DIÁRIO OFICIAL
RECIFE, QUINTA-FEIRA 28 DE MARÇO DE 2019 ANO XLVIII Nº 039 PREFEITURA DO RECIFE

RESOLUÇÃO Nº 01, DE 16 DE JANEIRO DE 2019

Institui a Política de Segurança da Informação da Autarquia Municipal de Previdência e Assistência à Saúde dos Servidores - AMPASS e as Regras Gerais de Uso de Ativos de TI (software e hardware).

O DIRETOR PRESIDENTE da Autarquia Municipal de Previdência e Assistência à Saúde dos Servidores - AMPASS, no exercício das competências e atribuições descritas no Inciso I do Anexo Único do Decreto nº 27.276, de 14.08. 2013,

CONSIDERANDO a exigência, na atualidade, de instituições que prezem pela transparência, sem prejuízo da preservação dos sigilos legais;

CONSIDERANDO o grande fluxo de informações públicas e privadas que transitam entre os diversos agentes internos e externos que se relacionam com esta autarquia;

CONSIDERANDO a importância dessas informações e a indispensabilidade de uma melhor gestão sobre o fluxo de dados, registros, documentos e demais temas correlatos;

CONSIDERANDO a necessidade de estabelecer diretrizes que norteiem o aspecto da segurança da informação nessas relações;

RESOLVE:
Art. 1º Aprovar a Política de Segurança da Informação da Autarquia Municipal de Previdência e Assistência à Saúde dos Servidores - AMPASS (Anexo I) e instituir as Regras Gerais de Uso de Ativos de TI (software e hardware), constante no Anexo II. Art.

2º A Política de Segurança da Informação da Autarquia Municipal de Previdência e Assistência à Saúde dos Servidores tem por finalidade:
a) Implementar a política de proteção das informações contra acesso não autorizado, manutenção da confidencialidade, da integridade e disponibilidade das informações utilizadas nas relações com a AMPASS;
b) Fomentar o gerenciamento de riscos, prevenir e minimizar os impactos dos incidentes de segurança para que seja preservado o patrimônio não físico desta entidade;
c) Definir e estimular o papel e as responsabilidades de cada um dos envolvidos que recebam, guardem, gerenciem, tenham acesso ou administrem informações públicas ou privadas relativas a esta AMPASS.

Art. 3º Todas as medidas cabíveis devem ser tomadas para a preservar a integridade e confidencialidade da informação, a fim de protegê-las de alteração, destruição ou divulgação não autorizada;

Art. 4º Esta Resolução entra em vigor na data de publicação.
Cumpra-se

Publique-se

MANOEL CARNEIRO SOARES CARDOSO
Diretor Presidente Republicada por incorreção no original

ANEXO I

INTRODUÇÃO
No mundo de hoje, globalizado, com recursos escassos, com cobranças crescentes da sociedade, a informação toma uma dimensão extremamente importante, pois decisões importantes são tomadas com base na mesma e há reflexos legais, nos quais a informação se torna um fator essencial e como tal, precisa estar disponível, mas também protegida.

OBJETIVO
Estabelecer os conceitos e diretrizes de segurança da informação, visando à utilização da infraestrutura tecnológica da Autarquia Municipal de Previdência e Assistência à Saúde dos Servidores, de acordo com princípios éticos e legais, bem como atitudes adequadas para proteger as informações da AMPASS e dos seus clientes. Desse modo, a Política busca preservar os seus ativos de informação, assim como a sua imagem institucional.

ABRANGÊNCIA
Esta Política aplica-se a todos os usuários, sendo esses internos ou externos.

CONCEITOS E DEFINIÇÕES
São recursos da infraestrutura tecnológica da AMPASS: os microcomputadores, as impressoras, os notebooks, as redes de comunicação de dados e voz, os periféricos associados aos computadores (câmeras, mouse, teclado, caixa de som, etc.), as câmeras de monitoramento e os equipamentos de controle de acesso, os equipamentos de projeção e painel de chamada, os smartfones corporativos, os softwares disponibilizados pela AMPASS como: e-mail, antivírus, sistemas e aplicativos, etc.

