.14. **Firewall**: Dispositivo de segurança de rede que monitora o seu tráfego de entrada e saída, permitindo ou bloqueando tráfegos específicos de acordo com um conjunto definido de regras de segurança;

5.15. **Hardware**: Envolve toda infraestrutura física de tecnologia de uma organização, oferecendo todo o suporte em armazenamento, processamento, nas transações e no uso das informações. São computadores, servidores, dispositivos de armazenamento, roteadores, switches, etc.;

5.16. **Incidente de segurança**: Qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;

5.17. **Integridade**: Propriedade de salvaguarda da precisão e consistência de dados durante todo o ciclo de vida da informação. A informação não pode ser alterada ou destruída sem a autorização adequada;

5.18. **LOG**: Termo técnico utilizado para descrever o registro das transações que ocorrem quando um software é utilizado;

5.19. **Logon:** Processo utilizado para acessar uma rede de computadores ou sistema informatizado restrito, realizado através da autenticação ou identificação do utilizador, usando credenciais previamente cadastradas no sistema;

5.20. **Logoff:** Processo utilizado para encerrar o acesso a uma rede de computadores ou um sistema informatizado restrito, realizado através da autenticação ou identificação do utilizador, usando credenciais previamente cadastradas no sistema;

5.21. **Mídias Removíveis**: Dispositivos que permitem a leitura e gravação de dados tais como: CD, DVD, Pen Drive, cartão de memória entre outros;

5.22. **Não repúdio**: Propriedade que assegura que nem o emissor nem o receptor de uma informação possam negar o fato, a autoria, a responsabilização;

5.23. **Proprietário da Informação**: Pessoa ou setor que produz a informação;

5.24. **Rede Corporativa:** Sistema de transmissão de dados que transfere ou compartilha informações entre diversos equipamentos de uma mesma corporação, tais como: computadores, servidores de documentos e arquivos, impressoras, etc; e entre alguns desses equipamentos com o mundo externo;

5.25. **Servidor de arquivos**: Ambiente dedicado ao armazenamento de arquivos na rede corporativa;

5.26. **Severidade**: Índice ou grau que se refere à medição do impacto de um evento ou incidente de segurança da informação;

5.27. **Software**: É todo programa executado em um computador, celular ou dispositivo que permita ao mesmo executar suas funções. Exemplo: sistemas operacionais e aplicativos;

5.28. **SPAM**: Tipo de mensagem eletrônica recebida pelo usuário sem que este tenha solicitado ou considere a hipótese de recebê-la. Em geral, essa prática tem finalidade comercial, mas também pode ser um meio para a disseminação de golpes (phishing), boatos, difamação, malwares, etc;

5.29. **USB (Universal Serial Bus):** É um padrão de tecnologia que permite a conexão e comunicação ente dispositivos, como teclados, mouses, mídias removíveis, etc.;

5.30. **Usuário**: Pessoa física ou jurídica, com vínculo oficial com a CDRJ ou em condição autorizada por ela que utiliza algum Recurso de TIC ou alguma informação de sua propriedade ou responsabilidade, em qualquer uma de suas formas. São empregados, terceirizados, colaboradores, consultores, auditores, estagiários e jovens aprendizes que obtiveram autorização do responsável pela área interessada para acesso aos Ativos de Informação;

5.31. **VPN (Virtual Private Network**): Modalidade de acesso remoto à rede corporativa utilizando uma rota criptografada. Comumente é utilizado por funcionários em trânsito ou em *home office*.

6. **DAS RESPONSABILIDADES GERAIS**

6.1. Compete a todos os usuários de recursos informatizados da CDRJ:

6.1.1. Acessar somente as informações e os ambientes previamente autorizados. Qualquer tentativa de acesso a ambientes não autorizados será considerada uma violação desta política.

6.1.2. Manter inalterada a configuração dos equipamentos informatizados disponibilizados pela Companhia, seguindo os devidos controles de segurança exigidos pela Política de Segurança da Informação e Comunicação e pelas normas específicas da instituição. Qualquer alteração de configuração nos ativos de TI será considerada uma violação desta política.

6.1.3. Acessar a rede corporativa utilizando-se somente de suas credenciais de acesso, não sendo autorizada a utilização de credenciais “genéricas”.

6.1.4. Assegurar a confidencialidade de sua senha de acesso à rede corporativa e aos sistemas informatizados, sendo proibida a sua anotação em suportes físicos de acesso coletivo.

