BOAS PRÁTICAS PARA SEGURANÇA DA INFORMÇÃO

EMPRESA MUNICIPAL DE INFORMÁTICA - EMPREL

RISI

REGULAMENTO INTERNO DE SEGURANÇA DA INFORMAÇÃO

Diretrizes Gerais
Versão 2.0

Palavras-chave: Segurança, Informação, Diretrizes, Regras, Normas,Risco, Continuidade, Vulnerabilidade, Incidente, ativo, Confidencialidade, Disponibilidade, Integridade, PCR.

Esse Documento é classificado como público

1. INTRODUÇÃO:

Este documento foi elaborado e visa implementar as orientações das mais atualizadas e confiáveis diretrizes de segurança mundiais, em especial aNBR 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, Lei Federal nº 13.079/2018, a Lei Geral de Proteção de Dados Pessoais (LGPD) 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 e atualização 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 comum parque tecnológico, composto da redes de dados municipal, servidores, armazanamento e também de exercer a função de provedor público de acesso à Internet através do CONECTA RECIFE.

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 comas 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, quepodem 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.

4. 4. Diretrizes Gerais

a) A aplicação desta Política de Segurança requer que seus efeitos sejam evidenciados, monitorados e controlados por um instrumento de gestão adequado :

1. Um SGSI – Sistema de Gestão da Segurança da Informação adequado com o disposto neste RISI deverá ser mantido continuamente;

2. O SGSI é o meio de controle que:

i) Evidenciará que o RISI está sendo cumprida no nível tático operacional, pelo acompanhamento das ações e monitoramento de métricas, de forma fornecer subsídios para as ações de controle;

ii). Fornecerá aos gestores as informações sobre a eficácia de suas ações, de forma manter os níveis de segurança dos ativos de informação dentro das expectativas da instituição, conforme o caso.

b) Os gestores da Emprel, de qualquer nível da sua estrutura administrativa e conforme o caso, são responsáveis por:

1. Fazer refletir de forma adequada e suficiente, em suas respectivas áreas de atuação e na forma da Lei, as diretrizes estabelecidas pelo RISI e seus documentos acessórios;
2. Usar os procedimentos técnico-administrativos adequados e cabíveis para propor e aperfeiçoar normas, procedimentos ou outros instrumentos afins, de forma a permitir o incremento da eficácia dos mesmos na aplicação deste Regulamento e suas decorrências na sua área de atuação;
3. Por identificar na sua área de competência, promovendo as ações cabíveis e adequadas em cada caso:

i). Riscos aos ativos de informação;

ii). Oportunidades de disseminar o aculturamento do elemento humano na segurança dos ativos de informação;

iii). Necessidades de implementação e oportunidades de uso adequado dos princípios doutrinários da segurança da informação na proteção dos ativos de informação;

4. Fornecer continuamente, no que lhe cabe, as informações necessárias e requeridas para alimentar o SGSI, bem como se utilizar destas para orientar suas ações futuras;
5. Usar dos meios administrativos cabíveis e adequados para reportar quaisquer informações, eventos ou situações que possam caracterizar não-conformidade com este Regulamento e suas decorrências, ou que apontem redundar em riscos não controlados para os ativos de informação;

6. Cumprir e fazer cumprir o RISI e suas decorrências.

i). Não são permitidas quaisquer atividades envolvendo direta ou indiretamente ativos de informação que ponham em risco, sem controle adequado, a informação e outros ativos da instituição, salvo explicitamente permitidas por este Regulamento, ou que tenha sido prévia e formalmente autorizada pelo setor ou gestor competente,

conforme o caso;

ii). É vedada a instalação e uso de quaisquer dispositivos, sistemas, informações ou outros recursos não autorizados, que violem propriedade intelectual ou comercial, alheios à missão da Emprel ou que infrinjam norma legal.

5. COMPROMISSO COM A SEGURANÇA DA INFORMAÇÃO

5.1 PRESSUPOSTO

A implantação e manutenção de um ambiente computacional seguro é tarefa inerente dos administradores e técnicos de TI. A segurança da REDE INTERNA DOS RECURSOS COMPUTACIONAIS da EMPREL depende da colaboração de todos os envolvidos. Portanto a responsabilidade com a Segurança da Informação não é apenas do DESI e da Gestão da Empresa, mas também dos demais colaboradres, prestadores de serviços, cargos comicionados e terceirizados.

