Política de Segurança de Tecnologia da Informação

Companhia Docas do Rio de Janeiro

GERSOL

Versionamento

Documento	Versão	Autor	Responsável	Data
Política de Segurança	1.0	Juliana Toledo	Juliana Toledo	01/07/2013
Política de Segurança de Tecnologia da Informação	2.0	Rafael Carlos	Rafael Carlos	28/03/2014
Política de Segurança de Tecnologia da Informação	3.0	Rodrigo Rangel	Rodrigo Rangel	07/10/2016

SUMÁRIO

1. INTRODUÇÃO

Neste documento é apresentado um conjunto de instruções e procedimentos para normatizar e melhorar a visão e atuação em segurança de Tecnologia da Informação – TI.

A Política de Segurança da Informação (PSI) na Companhia Docas do Rio de Janeiro – CDRJ aplica-se a todos os empregados, prestadores de serviços, sistemas e serviços, incluindo trabalhos executados externamente ou por terceiros, que utilizem o ambiente de processamento da Companhia ou acesso a informações pertencentes à CDRJ.

Todo usuário de recursos computadorizados da Companhia tem a responsabilidade de seguir as regras de segurança e proteger a integridade das informações e dos equipamentos de informática.

É função da GERSOL propagar o conhecimento e esclarecer eventuais dúvidas sobre este documento.

2. MISSÃO DO SETOR DE INFORMÁTICA

Ser o gestor do processo de segurança de TI e proteger as informações da organização, catalisando, coordenando, desenvolvendo e/ou implementando ações para esta finalidade.

3. OBJETIVO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Garantir que a informação e os recursos de informática sejam usados de maneira adequada. O usuário deve conhecer regras para utilização destes de maneira segura, evitando expor informações que possam prejudicar a CDRJ e/ou os seus colaboradores.

4. DA VIOLAÇÃO DA POLÍTICA DE SEGURANÇA

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

5. DAS RESPONSABILIDADES ESPECÍFICAS

5.1. Do Diretor/Superintendente/Gerente/Encarregado de cada área

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

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

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

- **Informação Interna:** É toda informação que só pode ser acessada por colaboradores da organização. São informações que possuem um grau de confidencialidade que pode comprometer a imagem da organização.

- **Informação Confidencial:** É toda informação que pode ser acessada por usuários da organização e por parceiros da organização. A divulgação não autorizada dessa informação pode causar impacto (financeiro, de imagem ou operacional) ao negócio da organização ou ao negócio do parceiro.

- **Informação Restrita:** É toda informação que pode ser acessada somente por usuários da organização explicitamente indicado pelo nome ou por 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.

5.1.2. 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.

5.1.3. 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.

5.1.4. Informar à GERSOL sobre o remanejamento de qualquer ativo de TI que esteja na carga patrimonial do órgão.

5.1.5. Solicitar o apoio da GERSOL e da GERCOS em qualquer projeto que tenha como ferramenta, o uso de sistemas computacionais, ou que necessite de infraestrutura de TI. A GERCOS não dará suporte a sistemas que não tenham passado por uma análise prévia.

5.2. Do Gerente da GERARH – Gerência de Administração de Recursos Humanos

5.2.1. Informar imediatamente à GERSOL sobre admissão, transferência, afastamento ou desligamento de qualquer empregado.

5.3. Do Gerente da GERCAR – Gerência de Gestão de Carreira

5.3.1. Informar imediatamente à GERSOL sobre qualquer novo estagiário contratado, afastado ou desligado.

5.4. Do Gerente da GERAIP – Gerência de Gestão de Ativos Imobiliários e Patrimônio

5.4.1. Informar à GERSOL sobre a incorporação, alteração de carga ou baixa patrimonial de ativos de TI.

5.5. Dos empregados

5.5.1. Cada usuário deve acessar apenas informações e os ambientes previamente autorizados. Qualquer tentativa de acesso a ambientes não autorizados será considerada como uma violação desta política.

5.5.2. Manter a configuração do equipamento disponibilizado pela empresa, seguindo os devidos controles de segurança exigidos pela Política de Segurança da Informação e pelas normas específicas da

instituição. Qualquer alteração de configuração nos ativos de TI será considerada uma violação desta política.

