BOAS PRÁTICAS PARA SEGURANÇA DA INFORMAÇÃO DA EMPRESA MUNICIPAL DE INFORMÁTICA - EMPREL

RISI
REGULAMENTO INTERNO DE SEGURANÇA DA INFORMAÇÃO

Diretrizes Gerais
Versão 2.6

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

Esse Documento é classificado como público.

Emprel - Empresa Municipal de Informática
Rua do Brum, 123|Empr. Maurício Brandão Mattos - 2º andar
Bairro do Recife - Recife/PE | 50030-260
(81) 3355.7000 | www.Emprel.gov.br

Emprel - Empresa Municipal de Informática
Rua do Brum, 123|Empr. Maurício Brandão Mattos - 2º andar
Bairro do Recife - Recife/PE | 50030-260
(81) 3355.7000 | www.Emprel.gov.br

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 27001, NBR ISO IEC 27002, 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 Infraestrutura de Informática para o município, e para tanto, conta com um parque tecnológico, composto das redes de dados municipal, servidores, armazenamento 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 infraestrutura tecnológica da EMPREL, de acordo com princípios éticos e legais. A utilização de dados, informações e recursos operacionais e de comunicações da EMPREL, tais como: e-mail, acesso à Internet, mídias sociais, computação em nuvem, dentre outros, deve estar em consonância com esta política e com as normas e padrões da Empresa.

São também objetivos deste documento:

a) Padronizar as atividades de segurança para o uso e administração dos recursos da Infraestrutura 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 os termos:

AUTENCIDADE	Propriedade pela qual se assegura que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, equipamento, sistema, órgão ou entidade;
CONFIDENCIALIDADE	Propriedade pela qual se restringi o acesso às informações, garantindo que ela só esteja disponível apenas às pessoas autorizadas;

Emprel - Empresa Municipal de Informática
Rua do Brum, 123|Empr. Maurício Brandão Mattos - 2º andar
Bairro do Recife - Recife/PE | 50030-260
(81) 3355.7000 | www.Emprel.gov.br

CONTA DE REDE	Identificação do usuário que permite o acesso aos recursos computacionais da rede corporativa, tais como, correio eletrônico, acesso à Internet e às informações da EMPREL;
DISPONIBILIDADE	Propriedade pela qual se assegura que às informações ficarão acessíveis sempre que necessário, sem interrupções, podendo ser acessados por qualquer pessoa ou processoautorizado quando for preciso;
GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO	Processo de natureza permanente, estabelecido, direcionado e monitorado pela alta administração, que contempla as atividades de identificação, avaliação e gerenciamento de potenciais eventos que possam afetar a organização, destinado a fornecer segurança razoável quanto à realização de seus objetivos;
GESTÃO DE SEGURANÇA DA INFORMAÇÃO	Processo que visa integrar atividades de gestão de riscos, gestão de continuidade do negócio, tratamento de incidentes, tratamento da informação, conformidade, credenciamento, segurança cibernética, segurança física, segurança lógica, segurança orgânica e organizacional, aos processos institucionais estratégicos, operacionais e táticos, não se limitando, portanto, à tecnologia da informação;
INFORMAÇÃO	Patrimônio da EMPREL, consistente nas suas informações, que podem ser de caráter comercial, estratégico, técnico, financeiro, mercadológico, legal, de recursos humanos, ou dequalquer outra natureza, não importando se protegidas ou não de confidencialidade, desde que se encontrem armazenadas e/ou trafegadas na infraestrutura tecnológica da EMPREL ou na rede corporativa;
INTEGRIDADE	Propriedade pela qual se assegura que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;
LOG	Registro de eventos relevantes em um dispositivo ou sistema computacional.
SEGURANÇA CIBERNÉTICA	Ações voltadas para a segurança de operações, visando garantir que os sistemas de informação sejam capazes de resistir a eventos no espaço cibernético, capazes de comprometer a disponibilidade, a integridade, a confidencialidade e a autenticidade dos dados armazenados, processados ou transmitidos e

Emprel - Empresa Municipal de Informática
Rua do Brum, 123|Empr. Maurício Brandão Mattos - 2º andar
Bairro do Recife - Recife/PE | 50030-260
(81) 3355.7000 | www.Emprel.gov.br

	dos serviços que esses sistemas ofereçam ou tornem acessíveis;
SEGURANÇA DA INFORMAÇÃO	Adoção de medidas eficazes para resguardar que as informações da EMPREL sejam conhecidas somente por aqueles que devem conhecê-las, evitando seu uso indevido, inadequado, ilegal, ou em desconformidade com este Regulamentode Segurança.
SEGURANÇA FÍSICA	Forma de proteger equipamentos e informações contra usuários que não possuem autorização para acessá-los;
SEGURANÇA LÓGICA	Conjunto de recursos executados para proteger o sistema, dados e programas contra tentativas de acessos de pessoas ou programas desconhecidos;
SEGURANÇA ORGÂNICA	Toda ação, cautelas e medidas de proteção adotadas por uma organização, é um modelo de segurança baseado na prevenção e no uso de recursos próprios da empresa ou organização, como treinamento de funcionários, investimentos em tecnologias de segurança, controle de acesso e gestão de riscos;
SEGURANÇA ORGANIZACIONAL	Esforço pautado por ações que objetivam mitigar riscos e garantir a continuidade das operações;
REDE INTERNA	Conjunto de computadores, equipamentos de rede e infraestrutura, bem como, os servidores com os aplicativos e bancos de dados corporativos;
USUÁRIOS	Colaboradores 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;