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 de Segurança da Infromação (*Item 6*.).

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.

5.2 COMPROMISSO DA DIRETORIA

É responsabilidade da Gestão da EMPREL disponibilizar uma infra-estrutura tecnológica que oferece um nível adequado de segurança e funcionalidade para os sistemas da Administração Municipal.

5.3 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.

6. COMITÊ DE SEGURANÇA DA INFORMAÇÃO:

O COMITÊ DE SEGURANÇA DA INFORMAÇÃO é o órgão que fará toda a gestão do presente Regulamento e tal Comitê será composto pelos seguintes membros:

1. Diretor de Assuntos Jurídicos,
2. Diretor de Infraestrutura de Informática;
3. Diretor de Sistemas e Negócios Corporativos;
4. Gerente de Gestão de Pessoas;
5. Gerente de Departamentos das áreas Tecnicas e
6. Gerente de Segurança da Informação, que deve ser funcionário efetivo com domínio técnico na área e será o CISO – Chief Information Security Officer - Gestor de Segurança da Informação, representante do Comitê.

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 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 gerência de Segurança da Informação, 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 contactado 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 apreciação e deliberação acerca da implantação.

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. Todas as intervenções na infraestrutura da Rede Corporativa como, por exemplo: instalação de equipamentos, criação de ambientes virtuais, hospedagem software ou serviço de agentes externos etc. devem ser submetidas ao Comitê de Segurança da Informação para análise dos impactos e riscos.

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.

7. PROCEDIMENTOS E BOAS PRÁTICAS NA UTILIZAÇÃO DOS RECURSOS:

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, cabos de rede, backbones,), equipamentos de roteamento (roteadores), equipamentos de distribuição (switches), 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:

7.1 USUÁRIOS (CONTAS DE REDE):

Todas as senhas de acesso dos usuários aos sistemas e/ou equipamentos 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 seja descoberta 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.

7.2 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.

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 Unidade Operacional ao qual o usuário afastado pertence deverá comunicar, com antecedência, mediante o formulário constante no anexo VII, sobre o afastamento e solicitar asuspensão 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.

7.3 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.

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 a2 (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.*

7.4 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.

7.5 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 sofrerrestrições 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.

7.6 RECEBIMENTO, INSERÇÃO e ENVIO DE ARQUIVOS

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 DAINFORMAÇÃO.

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

7.7 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.

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.

7.8 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.

O uso de quaisquer equipamentos que não sejam de propriedade da EMPREL para conexão na rede interna, especialmente os notebooks particulares, devem está em conformidade com as determinadções do COMITÊ DE SEGURANÇA DA INFORMAÇÃO (ANEXO VIII) para que não comprometam 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 competênte para esse fim na Emprel , com o conhecimento do usuário ou da chefia imediata.

7.9 EQUIPAMENTOS PORTÁTEIS:

Os equipamentos portáteis, tais como, notebooks e smartphones, somente poderão ser utilizados pelos usuários para as atividades da EMPREL se estiverem de acordo com a conformidade definida pelo COMITÊ DE SEGURANÇA DA INFORMAÇÃO (ANEXO VIII), em caso contrário terão acesso exclusivamente a Internet em rede própria definida pela Emprel sem acesso a intranet.

7.10 ACESSO REMOTO VIA VPN (Virtual Private Network)

As regras de acesso remoto via VPN aos sistemas da EMPREL são determinadas no anexo IV 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, 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.

7.11 PROCEDIMENTOS DE USO DE REDES EXTERNAS (INTERNET E OUTRAS):

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. A transferência de arquivos via FTP, quando imprescindível, será autenticada;
f. Dispositivos de controle e segurança deverão ser utilizados, para garantir a confidencialidade e a integridade das informações em tráfego por estas redes;
g. As conexões deverão ocorrer exclusivamente através de acesso autenticado.

7.12 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; 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 eaos bons costumes. Ocorrendo o recebimento involuntário de email deverá ser comunicado ao COMITÊ DE SEGURANÇA DA INFORMAÇÃO;

c) 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.

7.13 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.

