# REGULAMENTO INTERNO DE SEGURANÇA DA INFORMAÇÃO DA "EMPREL - EMPRESA MUNICIPAL DE INFORMÁTICA"

## 1. INTRODUÇÃO:

Este documento foi elaborado e visa implementar as orientações das mais atualizadas e confiáveis diretrizes de segurança mundiais, em especial a NBR ISO IEC 27002, NBR ISO IEC 27001, NBR ISO IEC 15408, ISO IEC PSTR 18044, NBR ISO 13335, NBR ISO 11514, NBR ISO 11515, NBR ISO 11584, BS 7799, do *British Standard Institute*, na reforma do *Bürgerliches Gesetzbuch* (BGB) envolvendo documentos eletrônicos, no *Data Protection Working Party*, da União Européia, no *Statuto dei Lavoratori Italiani*, *Codice della Privacy* (Itália), Diretiva 2002/58/CE; Decreto Legislativo Italiano n.º 196 de 30 de junho de 2003 *(Misure di Sicurezza)*, Instrução Normativa GSI/PR n.º 1, de 13 de junho de 2008, Instrução CVM n.º 380 de 23 de dezembro de 2002 e outros, tendo por finalidade atribuir responsabilidades, definir direitos, deveres, expectativas de acesso e uso, penalidades, e criar uma cultura educativa empresarial de proteção aos dados da EMPREL.

A justificativa da necessidade de implementação do presente Regulamento se faz ainda mais evidente, tendo em vista que a EMPREL é a empresa municipal de informática do Recife, voltada a propor e gerenciar as políticas de Infra-estrutura de Informática para o município, e para tanto, conta com um parque tecnológico, composto de redes de microcomputadores, geoprocessamento, multimídia, além de também exercer a função de provedor público de acesso à Internet.

## 2. OBJETIVO:

O objetivo deste documento é estabelecer as diretrizes e regras de Segurança da Informação, em relação à manipulação de informações e utilização da infra-estrutura tecnológica da EMPREL, de acordo com princípios éticos e legais.

São também objetivos deste documento:

a) Padronizar as atividades de segurança para o uso e administração dos recursos da Infra-estrutura de Informática;
b) Fornecer suporte às atividades de segurança que visem garantir a confidencialidade, integridade, disponibilidade e autenticidade das informações;
c) Assegurar que os recursos humanos e tecnológicos comprometidos com o manuseio e processamento da informação estão de acordo com as presentes regulamentações.

## 3. DEFINIÇÕES:

Para fins deste Regulamento de Segurança, o termo USUÁRIOS fica entendido da seguinte forma: empregados com vínculo empregatício, servidores postos à disposição por órgãos ou entidades da administração centralizada ou descentralizada, federal, estadual ou municipal, não

importando o regime jurídico a que estejam submetidos, prestadores de serviços que, de qualquer forma, estejam alocados na prestação de serviços, por força de contrato e colaboradores em geral que, direta ou indiretamente, utilizem os sistemas da EMPREL para o desenvolvimento de suas atividades profissionais.

O termo INFORMAÇÃO fica entendido como o patrimônio da EMPREL ou da Prefeitura da Cidade do Recife, consistente nas suas informações, que podem ser de caráter comercial, estratégico, técnico, financeiro, mercadológico, legal, de recursos humanos, ou de qualquer outra natureza, não importando se protegidas ou não de confidencialidade, desde que se encontrem armazenadas e/ou trafegadas na infra-estrutura tecnológica da EMPREL ou da Prefeitura da Cidade do Recife.

O termo SEGURANÇA DA INFORMAÇÃO, por sua vez, deve ser entendido como a adoção de medidas eficazes para resguardar que as informações da EMPREL ou da Prefeitura da Cidade do Recife sejam conhecidas somente por aqueles que devem conhecê-las, evitando seu uso indevido, inadequado, ilegal, ou em desconformidade com este Regulamento de Segurança.

O termo REDE INTERNA, deve ser entendido como o conjunto de computadores, equipamentos de rede e infra-estrutura, bem como os servidores com os aplicativos e bancos de dados corporativos da Prefeitura da Cidade do Recife.

O termo CONTA DE REDE, também chamado de conta de domínio, é a identificação do usuário que permite o acesso aos recursos computacionais da rede corporativa, tais como, correio eletrônico, acesso à internet e às informações da Prefeitura da Cidade do Recife.

O termo VNC significa "Virtual Network Computing" e é uma ferramenta de suporte remoto. Este serviço ficará disponibilizado para um grupo restrito de técnicos de manutenção e a intervenção remota dependerá da autorização do usuário.

# 4. COMPROMISSO COM A SEGURANÇA DA INFORMAÇÃO

## 4.1. PRESSUPOSTO

A implantação e manutenção de um ambiente computacional seguro é tarefa inerente dos administradores e técnicos de informática. A segurança da REDE INTERNA depende da colaboração de todos os envolvidos. Portanto a responsabilidade com a Segurança da Informação não é apenas da Supervisão de Segurança e da Diretoria, mas também dos demais funcionários e terceirizados.

O presente Regulamento de Segurança constitui um conjunto de normas e regras de Segurança da Informação a possibilitar o processamento,

compartilhamento e armazenamento de informações da EMPREL, através de sua infra-estrutura tecnológica e deve ser respeitado por todos, pois trará efeitos obrigacionais nos termos deste regulamento e da legislação vigente.

Assim sendo, tanto a Diretoria e demais gerentes, como também os usuários são responsáveis, por cumprir as regras, normas e procedimentos estabelecidos neste Regulamento de Segurança, bem como relatar possíveis falhas de segurança ao Comitê.

Este Regulamento de Segurança é destinado a todos que têm ou tiveram algum vínculo com a EMPREL assim compreendidos entre todos os seus empregados, ex-empregados, prestadores de serviços, ex-prestadores de serviços, colaboradores, ex-colaboradores, servidores e ex-servidores que têm, terão ou tiveram acesso às informações da EMPREL e utilizam, utilizarão ou utilizaram, sua infra-estrutura tecnológica.

### 4.2. COMPROMISSO DA DIRETORIA

É responsabilidade da Diretoria disponibilizar uma infra-estrutura tecnológica que oferece um nível adequado de segurança para os sistemas da Administração Municipal. Também cabe a Diretoria implantar as ferramentas necessárias para evitar violações das senhas dos usuários e evitar o uso indevido por terceiros.

### 4.3. COMPROMISSO DOS USUÁRIOS

É responsabilidade dos usuários respeitar todas as disposições do RISI, bem como colaborar com alertas, sugestões e criticas que possam melhorar a segurança da informação.

## 5. COMITÊ DE SEGURANÇA DA INFORMAÇÃO:

A EMPREL criou um COMITÊ DE SEGURANÇA DA INFORMAÇÃO, que será o órgão permanente que conduzirá toda a gestão do presente Regulamento de Segurança e será representado pelo Gestor de Segurança.

Tal Comitê será necessariamente composto pelo Diretor de Assuntos Jurídicos, pelo Diretor de Infra-estrutura de Informática, pelo Diretor de Sistemas e Negócios Corporativos, pelo Gerente de Gestão de Pessoas e pelo Supervisor de Segurança da Informação, este último sendo um funcionário com domínio técnico na área, designado como Gestor de Segurança para representação do Comitê, e todos juntos constituirão um grupo de trabalho para tratar de questões ligadas à Segurança da Informação e propor soluções específicas sobre Segurança da Informação, que envolvam direta ou indiretamente a EMPREL.

O Comitê será responsável pela análise de todas as infrações cometidas pelos usuários ao presente Regulamento, devendo gerar relatório que pondere acerca da gravidade e riscos sob o enfoque técnico e legal de cada

infração cometida, culminando na recomendação à Diretoria de instauração de processo administrativo disciplinar para apuração dos fatos e aplicação das ações disciplinares cabíveis, para eventual e futuro encaminhamento às autoridades policiais e/ou judiciais.

Portanto, todo e qualquer evento que coloque em risco a Segurança da Informação, assim como quaisquer outros incidentes relacionados que violem o presente Regulamento, deverão ser comunicados, de imediato, pela Supervisão de Segurança, pelo suporte ou por qualquer usuário que tenha conhecimento do mesmo, ao COMITÊ DE SEGURANÇA DA INFORMAÇÃO para que analise e recomende as medidas necessárias, sendo que, na omissão ou inércia daquele que tiver ciência da ocorrência de incidente relacionado à segurança da informação, este será responsabilizado na medida de sua omissão.