A segurança da informação é aqui caracterizada pela preservação dos seguintes conceitos:

Acesso: Ato de ingressar, transitar, conhecer ou consultar a informação, bem como a acessibilidade de usar os ativos de informação de um órgão ou entidade;

Confidencialidade: Garante que a informação seja acessível somente pelas pessoas autorizadas, pelo período necessário e para os fins de atividades relacionadas ao trabalho da AMPASS;

Disponibilidade: Garante que a informação esteja disponível para as pessoas autorizadas sempre que se fizer necessária;

Integridade: Garante que a informação esteja completa e íntegra e que não tenha sido modificada ou destruída de maneira não autorizada ou acidental durante o seu ciclo de vida;

Autenticidade: Garante que a informação é proveniente da fonte anunciada e que não foi alvo de mutações ao longo de um processo.

Informação: Conjunto de dados, textos, imagens, métodos, sistemas ou quaisquer formas de representação dotadas de significado em determinado contexto, independentemente do suporte em que resida ou da forma pela qual seja veiculado?

Usuário Interno: O empregado, o servidor, o contratado, o estagiário ou o conveniado da Administração Municipal, que no exercício de suas funções, tenham acesso a informações produzidas ou recebidas pelo Município do Recife;

Usuário Externo: A pessoa física ou a pessoa jurídica que tenha acesso concedido a informações produzidas ou recebidas pelo Município do Recife e que não seja caracterizada como Usuário Interno;

Comitê Gestor de Segurança da Informação: grupo multidisciplinar composto por membros da AMPASS, com o objetivo de avaliar a estratégia e diretrizes de segurança da informação seguidas pela AMPASS.

DIRETRIZES

As informações (em formato físico ou lógico) e os recursos tecnológicos utilizados pelos usuários são de exclusiva propriedade da AMPASS ou da Prefeitura da Cidade do Recife, não podendo ser interpretados como de uso pessoal.

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

É vedado a qualquer usuário da AMPASS o uso dos recursos de Tecnologia da Informação e Comunicação para fins pessoais (próprios ou de terceiros), veiculação de opiniões político-partidárias ou religiosas, bem como para praticar ações que, de qualquer modo, possam constranger, assediar, ofender, caluniar, ameaçar, violar direito autoral ou causar prejuízos a qualquer pessoa física ou jurídica, assim como aquelas que atentem contra a moral e a ética, ou que prejudiquem o cidadão ou a imagem da instituição, comprometendo a integridade, a confidencialidade, a confiabilidade, autenticidade ou a disponibilidade das informações.

Todos os funcionários, estagiários e prestadores de serviços devem ter ciência de que o uso das informações e dos sistemas de informação pode ser monitorado, e que os registros assim obtidos poderão ser utilizados para detecção de violações da Política e das Normas de Segurança da Informação, podendo estas servir de evidência para a aplicação de medidas disciplinares, processos administrativos e/ou legais;

Todo processo, sempre que possível, durante seu ciclo de vida, deve garantir a segregação de funções, por meio da participação de mais de uma pessoa ou equipe. Todas as informações devem estar adequadamente protegidas em observância às diretrizes de segurança da informação da AMPASS em todo o seu ciclo de vida, que compreende: geração, manuseio, armazenamento, transporte e descarte;

O acesso as informações e o uso dos sistemas e aplicativos deverão ser feito mediante identificação do usuário único, pessoal e intransferível, com utilização de senha de acesso. Cabe ao usuário a responsabilidade do sigilo das suas senhas de acesso aos recursos de Tecnologia da Informação e Comunicação da AMPASS;

As informações devem ser utilizadas de forma transparente e apenas para a finalidade para a qual foi coletada.

Gestão de acessos e identidades

O acesso às informações e aos ambientes tecnológicos da AMPASS deve ser controlado de acordo com sua classificação, de forma a garantir acesso apenas às pessoas autorizadas, mediante aprovação formal do gestor da informação. Os acessos dos funcionários, estagiários e prestadores de serviços devem ser solicitados e aprovados somente às informações necessárias ao desempenho de suas atividades.

