RIOPREVIDÊNCIA
FUNDO ÚNICO DE PREVIDÊNCIA SOCIAL DO ESTADO DO RIO DE JANEIRO

MANUAL NORMATIVO DE POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

SUMÁRIO

PREFÁCIO

TÍTULO
MANUAL NORMATIVO DE POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

UNIDADE GESTORA
GIN – GERÊNCIA DE INFORMÁTICA

PÚBLICO ALVO
Diretorias
Assessorias
Gerências
Coordenadorias
Servidores do Rioprevidência

LEGISLAÇÃO UTILIZADA
Decreto nº 2.479/79
Lei Federal nº 8.159/91
Decreto Federal nº 4.553/02
Lei Federal nº 9.610/98
Lei Federal nº 9.279/96
Lei Federal nº 3.129/82
Lei Federal nº 10.406/02
Decreto-Lei 2.848/40
Lei Federal nº 9.983/00
Decreto nº 3.505/00
Decreto n° 26.209/00
Norma ABNT NBR ISO/IEC 17799:2005
Norma ISO/IEC 13335 - 1:2004

1. DIRETRIZES GERAIS DE SEGURANÇA DA INFORMAÇÃO

1.1 Esta Política define as Diretrizes para a Segurança da Informação, visando preservar a integridade, confidencialidade e disponibilidade das informações sob gestão do Rioprevidência. Descreve a conduta considerada adequada para o manuseio, controle e proteção das informações contra destruição, modificação, divulgação indevida e acessos não autorizados, sejam acidentalmente ou intencionalmente.

1.2 A Política é aplicável às informações sob gestão do Rioprevidência, que podem existir de muitas maneiras: escrita em papel, armazenada e transmitida por meios eletrônicos, ou exibida em filmes. Seja qual for a forma apresentada ou o meio através do qual a informação seja apresentada ou compartilhada, ela deverá estar sempre protegida adequadamente, de acordo com controles definidos nesta política.

1.3 A Política deve ser conhecida e obedecida por todos os usuários que utilizam os recursos de processamento da informação de propriedade ou controlados pelo Rioprevidência, sendo de responsabilidade de cada um o seu cumprimento.

1.4 No âmbito do Rioprevidência, somente é permitido aos usuários o uso de recursos de processamento da informação disponibilizados pela Autarquia, de forma a garantir que os requisitos de segurança sejam atendidos. Os Gerentes das Unidades Administrativas do Rioprevidência são responsáveis em tomar as medidas cabíveis para o cancelamento do acesso aos recursos quando estes não forem mais necessários.

1.5 Somente atividades lícitas, éticas e administrativamente admitidas devem ser realizadas, pelos usuários, quando na utilização dos recursos de processamento da informação do Rioprevidência, ficando os transgressores sujeitos às sanções previstas nestas diretrizes.

1.6 Os documentos produzidos por intermédio dos recursos de processamento da informação do Rioprevidência são de propriedade da Autarquia. De igual modo, os programas desenvolvidos por servidores do quadro, extraquadro, cedidos e prestadores de serviço.

1.7 É de conhecimento do usuário que os dados, documentos, informações e programas armazenados nos equipamentos do Rioprevidência, estão sujeitos à auditoria a qualquer momento, a pedido da Autarquia.

1.8 Qualquer arquivo e programa acessado por meio externo (pen drive, cd, dvd, hd em nuvem, hd externo, etc...) bem como aqueles instalados na rede, estão sujeitos a mesma política instituída na presente diretriz; conforme item 1.6.

1.9 As informações de propriedade ou controladas pelo Rioprevidência devem ser utilizadas apenas para os propósitos definidos no Regimento Interno da Autarquia. Os usuários não podem, em qualquer tempo ou sob qualquer propósito, apropriar-se dessas informações.

1.10 A identificação do usuário (senha) é pessoal e intransferível, qualificando-o como responsável por todas as atividades desenvolvidas através dela, sendo pré-requisito para a liberação do uso o preenchimento de um termo de responsabilidade, indicando as suas condições de uso, seus direitos e deveres.

1.11 O Rioprevidência se reserva o direito de monitorar, automaticamente, o tráfego efetuado através das suas redes de comunicação, incluindo o acesso à Internet.

1.12 Os recursos de processamento da informação disponibilizados aos usuários têm que ser suportados por um projeto, a fim de evitar situações de risco à segurança da informação. Antes de serem colocados em produção terão que ser testados em ambiente de homologação.

1.13 Todas as informações devem ter classificação de segurança, aposta de maneira a serem adequadamente protegidas quanto ao seu acesso e uso.

1.14 Todos os usuários ao tomarem conhecimento de qualquer incidente de segurança da informação devem notificar o fato, imediatamente, a seu superior através de e-mail com cópia para sua Diretoria e à Gerência de Informática.

1.15 O cumprimento da Política de Segurança será auditado pela Gerência de Informática.

1.16 A não observância dos preceitos desta Política implicará na aplicação de sanções administrativas, cíveis e penais previstas no Estatuto do Servidor Público Civil Estadual (Decreto N° 2.479, Capítulos II, III, IV e V), no Código Penal (Decreto-Lei N°2.848/40, com as alterações da Lei N° 9.983/00 e no Decreto N° 2.910/98), no Código Civil (Lei 10.406 de 10/01/2002) ou em qualquer outra legislação que regule ou venha regular a matéria.