O COMITÊ DE SEGURANÇA DA INFORMAÇÃO poderá ser contatado a qualquer momento pelos usuários para esclarecer dúvidas, obter orientações, expressar opiniões, reportar situações de violação ao presente Regulamento e outros, através da conta de email comite.seguranca@recife.pe.gov.br

Sugestões que visem aumentar o nível de Segurança da Informação deverão ser encaminhadas ao COMITÊ DE SEGURANÇA DA INFORMAÇÃO para que este proceda à análise valorativa destas iniciativas, apresentando parecer à Diretoria no prazo máximo de 30 (trinta) dias do recebimento da sugestão, opinando ou não pela sua aprovação e posterior implementação.

São também atribuições do COMITÊ DE SEGURANÇA DA INFORMAÇÃO a coordenação da comunicação e divulgação institucional deste Regulamento, podendo recomendar as medidas que entender cabíveis e a coordenação de treinamentos periódicos e processos de conscientização que se fizerem necessários, podendo, para tanto, contar com a colaboração de equipes externas, desde que estas sejam formalmente aprovadas e contratadas para este fim.

A implantação de novos sistemas operacionais e/ou softwares deve ser informada ao COMITÊ DE SEGURANÇA DA INFORMAÇÃO, para que analise e recomende as alterações do presente Regulamento de Segurança, se for o caso.

## 6. PROCEDIMENTOS DE USO DA REDE INTERNA, HARDWARES E SOFTWARES:

A utilização da infra-estrutura tecnológica é fundamental para o desenvolvimento das atividades profissionais pelas quais os usuários da EMPREL foram contratados, sendo disponibilizada exclusivamente como ferramenta de trabalho. Com isso, alguns procedimentos devem ser adotados para delinear o que é permitido ou não, bem como garantir o adequado desempenho dessas atividades.

Assim, toda a rede, hardwares e softwares estão sujeitos à monitoração e, portanto, a EMPREL poderá manter, a seu critério, histórico de acessos realizados aos seus sistemas.

Para que esses procedimentos sejam adotados, é importante entender que os termos rede, hardware e software se referem a todos os equipamentos da EMPREL, tais como, mas não se limitando a: computadores desktop, notebooks, softwares homologados (vide relação no anexo III), cabos de rede, backbones, equipamentos de discagem (modems), equipamentos de roteamento (roteadores), equipamentos de distribuição (switches e hubs), servidores, firewalls, proxies, impressoras, scanners, smartphones ou qualquer outro equipamento pertencente à infra-estrutura tecnológica da EMPREL.

Sendo assim, e a partir desse entendimento, seguem as regras:

## 6.1. USUÁRIOS (CONTAS DE REDE):

Todas as senhas de acesso fornecidas aos usuários são pessoais e intransferíveis e de uso exclusivo dos mesmos, que assumem integral responsabilidade pela guarda e sigilo de sua senha pessoal, bem como pelo uso indevido por terceiros, sendo responsável o usuário pela sua disponibilização indevida.

Além de tais cuidados, o usuário não deve utilizar sua conta de rede, ou qualquer outra conta, para violar ou transpor as definições contidas neste Regulamento de Segurança.

Caso qualquer vulnerabilidade do sistema operacional seja constatada por usuário da EMPREL, este, imediatamente, deverá informar ao COMITÊ DE SEGURANÇA DA INFORMAÇÃO sobre tal vulnerabilidade, sendo que qualquer utilização ilícita da infra-estrutura tecnológica da EMPREL seja pelo aproveitamento de falhas de segurança, ou pela simples tentativa e erro de acerto de senhas, o sujeitará às devidas sanções civis e criminais, em especial como incurso nos crimes previstos na Lei 9.279/96 e em outras leis que sejam aplicáveis aos casos apurados, inclusive no que toca aos servidores da Administração Pública, quando for o caso.

Abaixo seguem as normas definidas:

a. Não é permitido compartilhar a conta de rede e senha com outro usuário e/ou terceiro;
b. Não é permitida nenhuma tentativa e/ou acesso de outras contas de rede que não a sua pessoal;
c. Não é permitida nenhuma tentativa e/ou acesso para transpor a autenticação ou segurança do computador, rede ou conta;
d. Não é permitida nenhuma tentativa e/ou interferência com serviços da rede, das máquinas e outros dispositivos.

O usuário será considerado inativo caso não acesse a sua conta de rede durante o período de 31 (trinta e um) dias, ocasião em que esta será bloqueada pela área de Infra-estrutura de Informática.

A Diretoria Administrativa e Financeira deve informar à área de Infra-estrutura de Informática, sempre que houver desligamento, no prazo de 24 (vinte e quatro) horas, a relação de usuários desligados, ou em processo de desligamento para que todos os acesos sejam imediatamente bloqueados.

## 6.2. SENHAS:

Toda conta de rede tem sua respectiva senha, que provê acesso aos recursos autorizados, a cada usuário da EMPREL, de acordo com seu perfil, que deverá mantê-la em segurança.

As solicitações de criação, exclusão e alteração de usuários deverão ser feitas através de formulário padrão, constantes nos anexos VII e VIII, e encaminhadas pelo gerente do departamento solicitante, à área de Infra-estrutura de Informática, que fornecerá a senha diretamente para o usuário.

A área de Infra-estrutura de Informática será a única responsável pela concessão de acessos e somente atenderá tais solicitações, com o posterior fornecimento de senha, mediante as seguintes condições:

a. Todos os campos do formulário devem estar preenchidos com informações fidedignas;
b. As solicitações devem ser provenientes de usuários que tenham autorização para efetuar tal solicitação em razão de seu nível hierárquico;
c. O usuário deve comparecer pessoalmente para receber sua senha;
d. O usuário deve assinar termo de recebimento da senha pelo qual se comprometa a alterá-la imediatamente.

O uso indevido de senhas poderá gerar responsabilidades civis e criminais, conforme dispõe o art. 325 do Código Penal: *Revelar fato de que tem ciência em razão do cargo e que deva permanecer em segredo, ou facilitar-lhe a revelação: pena - detenção, de seis meses a dois anos, ou multa, se o fato não constitui crime mais grave. § 1º Nas mesmas penas deste artigo incorre quem: I - permite ou facilita, mediante atribuição, fornecimento e empréstimo de senha ou qualquer outra forma, o acesso de pessoas não autorizadas a sistemas de informações ou banco de dados da Administração Pública; II - se utiliza, indevidamente, do acesso restrito.*

A senha do usuário será suspensa em situações de afastamento do trabalho, tais como nas hipóteses de férias, licença prêmio, licença maternidade, disponibilização a outro órgão da Administração Pública, mudança de função e outras. O gerente da divisão ao qual o usuário afastado pertence deverá comunicar, com antecedência, mediante o formulário constante no anexo VIII, sobre o afastamento e solicitar a suspensão da senha à área de Gestão de Pessoas, que, por sua vez,

encaminhará a comunicação e a solicitação à área de Infra-estrutura de Informática.

## 6.3. USO E CONTROLE DE INFORMAÇÕES, DADOS E ARQUIVOS:

Todos os documentos eletrônicos, dados e informações da atividade laborativa dos usuários devem estar centralizados no servidor, no diretório específico para cada usuário, para arquivos de trabalho, ou nos diretórios classificados e restritos por assunto.

O uso da capacidade de armazenagem de dados no servidor deve ser feito com tolerância em relação aos documentos da EMPREL, no sentido de armazenar arquivos sem duplicações, salvo quando estas forem exigidas.

Não é permitida a utilização do servidor para armazenar dados e arquivos pessoais dos usuários, assim entendidos como aqueles que não são de interesse, uso ou propriedade da EMPREL.

Os usuários, excetuando-se os que tenham autorização específica para esse fim em razão de seu perfil, não podem permitir ou causar qualquer alteração, bem como destruição de sistemas operacionais, dados ou comunicações de propriedade da EMPREL.

