RESOLUÇÃO DIREXE Nº 001/2015

A **DIRETORIA EXECUTIVA**, no uso de suas atribuições estatutárias;

Considerando a necessidade de implantar uma política de segurança da informação em consonância com o que preconiza a Secretaria de Fiscalização de Tecnologia da Informação do TCU;

R E S O L V E:

Art. 1° - Aprovar a Política de Segurança de Tecnologia da Informação anexa à presente.

Art. 2° - Esta Resolução DIREXE entra em vigor nesta data.

Rio de Janeiro, 04 de março de 2015.

HELIO SZMAJSER
Diretor-Presidente

AIRTON COSTA DO AMARAL
Diretor de Administração, Finanças e Recursos Humanos

HERALDO DA COSTA KREMER
Diretor de Engenharia e Gestão Portuária

CLAUDIO DE JESUS MARQUES SOARES
Diretor de Planejamento e Relações Comerciais

*** Original arquivada na DIVDOC**

POLÍTICA DE SEGURANÇA DE TECNOLOGIA DA INFORMAÇÃO DA CDRJ

Este documento foi elaborado seguindo o guia de Boas Práticas em Segurança da Informação, 4ª ed., do TCU.

O guia está disponível no endereço abaixo:

http://portal2.tcu.gov.br/portal/pls/portal/docs/2511466.pdf

POLÍTICAS DE SEGURANÇA

1 INTRODUÇÃO

Nesse documento apresentaremos um conjunto de instruções e procedimentos para normatizar e melhorar nossa visão e atuação em segurança de TI.

A Política de Segurança da Informação na 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.

Todos os usuários 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 DINFOR 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 os recursos de informática e a informação estarão sendo usados de maneira adequada. O usuário deve conhecer as regras para utilização da informação de maneira segura, evitando expor informação que possa 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 de conduta, e estará passível das punições administrativas cabíveis.

5 DAS RESPONSABILIDADES ESPECÍFICAS

No que tange a política de segurança da informação, é de responsabilidade:

5.1 DO DIRETOR / SUPERINTENDENTE / GERENTE / ENCARREGADO DA ÁREA

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

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

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

II- 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;

III- 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;

IV- 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.

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

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**.**

Informar à DINFOR sobre o remanejamento dos ativos de TI que estejam na carga patrimonial do órgão.

Solicitar o apoio da DINFOR em projetos que tenha como ferramenta o uso de sistemas computacionais ou que necessitem de infraestrutura de TI. A DINFOR não dará suporte a sistemas que não tenham passado por uma análise prévia

5.2 DO GERENTE DA DIAPES – DIVISÃO DE ADMINISTRAÇÃO DE PESSOAL

Informar imediatamente à DINFOR sobre admissão, transferência, afastamento ou desligamento de empregado, a fim de se atualizar seu acesso à rede de computadores.

5.3 DO GERENTE DO CEPORT – CENTRO DE ENSINO PORTUÁRIO

Informar imediatamente à DINFOR sobre novo estagiário contratado, afastado ou desligado, a fim de se atualizar seu acesso à rede de computadores.

5.4 DO GERENTE DA DIVPAT – DIVISÃO DE PATRIMÔNIO E ALMOXARIFADO

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

5.5 DOS EMPREGADOS

Cada usuário deve acessar apenas informações e os ambientes previamente autorizados. Tentativas de acesso a ambientes não autorizados serão consideradas como uma violação desta política.

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.

Toda solicitação feita à DINFOR 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.

É papel de todo empregado da CDRJ informar à DINFOR sobre a violação das políticas estabelecidas nesta PSI.

É de responsabilidade de cada usuário a memorização de sua própria senha, 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.

5.6 DOS PRESTADORES DE SERVIÇOS

Estão sujeitos às políticas de segurança de TI estabelecidas nesse plano todo empregado que faça parte do quadro funcional de terceiros, mas que estejam nas dependências da CDRJ.

É responsabilidade dos Gestores de contratos preencherem o Formulário de Solicitação de Recursos de TI para Terceiros (Anexo), 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), período de utilização do recurso. A DINFOR será responsável por autorizar ou não a utilização do recurso solicitado.