6.1.5. Modificar a sua senha a cada 45 (quarenta e cinco) dias. Alertas automáticos serão apresentados ao usuário para avisá-lo sobre o prazo e a necessidade da alteração da senha. Conforme a criticidade estabelecida ao ativo e às atividades desempenhadas, o prazo para alteração de senha pode ser inferior ou superior ao estabelecido neste item.

6.1.6. Não armazenar, transmitir ou compartilhar conteúdo indevido ou ilegal nos ativos de propriedade e/ou sob responsabilidade da CDRJ.

6.1.7. Não revelar, publicar ou divulgar quaisquer informações de propriedade ou sob a responsabilidade da CDRJ, sem prévia autorização.

6.1.8. As Unidades Administrativas devem observar as seguintes diretrizes fundamentais ao classificar e tratar informações da CDRJ:

I - A classificação de informações deve observar a publicidade como preceito geral e a atribuição do sigilo como exceção, conforme inciso I do artigo 3º da Lei 12.527/2011, de 18/11/2011 (Lei de Acesso à Informação), e o princípio da transparência, conforme consta no IN. OUVGER 01.008, de 26/08/2019;

II - As informações devem ser classificadas e tratadas segundo critérios e procedimentos estabelecidos em Instrumento Normativo que disponha sobre o assunto, atualmente o IN OUVGER 01.008, de 26/08/2019;

III - Os colaboradores devem observar as orientações do Instrumento Normativo supracitado para garantir o adequado tratamento às informações sigilosas, especialmente para evitar sua exposição indevida, o que começa com a adoção de cuidados básicos como, por exemplo, a guarda dos documentos em gavetas ou arquivos com tranca, a manutenção da mesa sem documentos ou informações sigilosas (mesa limpa) e a estação de trabalho bloqueada nos momentos de ausência de uso;

IV - O tratamento de informação relacionada a pessoa natural identificada ou identificável, especialmente de dados pessoais sensíveis, deve observar as exigências e os princípios da Lei 13.709/2018, de 14/08/2018 (Lei Geral de Proteção de Dados), com destaque à necessidade de consentimento pelo titular e, para os princípios da finalidade, da adequação, da necessidade, da transparência, da segurança e da prevenção.

V - A disponibilidade e a proteção das informações devem ocorrer de acordo com a sua classificação e de forma a preservar a continuidade de negócios da Companhia;

VI - Cláusulas de sigilo e confidencialidade devem constar nos contratos estabelecidos com profissionais terceirizados, prestadores de serviços e estagiários.

6.1.9. adotar política de mesa e tela limpa a fim de reduzir os riscos de acessos não autorizados, perda e dano da informação durante e fora do horário normal de trabalho.

I - informações sensíveis ou críticas, por exemplo, em papel ou mídia de armazenamento eletrônico, sejam guardadas em lugar seguro (idealmente em cofre, armário ou outras formas de mobília de segurança) quando não em uso, especialmente quando a sala está desocupada;

II - computadores e terminais sejam mantidos desligados ou protegidos com mecanismos de travamento de tela, com senha, ou mecanismos de autenticação similar quando sem
monitoração ou não usados;

7. DAS RESPONSABILIDADES ESPECÍFICAS

7.1. **Do Diretor/Superintendente/Gerente/Supervisor de cada área**

7.1.1. Ter postura exemplar em relação à segurança da informação, servindo como modelo de conduta para os colaboradores sob a sua gestão.

7.1.2. Estabelecer critérios relativos ao nível de confidencialidade da informação (relatórios e/ou mídias) gerada por sua área de acordo com a classificação abaixo:

a) **Informação Pública:** É toda informação que pode ser acessada por usuários da organização, clientes, fornecedores, prestadores de serviços e público em geral;

b) **Informação Restrita:** É toda informação que pode ser acessada exclusivamente pelas unidades (setores) da organização nas quais seu conteúdo foi delegado. São informações que possuem um certo grau de confidencialidade que pode comprometer a imagem da organização. Todo documento criado no SEI!, que contenha dado pessoal, deve ser possuir a classificação "restrito";

c) **Informação Sigilosa:** É toda informação que pode ser acessada somente por usuários da organização explicitamente indicado pelo nome e área a que pertence. A divulgação não autorizada dessa informação pode causar sérios danos ao negócio e/ou comprometer a estratégia de negócio da organização.

7.1.3. O acesso à informação deve ser autorizado apenas para os usuários que necessitam da mesma para o desempenho das suas atividades profissionais relacionadas à CDRJ.