2 DEFINIÇÕES

2.1 TERMOS UTILIZADOS

2.1.1 **Administrador -** Contas da Gerência de Informática que permitem acesso total e irrestrito a quaisquer recursos do sistema em que estão configuradas.

2.1.2 **Administrador Local** - Contas da Gerência de Informática que permitem acesso total e irrestrito a quaisquer recursos do sistema em que estão configuradas em um computador específico.

2.1.3 **Análise de Riscos -** Processo completo de análise e avaliação de riscos.

2.1.4 **Arquivos infectados -** Aqueles que sofreram a ação de vírus eletrônico.

2.1.5 **Ativo -** Qualquer coisa que tenha valor para a organização.

2.1.6 **Avaliação de Riscos -** Processo de comparar o risco estimado com critérios de risco pré-definidos para determinar a importância do risco.

2.1.7 **Backup** - Cópia de segurança de informações armazenada em meio magnético.

2.1.8 **Caixa Postal / Correio Eletrônico -** Espaço em disco, onde são armazenadas as mensagens de correio eletrônico.

2.1.9 **Chave de Acesso/ Conta** - Código de acesso atribuído a cada Usuário. A cada Chave de Acesso é associada uma senha individual e intransferível, destinada a identificar o Usuário, permitindo-lhe o acesso aos recursos disponíveis.

2.1.10 **Chefia Imediata** – Coordenador, Gerente, Assessor ou Diretor ao qual o usuário está diretamente subordinado.

2.1.11 **Códigos Maliciosos ou Agressivos** - Qualquer código adicionado, modificado ou removido de um Sistema, com a intenção de causar dano ou modificar o funcionamento correto desse Sistema, como por exemplo, vírus eletrônico.

2.1.12 **Controle** - Forma de gerenciar o risco, incluindo políticas, procedimentos, diretrizes, práticas ou estruturas organizacionais, que podem ser de natureza administrativa, técnica, de gestão ou legal. Controle é também usado como um sinônimo para proteção ou contramedida.

2.1.13 **Correio Eletrônico -** Meio de comunicação baseado no envio e recepção de mensagens, através de uma rede de computadores.

2.1.14 **Criptografia -** Ciência que consiste na codificação e decodificação de mensagens, de forma a garantir a segurança e o sigilo no envio de informações.

2.1.15 **Download** - Baixar um arquivo ou documento de outro computador, através da Internet.

2.1.16 **Drive H** - Espaços disponibilizados nos Servidores do Rioprevidência para cada Diretoria, Gerência ou Coordenação com o propósito de armazenamento de informações corporativas.

2.1.17 **Evento de Segurança da Informação** - Ocorrência identificada de um sistema, serviço ou rede, que indica uma possível violação da política de segurança da informação ou falta de controle, ou uma situação previamente desconhecida, que possa ser relevante para a segurança da informação.

2.1.18 **Ferramenta Tecnológica** - Sistema (conjunto de programas) e/ou equipamento destinado a proteger, monitorar ou agregar valor aos ativos de informações.

2.1.19 **FTP (File Transfer Protocol) -** Protocolo padrão da Internet, usado para transferência de arquivos entre computadores.

2.1.20 **Gestão de Riscos** - Atividades coordenadas para direcionar e controlar uma organização no que se refere a riscos.

2.1.21 **IMAP (Internet Message Access Protocol) -** Protocolo de acesso a mensagens eletrônicas.

2.1.22 **Incidente de Segurança da Informação** - Um incidente de segurança da informação é indicado por um simples ou por uma série de eventos de segurança da informação indesejados ou inesperados, que tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação.

2.1.23 **Informações Controladas pelo Governo** - São aquelas pertencentes a terceiros, sendo da competência dos Órgãos Públicos a responsabilidade sobre a sua guarda, utilização e divulgação.

2.1.24 **Informações de Propriedade do Governo** - São aquelas geradas nos ambientes dos Órgãos Governamentais.

2.1.25 **Internet** - Associação mundial de redes de computadores interligadas, que utilizam protocolos de comunicação de dados. A Internet provê um meio abrangente de comunicação através de: transferência de arquivos, conexões à distância, serviços de correio eletrônico, etc.

2.1.26 **Intranet -** Rede interna, de uso corporativo, que utiliza a mesma tecnologia da Internet, para que os funcionários possam acessar as informações dos seus respectivos Órgãos Públicos.

2.1.27 **Licença de Software** - Direito de uso de um determinado programa de computador, protegido pela legislação que dispõe sobre propriedade, marcas e patentes.

2.1.28 **Modem** - Equipamento de comunicação de dados que utiliza os mecanismos de modulação e desmodulação para transmissão de informações.

2.1.29 **Órgão Público** - Qualquer ente da Administração Pública Direta ou Indireta, Fundações, Autarquias e Empresas Públicas.

2.1.30 **Peer-to-Peer (P2P)** - É uma arquitetura de sistemas distribuídos caracterizada pela descentralização das funções na Internet, isto é, todos os computadores são considerados de igual nível, permitindo o compartilhamento de dados e recursos numa larga escala.

2.1.31 **POP (Post Office Protocol) -** Protocolo usado por clientes de correio eletrônico para manipulação de arquivos de mensagens em servidores de correio eletrônico.