5.5.3. Toda solicitação feita à GERSOL e à GERCOS deverá constar no sistema HELPDESK, para controle e processamento. Deve ser aberto um chamado que informe obrigatoriamente o setor, a descrição da solicitação ou problema, a categoria do chamado e o usuário solicitante, além das demais informações não obrigatórias. A descrição completa do problema facilita sua resolução.

5.5.4. É papel de todo empregado da CDRJ informar à GERSOL sobre a violação de qualquer uma das políticas estabelecidas nesta PSI.

5.5.5. É de responsabilidade de cada usuário a memorização da própria senha, a mesma tem caráter pessoal e intransferível, bem como a proteção e a guarda dos dispositivos de identificação que lhe forem designados. O usuário não deverá anotar a sua senha em hipótese alguma.

5.5.6. Não é permitido o acesso na rede através de usuários "genéricos", a menos que tenha sido autorizado previamente pela GERSOL.

5.6. Dos prestadores de serviços

5.6.1. Estão sujeitos às políticas de segurança de TI estabelecidas neste documento todos os empregados que façam parte do quadro funcional de terceiros, mas que estejam nas dependências da CDRJ.

5.6.2. É responsabilidade dos Gestores de contratos preencherem o Formulário de Solicitação de Recursos de TI para Terceiros (AnexoI), onde deverão obrigatoriamente constar os dados dos empregados terceirizados (nome, sobrenome, documento de identificação), recurso de TI a ser utilizado (internet, protocolo, impressoras, pastas de rede, etc) e período de utilização do recurso.

5.6.3. No caso de renovação do contrato com a empresa terceirizada, os formulários deverão ser reenviados informando o novo prazo de utilização do recurso.

5.6.4. O Gestor deverá informar se o empregado ou equipe terceirizada irá utilizar hardware próprio ou da CDRJ. O equipamento deverá ser inspecionado e homologado para utilização dentro do ambiente da CDRJ pela equipe da GERSOL.

5.7. Da Gerência de Operação de Soluções

5.7.1. Garantir a publicação, manutenção, atualização e aplicação das normas estabelecidas nesta PSI.

5.7.2. Garantir a disponibilidade, confidencialidade, integridade e autenticidade das informações que tenham sido armazenadas por sistemas homologados pela própria GERSOL, seguindo esta PSI.

5.7.3. Habilitar o acesso à rede de computadores da CDRJ aos empregados/estagiários/aprendizes/prestadores de serviços recém-contratados ou transferidos de outros setores.

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

5.7.5. Administrar, proteger e testar as cópias de segurança dos programas e dados relacionados aos processos críticos e relevantes para a CDRJ.

5.7.6. Quando ocorrer movimentação interna dos ativos de TI, garantir que as informações de um usuário foram removidas de forma irrecuperável antes de disponibilizar o ativo para outro usuário.

5.7.7. 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.

5.7.8. 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 empregado responsável.

5.7.9. Definir as regras formais para instalação de software e hardware em ambiente de produção Corporativo.

5.7.10. 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 fins de salvaguardar os ativos da empresa.

5.7.11. 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.

5.7.12. Elaborar, manter e publicar um Plano de Cópia de Segurança dos programas e dados relacionados aos processos críticos e relevantes para a CDRJ.

5.7.13. Gerir os recursos de TI da CDRJ. Por esse motivo, a GERSOL possui autonomia sobre o remanejamento de ativos de TI que se façam necessários para o bom andamento dos processos de negócio da CDRJ.

6. DOS SERVIÇOS DE TI

No que tange à Tecnologia da Informação, são serviços implantados e oferecidos pela GERSOL:

6.1. Internet

6.1.1. Entende-se como Internet o serviço de acesso a rede mundial de computadores, a World Wide Web.

6.1.2. Toda estação de trabalho inspecionada e homologada pela GERSOL, terá acesso restrito à Internet.

6.1.3. Todo acesso à internet será monitorado, com a finalidade de responsabilizar o usuário pelo acesso a sites ilícitos ou que causem impacto negativo à rede de dados da CDRJ quanto ao desempenho, estabilidade ou segurança.