7.1.4. Exigir dos colaboradores a assinatura do Termo de Compromisso e Ciência, assumindo o dever de seguir as normas estabelecidas e de manter sigilo e confidencialidade, mesmo quando desligado, sobre todos os ativos de informações.

7.1.5. Solicitar à GERSOL a exclusão de toda e qualquer informação pessoal de colaboradores transferidos, cedidos ou desligados que, eventualmente, esteja armazenada nos computadores e dispositivos informatizados sob sua responsabilidade.

7.1.6. Solicitar o apoio da SUPTIN ou de suas gerências subordinadas, em qualquer projeto que tenha como ferramenta, o uso de sistemas computacionais ou que necessite de infraestrutura de TIC. A SUPTIN não se responsabilizará por equipamentos informatizados e sistemas nos quais não tenha sido consultada em momento anterior à sua aquisição/ contratação.

7.1.7. Prever em suas contratações que os dispositivos informatizados utilizados pelas empresas contratadas possuam os requisitos mínimos de segurança adotados pela CDRJ.

7.1.8. Solicitar inspeção da GERSOL, nos casos de mudança ou alteração do espaço físico das instalações sob sua responsabilidade, para avaliação da infraestrutura de rede.

7.2. **Do Gerente da GERARH – Gerência de Administração de Recursos Humanos**

7.2.1. Informar à GERSOL e a GERCOS as ocorrências que justifiquem a ativação, bloqueio ou alteração no acesso de empregados à rede corporativa e sistemas informatizados da CDRJ, tais como:

a) Admissão;

b) Transferência de empregado;

c) Cessão de empregado;

d) Afastamento por licença não remunerada;

e) Afastamento por licença médica superior a 15 dias;

f) Férias;

g) Desligamento.

7.3. **Do Gerente da GERCAR – Gerência de Gestão de Carreira**

7.3.1. Informar à GERSOL e a GERCOS as ocorrências que justifiquem a ativação, bloqueio ou alteração no acesso de estagiários e jovens aprendizes à rede corporativa e sistemas informatizados da CDRJ, tais como:

a) Admissão;

b) Transferência de lotação;

c) Afastamento por licença médica superior a 15 dias;

d) Férias;

e) Desligamento.

7.4. **Da Gestão/Fiscalização dos Contratos**

7.4.1. Solicitar à SUPTIN, através do preenchimento do FORMULÁRIO DE SOLICITAÇÃO DE RECURSOS DE TIC PARA TERCEIROS 5290055, o que for necessário ao bom desempenho das atividades do Contrato. No caso de renovação do contrato com a empresa terceirizada, os formulários deverão ser reenviados informando o novo prazo de utilização do recurso.

7.4.2. Dar ciência do teor desta Política aos terceirizados que estiverem atuando nos contratos sob sua responsabilidade.

7.5. **Da Gerência de Operação de Soluções - GERSOL**

7.5.1. Garantir a publicação, manutenção, atualização e aplicação das normas estabelecidas nesta POSIC.

7.5.2. Garantir a disponibilidade, confidencialidade, integridade, autenticidade e não repúdio das informações que tenham sido armazenadas por sistemas homologados pela GERCOS, seguindo esta POSIC.

7.5.3. Habilitar e manter o acesso à rede informatizada da CDRJ a todo usuário, considerando os níveis de acesso especificado pelas áreas.

7.5.4. Configurar os equipamentos, ferramentas e sistemas concedidos aos colaboradores com todos os controles necessários para cumprir os requerimentos de segurança estabelecidos por esta POSIC.

7.5.5. Administrar, proteger e testar as cópias de segurança dos sistemas e informações relacionados aos processos críticos e relevantes para a CDRJ.

7.5.6. Proteger continuamente todos os ativos de informação da empresa e garantir que todos os novos ativos só entrem para o ambiente de produção após estarem livres de código malicioso e/ou indesejado.

7.5.7. Em caso de violação das políticas estabelecidas nesse documento, monitorar o acesso a recursos de TI, de forma que seja possível auditar e rastrear a identidade do usuário responsável.

7.5.8. Garantir, após o encaminhamento da GERARH, o bloqueio de acesso de usuários por motivo de desligamento da empresa, incidente, investigação ou outra situação que exija medida restritiva para salvaguardar os ativos da empresa.

7.5.9. Elaborar, manter e publicar um Plano de Contingência de TI, com a finalidade de dirimir o impacto e os riscos de incidentes relacionados à segurança de TI.