Gestão de incidentes de segurança da informação

Em casos de violação desta Política e Normas de Segurança da Informação, por ação ou omissão, intencional ou acidental, o Comitê Gestor de Segurança da Informação (CGSI) realizará deliberações sobre os incidentes classificados como de alta criticidade. Os demais casos serão tratados pelo fluxo normal de resposta a incidentes. Após deliberações, o CGSI recomendará ao Diretor Presidente da AMPASS as ações a serem tomadas e este deliberará sobre sua procedência ou não, observando os Códigos de Ética da AMPASS, do Servidor Público Civil do Poder Executivo Municipal, aprovado pelo Decreto nº 27.267, de 16 de dezembro de 2013, e às resoluções expedidas pela Comissão Central de Ética, sem prejuízo de outras legislações vigentes;

Os contratos entre a AMPASS e as empresas prestadoras de serviços com acesso às informações, aos sistemas e/ou ao ambiente tecnológico da AMPASS devem conter cláusulas que garantam a confidencialidade entre as partes e que assegurem minimamente que os profissionais sob sua responsabilidade cumpram a Política e as Normas de Segurança da Informação.

Os Usuários Internos e Externos estão sujeitos a esta Política e às Normas de Segurança da Informação.

A implantação e manutenção de um ambiente tecnológico seguro é tarefa inerente não só aos administradores e técnicos de informática, bem como a todos os envolvidos na estrutura da Administração Municipal, Usuários Internos e Externos.

De forma geral, cabe a todos os Usuários, Internos ou Externos

Cumprir fielmente a Política, as Normas e os Procedimentos de Segurança da Informação da AMPASS;

Proteger as informações contra acessos, modificação, destruição ou divulgação não autorizados pela AMPASS;

Assegurar que os recursos tecnológicos, as informações e sistemas a sua disposição sejam utilizados apenas para as finalidades aprovadas pela AMPASS;

Cumprir as leis e as normas que regulamentam a propriedade intelectual;

Garantir a segurança das informações da Administração Municipal a que tenham acesso;
Não discutir assuntos confidenciais de trabalho em ambientes públicos ou em áreas expostas (aviões, transporte, restaurantes, encontros sociais etc.) incluindo a emissão de comentários e opiniões em blogs e redes sociais;

Não compartilhar informações confidenciais de qualquer tipo;

Colaborar com alertas, sugestões e críticas que possam melhorar a segurança da informação;

Comunicar imediatamente à área de Gestão de Segurança da Informação ou a sua gerência, eventos potenciais ou reais de risco, descumprimento ou violação desta Política e/ou de suas Normas e Procedimentos, que tenham presenciado ou que tenham conhecimento.

Cabe ao Comitê Gestor de Segurança da Informação

Assessorar na implementação das ações de segurança da informação e comunicações na AMPASS ;

Constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação e comunicações;

Propor Normas e Procedimentos internos relativos à segurança da informação e comunicações, em conformidade com as legislações existentes sobre o tema;

Realizar deliberações sobre os incidentes classificados como de alta criticidade.

Cabe à área de Gestão de Segurança da Informação

Promover cultura de segurança da informação e comunicações;

Promover ampla divulgação da Política e das Normas de Segurança da Informação para todos os funcionários, estagiários e prestadores de serviços;

Promover ações de conscientização sobre Segurança da Informação para os funcionários, estagiários e prestadores de serviços;

Propor normas, projetos e iniciativas relativas à segurança da informação e comunicações e ao seu aperfeiçoamento;

Acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança.

Cabe às Gerências da AMPASS

As responsabilidades pela segurança da informação devem ser definidas nas descrições de cargos e funções, bem como nos termos e condições das contratações que envolvam o manuseio de dados, informações ou conhecimentos da AMPASS;

Promover ações para que todos os usuários sejam conscientizados e treinados nos procedimentos de segurança da informação;
Assegurar que o controle operacional de uma atividade crítica não seja de atribuição exclusiva de uma única pessoa;

Assegurar que quando do afastamento, mudança de responsabilidades e de lotação ou atribuições dentro da organização haja imediata revisão dos direitos de acesso e uso dos ativos e que quando da efetivação do desligamento de usuário, deverão ser extintos todos os direitos de acesso e uso dos ativos a ele atribuído. Todo ativo produzido pelo usuário, desligado, deverá ser mantido pela AMPASS garantindo o reconhecimento e o esclarecimento da propriedade do acervo para Instituição.