As alterações no banco de dados da EMPREL, incluindo a base de produção de fontes, podem gerar responsabilidade civil e penal, conforme dispõem os artigos 313-A e 313-B do Código Penal: Art. 313- A: *inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou bancos de dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano: pena - reclusão, de 2 (dois) a 12 (doze) anos, e multa. Art. 313-B. Modificar ou alterar, o funcionário, sistema de informações ou programa de informática sem autorização ou solicitação de autoridade competente: Pena - detenção, de 3 (três) meses a 2 (dois) anos, e multa. Parágrafo único. As penas são aumentadas de um terço até a metade se da modificação ou alteração resulta dano para a Administração Pública ou para o administrado.*

## 6.4. DIREITOS DE ACESSO A ARQUIVOS E DIRETÓRIOS:

O acesso às informações armazenadas na infra-estrutura tecnológica da EMPREL é restrito por perfis, que definem os documentos e diretórios que podem ser acessados por cada usuário, a exclusivo critério da Empresa, visando resguardar ao máximo a restrição do conhecimento de informações confidenciais.

## 6.5. PERFIS DE USUÁRIOS

São estabelecidos os seguintes perfis de usuário com as respectivas permissões:

| | |
|---|---|
| PERFIL A | Administrador – acesso à Intranet; acesso aos fontes, criação de senhas e/ou administração de BD/sistema operacional. |
| PERFIL B | Desenvolvedor – acesso à Intranet; acesso aos fontes. |
| PERFIL C | Usuário comum – acesso à Intranet. |

Não obstante a definição de perfis de usuário deste Regulamento, nada impede que, dependendo das atribuições, determinados usuários desenvolvedores, poderão ter acesso a senha de administrador da própria máquina, mediante a assinatura de um termo adicional. Além disso, dependendo das atribuições, alguns administradores poderão sofrer restrições nos acessos a determinados sistemas e bases, que serão controladas através da assinatura de um termo adicional que ficará armazenado no COMITÊ DE SEGURANÇA DA INFORMAÇÃO.

## 6.6. RECEBIMENTO, INSERÇÃO e ENVIO DE ARQUIVOS

Fica estabelecida a seguinte regra para recebimento de arquivos, por qualquer meio eletrônico, sem prejuízo de futuras regras que venham a ser acrescidas:

Somente será permitido o recebimento de arquivos para fins profissionais, necessários ao exercício das atividades dos usuários. Os arquivos não relacionados aos trabalhos, caso recebidos, deverão ser verificados por software anti-vírus, devendo o funcionário agir com prudência e cautela, especialmente para os arquivos com terminações tais como: .EXE, .COM, .SCR, ou outras que possam comprometer o sistema através da execução de comandos maliciosos, seguindo as normas gerais de segurança implantadas pela Empresa;

Apesar dos sistemas operacionais da EMPREL estarem protegidos por sistema antivírus, fica vedada a inserção ou disseminação intencional de arquivos que contenham vírus ou qualquer espécie de programas nocivos, sob pena de responsabilização do usuário nas esferas trabalhista, civil e criminal.

No tocante ao envio de arquivos, através de email, ou qualquer outra modalidade, fica estabelecido o seguinte conjunto de regras:

a) Não será permitido o envio de qualquer arquivo de desenvolvimento (arquivos-fonte), tais como: imagens, textos e/ou códigos de fontes de aplicações ou similares, quando o seu envio configurar desrespeito às normas de direito autoral, ou quaisquer outras normas vigentes no momento do envio do arquivo;
b) Não será permitido o envio de informação corporativa da EMPREL ou de seus parceiros, fornecedores, clientes e terceiros. As exceções serão objeto de autorização específica e expressa do COMITÊ DE SEGURANÇA DA INFORMAÇÃO, não se enquadrando nesta

determinação o envio de dados necessários para o desenvolvimento dos aplicativos solicitados pelos clientes, tais como, termo de referência de sistemas e telas de sistemas, no intuito de não ocasionar atrasos no atendimento de referidas demandas.

c) Não será permitido o envio de quaisquer arquivos que violem direitos de terceiros, ou que possam causar prejuízos, a terceiros e/ou à EMPREL;
d) Não será permitido o envio de qualquer arquivo com conteúdo que configure prática de infração penal ou ilícito civil em face da EMPREL e/ou de terceiros;
e) Não será permitida a prática de qualquer ato que configure concorrência desleal ou quebra de sigilo profissional;
f) Não será permitido o envio de qualquer arquivo de caráter ilegal, ofensivo e/ou imoral, de forma genérica.

Caso seja constatado o envio de qualquer arquivo elencado nos tópicos anteriores, os usuários ficam sujeitos ao pagamento de indenização por perdas e danos à EMPREL, sem prejuízo das sanções estabelecidas nas Leis nº 9.279/96 (Lei de Propriedade Industrial), 9.610/98 (Lei de Direitos Autorais) e 9.609/98 (Lei de Software).

As regras para uso de email aplicável a todos os perfis constam do anexo II deste Regulamento, que faz parte integrante do mesmo, e são definidas pela área de Infra-estrutura de Informática, com a devida ciência do COMITÊ DE SEGURANÇA DA INFORMAÇÃO, visando melhor proteger as informações e os sistemas informáticos da Administração Municipal.

Não obstante as regras aplicadas, scripts, binários, ou quaisquer arquivos executáveis, devido à sua alta periculosidade, serão bloqueados automaticamente em todos os perfis de usuários, salvo autorização expressa para tanto, concedida pelo COMITÊ DE SEGURANÇA DA INFORMAÇÃO.

Caso seja necessário o compartilhamento de arquivos confidenciais, deverá o usuário lançar o arquivo em área compartilhada do servidor, destinada para tal fim.

## 6.7. SOFTWARES:

A EMPREL disponibiliza para seus usuários um conjunto de softwares exclusivamente para o desempenho de suas atividades profissionais, assim, é vedada a utilização de quaisquer softwares não homologados pela EMPREL.

Dessa forma, os usuários somente poderão instalar programas que sejam autorizados pela Diretoria de Infra-Estrutura da EMPREL, e cientificado o COMITÊ DE SEGURANÇA DA INFORMAÇÃO. Fica, portanto, vedado ao usuário a instalação de qualquer software, sem autorização prévia e

expressa da Diretoria retro citada, excetuando-se aquele usuário que tem permissão expressa em razão de sua função.

Todos os softwares instalados nos computadores da EMPREL devem ser devidamente licenciados, e o uso de qualquer software que não seja autorizado e/ou que viole os direitos do autor do programa de computador, são terminantemente proibidos. O desrespeito a essas normas caracteriza infração à lei e ao contrato, gerando responsabilidade e será de culpa exclusiva do usuário que arcará com a responsabilidade criminal, trabalhista e civil, desde que comprovada a má fé do funcionário, verificada em processo administrativo e garantido o direito a ampla defesa e contraditório.

Portanto, os usuários infratores ficam cientes da possibilidade de indenizar a EMPREL caso esta venha a suportar qualquer prejuízo em demandas judiciais ou administrativas movidas pelos titulares dos direitos autorais de tais programas não autorizados, bem como de qualquer outra obra intelectual violada em seus direitos autorais, incluindo as despesas com custas e honorários advocatícios.

Os softwares permitidos e homologados pela EMPREL constam do anexo III do presente instrumento, que faz parte integrante do mesmo, nada impedindo que venham a ser alterados, em razão da necessidade constante de alteração e/ou exclusão de programas de computador, para melhor atender aos sistemas informáticos da EMPREL.

## 6.8. HARDWARES:

A EMPREL disponibiliza para seus usuários um conjunto de equipamentos e máquinas exclusivamente para o desempenho de suas atividades profissionais, assim, o uso inadequado desses equipamentos e para fins que não sejam os delineados pela Empresa, é proibido.

É vedado o uso de quaisquer equipamentos que não sejam de propriedade da EMPREL para conexão na rede interna, especialmente os notebooks particulares, vez que comprometem a Segurança da Informação.

Na utilização de todos os hardwares e periféricos de propriedade da EMPREL, o usuário deverá observar os seguintes cuidados:

a) Desligar o equipamento no final do expediente, ou em ausências prolongadas;
b) Toda vez que não for mais utilizar o computador, ou for se ausentar da sala, efetuar o log off ou bloqueio de tela, evitando que terceiros usem o nome de usuário ilicitamente;
c) Sempre que tiver dúvidas ou problemas nos equipamentos, contatar a área de help-desk, no ramal 7156, ou outro que venha a ser informado.

A alteração de qualquer periférico ou componente nos computadores não é permitida, ficando vedada aos usuários. A realização de qualquer

modificação ou manutenção deverá sempre ser realizada pela área de Infra-estrutura de Informática, com o conhecimento do usuário ou da chefia imediata.