7.5.10. Elaborar, manter e publicar um Plano de backup dos sistemas e informações relacionados

aos processos críticos e relevantes para a CDRJ.

8. **DIRETRIZES DE ACESSO**

8.1. Todo acesso aos dados e informações sob responsabilidade da CDRJ deve ser controlado de forma a garantir que somente os usuários autorizados pelo respectivo proprietário da informação tenham condições de acessá-la. O controle deverá adotar mecanismos físicos e lógicos específicos, de acordo com o tipo de acesso.

8.2. **Controle de Acesso Lógico:**

8.2.1. O controle de acesso lógico permite a verificação da identidade dos usuários a partir de informações de credenciais de acesso pré cadastradas nos sistemas informatizados.

8.2.2. **Criação de contas**

8.2.2.1. Será concedida uma conta de acesso à rede corporativa aos seguintes colaboradores:

a) Empregados;

b) Estagiários e jovens aprendizes;

c) Prestadores de serviço que necessitem de acesso, mediante solicitação prévia da fiscalização do respectivo contrato; e

d) Auditores de entidades públicas externas, mediante solicitação da AUDINT, DIRPRE e SUOCOL.

8.2.3. A inclusão de um novo usuário à rede corporativa da CDRJ dar-se-á mediante abertura de chamado técnico, onde o requisitante deverá incluir as seguintes informações:

a) Nome completo;

b) Lotação;

c) Diretórios e sistemas nos quais o usuário deverá ter acesso.

8.2.4. O padrão adotado para a criação de conta do usuário será <*primeiro_nome.ultimo_sobrenome*>, salvo na ocorrência de homônimos.

8.2.5. Os perfis de conta serão administrados pela GERSOL, que avaliará cada caso, aplicando os atributos de acesso mínimos necessários às atividades dos usuários.

8.3. **Manutenção de conta**

8.3.1. Todas as contas serão monitoradas pela equipe de GERSOL com o objetivo de verificar possíveis irregularidades no acesso à rede e demais serviços informatizados, tais como:

a) Acesso indevido às pastas de outros setores;

b) Acesso não autorizado às impressoras coloridas;

c) Acesso a sites de conteúdo não permitido e;

d) Acesso a equipamentos ou sistemas informatizados não autorizados.

8.3.2. Caso seja identificada alguma irregularidade, a GERSOL procederá imediatamente com os meios necessários à adequação do acesso, sem aviso prévio, visando a manutenção da segurança da rede corporativa e dos sistemas informatizados.

8.4. **Desativação de conta**

8.4.1. O usuário terá a sua conta desativada nos casos de:

a) Desligamento do empregado, estagiário ou jovem aprendiz;

b) Aposentadoria;

c) Licença sem vencimentos;

d) Cessão para outro órgão ou entidade pública;

e) Licença médica por período superior a 15 dias;

f) Gozo de férias, à exceção de empregados ocupantes de cargo comissionado;

g) Desligamento do empregado da empresa terceirizada que utiliza recursos informatizados da CDRJ e;

h) Término do contrato com a empresa terceirizada que utiliza recursos informatizados da CDRJ. Nesse caso, todos os usuários ligados a contratada terão suas contas desativadas.

8.4.2. Após o período de 180 dias, a conta desativada será permanentemente excluída do ambiente de dados da CDRJ, não sendo possível a sua reativação.

8.5. **Controle de Acesso Físico:**

8.5.1. Por questão de segurança, é obrigatório o uso de identificação física (crachá) em local visível em todos os ambientes e instalações da CDRJ;

8.5.2. Todos os recursos computacionais críticos da CDRJ devem ser mantidos em ambientes reservados, monitorados e com acesso físico controlado, não sendo permitida a entrada de pessoas não autorizadas pela SUPTIN/GERSOL.

9. **DIRETRIZES PARA CRIAÇÃO DE SENHAS**

9.1. Toda a conta criada receberá uma senha temporária que possibilite o primeiro acesso ao usuário.

9.2. O usuário deverá realizar a troca imediata senha, atendendo aos seguintes requisitos mínimos:

a) Possuir 8 (oito) caracteres;

b) Possuir 1 (um) caractere maiúsculo (A-Z);

c) Possuir 1 (um) caractere minúsculo (a-z);

d) Possuir 1 (um) número de 0 a 9;

e) Possuir 1 (um) caractere especial (@_&! $ # %=).

9.3. A senha não poderá ser igual às 3 (três) últimas senhas geradas pelo usuário.

9.4. Após cinco tentativas de acesso, a conta do usuário será bloqueada. Para o desbloqueio é necessário que o superior hierárquico do usuário abra um chamado no *helpdesk* solicitando a sua reativação.