2.1.32 **Proprietário do Ativo** - Identifica uma pessoa ou organismo que tenha uma responsabilidade autorizada para controlar a produção, o desenvolvimento, a manutenção, o uso e a segurança dos ativos. O termo "proprietário" não significa que a pessoa realmente tenha qualquer direito de propriedade ao ativo.

2.1.33 **Site de Proxy** – intermediário entre o usuário e seu servidor. Desempenha a função de conexão do computador à internet.

2.1.34 **Risco** - Combinação da probabilidade de um evento e de suas consequências.

2.1.35 **Recursos de Processamento da Informação** - Qualquer sistema de processamento da informação, serviço ou infra-estrutura, ou as instalações físicas que os abriguem.

2.1.36 **SAT** – Sistema de Atendimento.

2.1.37 **Servidores** - Ativos de armazenamento das informações (Sistemas, Banco de Dados, serviços em geral etc.).

2.1.38 **Servidor de Correio Eletrônico -** Equipamento que provê o serviço de envio e recebimento de mensagens de correio eletrônico.

2.1.39 **Sistemas Informatizados** - Sistema constituído de programas e/ou equipamentos computacionais.

2.1.40 **Site** - Páginas contendo informações, imagens, fotos, vídeos, sons, etc., que ficam armazenadas em provedores de acesso (computadores denominados servidores) à Internet, para serem acessadas por qualquer pessoa que se conecte à rede.

2.1.41 **SMTP (Simple Mail Transfer Protocol)** - Protocolo de comunicação usado para troca de mensagens na Internet via correio eletrônico.

2.1.42 **Spam** - Qualquer mensagem, independentemente de seu conteúdo, enviada para vários destinatários, sem que os mesmos a tenham solicitado.

2.1.43 **Software** - Programa de Computador.

2.1.44 **Tratamento do Risco** - Processo de seleção e implementação de medidas para modificar um risco.

2.1.45 **Upload** - Envio de um arquivo de seu computador para outro, através da Internet.

2.1.46 **URL** - Universal Resource Locator - LINK ou endereço de uma pagina Web.

2.1.47 **Usuários** – Servidores Públicos, prestadores de serviços, clientes, fornecedores, bolsistas e estagiários.

2.1.48 **Vírus Eletrônico** - São pequenos programas que têm a propriedade de se juntar a outros arquivos, alterar seu funcionamento normal e se reproduzir (fazer cópias de si), contaminando outros arquivos.

3. NORMAS DE UTILIZAÇÃO DA INTERNET

3.1 Objetivo

3.1.1 Estabelecer responsabilidades e requisitos básicos de utilização da Internet no ambiente de Tecnologia da Informação e Comunicação (TIC) do Rioprevidência.

3.2 Abrangência

3.2.1 Esta norma deverá ser aplicada a todos os usuários que utilizam os recursos de Tecnologia da Informação e Comunicação - TIC para acesso à Internet.

3.3 Conceito

3.3.1 A Internet é classificada como conexão de alto risco sob o aspecto de proteção e integridade dos sistemas de informação. Os usuários devem estar cientes da peculiaridade da navegação na Internet antes de acessá-la e de utilizar os seus recursos.

3.3.2 Considerando que o uso da Internet, no âmbito do Rioprevidência é uma concessão e não um direito é de extrema importância que se estabeleça um conjunto de regras que possibilitem a utilização adequada desse importante recurso tecnológico. Todos os usuários dos ativos de informação de propriedade ou controlados pelo Rioprevidência, ao utilizarem esse serviço, deverão fazê-lo no estrito interesse do Órgão, mantendo uma conduta profissional, especialmente em se tratando da utilização de bem público.

3.4 Normas

3.4.1 É expressamente proibida a divulgação e/ou o compartilhamento indevido de informações sigilosas.

3.4.2 Usuários com acesso à Internet não podem efetuar upload de qualquer software licenciado ao Rioprevidência ou de dados de propriedade do Rioprevidência sem

a autorização expressa da Gerência de Informática ou do responsável pelo software/dados.

3.4.3 Os usuários poderão fazer download de arquivos da Internet que sejam necessários ao desempenho de suas atividades desde que observado os termos de licença de uso e registro desses programas.

3.4.4 A Internet, no âmbito do Rioprevidência, é uma concessão e não um direito. Portanto, sua utilização, deve ser exclusivamente para atividades ligadas ao trabalho da Autarquia.

3.4.5 Haverá geração de relatórios gerenciais dos sites acessados por usuários. A Diretoria poderá ter acesso a essas informações a qualquer tempo.

3.4.6 O usuário deve utilizar a Internet de forma adequada e diligente.

3.4.7 O usuário deve utilizar a Internet observando a conformidade com a Lei.

3.4.8 O usuário deve se abster de utilizar a Internet com objetivos ou meio para a prática de atos ilícitos, proibidos pela lei ou pela presente norma, lesivos aos direitos e interesses do Órgão ou de terceiros, ou que, de qualquer forma, possam danificar, inutilizar, sobrecarregar ou deteriorar os recursos tecnológicos (hardware e software), bem como os documentos e arquivos de qualquer tipo, de seu uso ou de uso de terceiros.