A autorização terá validade de seis meses e no caso de renovação do contrato com a empresa terceirizada, os formulários deverão ser reenviados informando o novo prazo de utilização do recurso.

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 DINFOR.

5.7 DA DIVISÃO DE TECNOLOGIA DA INFORMAÇÃO (DINFOR)

Garantir a publicação, manutenção, atualização e aplicação das políticas estabelecidas nessa Política de Segurança da Informação.

Não acumular ou manter intencionalmente dados pessoais de funcionários além daqueles relevantes na condução do seu negócio. Todos os dados pessoais de funcionários que porventura sejam armazenados, e não constem do rol de informações públicas, segundo a Lei 12.527/2011 – Lei da Transparência Pública, serão considerados dados confidenciais.

Cabe a DINFOR garantir a disponibilidade, confidencialidade, integridade e autenticidade das informações, uma vez que tenham sido armazenadas por sistemas homologados pela própria DINFOR, seguindo esta Política de Segurança da Informação.

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

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

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

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.

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

Monitorar todo acesso a recursos de TI, de forma que seja possível auditar o acesso e rastrear a identidade do empregado responsável pelo acesso, em caso de violação das políticas estabelecidas nesse documento.

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

Garantir, da forma mais rápida possível, após o encaminhamento da DIAPES, 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.

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.

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

A responsabilidade pela gestão dos recursos de TI da CDRJ. Por esse motivo, a DINFOR possui autonomia sobre os remanejamentos 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 a Tecnologia da Informação, são serviços implantados e oferecidos pela CDRJ/DINFOR:

6.1 INTERNET

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

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

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

Não é permitido o acesso a sites categorizados como "Áudio/Vídeo", "Conteúdo Ilícito ou indesejável", "Drogas", "Entretenimento", "Material Adulto", "Relacionamento". Não são permitidos os acessos a sites ou sistemas hospedados na internet que utilizem porta de acesso diferente das amplamente utilizadas para esse propósito (80, 443). Todo usuário deste serviço poderá solicitar a liberação de um site específico, desde que homologado pela DINFOR através do procedimento de solicitação de liberação.

O site da CDRJ na internet possui recursos de Gerenciamento de Conteúdo. Para maiores detalhes sobre como publicar informações no site, use como referência as O.S.s 04/2014 e 16/2012, que regulamentam a publicação de informações no site da Companhia.

A DINFOR 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 ou confidencialidade dos dados da CDRJ.

6.2 INTRANET

Toda estação de trabalho inspecionada e homologada pela DINFOR, 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.

O site Intranet da CDRJ possui recursos de Gerenciamento de Conteúdo. Para maiores detalhes sobre como publicar informações no site, use como referência as O.S.´s 04/2014 e 16/2012, que regulamentam a publicação de informações no site da Companhia.

A DINFOR 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 ou confidencialidade dos dados da CDRJ.

Fazem parte da Intranet os subsistemas de: Protocolo, Helpdesk, Orçamento, Sistemas de Consultas de Empregados, de 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

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

A ferramenta está disponível através do site webmail.portosrio.gov.br e está acessível pela Internet ou Intranet.

Para configuração do serviço de webmail no celular, utilize o protocolo IMAP para recebimento e SMTP para envio dos emails, através dos endereços de servidor:

IMAP: imap.portosrio.gov.br (porta143)
SMTP: smtp.portosrio.gov.br (porta 2525)

6.4 PARQUE DE IMPRESSÃO

A DINFOR disponibiliza impressoras corporativas laser monocromáticas e coloridas distribuídas pelas dependências da CDRJ.

Para solicitar a instalação de uma ou mais impressoras, o usuário deve abrir um chamado no sistema HELPDESK e solicitando a instalação da impressora.

Todas as impressoras possuem um recurso de impressão segura. Através dele, é possível enviar um documento para a impressora passando uma senha e, após digitá-la no console da impressora, recuperar o documento impresso.

6.5 PASTAS PÚBLICAS

A rede de dados da CDRJ dispõe de uma pasta compartilhada a todos (COMUM) destinada a transferência de arquivos de um usuário para outro, sem necessitar do envio de email e possibilitando a troca de arquivos grandes demais para serem transferidos por email. A letra correspondente a essa pasta é a **Z**.