7.14 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:

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 específicae 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 CódigoPenal Brasileiro, bem como todas as demais leis e disposições cabíveis, inclusive no que toca aos servidores da Administração Pública.

8.1 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.

8.2 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 service desk, através do ramal 7156.

8.3 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.

8.4 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 01 (um) ano cosoante ao Marco Civil da Internet (Lei n.º 12.965/2014). 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 recomendaçãoà 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 COMITÊDE 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 90 (noventa) 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 08 (oito) 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	30 GB
Tamanho máximo de email	25 MB
Extensões de arquivos que requerem muita cautela	.exe, .com, .scr., .BAT
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:

I. Sistemas Operacionais

- ✓ Servidores de Produção

  a) Linux: Red Hat; CentOS;
  b) Windows SERVER.

- ✓ Servidores de Homologação

  a) Linux: Red Hat; CentOS;
  b) Windows SERVER.

- ✓ Servidores de Desenvolvimento Corporativo (Testes)

  a) Linux: Red Hat; CentOS;
  b) Windows SERVER.

- ✓ Estações de trabalho

  a) Linux - Ubuntu;
  b) Windows.

- ✓ Dispositivos móveis

  a) IOS;
  b) Android;
  c) Windows Mobile.

II. Virtualização de Servidores

a) Vmware;
b) Oracle VM e Oracle Linux, para servidores que hospedam o banco Oracle.

III. SGBD – Sistema Gerenciador de Banco de Dados

a) PostgreSql;
b) Oracle 12C Enterprise Edition;
c) DB2 10.5 Advanced Entreprise Server Edition.

Para soluções adquiridas (pacotes) que tenham o MySql como SGBD integrado, e sendo soluções baseadas na licença GPL do software Livre, este também poderá ser admitido na versão do pacote.

IV. Servidor de Aplicação

O servidor de aplicação padrão para os ambientes da Emprel será o **JBOSS**.

V. Servidor Web

O servidor web padrão para todos os ambientes é o **APACHE**.

VI. Linguagens de Desenvolvimento

As linguagens padrões para desenvolvimento de sistemas são as seguintes:

a) **Java,** como linguagem preferencial;
b) **PHP**, como linguagem secundária;
c) **HTML** (HiperText Markup Language),

- Javascript, versão mais atual suportada pelo cliente (browser) alvo do sistema;
- CSS, para a camada de apresentação das aplicações para a Web.

VII. Ambiente Integrado de Desenvolvimento e Teste Java (IDE)

O ambiente integrado de desenvolvimento, manutenção e teste de sistemas em Java é o **Eclipse**.

VIII. Ferramenta de BI – Business Inteligence

As ferramentas para a construção de Data Warehouses ou Data Marts são o **Qlikview** e o **Pentaho**.

IX. Ferramentas de Geoprocessamento

a) Família ArcGis;
b) Quantum Gis (QGis);
c) OpenJump;
d) MapServer (Servidor de Mapas);
e) PostGis (Banco Espacial).

X. Ferramenta de Automação de Escritório

A ferramenta de Automação de Escritório padrão é o **WPS**.

XI. Software de Controle de Versões

O **SVN** é a ferramenta padrão de controle de versões da Emprel, onde todos os artefatos (documentos e código) gerados em projetos de desenvolvimento e manutenção de sistemas deverão ser controlados.

XII. Software de Script Batch

O **Ant** e o **Maven** são as ferramentas padrões de geração e execução de scripts batch.

XIII. Software de Controle de Bugs e Mudanças

O **Redmine** é a ferramenta de Controle de Bugs e Mudanças.

XIV. Software para Modelagem de Sistemas e Dados

a) O **StarUML** é a ferramenta padrão para modelagem UML (Unified Modeling Language) de sistemas na Emprel.
b) O **SQL Power Architect** é a ferramenta de modelagem de dados padrão.

XV. Software de Testes de Unidade

O **JUnit** ou superior é o software a ser utilizado para a realização de testes de unidade em Java.

XVI. Software de Testes de Funcionalidade

O software padrão para a execução dos testes de funcionalidade é o **Selenium**.

XVII. Software de Testes de Performance, Carga e Stress

O software padrão para a realização de testes de performance, carga e stress é o **JMeter**.