AÇÕES EM CASOS DE NÃO CONFORMIDADE

Na ocorrência de violação desta Política ou das Normas de Segurança da Informação, o Diretor Presidente da AMPASS poderá adotar, com o apoio das Gerências sanções administrativas e/ou legais.

AS REVISÕES E COMENTÁRIOS FINAIS

A Autarquia Municipal de Previdência e Assistência à Saúde dos Servidores se reserva ao direito de revisar, adicionar ou modificar a Política de Segurança da Informação, bem como das Regras Gerais de Uso de Ativos de TI (software e hardware), para aprimorar e garantir o perfeito funcionamento das normas e regras.

Todas as diretrizes desta Política de Segurança se estenderão aos casos omissos, que deverão ser encaminhados a área de Gestão de Segurança da Informação para avaliação e resolução com o referendo do Presidente da AMPASS.

As normas e procedimentos acima não se esgotam neste instrumento, sobretudo em razão da constante evolução tecnológica, não consistindo em rol taxativo, motivo pelo qual é obrigação do CGSI, bem como dos usuários adotarem todo e qualquer outro procedimento de segurança que esteja ao seu alcance, visando sempre proteger as informações da Administração Municipal.

ANEXO II

REGRAS GERAIS DE USO DE ATIVOS DE TI (SOFTWARE E HARDWARE) - OS PROGRAMAS, A REDE DE COMPUTADORES, DE DISPOSITIVOS PORTÁTEIS E DE DEMAIS RECURSOS DE TECNOLOGIA DA INFORMAÇÃO DA AUTARQUIA MUNICIPAL DE PREVIDÊNCIA E ASSISTÊNCIA À SAÚDE DOS SERVIDORES - AMPASS

REGRAS GERAIS DE UTILIZAÇÃO DOS RECURSOS DE TI

1.Computadores e demais recursos da Autarquia devem ser utilizados exclusivamente para o serviço da AMPASS. Admite-se a utilização particular esporádica;
2.Por ser do interesse da AMPASS que os seus colaboradores estejam bem informados, o uso de sites de notícias ou de serviços de notícias é aceitável, desde que o seu uso não comprometa o uso de Banda da rede, nem perturbe o bom andamento dos trabalhos, observados em todos os casos os termos desta política de uso.
3.Os equipamentos devem ser manuseados com cuidado, considerando que os computadores e seus acessórios são patrimônio público. Em caso de o usuário notar alguma anormalidade com o computador e seus periféricos, ou a ausências desses, deve avisar imediatamente a equipe de TI para que sejam tomadas as devidas providências;
4.Alimentos e/ou bebidas não devem ser consumidos próximos dos equipamentos a fim de evitar danos aos mesmos;
5.Não é permitida a abertura física ou a desmontagem de equipamentos de TIC de propriedade da AMPASS, exceto se realizada pela correspondente ou por pessoa ou empresa autorizada;
6.As mudanças de local dos equipamentos (layout) devem ser realizadas/supervisionadas pela área de TIC com o objetivo de evitar danos aos equipamentos e acidentes provenientes de fiação exposta com risco de tropeços;
7.O acesso as informações e ao uso dos sistemas e aplicativos deverão ser feitos mediante identificação do usuário único, pessoal e intransferível, com utilização de senha de acesso. O usuário é responsável pelas ações realizadas por meio da utilização de sua conta. Cabe ao usuário a responsabilidade do sigilo das suas senhas de acesso aos recursos de Tecnologia da Informação e Comunicação da Autarquia;
8.O uso das informações, dos sistemas e aplicativos disponibilizados pela Autarquia é monitorado;
9.Não é permitida a instalação de softwares ou equipamentos na rede corporativa sem a prévia autorização da área responsável pela TIC;
10.É terminantemente proibido o envio de qualquer mensagem, seja entre usuários da empresa ou externos, com conteúdo difamatório, ofensivo, racista, especulativo, obsceno, bullying, SPAMs, correntes ou de qualquer natureza similar, indução religiosa, comércio, propaganda e incentivo a atos de terrorismo, ou que visem instigar, ameaçar, invadir a privacidade ou prejudicar pessoas e/ou organizações;
11.É terminantemente proibido utilizar os recursos de TI para executar quaisquer tipos de fraudes;
12.É proibido baixar (fazer download) e/ou armazenar, em computador local ou unidades de rede, software comercial, músicas, fotos, filmes ou qualquer outro material cujo direito pertença a terceiros (copyright), sem ter um contrato de licenciamento, compra ou outros tipos de licença, e programas ou arquivos com teor pornográfico;
13.A Autarquia disponibiliza área em servidor de arquivo para guarda de informações departamentais e coorporativas que precisam ser protegidas. É de responsabilidade exclusiva do usuário manter, no servidor, as informações produzidas a fim de facilitar as consultas pelos demais servidores e para que essas sejam preservadas através das rotinas de segurança e backup;
14.Arquivos de música, vídeo, jogos, fotos e outros que não estão de acordo com os serviços realizados pela Autarquia, ao serem encontrados na rede, serão excluídos sem aviso prévio.