## 6.9. EQUIPAMENTOS PORTÁTEIS:

É expressamente vedada a utilização de equipamentos portáteis particulares para o desenvolvimento das atividades profissionais relacionadas à EMPREL, bem como a cópia e/ou transferência de informações ou dados de propriedade da mesma através destes equipamentos.

Os equipamentos portáteis, tais como, notebooks e smartphones, somente poderão ser utilizados pelos usuários para as atividades da EMPREL se disponibilizados pela mesma, a seu exclusivo critério.

O uso de equipamentos particulares de armazenamento, tais como pendrives, memory cards, CDs, DVDs e disquetes, deverá ser evitado. Entretanto, estes poderão ser usados desde que sejam tomados todos os cuidados a fim de evitar riscos com contaminação tanto do equipamento de armazenamento como de todos os computadores em que este equipamento for plugado.

Por se tratarem de equipamentos portáteis nos quais informações da EMPREL estão armazenadas, o usuário não deve deixar esses equipamentos fora do alcance em locais públicos, onde haja acesso de múltiplas pessoas, bem como, não deve permitir que terceiros não autorizados tenham acesso às informações ou dados transportados nesses equipamentos, empregando todos os cuidados necessários para que não haja vazamento de informações.

## 6.10. ATIVAÇÃO DE TELA COM BLOQUEIO:

Os usuários devem ativar a proteção de tela com bloqueio de senha nas estações de trabalho, para que, inativos o mouse e o teclado pelo período de 05 (cinco) minutos, a tela do computador seja bloqueada automaticamente.

Os usuários são responsáveis por manter a proteção de tela com bloqueio de senha, haja vista a possibilidade de, em sua ausência, outra pessoa praticar atividade irregular, sem autorização, de sua autenticação de usuário.

Caso o usuário tenha dificuldade em ativar referido sistema, deverá contatar a área de help-desk, que ativará a proteção de tela com bloqueio de senha no prazo de 24 (vinte e quatro) horas.

## 6.11. IMPRESSORAS:

O uso das impressoras deve ser feito exclusivamente para impressão de documentos ou outras informações que sejam de interesse da EMPREL ou que estejam relacionados com o desempenho de suas atividades profissionais na EMPREL.

O usuário deve ter o cuidado de retirar com a maior brevidade da impressora os documentos que tenha solicitado a impressão que contenham informações sensíveis da EMPREL.

Impressões que contenham informações sensíveis que não tenham mais utilidade devem ser destruídas, visando preservar o sigilo.

A EMPREL, em cumprimento ao seu compromisso com a responsabilidade social, recomenda que sejam impressos apenas documentos indispensáveis, devendo os demais ser lidos na própria tela do computador.

## 6.12. CONTROLE E GERENCIAMENTO DE ANTIVÍRUS:

Sem prejuízo do controle automático dos servidores da EMPREL, além da Empresa e do antivírus corporativo, todos os usuários são responsáveis também pelo controle de dados que possam estar infectados.

Quando detectada uma mensagem ou anexo contaminados por código malicioso, esta mensagem e seus anexos serão eliminados.

Em quaisquer situações, todo e qualquer arquivo proveniente de redes ou usuários externos deverão, obrigatoriamente, ser verificados por sistemas de proteção contra vírus.

## 6.13. ACESSO REMOTO VIA VPN (Virtual Private Network)

As regras de acesso remoto via VPN aos sistemas da EMPREL são determinadas no anexo V e fazem parte integrante deste Regulamento.

A concessão de acesso remoto via VPN aos sistemas da EMPREL será a exclusivo critério da EMPREL, que optará por qual rede o usuário terá permissão de acesso.

Referida concessão será feita de forma individual, sob as condições previstas no item 6.2, sendo os usuários responsáveis por seus acessos via VPN, bem como, por qualquer atividade irregular exercida por outra pessoa de posse de seu acesso remoto. Com isso, os usuários deverão adotar medidas de cautela, para que terceiros não tenham acesso, sem autorização, à sua porta VPN.

# 7. PROCEDIMENTOS DE USO DE REDES EXTERNAS (INTERNET E OUTRAS):

O acesso a redes externas, principalmente a Internet, é fundamental para o desempenho de algumas atividades relacionadas ao trabalho, assim, o uso

da Internet deve estar voltado para o acesso à informações relacionadas somente com as atividades de interesse da Empresa.

Os acessos originados na rede interna da Empresa com destino a qualquer rede externa, só podem ser realizados através dos equipamentos da EMPREL destinados a realizar o roteamento das redes, bem como devem ser feitos com a utilização de firewall e proxy de acordo com as regras de navegação e acesso abaixo definidas.

A navegação a sites não relacionados diretamente à atividade laborativa do usuário, não é proibida, porém seu uso deve ser feito de maneira equilibrada e responsável, para assegurar ao usuário e à Empresa máxima segurança e performance no trabalho, de modo que abusos serão punidos. Excetuam-se desta previsão aqueles sites de categoria restrita pela EMPREL, cuja navegação é expressamente proibida (rol a seguir elencado).

Fica estipulada a seguinte política para acessos à Internet:

a. Da rede interna para a Internet somente poderá ser realizada a navegação através de acesso autenticado;

b. Fica terminantemente proibida a navegação aos sites pertencentes às categorias abaixo:
   - Pornográfico e de caráter sexual;
   - Compartilhamento de arquivos (ex.: *peer to peer*);
   - Pornografia infantil (pedofilia);
   - Terrorismo;
   - Drogas;
   - Crackers;
   - Sites de relacionamento;
   - Jogos;
   - Violência e agressividade (racismo, preconceito, etc);
   - Violação de direito autoral (pirataria, etc.);
   - Áudio e Vídeo, salvo com conteúdo relacionado, diretamente, a EMPREL;
   - Instant Messenger, exceto se provido pela EMPREL.
   - Propaganda político partidária;
   - Conteúdo impróprio, ofensivo, ilegal, discriminatório, e similares.

c. Não é permitida a troca de arquivos de vídeo ou música, bem como de quaisquer informações que estejam incluídas nas categorias acima, ou que sejam de propriedade da Empresa;
d. Não serão franqueados acessos à Internet às funções institucionais que não demandem o acesso à internet;
e. É proibida a transferência de qualquer tipo de programa, jogo, e similares, a partir da Internet, para a rede interna, à exceção de administradores com autorização específica para tal;
f. A transferência de arquivos via FTP, quando imprescindível, será autenticada;
g. Dispositivos de controle e segurança deverão ser utilizados, para garantir a confidencialidade e a integridade das informações em tráfego por estas redes;

As conexões deverão ocorrer exclusivamente através de acesso autenticado.

## 7.1 MENSAGENS ELETRÔNICAS (E.MAIL):

O email é um meio de comunicação institucional, motivo pelo qual será disponibilizado pela EMPREL aos usuários exclusivamente para uso das atividades laborativas.

O formato dos emails disponibilizados aos usuários será o seguinte: nome.sobrenome@recife.pe.gov.br

Todo e qualquer email enviado pelo correio corporativo deverá conter, ao final da mensagem, uma assinatura padrão, de acordo com o seguinte modelo:

*Nome Completo*
*EMPRESA MUNICIPAL DE INFORMATICA - EMPREL*
*Departamento*
*Telefones*

Após a assinatura padrão, a EMPREL providenciará a inserção automática do seguinte aviso de confidencialidade:

*As informações contidas nesta mensagem são CONFIDENCIAIS, protegidas pelo sigilo legal e por direitos autorais. A divulgação, distribuição, reprodução ou qualquer forma de utilização do teor deste documento depende de autorização do emissor, sujeitando-se o infrator às sanções legais. O emissor desta mensagem utiliza o recurso somente no exercício do seu trabalho ou em razão dele, eximindo-se o empregador de qualquer responsabilidade por utilização indevida ou pessoal. Caso esta comunicação tenha sido recebida por engano, favor avisar imediatamente, respondendo esta mensagem.*

Fica estabelecida a seguinte política com relação ao uso de email:

a) A conta de email corporativo, fornecida pela EMPREL deverá ser utilizada, exclusivamente, para o envio e recebimento de mensagens relacionadas aos trabalhos desenvolvidos pelos usuários, que anuem e conferem o direito da EMPREL em efetuar o monitoramento dos emails enviados e recebidos pelos usuários, através do email corporativo.
b) Fica proibida a inscrição do email corporativo em listas de tráfego não relacionado ao uso laborativo, a partir da data da implantação do RISI, devendo o usuário providenciar a exclusão das listas não relacionadas a assuntos profissionais, bem como o envio de todo e qualquer tipo de corrente, circulares, propaganda, boatos, conteúdo impróprio ou pornográfico e afins, ou, ainda, qualquer tipo de mensagem que possa prejudicar o trabalho de terceiros, causar excessivo tráfego na rede ou sobrecarregar a infra-estrutura tecnológica;

c) Os usuários serão responsáveis pelo uso inadequado de sua conta de email, não sendo permitida a transmissão de mensagens, vídeos e áudios, que contenham assuntos sobre violência, terrorismo, bem como qualquer outro conteúdo ilícito, ilegal, ou atentatório à moral e aos bons costumes. Ocorrendo o recebimento involuntário de email deverá ser comunicado ao COMITÊ DE SEGURANÇA DA INFORMAÇÃO;

d) Fica proibido, disseminar ou transmitir informações que violem a legislação em vigor, tais como ameaças, difamação, calúnia, injúria, racismo, pornografia infantil etc.