6.1.4. Não é permitido o acesso a sites categorizados como "Áudio/Vídeo", "Conteúdo Ilícito ou indesejável", "Drogas", "Entretenimento", "Material Adulto", "Relacionamento".

6.1.5. Não são permitidos os acessos a sites ou sistemas hospedados na internet que utilizem porta de acesso diferente das amplamente utilizadas para esse propósito. Todo usuário deste serviço poderá solicitar a liberação de um site específico, o atendimento dependerá de homologação da GERSOL.

6.1.6. O site da CDRJ na internet possui recursos de Gerenciamento de Conteúdo. Para mais detalhes sobre como publicar informações no site, use como referência as Instruções Normativas nº 72/2016 e 18/2017, que regulamentam a publicação de informações no site da Companhia.

6.1.7. A GERSOL registra os dados de cada publicação criada no Gerenciador de Conteúdo com a finalidade de identificar o autor da publicação, a estação de trabalho utilizada pelo usuário e a data da publicação. É proibida a publicação de conteúdo que não tenha sido autorizado ou que comprometa a integridade e confidencialidade dos dados da CDRJ.

6.2. Intranet

6.2.1. Toda estação de trabalho inspecionada e homologada pela GERSOL terá acesso irrestrito à página inicial da Intranet. 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.

6.2.2. A Intranet da CDRJ possui recursos de Gerenciamento de Conteúdo. Para mais detalhes sobre como publicar informações no site, use como referência as Instruções Normativas nº 72/2016 e 18/2017, que regulamentam a publicação de informações no site da Companhia.

6.2.3. A GERSOL registra os dados de cada publicação criada no Gerenciador de Conteúdo com a finalidade de identificar o autor da publicação, a estação de trabalho utilizada pelo usuário e a data da publicação. É proibida a publicação de conteúdo diferente do especificado para cada órgão, conforme o exposto na IN 18/2017.

6.2.4. Fazem parte da Intranet os subsistemas de: Protocolo, Helpdesk, Orçamento, Sistemas de Consultas de Empregados, Telefones e de Documentos do Protocolo. Todos os sistemas da Intranet são acessíveis através do mesmo nome de usuário e senha utilizados na rede.

6.3. Webmail

6.3.1. É conferido a todo empregado da CDRJ um endereço de e-mail corporativo, sob o domínio oficial da CDRJ: portosrio.gov.br

6.3.2. A ferramenta está disponível através do site https://webmail2.portosrio.gov.br/owa e acessível pela Internet ou Intranet.

6.3.3. Para configuração do serviço de webmail no celular coorporativo, baixe o Microsoft Outlook no Google Play, e após a instalação, coloque o endereço de e-mail e senha do usuário.

6.4. Parque de impressão

6.4.1. A GERSOL disponibiliza impressoras laser monocromáticas e coloridas distribuídas pelas dependências da CDRJ.

6.4.2. Para a instalação de uma ou mais impressoras, o usuário deverá acessar o manual através da Intranet, menu Gestão de TI, 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

6.4.3. Todas as impressoras possuem um recurso de impressão segura. Através dele, é possível enviar um documento para a impressora protegido por senha e, após digitá-la no console da impressora, imprimir o documento, o manual está na Intranet, menu Gestão de TI, Manual de impressão segura, ou diretamente pelo endereço http://intranet.portosrio.gov.br/downloads/files/gestao_de_ti/impressao_segura_novo_contrato.doc

6.5. Pastas públicas

6.5.1. A rede de dados da CDRJ dispõe de uma pasta compartilhada a todos (COMUM) destinada à transferência de arquivos de um usuário para outro, sem necessitar do envio de e-mail e possibilitando a troca de arquivos grandes (acima de 10MB) para serem transferidos por e-mail. A letra correspondente a unidade de mapeamento dessa pasta é a Z.

6.5.2. O usuário pode gravar ou excluir dados na pasta mapeada na unidade Z.

6.5.3. A GERSOL é responsável pela limpeza dessa pasta, a qual será realizada mensalmente. Vale ainda ressaltar que esta pasta não será passível de backup.