9.5. Os usuários podem alterar a própria senha e devem ser orientados a fazê-la, caso haja suspeita de que terceiros estejam utilizando indevidamente as suas credenciais.

9.6. Em caso de esquecimento ou necessidade de troca por motivo de segurança, o usuário deverá acessar https://trocadesenha.portosrio.gov.br, realizar o cadastro e inserir nova senha.

9.7. O usuário deve evitar a utilização de nomes, datas especiais e sequências óbvias de números e letras.

9.8. A periodicidade máxima para troca das senhas é 45 (quarenta e cinco) dias.

9.9. Todos os recursos tecnológicos adquiridos pela CDRJ devem ter imediatamente suas senhas iniciais alteradas assim que forem instalados.

10. DIRETRIZES DE UTILIZAÇÃO DOS SERVIÇOS DE TI

10.1. Rede Corporativa

10.1.1. O acesso à rede corporativa é concedido exclusivamente para os usuários listados no item 8.2.2, mediante a utilização de suas respectivas credenciais.

10.1.2. A credencial de acesso do usuário é pessoal e intransferível, não sendo permitida a utilização da conta de terceiros para acessar à rede da CDRJ.

10.1.3. Antes de ausentar-se do seu local de trabalho, o usuário deve realizar *logoff* em todos os sistemas em uso e bloquear sua área de trabalho, evitando assim o acesso por pessoas não autorizadas.

10.1.4. As estações de trabalho são bloqueadas automaticamente em 5 minutos de ociosidade.

10.1.5. Não são permitidas alterações das configurações de rede e inicialização das máquinas.

10.1.6. É vedado o acesso à rede interna da CDRJ, por meio de computadores próprios, ou seja, não fornecidos pela CDRJ.

10.2. Internet

10.2.1. A internet deve ser utilizada para fins corporativos, enriquecimento intelectual ou como ferramenta de busca de informações, de modo a contribuir para o desenvolvimento de atividades relacionadas à empresa.

10.2.2. Toda estação de trabalho inspecionada e homologada pela GERSOL, terá acesso controlado à Internet.

10.2.3. Qualquer informação que é acessada, transmitida, recebida ou produzida na internet está sujeita a divulgação e auditoria. Portanto, a CDRJ, em conformidade legal, reserva-se no direito de monitorar e registrar todos os acessos.

10.2.4. Os equipamentos, tecnologia e serviços fornecidos para o acesso à internet de propriedade da CDRJ poderão, a qualquer tempo, ser analisados e, se necessário, sofrer intervenções pela equipe da GERSOL e GERCOS para o bloqueio de arquivo, site, correio eletrônico, domínio ou aplicação armazenados, estejam eles em disco local da estação de trabalho ou em áreas privadas da rede, visando assegurar o cumprimento desta POSIC.

10.2.5. É vedado aos usuários, no uso do serviço de internet:

a) Utilizar programas ou *plugins* de camuflagem de navegação, deleção de histórico de navegação, de desvio de proxy e/ou tunelamento de navegação;

b) Abrir arquivos executáveis, com a extensão *.exe*, ou equivalentes, não autorizados pela CDRJ;

c) Efetuar o upload indevido de qualquer conteúdo de propriedade da CDRJ;

d) Acessar sites ou programas de compartilhamento de arquivos do tipo P2P, tais como, Skype, BitTorrent e o Emule, por exemplo;

e) Acessar sites de jogos on-line ou stand-alone (sem conexão de Internet);

f) Acessar sites que menosprezem, depreciem ou incitem o preconceito a determinadas classes;

g) Acessar sites que possibilitem a distribuição de informações de nível restrito ou sigiloso;

h) Acessar sites que permitam a transferência (downloads) de arquivos e/ou programas ilegais e;

i) Acessar sites de pornografia, pedofilia e incitação ao terrorismo.

10.2.6. Por ser passível de investigação criminal, será considerada infração grave o acesso aos conteúdos listados no subitem 10.2.5-i, estando o usuário sujeito a sanções administrativas e denúncia no conselho de ética, devendo à CDRJ, caso julgue necessário, proceder com a comunicação às autoridades competentes.

10.2.7. O acesso e uso de mídias sociais a partir da rede corporativa da CDRJ é permitido somente aos usuários lotados na ASSCOM, no estrito exercício de suas atividades.