XVIII. Software para Integração Contínua

O **Jenkins** é o software padrão utilizado na coordenação da integração contínua.

XIX. Ferramenta de Modelagem de Processos de Negócio

O software de modelagem de negócio é o **Bizagi** e o software de automatização de processos de negócio é o **Ágiles**.

XX. Ambiente de Desenvolvimento de Aplicações Móveis

O ambiente de desenvolvimento e manutenção de aplicações móveis é o **Titanium**.

XXI. Ferramenta para verificação de padrões e correção de código HTML

A ferramenta **HTML TIDY**, versão mais recente disponível em http://tidy.sourceforge.net, é a ferramenta padrão de validação e correção de código HTML Ela possibilita a correção e a arrumação, em um layout mais estruturado, de códigos HTML.

XXII. Ferramenta de validação de código fonte Java

A ferramenta de validação de código fonte na linguagem Java é o **Sonar**.

XXIII. Protocolo para Transferência de Dados entre aplicativos

O protocolo padrão para troca de dados entre sistemas é o **XML**. O XML também é largamente utilizado por diversos softwares nas suas configurações, além de ser utilizado pelos browsers e SGBDs.

XXIV. Ferramenta de Gerenciamento de Conteúdo

A ferramenta padrão para a criação de sites e de portais é o **Drupal**, que deverá ser executado tendo como infraestrutura o **Apache**, o **PHP**, o **PostFix**, e o **MySQL**.

XXV. Framework Para Desenvolvimento Web

O framework para desenvolvimento de sistemas Web em Java, pela Emprel ou por terceiros, deverá ser o **EWF – Emprel Web Framework**.
O EWF utiliza os seguintes componentes:

a) **Java Server Faces (JSF)** – Framework MVC para a construção de interfaces do usuário baseadas em componentes para aplicações Web;
b) **Spring** – Utilizado para a instanciação das classes das aplicações Java e definição das dependências entre elas através de arquivo configurações em XML;
c) **Hibernate** – Framework de mapeamento objeto-relacional;
d) **Maven** – Ferramenta de automação de builds; e,
e) **Log4j** – Fornece API para o log de dados na aplicação.

XXVI. Componentes Java

a) **JEP 1.0** – Avaliador de fórmulas matemáticas;
b) **iReport 5.6.0 ou superior** – Geração de relatórios. Os relatórios devem ser gerados no formato PDF e/ou HTML;
c) **Acme 1.0** – Gerador de imagens GIF; e,
d) **Log4j** 2 ou superior – Geração de log.

XXVII. Ferramenta de manipulação de banco de dados

O **Squirrel** é a ferramenta padrão para manipulação dos bancos de dados em ambientes de desenvolvimento.

XXVIII. Ferramenta de Elaboração de Cronogramas de Projetos

A ferramenta para planejamento e gerenciamento de projetos é o **ProjectLibre**, disponível em www.projectlibre.org.

XXIX. Ferramenta Servidora de E-mail (SMTP)

A ferramenta servidora de e-mails é o **PostFix**.

XXX. Ferramenta de DNS

A ferramenta para controle de domínios é o **BIND**.

ANEXO IV

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 IV, que faz parte integrante do Regulamento de Segurança, o TERMO DE USO VPN é um instrumento para efetivar o vínculo entre a Emprel e a Empresa contratada, nos projetos da Administração Municipal, através da VPN..

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 ou pela Chefia imediata do colaborador da PCR quando estiver submetido ao regime de Home office 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 da PCR e a sua Chefia imédiata devem assinar em conjunto o termo de uso
d. 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 até 60 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.

MODELOS DOS TERMOS

TERMO RESPONSABILIDADE

Declaro que recebi nesta data o **Certificado de Acesso à VPN da EMPREL**, identificado como " **xxxxxxxxx.crt** ", que permite acesso aos serviços disponibilizados no escopo definido no Termo de Uso, **xxxxxxxxxxxxxxxxxxx** – Empresa Municipal de Informática.

Tenho conhecimento que o acesso às informações, por meio desse Certificado é da minha inteira responsabilidade, cuja utilização deverá ser associada ao equipamento disponibilizado pela(o) xxxxxxxx para esta finalidade.
Comprometo-me a zelar pela guarda e, também, solicitar o cancelamento da senha, caso ocorra qualquer alteração da responsabilidade legal, que hoje detenho.
Comprometo-me a manter confidencialidade com relação a toda documentação e informações, obtidas por meio do acesso concedido.