4. Diretrizes Gerais

a) A aplicação deste Regulamento Interno 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 cumprido no nível tático operacional, pelo acompanhamento das ações e monitoramento de métricas, de forma

Emprel - Empresa Municipal de Informática
Rua do Brum, 123|Empr. Maurício Brandão Mattos - 2º andar
Bairro do Recife - Recife/PE | 50030-260
(81) 3355.7000 | www.Emprel.gov.br

a fornecer subsídios para as ações de controle;

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

b) Os gestores da EMPREL, de qualquer nível da sua estrutura administrativa e conforme ocaso, 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. 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.

7. 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 setorou gestor competente, conforme o caso;

8. 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 Departamento de Segurança da Informação - DESI e da Gestão da Empresa, mas também dos demais colaboradores, prestadores de serviços, cargos comissionados e terceirizados.

Emprel - Empresa Municipal de Informática
Rua do Brum, 123|Empr. Maurício Brandão Mattos - 2º andar
Bairro do Recife - Recife/PE | 50030-260
(81) 3355.7000 | www.Emprel.gov.br

A segurança da informação abrange processos, procedimentos, serviços e ações que visam assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade dos dados e das informações, da EMPREL ou sob sua guarda, incluindo a segurança cibernética, contemplando ações voltadas para a segurança de operações, bem como a proteção de dados pessoais.

A segurança da informação está alinhada ao planejamento estratégico da EMPREL, visando fomentar e viabilizar novos negócios e a evolução tecnológica de soluções íntegras e confiáveis.

Assegurar a adequação e a evolução das soluções de segurança para atender as necessidades dos clientes, os requisitos do negócio, legais e contratuais, assim como a inovação em soluções digitais.

Garantir condições para que os colaboradores sejam orientados sobre a existência e a utilização dos instrumentos normativos, procedimentos e controles de segurança adotados pela empresa.

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 Informação (*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, utilizaram ou utilizarão, sua infraestrutura tecnológica.

5.2 COMPROMISSO DA DIRETORIA

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

Os sistemas não desenvolvidos pela EMPREL para serem hospedados terão de ter uma análise da equipe técnica da EMPREL.

5.3 COMPROMISSO DOS USUÁRIOS

É responsabilidade dos usuários respeitar todas as disposições do RISI, bem como, colaborar com alertas, sugestões e críticas que possam melhorar a segurança da informação, devendo todos os usuários darem ciência do mesmo através do **TERMO DE CIÊNCIA DO RISI** (ANEXO IV).

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 Presidente;
2. Assessor Jurídico;
3. Diretor de Infraestrutura de Informática;
4. Diretor de Sistemas Financeiros Tributários;
5. Diretor de Transformação Digital;
6. Diretor de Inovação Aberta e Governança de Dados;
7. Gerente de Segurança da Informação, que deve ser funcionário efetivo com domínio

Emprel - Empresa Municipal de Informática
Rua do Brum, 123|Empr. Maurício Brandão Mattos - 2º andar
Bairro do Recife - Recife/PE | 50030-260
(81) 3355.7000 | www.Emprel.gov.br

técnico na área e será o CISO – *Chief Information Security Officer* - Gestor deSegurança da Informação.

O Diretor Presidente, ou sua indicação, é o representante do Comitê de Segurança da informação.

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 aopresente 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, para 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 omissãoou 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 *e-mail*: 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 sua implementação. 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 infraestrutura 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.

Os dados, informações e ativos de informação da EMPREL, ou sob sua guarda, de acordo com natureza, classificação, sensibilidade e exposição a riscos de segurança da informação, devem ser protegidos de forma a garantir a confidencialidade, a integridade, a disponibilidade e a autenticidade, em alinhamento com as necessidades do negócio, requisitos legais, regulamentares, estatutários e contratuais.

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,

Emprel - Empresa Municipal de Informática
Rua do Brum, 123|Empr. Maurício Brandão Mattos - 2º andar
Bairro do Recife - Recife/PE | 50030-260
(81) 3355.7000 | www.Emprel.gov.br

firewalls, proxies, impressoras, *scanners*, *smartphones*, IoT ou qualquer outro equipamento pertencente à infraestrutura tecnológica da EMPREL.