10.2.8. O acesso e uso de sites da categoria "áudio/vídeo" será concedido apenas para atividades relacionadas ao treinamento de empregados e palestras de interesse da CDRJ, mediante abertura de chamado técnico.

10.2.9. No caso de um site bloqueado, cujo conteúdo esteja em conformidade com as regras e diretrizes do presente documento, o usuário pode solicitar a liberação de acesso junto a GERSOL, mediante abertura de chamado técnico.

10.3. **Intranet e Site institucional**

10.3.1. Toda estação de trabalho inspecionada e homologada pela GERSOL terá acesso irrestrito à página inicial da Intranet e ao site institucional da Companhia. As estações de trabalho que estão fora do ambiente da CDRJ necessitarão fazer *login* para acessar a página inicial e os demais conteúdos da Intranet.

10.3.2. A Intranet da CDRJ possui recursos de Gerenciamento de Conteúdo. Para maiores detalhes sobre como publicar informações, deve-se utilizar o IN.OUVGER.01.008 e o IN.OUVGER.01.009 como referência.

10.3.3. O Gerenciador de Conteúdo registra os dados de cada publicação criada, com a finalidade de identificar o autor e a data da publicação. É proibida a publicação de conteúdo diferente do especificado para cada área, conforme o exposto no IN.OUVGER.01.009.

10.4. **E-mail Corporativo**

10.4.1. O correio eletrônico (e-mail) fornecido pela CDRJ é o instrumento de comunicação interna e externa oficial para a realização do negócio da empresa.

10.4.2. É conferido a todo empregado da CDRJ em exercício, uma conta de e-mail institucional, sob o domínio oficial da CDRJ (portosrio.gov.br), destinada a finalidades profissionais.

10.4.3. A conta de e-mail institucional disponibilizada ao usuário é pessoal e intransferível, sendo seu titular o único e total responsável pelo seu uso e suas consequências.

10.4.4. A caixa postal corporativa possui um limite máximo pré-definido para o armazenamento das mensagens. Em caso de necessidade, o usuário poderá pedir o aumento de sua capacidade, mediante abertura de chamado técnico. A GERSOL fará a análise da justificativa e da viabilidade da solicitação.

10.4.5. O usuário deve efetuar, periodicamente, a limpeza de sua caixa postal corporativa, com a exclusão das mensagens desnecessárias e esvaziamento da lixeira, para não exceder o limite de armazenamento.

10.4.6. É vedada a utilização do e-mail institucional para:

a) Enviar mensagem cujo conteúdo possa gerar, de forma direta ou indireta, riscos à imagem institucional da CDRJ;

b) Realizar cadastros para fins pessoais (comércio, acessos a sites, etc...);

c) Reenviar ou propagar mensagens em cadeia (correntes), independentemente da vontade do destinatário de receber tais mensagens;

d) Utilizá-lo com objetivos político-partidários, religiosos, entre outros;

e) Abrir mensagens consideradas suspeitas ou caracterizadas como spam e *phishing scam;*

f) Abrir e-mail que contenham arquivos anexos com as extensões .bat,, .exe,.src,.lnk.

g) Produzir, armazenar, transmitir ou divulgar mensagem que:

I - Que não sejam compatíveis com a missão, visão e valores da CDRJ;

II - Represente uma quebra da confidencialidade de informações relacionadas à CDRJ ou aos terceiros com as quais mantenham relação;

III - Caracterize invasão da privacidade e/ou intimidade de terceiros.

10.4.7. O bloqueio da conta de e-mail institucional do usuário deve ser realizado nas seguintes situações:

a) Desligamento do empregado;

b) Encerramento de seu contrato junto à CDRJ (no caso de terceiros);

c) Concessão de licença não remunerada; e

d) Cessão do empregado a outro órgão ou entidade governamental.

10.4.8. O bloqueio é realizado pela GERSOL, na comunicação do desligamento do usuário, efetuada pela GERARH.

10.4.9. Os arquivos a serem anexados às mensagens no correio eletrônico institucional não poderão ultrapassar 30MB.

10.4.10. A caixa de e-mail do usuário será mantida, após a desativação, pelo período de 30 dias, não sendo possível a sua recuperação depois desse prazo.

10.5. **Pasta Pública**

10.5.1. A rede de dados da CDRJ dispõe de pasta pública destinada ao compartilhamento de arquivos entre usuários de setores distintos, possibilitando a troca de arquivos grandes, o que não seria possível através de e-mail.

10.5.2. É vedada a inclusão de arquivos que contenham informações restritas e sigilosas na pasta pública.