Declaro ter conhecimento de que os acessos realizados através do certificado que detenho são passíveis de auditoria técnica; que a Diretoria da EMPREL pode aprovar a investigação dos acessos realizados, bem como do que dispõem as Leis: 17.866/2013 da Prefeitura do Recife, abaixo transcrito:

> "art. 23 – Constituem condutas ilícitas que ensejam responsabilidade do agente público municipal:
> (...)
> II – Utilizar indevidamente, bem como subtrair, destruir, inutilizar, desfigurar, alterar ou ocultar, total ou parcialmente, informações que se encontre sob sua guarda ou a que tenha acesso ou conhecimento em razão do exercício das atribuições de cargo, emprego ou função pública;
> III – Agir com dolo ou má-fé na análise das solicitações de acesso à informação;
> IV – divulgar ou permitir a divulgação ou acessar ou permitir acesso indevido à informação sigilosa ou informação pessoal;(...)"

CERT-ID: xxxxxxxxxx.crt **VALIDADE: xx/xx/xxxx**
NOME: xxxxxxxxxxxxxxxx
Email: xxxxxxxxxxxxxxxxxxxxxxx
CPF: xxxxxxxxxxxxxxxxxxxx
Telefone(s): ( )

Local e Data:_____

Assinatura:_____
< usuário >

Assinatura:_____
< responsável pela solicitação >

TERMO DE USO DA VPN DA EMPREL
Empresa xxxxxx

ÓRGÃO SOLICITANTE RESPONSÁVEL PELO CONTRATO NA ADM. MUNICIPAL

ÓRGÃO	
NOME	
EMAIL	
TELEFONE	
MOTIVO DA SOLICITAÇÃO	
DATA EXPIRAÇÃO	

Se o órgão solicitante não for a EMPREL, informar no quadro abaixo os dados do responsável na Emprel pela presente solicitação

NOME		
EMAIL		
TELEFONE		
		ASSINATURA

USUÁRIO

CONTRATO	
RAZÃO SOCIAL	
CNPJ	
IPv4 ORIGEM	
NOME RESPONSÁVEL	
CPF RESPONSÁVEL	
EMAIL RESPONSÁVEL	
TELEFONE	
ENDEREÇO	
CONEXÕES SIMULTÂNEAS	
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, de de 20XX.

_____ _____

<usuário> <responsável>
<empresa> <órgão>

ANEXO V

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 princípiosconstitucionais da ampla defesa e do contraditório.

Recife,_____de_____de 20xx.

_____

Nome:
RG:
CPF:

ANEXO VI

FORMULÁRIO PARA SOLICITAÇÃO DE CONTA DE REDE

Nome completo: _____

CPF:_____._____._____-___

Secretaria/órgão:_____Complemento:_____

Matrícula:_____ Qual os serviços: Telefone que o solicita _____

Descreva os serviços que o usuário terá acesso

_____

_____

_____

_____

Nome do gerente:_____

Matr. do gerente:_____

ANEXO VII

RISI - Cancelamento de Acesso

DEGP/UOFC – Unidade Operacional de Folha,Carreira e Cadastro

I – Nome do funcionário:_____

Mat.: Lotação:

Período de afastamento: ☐ Temporário

Data: / / ☐ Definitivo

Assinatura:

Obs.: Encaminhar formulário preenchido para a GGP/GSCF

Órgão de Lotação do Funcionário

II – Informações sobre acessos

Quais Sistemas / Serviços

_____ _____

_____ _____

_____ _____

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

Data: / / Assinatura do Gerente:

DEOS /UOSB – Unidade Operacional de Suporte a Sistemas Básicos

Providência(s) adotada(s):

Data: / / Assinatura do Técnico:

ANEXO VIII

CRITÉRIOS QUANTO A CONFORMIDADE PARA ACESSO A REDE CORPORATICA

- Usuário deve possuir Login da Rede Corporativa;
- Sistema Operacional Atualizado;
- Softwares homolgados pela Emprel com licenças válidas;
- O Antivírus corporativo deve está instalado e atualizado.