6.6. Pastas Compartilhadas

6.6.1. A GERSOL poderá criar uma pasta compartilhada entre os membros do órgão solicitante. A pasta receberá o nome do próprio órgão (GERSOL ou SUPTIN, por exemplo) e a letra correspondente a essa pasta será a letra U. Apenas os usuários autorizados pelo órgão solicitante poderão ler, gravar ou excluir arquivos da pasta.

6.6.2. As pastas compartilhadas fazem parte da rotina de backup dos servidores, então é possível restaurar versões antigas de seus respectivos arquivos. Para isso, o usuário deverá abrir uma solicitação no HELPDESK, descrevendo detalhadamente as informações sobre o que será restaurado, como nome, tipo, tamanho, data de criação ou última modificação do arquivo.

6.7. Servidores e Máquinas Virtuais

6.7.1. O ambiente de servidores da CDRJ é virtualizado, por isso é possível criar servidores virtuais de aplicação, bancos de dados e arquivos, à medida que as demandas surgirem.

6.7.2. Todo projeto de Tecnologia da Informação poderá ser hospedado nesses servidores virtuais criados no datacenter da CDRJ, desde que

tenha sido feito um estudo prévio de capacidade de processamento e armazenamento pela própria GERSOL em conjunto com órgão responsável pelo projeto.

6.8. Estações de Trabalho

6.8.1. Toda estação de trabalho que faz parte do patrimônio da CDRJ possui as seguintes ferramentas de trabalho:

- Sistema Operacional (Windows);
- Solução de Suíte de escritório (Microsoft Office);
- Navegadores web (Internet Explorer, Google Chrome e Mozilla Firefox);
- Aplicativo de compressão de arquivos (WINRAR);
- Software leitor de arquivos PDF (Adobe Reader);
- Suíte de proteção contra ameaças digitais (Trend Antivirus);
- Ferramenta de mensagens instantâneas (Spark);
- Além das aplicações listadas acima, a CDRJ poderá fazer instalação de outro software de mercado, desde que seja aberta uma solicitação no HELPDESK pelo responsável do setor, divisão, superintendência ou diretoria, sendo o seu impacto analisado pela GERSOL.

6.8.2. Não é autorizada a utilização de dispositivo de TI que não tenha sido registrado pela GERSOL nas dependências da CDRJ.

7. POLÍTICA DE UTILIZAÇÃO DAS ESTAÇÕES DE TRABALHO

Esse tópico visa definir as normas de utilização das estações de trabalho (computadores) e Notebooks da CDRJ.

7.1. Regras gerais de utilização

7.1.1. Os equipamentos disponíveis aos colaboradores são de propriedade da CDRJ, cabendo a cada um utilizá-los e manuseá-los corretamente para as atividades de interesse da Companhia;

7.1.2. Equipamentos fornecidos através de contratos com empresas terceirizadas não deverão ser incluídos na rede de computadores da CDRJ sem a devida inspeção da GERSOL;

7.1.3. É proibido procedimento de manutenção física ou lógica, instalação, desinstalação, configuração ou modificação sem o conhecimento prévio e o acompanhamento de um técnico da GERSOL, ou de quem este determinar;

7.1.4. Os sistemas e computadores devem ter versões do software antivírus instaladas, ativadas e atualizadas permanentemente. O usuário, em caso de suspeita de vírus ou problemas na funcionalidade, deverá acionar a GERSOL mediante registro de chamado no HELPDESK.

7.1.5. Os arquivos armazenados nos discos rígidos (unidades C e D) das estações de trabalho não serão considerados arquivos de trabalho, por isso não serão restaurados em qualquer circunstância;

7.1.6. 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;

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

8. POLÍTICA DE UTILIZAÇÃO DA REDE

Esse tópico visa definir as normas de utilização da rede que abrangem a conta de usuário, a manutenção de arquivos no servidor e tentativas não autorizadas de acesso.