Para garantir a autenticidade do remetente, todo email corporativo será assinado digitalmente, assegurando não repúdio.

O usuário fica ciente da inexistência de expectativa de privacidade na utilização da conta de email corporativo e na sua navegação em sites da internet, através da infra-estrutura tecnológica da EMPREL, inclusive dispositivos portáteis disponibilizados pela EMPREL como ferramenta de trabalho. Fica ciente, ainda, da existência de monitoração do conteúdo de suas mensagens, bem como, do conteúdo armazenado na infra-estrutura tecnológica da EMPREL.

O monitoramento descrito neste Regulamento tem por objetivo verificar o respeito dos usuários às regras estabelecidas no presente instrumento, bem como produzir prova de eventual violação das condições constantes do mesmo, e na legislação em vigor, uma vez que todos os atos praticados através do email, bem como dos sites navegados na Internet são exercidos pela utilização da infra-estrutura tecnológica da EMPREL, disponibilizada estritamente para as atividades laborativas, não constituindo qualquer violação à intimidade, vida privada, honra ou imagem da pessoa monitorada, com o que os USUÁRIOS declaram, expressamente, neste ato, concordar.

O referido monitoramento é justificado, ainda, pelo fato do artigo 932, inciso III, do Código Civil, estabelecer responsabilidade do empregador pelos atos de seus prepostos ou empregados.

O monitoramento será realizado a qualquer momento, através do uso de programas de computadores específicos para tal finalidade, a critério da EMPREL.

Sem prejuízo destas regras, a EMPREL garante a privacidade dos usuários perante terceiros de forma recíproca.

As mensagens enviadas para um email corporativo poderão ser compartilhadas e/ou redirecionadas para outro email , sem necessidade de qualquer aviso prévio e sem conhecimento do emissor e do receptor da mensagem, não havendo expectativa de privacidade dos usuários, visando a identificação de eventual conduta em desacordo com este Regulamento ou com a legislação vigente.

A EMPREL se reserva o direito de, sem qualquer notificação ou aviso ao usuário, recusar o envio ou recebimento de mensagens que não expressem os interesses da mesma ou que possam colocar em risco o funcionamento dos sistemas, por conterem elementos nocivos ou contrários às regras estabelecidas, visando preservar seus equipamentos e recursos computacionais.

O usuário fica ciente que não é realizada cópia de segurança das caixas de email

As contas de email serão vinculadas a um único usuário, sendo de exclusiva responsabilidade deste qualquer ocorrência relacionada à conta.

### 7.2 SUSPENSÃO DA CONTA DE EMAIL:

A critério da EMPREL, esta poderá, a qualquer momento, e sem prévio aviso, suspender, pelo período que julgar necessário, a conta de email de qualquer usuário, caso seja constatado mau uso, risco aos sistemas, ou por haverem indícios de conduta ilícita e/ou em desacordo com esse Regulamento.

### 7.3 ACESSO A CONTAS DE EMAIL PARTICULAR (WEBMAIL):

Caso o usuário tenha seu acesso a sites de email gratuitos ou pagos, que disponibilizem o envio e recebimento de emails através da tecnologia de webmail, o usuário fica ciente que tais acessos podem comprometer a segurança das informações da EMPREL, motivo pelo qual tais acessos devem ser extremamente cautelosos e feitos de forma moderada.

Além disso, considerando que os emails pessoais acessados através da infra-estrutura tecnológica da EMPREL, serão, via de regra, realizados através da conexão à Internet pertencente à mesma e, considerando que o endereço IP (Internet Protocol) de tais conexões será vinculado à Empresa, a utilização de emails pessoais poderá gerar responsabilidades à EMPREL, o que justifica a necessidade de maior cautela por parte dos usuários.

Neste sentido, caso o acesso à conta de email do usuário cause qualquer tipo de dano à EMPREL este será integralmente responsável por seus atos, respondendo civil e criminalmente.

É absolutamente vedado o envio de informações, dados ou arquivos relacionados, direta ou indiretamente, aos interesses da EMPREL via email pessoal.

## 8. NORMAS E PROCEDIMENTOS GERAIS:

Abaixo seguem algumas normas e procedimentos a serem adotadas independentemente do uso da rede interna ou externa:

## 8.1 CONFIDENCIALIDADE:

Os usuários concordam que as informações obtidas na execução de suas atividades junto à EMPREL, em virtude de sua natureza, deverão ser tratadas como sigilosas e restritas, e que não deverão divulgar as referidas informações a terceiros. As exceções serão objeto de autorização específica e expressa do COMITÊ DE SEGURANÇA DA INFORMAÇÃO.

Neste sentido, os usuários concordam em manter sigilo sobre todas as informações que venham a tomar conhecimento em virtude das atividades profissionais, o que deverá permanecer em vigor e vincular legalmente as partes enquanto vigorar seu vínculo, vigorando, ainda, após a eventual rescisão, a qualquer título, por qualquer das partes, de maneira permanente, sob pena do direito da EMPREL pleitear o ressarcimento das perdas e danos decorrentes da violação do sigilo pelo usuário, sem prejuízo da responsabilidade criminal, em especial como incurso nas penas dos artigos 183, 184 e 195, da Lei 9.279/96, e dos artigos 153 e 154, do Código Penal Brasileiro, bem como todas as demais leis e disposições cabíveis, inclusive no que toca aos servidores da Administração Pública.

## 8.2 CERTIFICAÇÃO DIGITAL:

A EMPREL fornecerá, a seu exclusivo critério, um certificado digital ao usuário de acordo com a necessidade da atividade profissional desenvolvida.

Constitui obrigação exclusiva do usuário zelar pela guarda e conservação de seu certificado digital, bem como pela sua senha, cabendo ao usuário informar ao COMITÊ DE SEGURANÇA DA INFORMAÇÃO sobre qualquer ameaça de uso, ou efetivo uso indevido de sua assinatura digital, para que esta recomende a imediata revogação do certificado digital, sem que tal ato exima a responsabilidade do usuário pelo uso de sua assinatura eletrônica por terceiros em virtude de sua culpa na guarda da mesma, e da sua respectiva senha.

O usuário desligado ou em processo de desligamento deve devolver o certificado digital expedido pela EMPREL que esteja em seu poder, para que seja imediatamente revogado.

## 8.3 SUPORTE TÉCNICO

Está disponibilizado a todos os usuários suporte técnico permanente para auxiliá-los no uso dos recursos informáticos disponibilizados pela EMPREL.

Qualquer ajuda deverá ser solicitada ao help-desk, através do ramal 7156.

## 8.4 CÂMERAS DE FILMAGEM

A EMPREL fará uso de câmeras de segurança instaladas em suas dependências, ficando resguardada a dignidade humana dos usuários, sendo vedada a instalação de câmeras de filmagem nos banheiros e lavabos.

A filmagem descrita neste Regulamento tem por objetivo verificar o respeito dos usuários às regras estabelecidas no presente instrumento, bem como assegurar segurança física aos mesmos, não constituindo qualquer violação à intimidade, vida privada, honra ou imagem da pessoa filmada, com o que os usuários declaram, expressamente, neste ato, concordar.