3.4.9 O usuário é pessoalmente responsável por todas as atividades realizadas por intermédio de sua chave de acesso.

3.4.10 É vedada a utilização de “modem” em máquinas que estejam conectadas ao ambiente da Rede do Rioprevidência.

3.4.11 Os usuários que desejarem utilizar outras conexões, além daquelas já estabelecidas, deverão obrigatoriamente informar à Gerência de Informática, via SAT ou e-mail, de forma a não comprometer a segurança da Rede Rioprevidência.

3.4.12 Será de responsabilidade de cada usuário zelar pelo fiel cumprimento ao estabelecido na presente norma.

3.4.13 O uso de softwares de comunicação instantânea, tais como ICQ, Microsoft Messenger (MSN) e afins, caso autorizado, deverão ser utilizados exclusivamente para fins de trabalho.

3.4.14 Não é permitida a utilização de software de peer-to-peer (P2P), tais como Kazaa, Emule e afins.

3.4.15 Não é permitido o acesso a sites de relacionamento, tais como Orkut, Gazzag, redes sociais e afins.

3.4.16 Não é permitido acesso a sites burladores de Proxy, pois esses servem para acessar páginas proibidas pela política de segurança do Rioprevidência.

3.4.17 O Rioprevidência monitora e bloqueia automaticamente sites de pornografia, pedofilia e outros contrários à lei. O acesso a esses sites é terminantemente proibido, mesmo que os mesmos não estejam sendo bloqueados no sistema de segurança.

3.4.18 A não observância de qualquer item acima implicará nas sanções previstas nesta norma.

3.5 Observações

3.5.1 Devido ao bloqueio de sites ser baseado em um sistema automatizado, algumas páginas poderão ser bloqueadas inadvertidamente. Caso seja bloqueado um site cujo conteúdo esteja de acordo com a norma, o usuário pode solicitar o desbloqueio à Gerência de Informática bastando informar qual a URL bloqueada.

3.5.2 O fato de um site não estar bloqueado não significa que o mesmo possa ser acessado pelos usuários. Deverão ser observados todos os preceitos da norma desde a proibição de acesso a sites contrários à lei até ao uso excessivo da Internet para assuntos não relativos a trabalho no horário do expediente.

3.6 Liberação de Site

3.6.1 O acesso à Internet está liberado apenas com a conexão através do firewall. Caso não ocorra a conexão com a internet, por favor, verificar a sua conexão ao firewall. O procedimento de verificação está disponível na intranet do Rioprevidência, através dos seguintes passos: Setores → DAF → Gerência de Informática.

3.6.2 Não existe caso de acesso irrestrito dentro da política de firewall.

3.6.3 A liberação de site será feita através de pedido via SAT ou e-mail (suporte.rioprevidência@rioprevidência.rj.gov.br), desde que atenda os seguintes requisitos abaixo descritos:

I- O pedido de solicitação só será aceito quando partir de um coordenador, gerente ou diretor do Rioprevidência.

II- A solicitação deverá conter o endereço completo, a finalidade de seu uso e o período de utilização.

III- O endereço será avaliado pela informática e após a avaliação o solicitante será informado da liberação ou não.

IV- O prazo para liberação é de 48 horas, lembrando que vídeos e som serão baixados e disponibilizados em arquivos na rede.

3.6.4 O Site deixará de ser disponibilizado caso se enquadre num dos casos abaixo descritos:

I- Em caso de ser diagnosticada utilização contrária a essa norma pelo usuário;

II- O tempo de utilização estipulado se expire;

III- Se for identificado algum problema no site, mesmo que este já tenha sido avaliado pela equipe de informática;

IV- Quando um site é liberado por um setor e a utilização do site esteja acontecendo por outro usuário que não tenha liberação. Este será bloqueado e sua Chefia Imediata será notificada. A Chefia Imediata do setor que está liberado também será avisada.

3.7 Sanções

3.7.1 De acordo com as diretrizes gerais da Política de Segurança da Informação do Rioprevidência, este se reserva ao direito de monitorar o tráfego efetuado através das suas redes de comunicação, incluindo o acesso à Internet.

3.7.2 O monitoramento do cumprimento das normas de utilização da INTERNET dar-se-á da seguinte forma:

I- Técnicos da Gerência de Informática identificarão os usuários, doravante chamados de infratores, que violarem qualquer item desta norma de segurança;

II- Na primeira transgressão, esses infratores serão notificados, por escrito, do descumprimento das normas estabelecidas neste documento;

III- Caso na infração cometida esteja caracterizado qualquer tipo de crime (acesso a sites de pedofilia, racismo etc.), aplicar-se-á a sanção especial desta norma;

IV- Caso haja uma segunda transgressão da norma, num período de 90 dias, esses infratores serão novamente notificados, por escrito, sendo que uma cópia da notificação será enviada para o Gerente da área e para o Diretor;

V- Na terceira transgressão, as sanções administrativas previstas nas diretrizes gerais da Política de Segurança da Informação do Rioprevidência serão aplicadas.

3.7.3 Em caso de recusa ao recebimento da notificação, a Gerência de Informática certificará o ocorrido e duas pessoas de diferentes setores assinarão que o funcionário se recusou a assinar.