10.5.3. Por se tratar de uma pasta para compartilhamento transitório de arquivos, a pasta pública não será incluída nos procedimentos de backup da GERSOL, sendo impossível realizar a restauração de arquivos, no caso de exclusão acidental.

10.5.4. A GERSOL realizará a limpeza mensal da pasta COMUM, no último dia útil do mês corrente.

10.6. **Diretórios de rede**

10.6.1. A rede de dados da CDRJ dispõe de diretórios exclusivos para cada um dos seus setores, para o armazenamento e a gestão de seus arquivos.

10.6.2. O acesso às pastas será restrito aos colaboradores do setor para leitura, gravação e/ou exclusão de arquivos e subpastas.

10.6.3. Arquivos pessoais e/ou não pertinentes ao negócio da CDRJ (fotos, músicas, vídeos, etc.) não deverão ser salvos/copiados/movidos para estas pastas.

10.7. **Acesso remoto**

10.7.1. Todo acesso à rede corporativa da CDRJ realizado externamente (acesso remoto) deverá ser feito a partir de uma ferramenta de VPN disponibilizada pela GERSOL.

10.7.2. A concessão de uso de acesso remoto deve ser realizada de modo a atender aos objetivos de negócio da CDRJ, sendo restrita aos usuários autorizados pelas superintendências a que são subordinados, limitado às atribuições do usuário, sendo vedado o acesso para outras finalidades e em horário diverso ao período regular de trabalho.

10.7.3. A definição dos usuários que terão acesso remoto concedido deverá levar em consideração critérios objetivos e criteriosos, de forma a garantir que somente o mínimo necessário para a boa execução das atividades seja autorizado.

10.7.4. O acesso remoto a uma rede de dados da CDRJ deve ser realizado por meio de canal criptografado e solicitação de dupla autenticação do usuário.

10.7.5. O usuário que utiliza os recursos de acesso remoto ao ambiente corporativo da CDRJ deve proteger suas credenciais de acessos e realizar o encerramento da sessão ao término de suas atividades.

10.7.6. A GERSOL pode desabilitar ou restringir as condições de acesso remoto de qualquer usuário que descumprir com as disposições do presente documento, demonstrar incapacidade ou negligência no uso desta facilidade tecnológica.

11. **DIRETRIZES DE UTILIZAÇÃO DOS EQUIPAMENTOS INFORMATIZADOS**

11.1. **Servidores**

11.1.1. O acesso aos servidores é exclusivo aos usuários da SUPTIN e gerências subordinadas com perfil de administrador.

11.1.2. Todo servidor, físico ou virtual, deverá possuir uma suíte de proteção contra ameaças digitais (antivírus) instalada e atualizada.

11.1.3. Todo e qualquer processo de manutenção, instalação, configuração, desinstalação, substituição ou remanejamento de qualquer servidor, ainda que parcial, deve ser realizado pela GERSOL ou sob sua supervisão.

11.1.4. É proibido o uso de programas ilegais (software sem a devida licença adquirida ou cuja funcionalidade infrinja as políticas determinadas neste documento) nos servidores da CDRJ.

11.2. **Estações de Trabalho**

11.2.1. As estações de trabalho da CDRJ são destinadas a finalidades profissionais e restritas às atividades do usuário, podendo ser utilizados para fins pessoais dentro de critérios de razoabilidade e responsabilidade. Contudo, não cabe a GERSOL a salvaguarda de dados pessoais que, porventura, tenham sido armazenados nesses dispositivos.

11.2.2. Toda estação de trabalho (notebook ou desktop) de propriedade da CDRJ deverá:

a) Possuir uma suíte de proteção (antivírus) instalada e atualizada;

b) Estar configurado no domínio portosrio.gov.br;

c) Exigir credenciais de acesso na inicialização do sistema operacional;

d) Ter suas portas USB desabilitadas.

11.2.3. Todo e qualquer processo de manutenção, instalação, configuração, desinstalação, substituição ou remanejamento de qualquer estação de trabalho, ainda que parcial, deve ser realizado pela GERSOL ou sob sua supervisão.

11.2.4. O usuário deve utilizar apenas programas, aplicativos, recursos, ferramentas ou *plugins* homologados para uso pela GERSOL, sejam eles gratuitos, livres ou licenciados.