As imagens captadas dentro das dependências da EMPREL serão arquivadas pelo prazo de 06 (seis) meses e mantidas em caráter estritamente confidencial, somente podendo ser divulgadas em caso de infração às regras constantes do presente Regulamento e/ou infração de legislação vigente.

## 8.5 GUARDA DE LOGS E AUDITORIA:

Todas as atividades desenvolvidas com a utilização da infra-estrutura tecnológica da EMPREL serão registradas para eventual fim judicial, além de análise ou auditoria, por um período de 03 (três) anos. Essas atividades incluem acesso à rede, informações, logs de envio e recebimento de mensagens eletrônicas, acesso e navegação a sites e outros.

Mensalmente será realizada auditoria interna pela Área de Supervisão de Segurança.

# 9. REVISÕES E COMENTÁRIOS FINAIS:

A EMPREL se reserva ao direito de revisar, adicionar ou modificar esse Regulamento de Segurança para aprimorar e garantir o perfeito funcionamento das normas e regras por ele definidas, que deverá ser submetido à apreciação dos representantes dos empregados da EMPREL, exceto em situações emergenciais.

Essa revisão, adição ou modificação será notificada aos seus usuários com antecedência, exceto em situações emergenciais, por meio eletrônico. Esta deverá ser feita junto com um novo termo de conhecimento para o funcionário assinar, quando houver necessidade.

# 10. ENCERRAMENTO:

Todas as diretrizes deste Regulamento de Segurança se estenderão aos casos omissos, que deverão ser encaminhados ao COMITÊ DE SEGURANÇA DA INFORMAÇÃO para avaliação do caso concreto e posterior recomendação à Direção de como proceder.

Ademais, todas as normas e procedimentos acima não se esgotam neste instrumento, sobretudo em razão da constante evolução tecnológica, não consistindo em rol enumerativo, motivo pelo qual é obrigação do COMITÊ DE SEGURANÇA DA INFORMAÇÃO, bem como dos usuários adotar todo e qualquer outro procedimento de segurança que esteja ao seu alcance, visando sempre proteger as informações da Empresa.

Para publicidade e conhecimento geral dos usuários da EMPREL, este documento será publicado na rede interna, bem como será afixado em murais instalados em pontos estratégicos de circulação nas dependências da Empresa.

Este documento entrará em vigor a partir da data de sua efetiva implantação.

## ANEXO I

## CRITÉRIOS PARA CRIAÇÃO DE SENHA

A senha deverá ser mantida de acordo com as seguintes normas, sem prejuízo de outras que venham a ser acrescentadas:

a. Freqüência de expiração: a senha será válida por 30 (trinta) dias, assim o sistema solicitará a alteração após a expiração do prazo;
b. Quantidade de caracteres: a senha da conta de rede deve ter a quantidade mínima de 06 (seis) caracteres, combinando letras, números e caracteres especiais, em grafia maiúscula e minúscula, seguindo o conceito de senha forte, a seguir detalhado;
c. Tentativas de acesso (login): após 03 (três) erros do nome de usuário e/ou senha, o acesso daquele usuário será bloqueado;
d. Histórico de últimas senhas: o sistema guarda as últimas 12 (doze) senhas utilizadas, com isso, não é permitida a utilização das mesmas no processo de alteração.

Os usuários devem seguir as seguintes normas para escolha de senhas, adotando o conceito de senha forte:

a. Não deverá usar como senha o nome de sua conta de rede, ou qualquer variação do mesmo (invertido, com letras maiúsculas, duplicado, etc.);
b. Não deverá usar como senha qualquer um de seus nomes ou sobrenomes, ou qualquer variação destes;
c. Não deverá usar como senha qualquer informação a seu respeito que possa ser facilmente obtida (placa de automóvel, número de telefone, nome de pessoas de sua família próxima, data de nascimento, endereço, etc.);
d. Não deverá usar como senha apenas números, ou repetições de uma mesma letra;
e. Deverá usar uma senha que combine letras, números e caracteres especiais, em grafia maiúscula e minúscula, seguindo o conceito de senha forte.

## ANEXO II

## REGRAS DE EMAIL

As regras para uso de email são as seguintes:

| | |
|---|---|
| Caixa de Mensagem | 40 MB |
| Tamanho máximo de email | 9 MB |
| Extensões de arquivos que requerem muita cautela | .exe, .com, .scr. |
| Assuntos proibidos | Propaganda político partidária; propaganda com finalidades comerciais; Pornografia e de caráter sexual; Pornografia infantil (pedofilia); Terrorismo; Drogas; Crackers; Sites de relacionamento; Jogos; Violência e Agressividade (racismo, preconceito, etc.); Violação de direito autoral (pirataria, etc.); Áudio e Vídeo, salvo com conteúdo relacionado, diretamente, a EMPREL; Conteúdo impróprio, ofensivo, ilegal, discriminatório, e similares. |

## ANEXO III

## RELAÇÃO DE SOFTWARES HOMOLOGADOS PARA A EMPREL

Os softwares homologados, dentre outros, são os seguintes:

Ambiente Mainframe: OS390 2.8, CICS 5.3.0, TSO 2.6, RACF 2.6, DFSMS 1.5, DB2 1.7, TCP/IP 97.231, VTAM 4.8;

Sistemas Operacionais: OS/390 para o mainframe; Linux Fedora e Windows XP para as estações de trabalho, Linux Enterprise e Windows 2003 Server para os servidores das máquinas PCs, sendo que para os servidores a distribuição Linux deverá ser a Red Hat Enterprise 5.1/5.2;

Linguagens de Desenvolvimento Alta Plataforma: Cobol, Language Enviroment, REXX, Sort;

Linguagens de Desenvolvimento Baixa Plataforma: Natural, Delphi 5.0, Gupta Centura 5.1, PHP;

Linguagens de Desenvolvimento: Fica definido que as linguagens padrão para desenvolvimento de sistemas são as seguintes: Java, como linguagem básica, HTML (HiperText Markup Language) e o Javascript para a camada de apresentação das aplicações para a Web e o XML(Extensible Markup Language). Eventualmente, poderá ser utilizado o PHP (um acrônimo recursivo para "PHP: Hypertext Preprocessor") para sistemas especiais;

Ambiente Integrado de Desenvolvimento e Teste Java (IDE): Fica definido que o ambiente integrado de desenvolvimento, manutenção e teste de sistemas em Java é o Rational Application Developer (RAD) 7.0 da IBM. Eventualmente, poderá ser utilizado o ECLIPSE EUROPA 3.3 como ferramenta IDE para sistemas especiais, assim considerados pelo Gerente do Projeto. Dentro da segunda opção mais ágil, que só deve ser usada após uma análise de viabilidade do uso da ferramenta para desenvolver os requisitos, fica definido o MAKER como ferramenta IDE de geração automática de código. Essa abordagem de desenvolvimento utiliza fluxogramas para representar as regras de negócio e disponibiliza assistentes para construção rápida e visual de formulários e relatórios;

Linguagens de tecnologia WEB: Linguagem Visual Padrão: HTML, Linguagem Visual Acessória: FLASH; Linguagem de Programação WEB Padrão: JAVA e suas variantes (SERVLETS, APPLETS, JSP); Linguagem de programação WEB Acessória: PHP; Linguagem de programação Acessória: JAVA Script; Editor HTML MS-FRONT PAGE WYSIWYG (What you see, is what you get) para plataforma WINDOWS, Editor HTML IBM TOP PAGE – WYSIWYG (What you see, is what you get) para plataforma LINUX.

Servidor de Aplicações: Fica definido que o servidor de aplicações padrão para todos os ambientes é o WebSphere da IBM. Eventualmente, poderá ser utilizado o JBOSS como Servidor de Aplicações para sistemas especiais,

assim considerados pelo GCT.

Servidor Web: Fica definido que o servidor web padrão para os ambientes de desenvolvimento e de testes é o Tomcat, da Jakarta, e o servidor web dos ambientes de homologação e produção é o Apache;

Container de Servlet: Fica definido que o container de Servlet para todos os ambientes é o Tomcat, da Jakarta;

SGBD – Sistema Gerenciador de Bancos de Dados: Fica definido que o SGBD padrão para todos os sistemas é o DB2 da IBM. Eventualmente, poderão ser utilizados o Postgress (PostgreSQL) e o Oracle para sistemas especiais.