3.8 Sanção Especial

3.8.1 Qualquer acesso a sites que tiverem conteúdo de pedofilia, racismo ou qualquer outro assunto contrário à lei que, eventualmente, não esteja bloqueado no sistema de proteção do Rioprevidência, é terminantemente proibido.

3.8.2 A violação deste item implica em abertura de registro de ocorrência na Delegacia de Repressão a crimes de Informática do Estado do Rio de Janeiro – DRCI.

4 NORMAS DE CONTAS E SENHAS PARA USUÁRIOS

4.1 Objetivo

4.1.1 Estabelecer os procedimentos adequados para a correta utilização das contas de usuários no ambiente de Tecnologia da Informação e Comunicação - TIC do Rioprevidência.

4.2 Abrangência

4.2.1 Esta norma deverá ser aplicada a todos os usuários que possuam contas (sem privilégios de "administrador") nos ativos do tipo **estações de trabalho** e **servidores** do ambiente de Tecnologia da Informação e Comunicação - TIC do Rioprevidência.

4.3 Conceito

4.3.1 A Rioprevidência controla a distribuição de direitos de acesso a sistemas de informação e serviços.

4.3.2 A concessão e o uso de privilégios são restritos e controlados e a concessão de senhas é controlada através de um processo de gerenciamento formal, todo controle é feito pela Gerência de Informática.

4.3.3 Deste modo, o Rioprevidência elaborou esta norma de contas e senhas para Usuários, de forma a evitar o uso inapropriado de senhas, que pode vir a ser um grande fator de contribuição para falhas ou violações de sistemas.

4.4 Procedimentos Administrativos e Operacionais para Criação, Alteração e Exclusão de Contas e Senhas

4.4.1 Cabe à Chefia Imediata de cada setor do Rioprevidência solicitar, através de CI ou formulário da Intranet, à Gerência de Informática, a Criação, Alteração ou Exclusão de Contas/Senhas de seus respectivos usuários. No caso de Criação ou Alteração, deverão ser informados os níveis de acesso de cada usuário.

4.5 Criação de Contas e Senhas

4.5.1 As senhas para usuários finais deverão conter no mínimo 8 (oito) caracteres, sendo aconselhável o uso de letras e números. Como recomendação adicional sugere-se a utilização de maiúsculas, minúsculas e caracteres especiais (“$”, “%”, “&”,...).

4.5.2 Os sistemas e aplicações deverão prover algum mecanismo ou instrução que garanta que só sejam aceitas senhas com a formação acima citada.

4.5.3 Deverá ser evitada a composição de senhas com seqüências numéricas (123...) e/ou alfabéticas (abc...), além de senhas de fácil dedução (nome da máquina, nome do usuário, data de nascimento...).

4.6 Procedimento padrão para utilização de Contas e Senhas

4.6.1 Para as contas de rede, é obrigatório que o usuário troque a senha no primeiro acesso.

4.6.2 Para as contas de E-mail, é também obrigatório que o usuário troque a senha no primeiro acesso. As solicitações dos usuários são feitas via CI e o novo E-mail e senha são enviados através de comprovante de cadastramento fechado, seguindo junto com o CI.

4.7 Tempo de vida de Contas e Senhas

4.7.1 O usuário deverá ser forçado a trocar a senha no seu primeiro login.

4.7.2 Após o período de 45 dias, será solicitado para o usuário a troca de sua senha. A senha não poderá se repetir até a 13ª troca.

4.7.3 Histórico composto, pelo menos, das 8 (oito) últimas senhas será guardado no servidor.

4.7.4 A conta deverá ser bloqueada após a 5ª (quinta) tentativa de login.

4.7.5 Contas que ficarem inativas por mais de 60 (sessenta) dias serão bloqueadas.

4.8 Reinicialização de Senhas

4.8.1 As contas só poderão ser reinicializadas por solicitação formal do seu detentor, à Gerência de Informática.

4.8.2 Caso o usuário suspeite do comprometimento de sua senha, deverá informar imediatamente a Gerência de Informática para que a mesma providencie a sua troca.

4.9 Disposições Gerais

4.9.1 Os sistemas e aplicações que impedem a exibição na tela de login do último usuário a acessá-lo, poderão ser acionados quando a Gerência de Informática achar necessário.

4.9.2 Os sistemas e aplicações que impedem a mesma conta de estar ativa, simultaneamente, em mais de uma estação, poderão ser acionados quando a Gerência de Informática achar necessário.

4.9.3 Os sistemas e aplicações que impedem a exibição automática, na tela de login, da senha referente ao respectivo login em uso, poderão ser acionados quando a Gerência de Informática achar necessário.

4.9.4 Após o período de 5 minutos o descanso de tela entra automaticamente. A máquina bloqueia e só é liberada com o Ctrl + Alt + Del, seguido de login e senha.

4.9.5 A senha é pessoal e intransferível devendo ser mantida em sigilo. O usuário será responsabilizado pelo mau uso da mesma conforme previsto na legislação.

4.9.6 A Chefia Imediata deverá comunicar à Gerência de Informática o desligamento ou remanejamento de qualquer usuário.

4.9.7 Para o novo usuário ou para aquele que esteja retornando após desligamento ou remanejamento, o coordenador ou gerente deverá solicitar à Gerência de Informática a concessão de acesso mínimo necessário, para que este exerça sua respectiva tarefa (ex: chave de rede).