Sendo assim, e a partir desse entendimento, são definidas as seguintes regras:

7.1 USUÁRIOS (CONTAS DE REDE):

Caso o usuário não possua sua conta de rede, caberá ao gerente da área onde o mesmo estiver lotado solicitar a criação da sua conta através de formulário próprio (Anexo V).

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 infraestrutura 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, não estando o mesmo em gozo de férias, licença prêmio ou licença maternidade, ocasião em que esta será bloqueada pelo Departamento de Operação e Suporte- DEOS da Diretoria de Infraestrutura de Informática - DII.

A Diretoria Administrativa e Financeira deve informar à área de Infraestrutura 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 (Anexo VI)

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, Decreto Lei nº 2.848 de 07 de dezembro de 1940:

> *Art 325 - 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.*

7.3 USO E CONTROLE DE INFORMAÇÕES, DADOS E ARQUIVOS:

Todos os documentos eletrônicos, dados e informações da atividade laborativa dos usuários deve estar centralizados em um Servidor, em diretório específico para cada usuário, paraarquivos 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 indevidas 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 resultar dano para a Administração Pública ou para o administrado.*

7.4 DIREITOS DE ACESSO A ARQUIVOS E DIRETÓRIOS:

O acesso às informações armazenadas na infraestrutura 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.

Emprel - Empresa Municipal de Informática
Rua do Brum, 123|Empr. Maurício Brandão Mattos - 2º andar
Bairro do Recife - Recife/PE | 50030-260
(81) 3355.7000 | www.Emprel.gov.br

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 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 quaisquer arquivos que violem direitos de terceiros, ou que possam causar prejuízos, a terceiros e/ou à EMPREL;
c) 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;
d) Não será permitida a prática de qualquer ato que configure concorrência desleal ou quebra de sigilo profissional;
e) 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), Lei nº 13.709/18 (Lei Geral de Proteção de Dados Pessoais - LGPD).

As regras para uso de e-mail aplicável a todos os perfis constam do anexo II deste Regulamento. Caso seja necessário o compartilhamento de arquivos confidenciais, deverá o usuário lançar o arquivo em área compartilhada do servidor permitindo o acesso apenas para quem tem o direito de fazê-lo respeitando o princípio da confidencialidade.

7.7 *SOFTWARES*:

Todos os *Softwares* utilizados na EMPREL devem ser licenciados.

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* homologados pela EMPREL constam no Padrão Tecnológico de Referência - PTR disponível para consulta no Portal da EMPREL (https://www.Emprel.gov.br/padrao-tecnologico-de-referencia-versao-20).

Só poderão ser hospedados na EMPREL *softwares* desenvolvidos baseados no Padrão Tecnológico de Referência - PTR, ou expressamente autorizada pelo gestor maior do órgão de acordo com o Anexo (VIII);

7.8 *HARDWARES*:

a. 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 EMPREL,

Emprel - Empresa Municipal de Informática
Rua do Brum, 123|Empr. Maurício Brandão Mattos - 2º andar
Bairro do Recife - Recife/PE | 50030-260
(81) 3355.7000 | www.Emprel.gov.br

é proibido;

b. 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 determinações do anexo VII para que não comprometam a Segurança da Informação;
c. A alteração de qualquer periférico ou componente nos computadores não é permitida, ficando vedada aos usuários. A realização de qualquer modificação ou manutençãodeverá sempre ser realizada pela área competente para esse fim na EMPREL, com o conhecimento do usuário ou da chefia imediata;
d. A desconexão (l*og off*) da rede deverá ser efetuada nos casos em que o usuário não for mais utilizar o equipamento ou venha a ausentar-se por um período;
e. O bloqueio de tela protegido por senha deverá ser ativado sempre que o usuário se afastar do computador de mesa ou móvel que esteja utilizando;

f. Computadores de mesa (*desktops*) ou móveis (*notebooks*) devem ser desligados no final do expediente ou sempre que um usuário estiver ausente por um período prolongado, excetuando-se quando existir uma justificativa plausível em virtude de atividades de trabalho;
g. Ao final do contrato de trabalho, os equipamentos disponibilizados para a execução de atividades profissionais devem ser devolvidos em estado de conservação adequado quando no desligamento ou término da relação do usuário com a EMPREL;
h. Qualquer dano aos equipamentos da EMPREL será devidamente analisado pela área de tecnologia da informação. Havendo a constatação de que tal dano decorreu de ação direta ou omissão do usuário, caberá a EMPREL exercer seu direito de reparação ao prejuízo, através da tomada das medidas cabíveis.