Ferramentas de Construção de Interface com o Usuário e Prototipação da Interface: Ficam definidas as seguintes ferramentas para construção da interface gráfica dos sistemas: Suite Corel Draw X3, Macromedia Flash, UltraEdit, MapEdit;

Ferramentas de Geoprocessamento: Ferramentas para uso Local ou Desktop: ArcGIS Explorer 9.2 for Windows (como ferramenta desktop cliente para consulta a dados georreferenciados); ArcGIS Desktop 9.2 for Windows que poderá vir habilitado para as funcionalidades disponíveis no ArcView (como ferramenta desktop para elaboração de Sistemas de Informações Geográficas – SIG, incluindo recursos de mapeamento, análise, e recursos básicos para edição de dados gráficos); ArcEditor (inclui todas as funções do ArcView, além de recursos avançados para edição de mapas e banco de dados geográfico); ArcInfo (inclui todas as funções do ArcView e do ArcEditor, incluindo recursos avançados de geoprocessamento);

Solução Corporativa: ArcSDE 9.2 for SUSE Linux and Red Hat Linux (Intel) (x86) (para gerenciamento e acesso aos dados espaciais, de forma integrada com os dados descritivos no SGBD); ArcGIS Server 9.2 Enterprise for Java Plataform (SUSE Linux and Red Hat Linux [Intel]) (para criação e gerenciamento de esquemas e serviços de mapas na Internet, permitindo a visualização de mapas e edição de base de dados vetoriais, fornecimento de acesso e processamento a serviços de geoprocessamento, suporte ao desenvolvimento de GIS específicos para organização disponibilizando um framework de desenvolvimento de aplicações Java, o ArcGIS Server 9.2 ADF for Java Plataform, bem como para geração de sites para manipulação de dados georreferenciados através de funcionalidades/ferramentas de geoprocessamento);

Modelagem de dados: System Archetect da Telelogic;

Ferramenta de Data Warehouse: A ferramenta adotada para a construção de Data Warehouses ou Data Marts é o Sagent;

Ferramenta de Automação de Escritório: A ferramenta de automação de escritório adotada é o BROffice;

Sistema de Correios Corporativo: Postfix;

Software de Controle de Versões: Fica definido o CVS – Concurrent Versions System, como a ferramenta padrão de controle de versões da EMPREL, e que todos os artefatos (documentos e código) gerados em projetos de desenvolvimento e manutenção de sistemas deverão ser controlados pelo CVS;

Software de Script Batch: Fica definido o Ant como sendo a ferramenta padrão de geração e execução de scripts batch da EMPREL;

Software de Controle de Bugs e Mudanças: Fica definido o Mantis como ferramenta de controle de mudanças;

Software para Modelagem de Sistemas: Fica definido o ArgoUML como ferramenta de modelagem UML;

Software de Testes de Unidade: Fica definido o JUnit como o software a ser utilizado para a realização de testes de unidade em Java;

Software de Testes de Funcionalidade: Fica definido que o software padrão para a execução de testes de funcionalidade é o Canoo Web Test;

Software de Testes de Stress: Fica definido que o software padrão para a realização de testes de stress é o JMeter;

Software para Integração Contínua: Fica definido o CruiseControl como o software utilizado na integração contínua, conjuntamente com o CVS e o Ant. Esse procedimento é realizado pelas ferramentas CVS, Ant, compilador Java, JUnit, Canoo Web Test e CruiseControl, em conjunto;

Ferramenta de Geração de Help: Fica definido que o software de geração de Help é o Robohelp;

Ferramenta de Refactoring: Fica definido que a ferramenta de refactoring é o JRefactoring;

Ferramenta para verificação de padrões e correção de código HTML: Fica definido como padrão de validação e correção de código HTML a ferramenta HTML TIDY;

FrameWorks: Fica definido o uso do JSF 1.1 (Java Server Faces) como framework usado para simplificar a construção da interface gráfica para aplicações web utilizando Java; Fica definido o uso do framework Hibernate 3, que tem a finalidade de abstrair do desenvolvedor o mapeamento objeto relacional da persistência de dados; Fica definido o uso do framework Spring 2.5 que tem como principal objetivo gerenciar a complexidade do desenvolvimento de aplicações corporativa em um ambiente mais "leve" conseguindo executar funcionalidades que anteriormente só poderiam ser conseguidas através de EJB;

Protocolo para Transferência de Dados: Fica estabelecido que o protocolo padrão para troca de dados entre sistemas é o XML;

Componentes Java: Ficam definidos como padrões os componentes abaixo, com suas respectivas finalidades: Avaliador de fórmulas matemáticas: JEP; Gerador de imagens GIF: Acme; Controle de transações: EJB - Enterprise Java Beans e o cesar.persistencia.transações; Gerenciador Transações Pool de conexões: EJB - Enterprise Java Beans e o cesar.persistencia.poolConexoes. GerenciadorPollConexoes;

Geração de log: Log4j;

Ferramentas de suporte à Rede: Cacti, Sniffer;

Anti-Spam: Iron Port;

Sistema de Detecção de Intrusão: IPS da 3Com;

Gerenciador de Rede: Network Director 3Com, Nagios. E Wire Shark;

Sistema de Backup: Bacula;

Sistema de Storage: IBM DS 4700;

Sistema de Abertura e Registro de ocorrências: OCOMON;

Sistema de Correio Corporativo: PostFix;

Estação de Trabalho: As aquisições são realizadas com pacote Windows-XP O&M e adicionamos o seguinte pacote: BROffice 2.2; Mozila Firefox; Mozila Thunderbird; DOS-VOX; TREND (anti-vírus Officescan); Controle Remoto VNC; Cacic; Instalamos outros pacotes para uso do SOFIN: Client Oracle, Controle de Acesso: EMAC, Emulador de Terminal IBM X3270. Secretaria de Educação: Sistema Operacional LINUX (FEDORA 8.0). Para o Projeto PROJOVEM: Windows2000 + Linux.

## ANEXO IV

## ROTINAS DE CÓPIAS DE SEGURANÇA

| Banco de dados | Backup diário | Backup semanal | Backup Quinzenal | Backup mensal | Backup anual |
|---|---|---|---|---|---|
| Adabas - Baixa | 60 dias | | | 12 meses | |
| Adabas-Cópia-Baixa | 60 dias | | | 12 meses | |
| DB2 – OS390 | | 5 semanas | | 03 meses | |
| DB2 – OS390 - SFAU | 05 dias | 5 semanas | | 03 meses | |
| DB2-OS390-LOG | 05 dias | | | | 1 ano |
| DB2 - baixa | 90 dias | | | 12 meses | |
| Oracle (lógico) | 30 dias | | | 12 meses | |
| Oracle (físico) | 90 dias | | | 12 meses | |
| Postgres | 90 dias | | | 12 meses | |
| | | | | | |
| | | | | | |
| OS390 - VSAM | 8 dias | | | 3 meses | |
| OS390 - Bibliotecas | 7 dias | | 1 ano | | |
| Servidores - Baixa | 45 dias | 30 dias | | 24 meses | |
| Sist. Oper. – OS390 | | 3 semanas | | 12 meses | |
| Sist. Oper. – baixa | 90 dias | | | 24 meses | |

| | |
|---|---|
| Log | |
| Squid - http | 5 semanas |
| Sist. Operacional | 100 semanas |
| Correio | 100 semanas |
| FW | |

## ANEXO V

## REGRAS PARA ACESSO VPN

A VPN *(Virtual Private Network)* é um túnel de criptografia entre pontos autorizados, criado através de redes públicas e/ou privadas, para transferência de dados de modo seguro, entre redes corporativas ou usuários remotos.

Assim, a utilização de uma rede pública para o acesso VPN justifica a adoção de medidas especiais de proteção de forma a não permitir que os dados sejam acessados ou modificados por terceiros que não tenham permissão.

A EMPREL emitirá certificados de identificação para os acessos VPN em razão da solicitação de órgão da Administração Municipal, os quais garantirão a autenticidade, integridade e não repúdio dos acessos.

Os certificados terão validade por 06 (seis) meses ou pelo prazo de duração do vínculo com a Administração Municipal, o que for menor.

Para fins deste anexo V, que faz parte integrante do Regulamento de Segurança, o TERMO DE USO VPN é instrumento específico que vincula a Administração Municipal ao usuário cujo acesso VPN está sendo concedido.

O TERMO DE RESPONSABILIDADE PARA USO DA VPN, por sua vez, é instrumento que vincula individualmente usuário a um respectivo certificado de acesso.