4.9.8 Deve-se atribuir a uma conta somente permissão para a realização das tarefas pertinentes ao seu usuário.

4.9.9 Os usuários finais não poderão ter contas com perfil de administrador, nem contas do domínio com privilégio de administrador local da estação.

4.9.10 Não é permitido o uso de contas compartilhadas.

4.9.11 Os acessos e as falhas nas tentativas de login deverão ser auditados pela Gerência de Informática.

4.9.12 A eventual necessidade de instalação de softwares deve ser atendida via CI, ou formulário da Intranet pela Gerência de Informática, de forma que haja um controle centralizado de softwares e licenças disponíveis para o Órgão.

4.9.13 No caso de necessidade de utilização temporária de Notebooks privativos de funcionários ou pessoas externas ao Rioprevidência, o mesmo deve ser submetido à Gerência de Informática para que seja feita a configuração da máquina como se fosse uma estação padrão de trabalho do Órgão.

5 NORMAS DE UTILIZAÇÃO DE E-MAIL

5.1 Objetivo

5.1.1 Estabelecer responsabilidades e requisitos básicos de uso dos serviços de Correio Eletrônico no ambiente de Tecnologia da Informação e Comunicação (TIC) do Rioprevidência.

5.2 Abrangência

5.2.1 Esta norma deverá ser aplicada aos Usuários do Rioprevidência.

5.3 Conceito

5.3.1 Prover a comunicação é, sem dúvida, a essência das redes. As pessoas sempre procuraram se corresponder da maneira mais rápida e fácil possível. O correio eletrônico (e-mail) é a aplicação que mais ilustra esta procura, pois reúne, entre outros, estes atributos. Entretanto, a facilidade de utilização do correio eletrônico fornecido pelo Rioprevidência deve ser usada no interesse do serviço, podendo ser, ocasionalmente, utilizada para mensagens pessoais curtas e pouco freqüentes.

5.3.2 Considerando que o uso dos serviços de Correio Eletrônico no âmbito do Rioprevidência é uma concessão e não um direito, é de extrema importância que se estabeleça um conjunto de regras que possibilitem a utilização adequada desse importante recurso tecnológico.

5.3.3 Todos os Usuários do Rioprevidência ao utilizarem esse serviço deverão fazê-lo no estrito interesse do Órgão, mantendo uma conduta profissional, especialmente em se tratando da utilização do bem público.

5.4 Acesso ao Correio Eletrônico

5.4.1 Todas as contas de correio eletrônico terão uma titularidade, determinando a responsabilidade sobre a sua utilização.

5.4.2 Os usuários do Rioprevidência poderão ser titulares de uma única caixa postal individual no Servidor de Correio Eletrônico, com direitos de envio/recebimento de mensagens, via Intranet e Internet, a critério do titular de Área/Gerência, enquanto perdurar o seu vínculo com a Autarquia.

5.4.3 Contas com inatividade por um período igual ou superior a 60 (sessenta) dias serão bloqueadas, a fim de evitar o recebimento de novas mensagens. Esta regra não se aplica às contas vinculadas aos cargos/funções, por serem inerentes às atribuições.

5.4.4 O tamanho das caixas postais será de 200 MB para os usuários classificados como preferenciais, Presidente, Diretores, Assessores e Gerentes, e de 100 MB para os demais usuários.

5.4.5 As mensagens com arquivos anexados texto e anexo terão no máximo 10 MB.

5.5 Regras para utilização do Correio Eletrônico (E-mail)

5.5.1 O usuário é o responsável direto pelas mensagens enviadas por intermédio do seu endereço de correio eletrônico.

5.5.2 O usuário deve utilizar o Correio Eletrônico de forma adequada e diligente.

5.5.3 É vedada a utilização do Correio Eletrônico, nas situações abaixo:

I- Envio de mensagens não autorizadas divulgando informações sigilosas e/ou de propriedade do Governo;

II- Acesso não autorizado à caixa postal de outro usuário;

III- Acesso não autorizado ao Banco de Dados do Correio Eletrônico de outro Órgão;

IV- Envio armazenamento e manuseio de material que contrarie o disposto na legislação vigente;

V- Envio armazenamento e manuseio de material que caracterize a divulgação, incentivo ou prática de atos ilícitos, proibidos pela lei ou pela presente Norma, lesivos aos direitos e interesses do Órgão ou de terceiros, ou que, de qualquer forma, possam danificar, inutilizar, sobrecarregar ou deteriorar os recursos tecnológicos (hardware e software), bem como os documentos e arquivos de qualquer tipo, do usuário ou de terceiros;

VI- Envio armazenamento e manuseio de material que caracterize promoção, divulgação ou incentivo a ameaças, difamação ou assédio a outras pessoas, assuntos de caráter obsceno, prática de qualquer tipo de discriminação relativa à raça, sexo ou credo religioso, distribuição de qualquer material que caracterize violação de direito autoral garantido por lei, uso para atividades com fins comerciais e o uso extensivo para assuntos pessoais ou privados;

VII- Envio de mensagens do tipo “corrente” e “spam”;

VIII- Envio intencional de mensagens que contenham vírus eletrônico ou qualquer forma de rotinas de programação de computador, prejudiciais ou danosas;

IX- Envio de mensagens que contenham arquivos com código executável (exe, .com, .bat, .pif, .js, .vbs, .hta, .src, .cpl, .reg, .dll, .inf) ou qualquer

outra extensão que represente um risco à segurança do Rioprevidência;

X- Utilização de listas e/ou caderno de endereços do Rioprevidência ou de qualquer Órgão para a distribuição de mensagens que não sejam de estrito interesse funcional e sem a devida permissão do responsável pelas listas e/ou caderno de endereços em questão;

XI- Todo e qualquer procedimento de uso do Correio Eletrônico não previsto nesta Política, que possa afetar de forma negativa o Órgão ou o Governo.