O usuário pode gravar ou excluir dados que ali forem gravados.

A DINFOR é responsável pela limpeza dessa pasta, a qual será realizada mensalmente.

6.6 PASTAS COMPARTILHADAS

Para compartilhamento de arquivos na rede de dados da CDRJ que precisem ter níveis de sigilo respectivos ao Setor, Superintendência ou Diretoria, a DINFOR poderá criar uma pasta compartilhada entre os membros do órgão solicitante. A pasta receberá o nome do próprio órgão (DINFOR ou SUPINF, por exemplo) e as letras correspondentes a essas pastas serão da letra **V** a letra **Y**, dependendo do grau hierárquico do órgão. Apenas os usuários autorizados pelo órgão solicitante poderão ler, gravar ou excluir arquivos da pasta.

As pastas compartilhadas fazem parte da rotina de backup dos servidores, e por isso, é possível restaurar versões antigas de arquivos ou pastas. Para isso, o usuário deverá abrir uma solicitação no HELPDESK, descrevendo o máximo de informações sobre a informação que será restaurada possível, como nome, tipo, tamanho e data de criação ou última modificação do arquivo.

6.7 PASTAS EXCLUSIVAS

Cada usuário autorizado a utilizar a rede de dados da CDRJ, possui uma pasta de rede individual, onde serão armazenados seus arquivos de trabalho.

O nome da pasta será correspondente ao login do usuário (rafael.carlos) por exemplo, e receberá a letra **U.**

6.8 SERVIDORES E MÁQUINAS VIRTUAIS

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

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 DINFOR em conjunto com órgão responsável pelo projeto.

6.9 ESTAÇÃO DE TRABALHO

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

I- Sistema Operacional (Windows);
II- Solução de Suíte de escritório (Microsoft Office);
III- Navegadores web (Internet Explorer e Mozilla Firefox);
IV- Aplicativo de compressão de arquivos (WINRAR);
V- Software leitor de arquivos PDF (Adobe Reader);
VI- Suíte de proteção contra ameaças digitais (Trend Antivirus);

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 pelo Setor, Divisão, Superintendência ou Diretoria.

Não é autorizada a utilização de outro dispositivo de TI que não tenha sido registrado pela DINFOR, 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 notebook’s da CDRJ.

7.1 REGRAS GERAIS DE UTILIZAÇÃO

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;

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

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

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 DINFOR mediante registro de chamado no HELPDESK.

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

É terminantemente proibido o uso de programas ilegais (software sem a devida licença adquirida, ou cuja funcionalidade infrinja as políticas determinadas nesta política) nas estações de trabalho conectadas a rede de dados da CDRJ;

Ao final do expediente, todo 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 na rede, a manutenção de arquivos no servidor e tentativas não autorizadas de acesso.

8.1 REGRAS GERAIS DE UTILIZAÇÃO

Não são permitidas tentativas de obter acesso não autorizado, tais como tentativas de 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 cujo acesso não seja expressamente autorizado ao usuário ou colocar à prova a segurança de outras redes.

Não é permitido ao usuário efetuar logon com a conta de outro usuário. O usuário só poderá efetuar logon com a sua própria conta de usuário. A conta do usuário é pessoal e intransferível, e todo acesso a recurso de TI que exija logon, será

registrado, e o responsável pela conta responderá pelos acessos que forem realizados por ele.

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

Antes de ausentar-se do seu local de trabalho, o usuário deverá efetuar o logout/logoff da rede ou bloqueio do computador através de senha (CTRL + ALT + DEL). Evitando, desta maneira, o acesso por pessoas não autorizadas a sua estação de trabalho.

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

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

É obrigatório armazenar os arquivos inerentes à empresa no servidor de arquivos para garantir a cópia de segurança destes.

Quando um funcionário é transferido entre divisões/setores, os gerentes/encarregados envolvidos na transferência devem certificar-se de que todos os direitos de acesso aos sistemas e outros controles de segurança foram removidos e/ou concedidos. Além disso, devem informar a equipe de TI sobre modificações necessárias.

9 POLÍTICA DE ADMINISTRAÇÃO DE CONTAS

Este tópico visa definir as normas de administração das contas de usuários que abrange criação, manutenção e desativação.