As informações constantes no termo de uso e do termo de responsabilidade comprovarão o vínculo e a validade da concessão, assim como identificarão os responsáveis de cada uma das partes e seus respectivos contatos.

A concessão de acesso somente ocorrerá mediante o preenchimento, pelo órgão solicitante e pelo usuário, do termo de uso e do termo de responsabilidade da seguinte forma:

a. Todos os campos de ambos os termos devem estar preenchidos com informações fidedignas;
b. O usuário e o órgão devem assinar em conjunto o termo de uso;
c. O usuário deve assinar isoladamente o termo de responsabilidade.

Cada TERMO DE USO pode ser vinculado a tantos termos de responsabilidade quantos forem necessários.

Os acessos VPN serão separados de acordo com o alvo de interesse definido no escopo do termo de uso.

A concessão atingirá a rede de teste, a rede de homologação ou serviço cujo acesso seja restrito à Intranet.

Não será concedido acesso completo à rede interna.

Serão liberados grupos de 2, 6, 14 ou 30 acessos simultâneos, para cada contrato. Esse quantitativo deve ser estabelecido na ocasião do preenchimento do termo de uso.

O desligamento do usuário do quadro da Administração Municipal implica na necessidade de emissão de um novo termo de uso assinado pelo seu substituto.

O cessionário deve informar imediatamente a EMPREL o extravio ou descredenciamento que qualquer um dos certificados sob sua responsabilidade.

A informação "IPV4" de origem, solicitada no termo de uso, trata-se de um elemento de segurança técnico e pode ser obtida com o administrador de redes do usuário.

Ao utilizar o acesso VPN, o usuário assume a responsabilidade final pelos acessos registrados por seu certificado e aceita os termos de não repúdio e autenticidade inerentes a esses certificados, que garantem a identidade e autenticidade de um agente e asseguram a integridade de origem.

O usuário poderá contatar a qualquer momento a EMPREL para esclarecer dúvidas, obter orientações e reportar situações de violação ao presente anexo e outros, através da conta de email suporte.vpn@recife.pe.gov.br.

A solicitação para criação ou renovação de certificados, para concessões em atividade, será atendida em até dois dias úteis.

Qualquer ocorrência relevante na configuração ou disponibilidade do serviço VPN, será informada por email.

Será enviado para o email informado no termo de responsabilidade, juntamente com o certificado, as orientações para uso da VPN.

## ANEXO VI

## TERMO DE USO DOS SISTEMAS INTERNOS DA "EMPRESA MUNICIPAL DE INFORMÁTICA – EMPREL" (TERMO DE CIÊNCIA DO RISI)

**CONSIDERANDO** a disponibilização, pela EMPREL, de infra-estrutura tecnológica, como ferramenta de trabalho, para que seus usuários possam exercer o pleno desenvolvimento de suas atividades;

**CONSIDERANDO** que a infra-estrutura tecnológica é de exclusiva propriedade da EMPREL, que arca com todos os custos da mesma, não havendo expectativa de privacidade no uso de tais equipamentos, tendo em vista que apenas poderão ser utilizados para fins profissionais;

**CONSIDERANDO** que a má utilização da mencionada infra-estrutura tecnológica poderá ocasionar sérios prejuízos à EMPREL;

**CONSIDERANDO** que este documento e o Regulamento de Segurança da Informação (RISI) foram objetos de consenso entre a EMPREL e a representação dos empregados (SINDPD-PE e Comissão de Funcionários da EMPREL);

**DECLARO QUE:**

1. Tenho conhecimento e acesso ao Regulamento de Segurança da Informação, que se encontra disponível na Intranet, o qual li na íntegra, tomando integral conhecimento e ciência de suas disposições;

2. Estou ciente que é realizado o monitoramento de todos os acessos e comunicações ocorridos através da infra-estrutura tecnológica da EMPREL, sendo indispensável para manter o nível de segurança desejável;

3. Tenho ciência que não devo revelar fatos ou informações sensíveis a que tenha conhecimento por força de minhas atribuições;

4. Estou ciente de que no caso de transgressão de preceitos legais e contidos no Regulamento de Segurança da Informação, responderei por minhas ações e omissões, observando os princípios constitucionais da ampla defesa e do contraditório.

Recife, _____de_____de 2009.

_____

Nome:
RG:
CPF:

## ANEXO VII

FORMULÁRIO PARA SOLICITAÇÃO DE CONTA DE REDE

Nome completo: _____

CPF: _____._____._____-__

Secretaria/órgão: _____ Complemento:_____

Matrícula: _____ Telefone:_____

Coloque um "x" se precisa acessar

- ☐ SOFIN
- ☐ TOM
- ☐ GUPTA

Nome do gerente:_____

Matr. do gerente:_____

**ANEXO VIII**

# RISI - Cancelamento de Acesso

**GGP / GSCF – Gerência de Serviços de Cadastro e Folha**

I – Nome do funcionário: _____

Mat.:_____ Lotação:_____

Período de afastamento: ☐ Temporário __/__/__ a __/__/__

☐ Definitivo

Data: __/__/__ Assinatura:_____

**Órgão de Lotação do Funcionário**

II – Informações sobre acessos

| | Sistema | Identificação |
|---|---|---|
| ☐ | Conta de rede (domínio) | _____ |
| ☐ | CICS/TSO (RACF) | _____ |
| ☐ | EMAC | _____ |
| ☐ | _____ | _____ |
| ☐ | _____ | _____ |

Declaro que as informações acima contemplam todos os acessos do funcionário aos sistemas da EMPREL

Data: __/__/_____ Assinatura do Gerente: _____

**GSB/GSSB – Gerência de Suporte a Sistemas Básicos**

Providência(s) adotada(s): _____

_____

_____

Data: __/__/__ Assinatura do Técnico: _____

Obs.: Encaminhar formulário preenchido para a GGP/GSCF

# ANEXO IX

EMPREL
EMPRESA MUNICIPAL DE INFORMÁTICA - RECIFE

## TERMO DE USO DA VPN DA EMPREL
<>-nn

**ÓRGÃO SOLICITANTE RESPONSÁVEL PELO CONTRATO NA ADM. MUNICIPAL**

| | |
|---|---|
| ÓRGÃO | |
| NOME | |
| EMAIL | |
| TELEFONE | |
| MOTIVO DA SOLICITAÇÃO | |
| DATA EXPIRAÇÃO | |

**USUÁRIO**

| | |
|---|---|
| CONTRATO | |
| RAZÃO SOCIAL | |
| CNPJ | |
| IPv4 ORIGEM | |
| NOME RESPONSÁVEL | |
| CPF RESPONSÁVEL | |
| EMAIL RESPONSÁVEL | |
| TELEFONE | |
| ENDEREÇO | |
| CONEXÕES SIMULTÂNEAS | 2, 6,14 ou 30 |
| ESCOPO DE ACESSO | |

Por este instrumento, declaram-se entendidas e aceitas as condições para uso da VPN da Emprel descritas nas Normas de Uso.

Recife, 22 de agosto de 2008

_____
<usuário>
<empresa>

_____
<responsável>
<órgão>

## ANEXO X

EMPREL
EMPRESA MUNICIPAL DE INFORMÁTICA - RECIFE

## TERMO DE RESPONSABILIDADE DA VPN

Declaro que recebi nesta data, o certificado de acesso a VPN da Emprel, identificado como: **<>.crt** que permite acesso aos serviços disponibilizados no escopo definido no Termo de Uso número: **VPN-<>** da EMPREL – Empresa Municipal de Informática.

Tenho conhecimento que o acesso às informações por meio desse certificado é de minha inteira responsabilidade.

Comprometo-me a zelar pela sua guarda e, também, a solicitar o cancelamento da senha caso ocorra qualquer alteração da representatividade legal que hoje detenho.

Comprometo-me a manter confidencialidade com relação a toda documentação e informações obtidas por meio desse acesso.

Declaro ter conhecimento:

- de que os acessos realizados são passíveis de auditoria técnica;
- de que a Diretoria da Emprel pode aprovar a investigação dos acessos

**CERT-ID** <> **VALIDADE:**

NOME _____

EMAIL _____

CPF _____

TELEFONE

| Local e Data | Declarante | Usuário Responsável pelo Termo de Uso |
|---|---|---|
| Recife, 22 de agosto de 2008 | | |