5.6 Cadastramento e Descadastramento

5.6.1 A Gerência de Informática do Rioprevidência é a área responsável pela Inclusão, Alteração e Exclusão dos usuários de correio eletrônico do Rioprevidência.

5.6.2 Cabe a cada setor do Rioprevidência solicitar, através de CI ou formulário da Intranet à Gerência de Informática, via DAF - Diretoria de Administração e Finanças, a Inclusão, Alteração ou Exclusão de seus usuários de correio eletrônico.

5.7 Disposições Finais

5.7.1 O Rioprevidência se reserva ao direito de verificar, sempre que julgar necessário, a obediência às normas/procedimentos citados neste documento.

5.7.2 As mensagens eletrônicas trafegam de forma aberta na Internet, passíveis de visualização. Para evitar que pessoas não autorizadas possam ter acesso a essas mensagens, o Rioprevidência fez uso de técnicas e ferramentas de criptografia.

5.7.3 O uso indevido dos serviços de Correio Eletrônico tratados neste documento, é passível de sanção disciplinar, de acordo com a legislação vigente e demais normas aplicadas à matéria.

5.7.4 Será de responsabilidade de cada Usuário zelar pelo fiel cumprimento ao estabelecido na presente norma, devendo também assinar o “Termo Individual de Responsabilidade”, em anexo.

6 NORMAS DE CONTAS E SENHAS PARA ADMINISTRADORES

6.1 Objetivo

6.1.1 Estabelecer os procedimentos adequados para a correta utilização das contas com privilégios de “Administrador” das estações de trabalho e servidores do ambiente de Tecnologia da Informação e Comunicação do Rioprevidência.

6.2 Abrangência

6.2.1 Esta norma deverá ser aplicada a todos os Usuários que possuam contas com privilégios de “Administrador” nas estações de trabalho e servidores do ambiente do Rioprevidência.

6.3 Conceito

6.3.1 O Rioprevidência elaborou esta norma de contas e senhas para Administradores, de forma a evitar o uso inapropriado de privilégios de Administrador de Sistemas, que pode vir a ser um grande fator de contribuição para falhas ou violações de Sistemas.

6.4 Usuários com Privilégios de Administrador

6.4.1 As **estações de trabalho ou servidores** instalados na Autarquia e utilizados pelo Rioprevidência terão as seguintes regras para as senhas com privilégios de Administrador:

I- Somente alguns funcionários da Gerência de Informática, pertencentes à Coordenação de TI, poderão ter contas com privilégios de Administrador Local da rede;

II- Somente alguns funcionários da Gerência de Informática, pertencentes à Coordenação de Sistemas, poderão ter contas com privilégios de Administrador de Sistemas Locais.

6.5 Formação de Contas e Senhas

6.5.1 As senhas para Administradores deverão conter no mínimo 10 caracteres, sendo obrigatório o uso de letras maiúsculas, minúsculas e caracteres numéricos e especiais (“$”, “%”, “&”,...). Para aqueles ambientes que não suportarem o mínimo de 10 caracteres, deverão ser utilizados o limite máximo que o ambiente permitir.

6.5.2 Os sistemas e aplicações deverão prover algum mecanismo ou instrução que garanta que só sejam aceitas senhas com a formação acima citada.

6.5.3 As contas com privilégio de administrador não poderão conter em sua formação algo que as identifique como sendo uma conta de administrador. (Ex. Admin, Adm, Administrador, Administrator, pradmin etc.).

6.5.4 Deverão ser evitadas as composições de senhas com seqüências numéricas (123...) e/ou alfabéticas (abc...), além de senhas de fácil dedução (nome da máquina, nome do usuário, data de nascimento...).

6.6 Tempo de vida de Contas e Senhas

6.6.1 Histórico composto, pelo menos, das 8 (oito) últimas senhas, será guardado no servidor.

6.6.2 A conta deverá ser bloqueada após a 5ª (quinta) tentativa de login.

6.6.3 O tempo de vida das senhas deverá obedecer aos seguintes critérios:

I- Administrador de Servidores e de Domínio – validade de, no máximo, 90 (noventa) dias, devendo ser forçada a troca no primeiro login após esse período;

II- Administrador Local – válida por tempo indeterminado.

6.7 Reinicialização de Senhas

6.7.1 Caso haja suspeita do comprometimento de uma senha esta deverá ser reinicializada.

6.8 Disposições Gerais

6.8.1 Os sistemas e aplicações que impedem a exibição na tela de login do último usuário a acessá-lo, poderão ser acionados quando a Gerência de Informática achar necessário.