11.2.5. Não será realizado procedimento de backup das estações de trabalho.

11.2.6. É vedado aos usuários:

a) Proceder à abertura ou manuseio de qualquer ativo pertencente à CDRJ, com a finalidade de realização de qualquer tipo de reparo;

b) Utilizar dispositivos de comunicação (modens celulares e similares) de origem externa nos ativos da CDRJ, exceto nos casos autorizados;

c) Desinstalar programas, aplicativos, recursos, ferramentas ou *plugins* da CDRJ, seja por qualquer motivo, sem a devida autorização e acompanhamento da GERCOS ou GERSOL.

11.2.7. Quando ocorrer o desligamento do usuário, as informações armazenadas na estação de trabalho em sua posse deverão ser avaliadas pela sua chefia imediata, sendo transferido para um diretório em rede, o que for pertinente ao trabalho.

11.2.8. Todo arquivo gerado em função do trabalho na CDRJ deve ser armazenado em diretório de rede, sendo vedada a sua manutenção em disco local, na estação de trabalho.

11.2.9. É proibido o uso de programas ilegais (software sem a devida licença adquirida ou cuja funcionalidade infrinja as políticas determinadas neste documento) nas estações de trabalho conectadas a rede de dados da CDRJ.

11.2.10. Ao final do expediente, o usuário deverá desligar o computador corretamente, utilizando a função de desligamento do sistema operacional.

11.3. **Impressoras e Multifuncionais**

11.3.1. A GERSOL disponibiliza equipamentos multifuncionais e impressoras laser monocromáticas e coloridas, distribuídas pelas dependências da CDRJ.

11.3.2. Para a instalação de uma ou mais dispositivos de impressão, o usuário deverá acessar o manual através da Intranet, no menu Gestão de TI, pelo link relativo ao Manual de instalação de impressora, ou diretamente pelo endereço: http://intranet.portosrio.gov.br/downloads/files/gestao_de_ti/instalar_impressora_de_rede_no_computador_contrato_novo.doc.

11.3.3. Todas os equipamentos serão configurados, por padrão, para executar o recurso de impressão segura, resguardando assim o acesso indevido aos documentos impressos.

12. **VIOLAÇÃO DA POLÍTICA, ADVERTÊNCIA E PUNIÇÕES**

12.1. Caberá a GERSOL, quando detectada uma violação, averiguar suas causas, consequências e circunstâncias nas quais ocorreu, verificando tanto se foi de um simples acidente, erro ou mesmo desconhecimento da política, como também se configurou um caso de negligência, ação deliberada ou fraudulenta. Essa averiguação possibilita o devido enquadramento de infração da conduta, assim como permite que as vulnerabilidades até então desconhecidas pela GERSOL passem a ser consideradas, exigindo, se for o caso, alterações na política.

12.2. O descumprimento da POSIC poderá acarretar responsabilização, nos termos do IN ASSIND 01.012 e demais regulamentos da CDRJ e nos termos dos contratos ou convênios para estagiários,

menores aprendizes, empresas prestadoras de serviço e seus empregados, sem prejuízo das responsabilidades civis e penais eventualmente cabíveis.

13. **CONSIDERAÇÕES FINAIS**

13.1. A POSIC será ser amplamente divulgada aos usuários dos recursos de TI da CDRJ e o seu acesso disponibilizado nos canais internos de comunicação.

13.2. Deve ser aprovado pela Diretoria Executiva e Conselho de Administração;

13.3. Deve ser formalmente publicada por Resolução e aplicada a todos os usuários com acesso aos bens de informação da CDRJ.

13.4. Todos os colaboradores deverão confirmar ciência da POSIC e assinar o Termo de Compromisso e Ciência 5290128.

13.5. Casos excepcionais ou não contemplados nesta POSIC devem ser tratados individualmente, mediante orientação da SUPTIN;

13.6. Eventualmente, por decisão da SUPTIN ou para resolução de conflitos, o Comitê de Segurança da Informação poderá ser envolvido e chamado a manifestar-se em casos excepcionais;

13.7. A POSIC deve ser atualizada bienalmente, objetivando refletir os avanços tecnológicos e as alterações dos ambientes interno e externo.

Documento assinado eletronicamente por **Eduardo Moreira Da Silva**, **Gerente**, em 27/05/2022, às 16:03, 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 **5656820** e o código CRC **80B9094F**.

Referência: Processo nº 50905.001042/2022-66 SEI nº 5656820

Rua Dom Gerardo 35, 10º andar - Edifício Sede - Bairro Centro
Rio de Janeiro/RJ, CEP 20090-905
Telefone: 2122198600 - www.portosrio.gov.br