8.1. Regras gerais de utilização

8.1.1. Não são permitidas tentativas para fraudar autenticação de usuário ou segurança de servidor, rede ou conta. Isso inclui acesso aos dados não disponíveis para o usuário, conectar-se a servidor ou conta que coloque em risco a segurança de outras redes;

8.1.2. O usuário só poderá efetuar logon com a própria conta, não sendo permitida a utilização da conta de terceiros. Esta é pessoal e intransferível. Todo acesso a recurso de TI que exija logon será registrado e o responsável pela conta responderá pelos acessos que forem realizados;

8.1.3. Não são permitidas tentativas de interferir nos serviços de outro usuário, servidor ou rede. Isso inclui ataques, tentativas de provocar congestionamento em redes, de sobrecarregar um servidor e de "quebrar" (invadir) um servidor;

8.1.4. Antes de ausentar-se do seu local de trabalho, o usuário deverá fechar todos os programas em uso, evitando desta maneira o acesso por pessoas não autorizadas. Se possível, efetuar o logout/logoff da rede ou bloqueio do computador através de senha;

8.1.5. As estações de trabalho serão bloqueadas automaticamente em 5 minutos de ociosidade;

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

8.1.7. É obrigatório armazenar os arquivos inerentes à empresa no servidor de arquivos para garantir a cópia de segurança dos mesmos;

8.1.8. Quando um funcionário é transferido entre departamentos, o responsável pela transferência deve certificar-se de que todos os direitos de acesso aos sistemas e outros controles de segurança ainda serão necessários na sua nova função e informar à equipe de TI sobre modificações necessárias.

9. POLÍTICA DE ADMINISTRAÇÃO DE CONTAS

9.1. Criação de contas

9.1.1. A inclusão de um novo usuário na rede dar-se-á mediante solicitação prévia com, no mínimo, cinco dias de antecedência.

9.1.2. Devem possuir uma conta de acesso à rede de computadores na CDRJ:

- Empregados (incluindo-se os cedidos e em cargos comissionados);
- Estagiários e aprendizes;
- Prestadores de serviço.

9.1.3. Toda conta dá acesso aos serviços de TI estipulados nesta PSI.

9.2. Manutenção de conta

9.2.1. Cada usuário que tiver sua conta criada terá um espaço no servidor para gravar seus arquivos de trabalho. Será feita cópia de segurança destes arquivos diariamente.

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

9.2.3. As contas serão monitoradas pela equipe de segurança com o objetivo de verificar possíveis irregularidades no armazenamento ou manutenção dos arquivos nos diretórios pessoais. Caso seja identificada a existência desses arquivos, eles poderão ser excluídos definitivamente sem comunicação prévia ao usuário.

9.2.4. No caso de algum arquivo ter sido excluído indevidamente, o usuário poderá pedir sua restauração mediante justificativa na descrição do chamado aberto no HELPDESK.

9.2.5. Não cabe a GERSOL fazer cópias de segurança ou qualquer outro procedimento que garanta a integridade de arquivos pessoais.

9.3. Desativação de conta

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

- Desligamento do empregado, estagiário ou aprendiz;
- Aposentadoria;
- Desligamento do empregado da empresa terceirizada que utiliza algum dos recursos de informática da CDRJ;
- Término do contrato com a empresa terceirizada que utiliza algum dos recursos de informática da CDRJ. Nesse caso, todos os usuários ligados a esta terão suas contas desativadas.

10. POLÍTICA DE SENHAS

10.1. A senha inicial padrão adotada pela CDRJ para acesso a conta do usuário é **123abc@** e deverá ser trocada após o primeiro acesso. A senha deve atender aos seguintes requisitos:

10.1.1. Ter, no mínimo, seis caracteres;

10.1.2. Não conter nome da conta ou mais de dois caracteres consecutivos de partes do nome completo do usuário;

10.1.3. Conter ao menos três destas quatro categorias:

- Caractere maiúsculo (A-Z).
- Caractere minúsculo (a-z).
- Número de 1 a 9.
- Caracteres especiais (! $ # %=).

10.2. A senha não poderá ser igual às três últimas senhas.

10.3. Após cinco tentativas de acesso, a conta do usuário será bloqueada. Para o desbloqueio é necessário que o usuário entre em contato com a GERSOL.

10.4. Os usuários podem alterar a própria senha, e devem ser orientados a fazê-lo, caso haja suspeita de que terceiros estejam utilizando indevidamente o seu login/senha.