9.1 CRIAÇÃO DE CONTAS

A inclusão de um novo usuário na rede dar-se-á mediante solicitação prévia com, no mínimo 5 dias de antecedência.

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

I- Empregados (incluindo-se os cedidos e em cargos comissionados);
II- Estagiários;

III- Terceirizados autorizados;

Toda conta dá acesso aos serviços de TI estipulados nesta política de segurança.

9.2 MANUTENÇÃO DE CONTA

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.

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.

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.

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

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

9.3 DESATIVAÇÃO DE CONTA

O usuário terá a sua conta desativada nos casos de:

I- Desligamento do empregado ou estagiário;
II- Aposentadoria;
III- Desligamento do empregado da empresa terceirizada que utiliza algum dos recursos de informática da CDRJ;
IV- 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 POLÍTICAS DE SENHAS

A senha inicial padrão adotada pela CDRJ para acesso a conta do usuário será informada quando da solicitação e deverá ser trocada após o primeiro acesso. A senha deve atender aos seguintes requisitos:

I- Ter, no mínimo, seis caracteres;

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

III- Conter ao menos três destas quatro categorias:

a) caractere maiúsculo (A-Z);
b) caractere minúsculo (a-z);
c) número de 1 a 9;
d) Caracteres especiais (! $ # %=).

A senha não poderá ser igual às 3 últimas senhas.

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

Os usuários devem alterar a própria senha e podem ser orientados sobre como fazê-lo mediante solicitação via Helpdesk.

A periodicidade máxima para troca das senhas é 90 (noventa) dias.

Os sistemas críticos e sensíveis para a companhia e suas respectivas políticas de acesso, devem exigir a troca de senhas a cada 90 dias. Os sistemas devem forçar a troca das senhas dentro desse prazo máximo.

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)

Esse tópico visa definir as normas de utilização do correio eletrônico que engloba desde o envio, recebimento e gerenciamento das contas de e-mail.

11.1 REGRAS GERAIS DE UTILIZAÇÃO

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

Para os empregados, a criação de um novo e-mail será feita juntamente com a criação de seu usuário na rede de computadores da CDRJ. No caso dos estagiários, o e-mail será criado mediante solicitação do seu responsável.

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.

As mensagens:

I- Devem ser escritas em linguagem profissional;
II- Não devem comprometer a imagem da empresa;
III- Não podem ser contrárias à legislação vigente e nem aos princípios éticos da CDRJ.

E-mails que contenham arquivos anexos com as extensões .bat, .exe, .src, .lnk são automaticamente excluídos pelo sistema Antispam.

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

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 engloba desde a navegação a sites, downloads e uploads de arquivos.

A informação que é acessada, transmitida, recebida ou produzida na internet está sujeita a monitoração e auditoria. Portanto, a CDRJ, em conformidade legal, reserva-se o direito de monitorar e registrar todos os acessos a ela.

A definição dos empregados que terão permissão para uso (navegação) da Internet é atribuição da Direção Executiva da Companhia, com base em recomendação da DINFOR.

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 Política de Segurança da Informação.

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

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

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

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

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

Caso a DINFOR 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

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

O não cumprimento desta Política de Segurança da Informação implicará em infração e poderá resultar nas sanções administrativas competentes, tais como: advertência formal, bloqueio de login, suspensão, dentre outras, na forma da lei e das

normas internas da CDRJ. Além de responsabilização dos infratores nas esferas, civil e/ou criminal, conforme o caso, de acordo com a severidade, amplitude, tipo de violação, entre outros, e devem ser definidos pelos setores competentes da CDRJ.

Sempre por meio de procedimento administrativo competente, em que seja observado o Devido Processo Legal e os princípios do Contraditório e da Ampla Defesa.

14 CONSIDERAÇÕES FINAIS

A Política Interna de Segurança da Informação deverá ser amplamente divulgada a todos os usuários dos bens de informação da CDRJ e o seu acesso disponibilizado nos canais internos de comunicação.

Deve ser aprovado pela Diretoria Executiva e Conselhos.

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

ANEXO I – TERMO DE COMPROMISSO E CIÊNCIA

ANEXO II – FORMULÁRIO DE SOLICITAÇÃO DE RECURSOS DE TI PARA TERCEIROS