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 no anexo VII, em caso contrário terão acesso exclusivamente a Internet em rede própria definida pela EMPREL sem acesso a *intranet.*

7.10 DISPOSITIVOS DE ARMAZENAMENTO REMOVÍVEL

a) A EMPREL poderá, a seu critério exclusivo, fornecer a seus usuários dispositivos móveis ou com capacidade de armazenamento removível para execução de atividades profissionais, devendo ser observadas além das diretrizes acima, as seguintes:

- ✓ O usuário é o responsável direto pela segurança física e lógica dos dispositivos móveis sob sua guarda. Portanto, os mesmos não devem ficar fora de seu alcance em locais públicos onde haja acesso não controlado de pessoas;

- ✓ Durante o deslocamento o usuário deverá estar alerta e ter uma conduta discreta, dando preferência para compartimentos de armazenamento resistentes e não chamativos e nunca deixando o dispositivo móvel desacompanhado em veículos; e

- ✓ Em caso de perda ou furto de um dispositivo de armazenamento removível, o usuário deve comunicar imediatamente a EMPREL para que possam ser tomadas as medidas cabíveis.

7.11 ARMAZENAMENTO REMOTO (NUVEM)

a) A EMPREL disponibiliza para seus usuários espaço para armazenamento remoto de

Emprel - Empresa Municipal de Informática
Rua do Brum, 123|Empr. Maurício Brandão Mattos - 2º andar
Bairro do Recife - Recife/PE | 50030-260
(81) 3355.7000 | www.Emprel.gov.br

arquivos na nuvem, através de sua solução corporativa;

b) Não é permitido o uso de qualquer outra solução de armazenamento na nuvem, que não seja a oficialmente adotada pela empresa e homologada pela equipe de segurança da informação da EMPREL.

7.12 SEGURANÇA FÍSICA

a) As instalações de processamento das informações da EMPREL serão mantidas em áreas seguras, cujo perímetro é fisicamente isolado contra o acesso não autorizado, os danos e quaisquer interferências de origem humana ou natural.

b) O usuário deve observar as seguintes disposições específicas quanto à segurança física:

- ✓ Crachás de identificação, inclusive temporários, são pessoais e intransferíveis. Sob nenhuma circunstância será permitido o seu compartilhamento;
- ✓ Nas dependências da EMPREL os colaboradores devem portar crachás de identificação que exibam claramente seu nome e fotografia. Terceiros autorizados devem portar crachás temporários identificando claramente que os mesmos não são colaboradores da EMPREL;
- ✓ Excetuando-se quando formalmente autorizado, terceiros nunca devem ser deixados sozinhos em áreas sensíveis;
- ✓ É proibida qualquer tentativa de se obter ou permitir o acesso a indivíduos não autorizado a áreas sensíveis da EMPREL;
- ✓ É resguardado a EMPREL o direito de inspecionar malas, maletas, mochilas e similares, assim como quaisquer equipamentos, incluindo dispositivos móveis, antes de permitir a entrada ou saída de colaboradores ou terceiros de áreas sensíveis;
- ✓ É resguardado a EMPREL o direito de monitorar seus ambientes físicos. Para isso será utilizado sistema de circuito fechado de televisão em áreas comuns. As imagens obtidas serão armazenadas e protegidas contra qualquer tipo de manipulação indevida;
- ✓ Os documentos classificados como internos ou confidenciais, após manuseados, não deverão ser deixados expostos em cima de mesas, assim, ao se ausentar cabe usuário o dever de mantê-los guardados ou descartá-los de acordo com os procedimentos determinados pela EMPREL;
- ✓ Não é permitido consumir qualquer tipo de alimento, bebida ou fumar em áreas apontadas como sensíveis.

7.13 ACESSO REMOTO VIA VPN (*Virtual Private Network*)

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

7.14 PROCEDIMENTOS DE USO DE REDES EXTERNAS (*INTERNET* E OUTRAS):

A navegação a sites não relacionados diretamente à atividade laborativa do usuário, não éproibida,

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, misoginia, etc);
   - Violação de direito autoral (pirataria, etc.);
   - Áudio e Vídeo, salvo com conteúdo relacionado, diretamente, a 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;
d. A transferência de arquivos via FTP, quando imprescindível, será autenticada;
e. Dispositivos de controle e segurança deverão ser utilizados, para garantir a confidencialidade e a integridade das informações em tráfego por estas redes;
f. As conexões deverão ocorrer exclusivamente através de acesso autenticado.

7.15 MENSAGENS ELETRÔNICAS (*E-MAIL*):

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

O formato dos *e-mails* disponibilizados aos usuários será o seguinte: nome.sobrenome@recife.pe.gov.br.

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

Nome Completo
EMPREL - EMPRESA MUNICIPAL DE INFORMATICA
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*

Emprel - Empresa Municipal de Informática
Rua do Brum, 123|Empr. Maurício Brandão Mattos - 2º andar
Bairro do Recife - Recife/PE | 50030-260
(81) 3355.7000 | www.Emprel.gov.br

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 *e-mail*:

a) A conta de e-mail 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 omonitoramento dos e-mails enviados e recebidos pelos usuários, através do e-mail corporativo.

b) Fica proibida a inscrição do e-mail 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 todos e quaisquer tipo de correntes, circulares, propagandas, boatos, conteúdos impróprios ou pornográficos e afins, ou, ainda, qualquer tipo de mensagem que possa prejudicar o trabalho de terceiros, causar excessivo tráfego na rede ou sobrecarregar a infraestrutura tecnológica;

c) Os usuários serão responsáveis pelo uso inadequado de sua conta de e-mail, 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;

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 e-mail corporativo será assinado digitalmente, assegurando não repúdio.