6.8.2 Os sistemas e aplicações que impedem a mesma conta de estar ativa, simultaneamente, em mais de uma estação, poderão ser acionados quando a Gerência de Informática achar necessário.

6.8.3 Os sistemas e aplicações que impedem a exibição automática, na tela de login, da senha referente ao respectivo login em uso, poderão ser acionados quando a Gerência de Informática achar necessário.

6.8.4 A senha deverá ser mantida em sigilo pelo Administrador durante o período de uso. O Administrador será responsabilizado, conforme previsto na legislação, pelo mau uso da mesma.

6.8.5 Em caso de desligamento de Administrador, o gerente ou coordenador deverá solicitar à Gerência de Informática o cancelamento da senha de Administrador do mesmo.

6.8.6 Os servidores/estações de trabalho deverão ter, no máximo, três contas com privilégio de Administrador.

6.8.7 Os acessos realizados e as falhas nas tentativas de login deverão ser auditados pela Gerência de Informática.

7 NORMAS DE OPERAÇÃO DE CÓPIA DE SEGURANÇA – BACKUP

7.1 Objetivo

7.1.1 Estabelecer os procedimentos adequados para a correta geração e recuperação de **Cópias de Segurança** das informações corporativas desta Autarquia, definindo, como e onde guardá-las em segurança.

7.2 Abrangência

7.2.1 Esta norma deverá ser aplicada a todos os arquivos/informações armazenados nos Servidores do Rioprevidência.

7.3 Conceito

7.3.1 Sob o aspecto da proteção e integridade física das informações manipuladas no Rioprevidência, esta Política tem por objetivo definir as diretrizes para a geração, guarda e recuperação das Cópias de Segurança das Informações no que diz respeito aos riscos de perda, sejam elas acidentais ou intencionais.

7.4 Dados a serem copiados

7.4.1 Serão feitas Cópias de Segurança de todas as informações corporativas (documentos e arquivos) dos diversos setores desta Autarquia que forem salvas/gravadas pelos usuários no *drive* **'H'**. O *drive* **'H'** está disponibilizado para cada setor do Rioprevidência.

7.4.2 Serão feitas Cópias de Segurança de todas as informações (banco de dados, sistemas, arquivos, serviços, etc.) armazenadas nos Servidores do Rioprevidência.

7.5 Armazenamento

7.5.1 Cabe a Gerência de Informática escolher as mídias de armazenamento para as Cópias de Segurança, mantendo a quantidade necessária para prover as cópias.

7.5.2 As Copias de Segurança serão guardadas em local apropriado localizado no Rioprevidência.

7.5.3 Semanalmente, um jogo de mídias contendo as Cópias de Segurança será enviado para ser guardado em ambiente externo, atualmente, junto ao PRODERJ.

7.5.4 Somente alguns funcionários da Gerência de Informática estão autorizados a executar os procedimentos de cópia e recuperação das informações no ambiente do Rioprevidência.

7.6 Tempo de vida das Cópias de Segurança

7.6.1 Os Procedimentos de geração das Cópias de segurança serão efetuados diariamente à noite.

7.6.2 As Cópias de Segurança serão mantidas por 90 dias para fins de recuperação das informações. Após esse período as mídias serão reutilizadas, não havendo como recuperar informações de tempo superior ao mencionado.

7.7 Recuperação das informações

7.7.1 Para recuperação de informações do *Drive* H ou de quaisquer outros dados danificados ou excluídos nos Servidores da Autarquia, o procedimento será solicitar, através de CI, a recuperação dos mesmos à Gerência de Informática.

7.7.2 Cabe a Gerência de Informática proceder, quinzenalmente, teste de recuperação dos dados para assegurar a eficácia dos procedimentos de "Cópias de Segurança".

7.8 Disposições Gerais

7.8.1 A Gerência de Informática será responsável pelo cumprimento das normas contidas nesse manual.

TERMO INDIVIDUAL DE RESPONSABILIDADE

Pelo presente instrumento, eu, _____, matrícula/identidade nº _____, perante o FUNDO ÚNICO DE PREVIDÊNCIA SOCIAL DO ESTADO DO RIO DE JANEIRO - Rioprevidência, na qualidade de usuário dos recursos de processamento da informação do Rioprevidência, declaro estar ciente e concordar com a **Política de Segurança da Informação** composta por suas Diretrizes Gerais, Normas, Procedimentos e Instruções, que estão disponíveis na INTRANET, seção Política de Segurança.

Declaro, também, estar ciente de que os acessos por mim realizados à internet, bem como o conteúdo das mensagens enviadas através do Correio Eletrônico corporativo são monitorados automaticamente.

É de conhecimento do usuário que os dados, documentos, informações e programas armazenados nos equipamentos do Rioprevidência, estão sujeitos à auditoria a qualquer momento, a pedido da Autarquia.

Qualquer arquivo e programa acessado por meio externo (pen drive, cd, dvd, hd em nuvem, hd externo, etc...) bem como aqueles instalados na rede, estão sujeitos a mesma politica instituída na politica de segurança no item 1.6.

Declaro, ainda, estar ciente das minhas responsabilidades descritas nas normas da Política de Segurança da Informação e que, a não observância desses preceitos, implicará na aplicação das sanções previstas nas Diretrizes Gerais desta Política.

Rio de Janeiro, _____ de _____de _____.

_____

(Assinatura)