10.5. A periodicidade máxima para troca das senhas é noventa dias.

10.6. Os sistemas críticos e sensíveis para a Companhia e suas respectivas políticas de acesso, devem exigir a troca de senhas a cada noventa dias. Os sistemas devem forçar a troca das senhas dentro desse prazo máximo.

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

11. POLÍTICA DE UTILIZAÇÃO DE CORREIO ELETRÔNICO (E-MAIL)

11.1. Regras gerais de utilização

11.1.1. O correio eletrônico fornecido pela CDRJ é o instrumento de comunicação interna e externa oficial para a realização do negócio da empresa.

11.1.2. A inclusão de um novo usuário no e-mail será feita juntamente com a criação de seu usuário na rede de computadores da CDRJ, com exceção dos estagiários e aprendizes, que terão esse serviço mediante requisição do gestor da área.

11.1.3. O uso do correio eletrônico é pessoal e o usuário é responsável por toda mensagem enviada pelo seu endereço. Deve ser evitada a utilização do e-mail corporativo para assuntos pessoais.

11.2. As mensagens:

11.2.1. Devem ser escritas em linguagem profissional;

11.2.2. Não devem comprometer a imagem da empresa;

11.2.3. Não podem ser contrárias à legislação vigente e nem aos princípios éticos da CDRJ;

11.2.4. E-mail que contenham arquivos anexos com as extensões .bat, .exe, .src, .lnk e .com só devem ser abertos se o usuário tiver certeza sobre o seu remetente e conteúdo.

11.2.5. É proibido reenviar ou propagar mensagens em cadeia (correntes), independentemente da vontade do destinatário de receber tais mensagens.

11.2.6. É obrigatória a manutenção da caixa de e-mail, evitando acúmulo de e-mails e arquivos desnecessários

12. POLÍTICAS DE ACESSO À INTERNET

Esse tópico visa definir as normas de utilização da Internet que englobam a navegação em sites, downloads e uploads de arquivos.

12.1. 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 o direito de monitorar e registrar todos os acessos.

12.2. Os equipamentos, tecnologia e serviços fornecidos para o acesso à internet são de propriedade da CDRJ, que pode analisar e, se necessário, bloquear 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 de sua PSI.

12.3. Somente a navegação de sites é permitida. Casos específicos deverão ser solicitados diretamente à GERSOL com prévia autorização do responsável pelo setor.

12.4. Acesso a sites com conteúdo pornográfico, jogos, bate-papo, apostas e assemelhados estará bloqueado e monitorado.

12.5. É proibido o uso de ferramentas P2P (Ares Galaxy, kazaa, emule, etc).

12.6. É proibido a visualização, transferência (downloads), cópia ou outro tipo de acesso a sites:

- De estações de rádio, TV, jogos e filmes;
- De relacionamentos;
- De conteúdo pornográfico ou relacionado a sexo;
- Que defendam atividades ilegais;
- Que menosprezem, depreciem ou incitem o preconceito a determinadas classes;
- Que possibilitem a distribuição de informações de nível "Confidencial";
- Que permitam a transferência (downloads) de arquivos e/ou programas ilegais.

12.7. Caso a GERSOL julgue necessário haverá bloqueios no acesso a sites e serviços específicos que possam comprometer o uso da banda ou perturbar o bom andamento das atividades profissionais da CDRJ.

13. VIOLAÇÃO DA POLÍTICA, ADVERTÊNCIA E PUNIÇÕES

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

13.2. O não cumprimento desta PSI implicará em infração e poderá resultar nas sanções administrativas cabíveis, tais como: advertência formal, bloqueio de login, suspensão, dentre outras, na forma da lei e das normas internas da CDRJ. A IN 38/2017 regulamenta os Procedimentos Disciplinares da CDRJ, sem prejuízo da responsabilidade civil e criminal.

14. CONSIDERAÇÕES FINAIS

14.1. A PSI deve ser amplamente divulgada aos usuários dos recursos de TI da CDRJ e o seu acesso disponibilizado nos canais internos de comunicação.

14.2. Deve ser aprovada pela Diretoria Executiva e Conselhos.

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

Anexo I – Formulário de Solicitação de Recursos de TI para Terceiros.

Anexo II – Termo de Compromisso e Ciência.