O usuário fica ciente da inexistência de expectativa de privacidade na utilização da conta de *e-mail* corporativo e na sua navegação em sites da Internet, através da infraestrutura 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 infraestrutura 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 e-mail, bem como dos sites navegados na Internet são exercidos pela utilização da infraestrutura 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 e-mail corporativo poderão ser compartilhadas e/ou redirecionadas para outro *e-mail*, sem necessidade de qualquer aviso prévio e sem conhecimento do emissor e do receptor da mensagem, não havendo expectativa deprivacidade dos usuários, visando a identificação de eventual conduta em desacordo com este Regulamento ou com

Emprel - Empresa Municipal de Informática
Rua do Brum, 123|Empr. Maurício Brandão Mattos - 2º andar
Bairro do Recife - Recife/PE | 50030-260
(81) 3355.7000 | www.Emprel.gov.br

a legislação vigente.

A EMPREL se reserva o direito de, sem qualquer notificação ou aviso ao usuário, recusar o envio ourecebimento 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, pela EMPREL, das caixas de *e-mail*. As contas de e-mail serão vinculadas a um único usuário, sendo de exclusiva responsabilidade desta qualquer ocorrência relacionada à conta.

7.16 SUSPENSÃO DA CONTA DE E-MAIL:

A critério da EMPREL, esta poderá, a qualquer momento, e sem prévio aviso, suspender, pelo período que julgar necessário, a conta de e-mail 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.

7.17 ACESSO A CONTAS DE E-MAIL PARTICULAR (WEBMAIL):

Caso o usuário tenha seu acesso a sites de e-mail gratuitos ou pagos, que disponibilizem o envio e recebimento de e-mails 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 e-mails pessoais acessados através da infraestrutura tecnológica da EMPREL, serão, via de regra, realizados através da conexão à Internet pertenceteà mesma e, considerando que o endereço IP (Internet Protocol) de tais conexões será vinculadoà Empresa, a utilização de e-mails 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 e-mail 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 oficiais, dados ou arquivos relacionados, direta ou indiretamente, aos interesses da EMPREL via e-mail pessoal.

8. NORMAS E PROCEDIMENTOS GERAIS:

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

- ✓ 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;
- ✓ 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;

Emprel - Empresa Municipal de Informática
Rua do Brum, 123|Empr. Maurício Brandão Mattos - 2º andar
Bairro do Recife - Recife/PE | 50030-260
(81) 3355.7000 | www.Emprel.gov.br

- ✓ As instalações da EMPREL devem ser protegidas contra acessos não autorizados, danos e interferência nos recursos de tratamento de dados;
- ✓ Equipamentos, materiais e documentos da EMPREL ou sob sua guarda devem estar protegidos contra perda, danos, roubo ou comprometimento, bem como a interrupção das operações, tanto em trabalho remoto ou em trânsito.

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 a EMPREL 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.

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 infraestrutura tecnológica da EMPREL, que deve assegurar processos eficientes para gerir o ciclo de vida dos registros de eventos (logs) em ativos de informação, garantindo o adequado tratamento e monitoramento em conformidade com os requisitos de segurança e proteção dos dados, a fim de prover a rastreabilidade.

Serão registradas para eventual fim judicial, além de análise ou auditoria, por um período de 01 (um) ano consoante 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.

8.5 RESPOSTA A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

8.5.1 Incidentes de segurança da informação

a) Todas as ocorrências que possam vir a ter impacto negativo sobre a confidencialidade, integridade ou disponibilidade dos ativos/serviços de informação ou recursos computacionais da EMPREL serão caracterizadas como um incidente de segurança da informação, devendo as referidas ocorrências serem tratadas de maneira a minimizar qualquer tipo de impacto e recuperar as características de segurança da informação dos itens afetados;
b) Incidentes de segurança devem ser priorizados com base na criticidade dos ativos/serviços de informação ou recursos computacionais afetados, combinada com a estimativa de impacto prevista;
c) Todos os incidentes de segurança da informação ou suspeitas de incidentes de segurança da informação devem ser imediatamente comunicados ao DESI - Departamento de segurança da informação;
d) O DESI deverá determinar a criticidade do incidente e, quando pertinente, comunicar as partes interessadas como, por exemplo, membros do COMITÊ DE SEGURANÇA DA INFORMAÇÃO;
e) Na ocorrência de um incidente de segurança da informação, ativos/serviços de informação ou recursos computacionais com suspeita de ter sua segurança comprometida, devem ser isolados do ambiente corporativo, de forma a garantir a contenção do incidente;
f) Após a erradicação completa do incidente, deve ser realizada uma revisão completa da ocorrência, identificando o nível real de impacto, vulnerabilidades exploradas, a efetividade do tratamento aplicado e a necessidade de maiores ações para evitar a recorrência do incidente;
e) Nenhum tipo de informação sobre incidentes e ocorrências de segurança da informação poderá ser divulgado para entidades ou pessoas externas a EMPREL sem aprovação expressa e formal do COMITÊ DE SEGURANÇA DA INFORMAÇÃO.

8.6 PROTEÇÃO CONTRA CÓDIGOS MALICIOSOS

8.6.1 Ferramenta de proteção contra códigos maliciosos

a) A EMPREL disponibiliza ferramentas para proteção dos seus ativos/serviços de informação e recursos computacionais, incluindo estações de usuários, dispositivos móveis e servidores corporativos, contra ameaças e códigos maliciosos;
b) Apenas a ferramenta disponibilizada pela EMPREL deve ser utilizada na proteção contra códigos maliciosos;
c) Caso uma estação de trabalho ou dispositivo móvel esteja infectado ou com suspeita de infecção de código malicioso, a mesma deverá ser imediatamente isolada da rede corporativa da EMPREL e de qualquer comunicação com a Internet;
d) Caso um servidor corporativo esteja infectado ou com suspeita de infecção de código malicioso, deverão ser adotadas medidas para garantir o isolamento do mesmo da rede corporativa e da Internet, levando em consideração o impacto da desativação dos serviços publicados no referido servidor;

8.6.2 Prevenção dos usuários contra códigos maliciosos

Mesmo com a existência de ferramentas para proteção contra códigos maliciosos, os usuários da EMPREL devem adotar um comportamento seguro, reduzindo a probabilidade de infecção ou propagação de códigos maliciosos, seguindo as seguintes regras:

a) Não tentar efetuar o tratamento e correção de códigos maliciosos por iniciativa própria;
b) Reportar imediatamente a área de segurança da informação qualquer infecção ou suspeita de infecção por código malicioso;
c) Não desenvolver, testar ou armazenar qualquer parte de um código malicioso de qualquer tipo, a menos que expressamente autorizado;
d) Efetuar uma varredura com a ferramenta de proteção contra códigos maliciosos fornecida pela EMPREL antes de utilizar arquivos armazenados em mídias removíveis, baixados da Internet ou recebidos nos serviços de e-mail ou comunicadores instantâneos;
e) Não habilitar MACROS para arquivos recebidos de fontes suspeitas, baixados da Internet ou recebidos nos serviços de e-mail ou comunicadores instantâneos. Caso necessário, poderá ser solicitado o apoio da equipe de segurança da informaçãopara validar se o arquivo representa ou não uma ameaça.

9. REVISÕES E COMENTÁRIOS FINAIS:

a) 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 do COMITÊ DE SEGURANÇA DA INFORMAÇÃO;
b) 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 doCOMITÊ DE SEGURANÇA DA INFORMAÇÃO, bem como, de todos os usuários adotar todo e qualquer outro procedimento de segurança que esteja ao seu alcance, visando sempre proteger asinformações da EMPREL.

Para publicidade e conhecimento geral dos usuários da EMPREL, este documento será publicado na *intranet*.

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

ASSINADO DIGITALMENTE POR
BERNARDO JUAREZ D'ALMEIDA
CPF: ***.537.854-68 **DATA:** 11/11/2024 15:18
LOCAL: RECIFE - PE
CÓDIGO: fbb5dc6a-52f0-4332-a192-72c9b6beae1d
REGULADO PELO DECRETO MUNICIPAL N° 33.682 de 25/05/2020 (RECIFE-PE)

Bernardo Juarez D´Almeida
Diretor Presidente

ASSINADO DIGITALMENTE POR
ALYSON CARVALHO PEREIRA DE MATOS
CPF: ***.988.044-25 **DATA:** 11/11/2024 11:03
LOCAL: RECIFE - PE
CÓDIGO: 4c9882f3-f9b0-4acd-a3e7-27fa0bf86d48
REGULADO PELO DECRETO MUNICIPAL N° 33.682 de 25/05/2020 (RECIFE-PE)

Alyson Carvalho Pereira de Matos
Diretor de Infraestrutura de Informática

ASSINADO DIGITALMENTE POR
JORGE LUIZ PINTO DE SOUZA
CPF: ***.523.874-72 **DATA:** 11/11/2024 12:07
LOCAL: RECIFE - PE
CÓDIGO: d46de340-3ef0-4106-aad3-965452be97f4
REGULADO PELO DECRETO MUNICIPAL N° 33.682 de 25/05/2020 (RECIFE-PE)

Jorge Luiz Pinto de Souza
Gerente de Segurança da Informação

Emprel - Empresa Municipal de Informática
Rua do Brum, 123|Empr. Maurício Brandão Mattos - 2º andar
Bairro do Recife - Recife/PE | 50030-260
(81) 3355.7000 | www.Emprel.gov.br

ANEXO I

CRITÉRIOS PARA CRIAÇÃO DE SENHA

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

a. Frequência 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, númerose 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, adotandoo 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 desenha forte.

Emprel - Empresa Municipal de Informática
Rua do Brum, 123|Empr. Maurício Brandão Mattos - 2º andar
Bairro do Recife - Recife/PE | 50030-260
(81) 3355.7000 | www.Emprel.gov.br

ANEXO II

REGRAS DE E-MAIL

As regras para uso de *e-mail* são as seguintes:

Caixa de Mensagem	1 TB
Tamanho máximo de *e-mail*	25 MB
Extensões de arquivos que requerem muitacautela	.exe, .com, .scr., .BAT
Assuntos proibidos	Propaganda político partidária; propagandacom 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.

Emprel - Empresa Municipal de Informática
Rua do Brum, 123|Empr. Maurício Brandão Mattos - 2º andar
Bairro do Recife - Recife/PE | 50030-260
(81) 3355.7000 | www.Emprel.gov.br

ANEXO III

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 sejamacessados 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 III, 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 cominformações fidedignas;
b. O usuário e o órgão devem assinar em conjunto o termo de uso;
c. O usuário da PCR e a sua Chefia imediata devem assinar em conjunto otermo de uso;
d. O usuário deve assinar isoladamente o termo de responsabilidade.

Cada TERMO DE USO pode ser vinculado a tantos termos de responsabilidadequantos 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 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.

Emprel - Empresa Municipal de Informática
Rua do Brum, 123|Empr. Maurício Brandão Mattos - 2º andar
Bairro do Recife - Recife/PE | 50030-260
(81) 3355.7000 | www.Emprel.gov.br

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, atravésda conta de *e-mail* 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, seráinformada por *e-mail*.

Será enviado para o *e-mail* informado no termo de responsabilidade, juntamente com o certificado, as orientações para uso da VPN.

Emprel - Empresa Municipal de Informática
Rua do Brum, 123|Empr. Maurício Brandão Mattos - 2º andar
Bairro do Recife - Recife/PE | 50030-260
(81) 3355.7000 | www.Emprel.gov.br

ANEXO IV

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: xxxxxxxxxxxxxxxxxxxxxxxx
CPF: xxxxxxxxxxxxxxxxxxxx
Telefone(s): ( )

Local e Data:

Assinatura:_____
< usuário >

Assinatura:
< responsável pela solicitação >

Emprel - Empresa Municipal de Informática
Rua do Brum, 123|Empr. Maurício Brandão Mattos - 2º andar
Bairro do Recife - Recife/PE | 50030-260
(81) 3355.7000 | www.Emprel.gov.br

ANEXO IV
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 EMPRELpela 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 EMPRELdescritas nas Normas de Uso.

Recife, de de 20XX.

_____ _____

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

Emprel - Empresa Municipal de Informática
Rua do Brum, 123|Empr. Maurício Brandão Mattos - 2º andar
Bairro do Recife - Recife/PE | 50030-260
(81) 3355.7000 | www.Emprel.gov.br

ANEXO IV

TERMO DE USO DOS SISTEMAS INTERNOS DA EMPREL
(TERMO DE CIÊNCIA DO RISI)

CONSIDERANDO a disponibilização, pela Emprel, de infraestrutura tecnológica, como ferramenta de trabalho, para que seus usuários possam exercer o pleno desenvolvimento de suas atividades;

CONSIDERANDO que a infraestrutura tecnológica é de exclusiva propriedade daEmprel, 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 infraestrutura tecnológica poderá ocasionar sérios prejuízos à Emprel;

DECLARO QUE:

1. Tenho conhecimento e acesso ao Regulamento Interno 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 infraestrutura tecnológica da Emprel, sendoindispensável 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 Interno de Segurança da Informação, responderei por minhas ações e omissões, observando os princípios constitucionais da ampla defesa e do contraditório.

Recife,_____de_____de 20xx.

Nome: _____
RG:
CPF:

Emprel - Empresa Municipal de Informática
Rua do Brum, 123|Empr. Maurício Brandão Mattos - 2º andar
Bairro do Recife - Recife/PE | 50030-260
(81) 3355.7000 | www.Emprel.gov.br

ANEXO V

FORMULÁRIO PARA SOLICITAÇÃO DE CONTA DE REDE

Nome completo: _____.

CPF:_____._____._____-____

Secretaria/órgão:_____

Complemento:_____

Matrícula:_____

Telefone:_____

Descreva os serviços que o usuário terá acesso

_____

_____

_____

_____

Nome do gerente: _____.

Matr. do gerente:_____

Emprel - Empresa Municipal de Informática
Rua do Brum, 123|Empr. Maurício Brandão Mattos - 2º andar
Bairro do Recife - Recife/PE | 50030-260
(81) 3355.7000 | www.Emprel.gov.br

ANEXO VI

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:

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:

Obs.: Encaminhar formulário preenchido para a DEGP/UOFC

DEOS /UOSB – Unidade Operacional de Suporte a Sistemas Básicos

Providência(s) adotada(s):

Data: / / Assinatura do Técnico:

Emprel - Empresa Municipal de Informática
Rua do Brum, 123|Empr. Maurício Brandão Mattos - 2º andar
Bairro do Recife - Recife/PE | 50030-260
(81) 3355.7000 | www.Emprel.gov.br

ANEXO VII

CRITÉRIOS QUANTO A CONFORMIDADE PARA ACESSO A REDE CORPORATIVA

- Usuário deve possuir Login da Rede Corporativa;
- Sistema Operacional Atualizado;
- Softwares licenciados;
- O Antivírus corporativo deve estar instalado e atualizado.

Emprel - Empresa Municipal de Informática
Rua do Brum, 123|Empr. Maurício Brandão Mattos - 2º andar
Bairro do Recife - Recife/PE | 50030-260
(81) 3355.7000 | www.Emprel.gov.br

ANEXO VIII

Termo de Compromisso de Responsabilidade pela Hospedagem de Software Fora do Padrão Tecnológico de Referência (PTR)

Este termo de compromisso é firmado entre [***Nome do Gerente***], CPF [***Número do CPF***], ocupando a [***Função***] da [***Nome do órgão***], doravante denominado "*COMPROMISSADO*", e a Empresa Municipal de Processamento de Dados - EMPREL, doravante denominada "*EMPREL*".

Este termo formaliza a autorização e o compromisso do COMPROMISSADO em hospedar softwares fora do Padrão Tecnológico de Referência (PTR) da EMPREL, assumindo integral responsabilidade pela hospedagem desses softwares e reconhecendo os riscos inerentes à sua não conformidade.

Para fins deste termo, considera-se Padrão Tecnológico de Referência (PTR) o conjunto de normas e diretrizes estabelecidas pela EMPREL, visando garantir a segurança, a eficiência e a compatibilidade dos sistemas e softwares utilizados na Unidade. A lista completa dos padrões pode ser consultada em:[***https://www.emprel.gov.br/padrao-tecnologico-de-referencia-versao-20***]***.***

O COMPROMISSADO declara estar ciente de que o software a ser hospedado não está em conformidade com o PTR da EMPREL e, ainda assim, autoriza sua hospedagem devido a motivos específicos de necessidade operacional, técnica ou estratégica.

O COMPROMISSADO assume total responsabilidade por qualquer consequência decorrente da hospedagem de software fora do PTR, incluindo, mas não se limitando a problemas de segurança, manutenção e suporte técnico, bem como a qualquer impacto operacional.
O COMPROMISSADO compromete-se a:

- Informar à EMPREL, por meio de documento formal enviado para o e-mail comite@recife.pe.gov.br, o software fora do PTR que será hospedado, com justificativas e análises de risco;
- Monitorar continuamente o software para mitigar possíveis riscos associados à sua não conformidade com o PTR, com a entrega de relatórios trimestrais à EMPREL, abordando a análise de riscos, a eficácia das medidas de mitigação adotadas e quaisquer incidentes relevantes;
- Colaborar com a EMPREL na busca de alternativas ou adaptações que possam vir a adequar o software ao PTR no futuro.

O COMPROMISSADO reconhece que a hospedagem de software fora do PTR pode acarretar riscos, incluindo, mas não se limitando a:

- Vulnerabilidades de segurança que possam ser exploradas;
- Dificuldades de manutenção e suporte técnico;
- Incompatibilidade com outros sistemas operacionais ou softwares utilizados na EMPREL;
- Impacto na performance e na continuidade das operações.

O COMPROMISSADO reconhece que, em caso de falha no cumprimento das obrigações mencionadas ou na administração dos riscos decorrentes, poderá ser submetido a sanções administrativas e/ou responder por quaisquer danos à EMPREL, conforme previsto nas políticas internas e legislação aplicável.

Este termo de compromisso entra em vigor na data de sua assinatura e será válido enquanto o software permanecer hospedado fora do PTR. A rescisão deste termo poderá ser realizada a qualquer momento, mediante notificação formal, caso a hospedagem deixe de ser necessária ou se o software for adaptado aos padrões PTR. A rescisão pode ser precedida pelo desligamento do ambiente de hospedagem, que deve ser realizado de acordo com as diretrizes estabelecidas pela EMPREL.

Recife, _____ de _____ de _____

[Nome do Gerente]
COMPROMISSADO

[Nome do Responsável da EMPREL]
EMPREL