REGRAS GERAIS PARA USO DA REDE DE COMPUTADORES, DE DISPOSITIVOS PORTÁTEIS E DE DEMAIS RECURSOS DE TI DA AMPASS

CAPÍTULO I
DAS DISPOSIÇÕES GERAIS

Art. 1 As regras gerais para uso da rede de computadores, de dispositivos portáteis e de demais recursos de TIC da AMPASS obedecem à legislação pertinente, e estão alinhadas com os princípios e as diretrizes da Política de Segurança da Informação da AMPASS.
Parágrafo único. Para os fins desta norma, o conceito de recursos de TI abrange as soluções de TI e compreende os equipamentos, dispositivos e funcionalidades - que sejam utilizados para prover serviços de TI da rede de computadores da AMPASS ou que utilizem esses serviços.
Art. 2 A rede de computadores, os dispositivos portáteis e demais recursos de TI de propriedade da AMPASS constituem recursos corporativos para utilização no interesse do serviço.
Art. 3 Para efeito do disposto nesta Portaria, entende-se por:
I - Rede de computadores da AMPASS (REDE CORPORATIVA): conjunto de computadores, funcionalidades e outros dispositivos, de propriedade da AMPASS ou por ela providos, que, ligados em uma rede de comunicação de dados, possibilitam a prestação de serviços de TI;
II - Conta: identificação de usuário, com senha associada, para acesso à Sistemas disponibilizados pela AMPASS;
III - login de rede: conta para acesso à REDE CORPORATIVA utilizada por usuário, com finalidade de acesso ao ambiente corporativo;
IV - Estação de trabalho: computador de mesa (desktop) de propriedade da AMPASS;
V - Dispositivo portátil: qualquer dispositivo utilizado para acessar a REDE CORPORATIVA e que tenha como característica a portabilidade, tais como notebooks, organizadores pessoais eletrônicos (PDAs) e smartphones;
VI - Dispositivo de comunicação: equipamento, como roteador e switch, utilizado para prover serviços de TI e comunicação entre estações de trabalho e dispositivos portáteis por meio da REDE CORPORATIVA, com ou sem fio;
VII - Diretório: espaço de armazenamento específico na REDE CORPORATIVA;
VIII - Administrador de diretório: servidor que responde pela unidade, subunidade, projeto, comissão, comitê ou grupo de trabalho em relação à utilização do diretório
X - Administrador de recurso de TI: usuário ou grupo de usuários responsável por definir critérios de utilização e autorizar, conceder ou modificar permissões de uso sobre o recurso de TI;
XI - Administrador de grupo: usuário responsável pela criação manual e manutenção de grupos de usuários;
XII - Privilégio: permissão concedida a usuário e grupos de usuários de um recurso de TI;
XIV - Acesso interno: acesso a serviços de TI providos pela AMPASS, por meio de equipamento conectado diretamente à REDE CORPORATIVA;
XV - Acesso externo: acesso a serviços de TI providos na REDE CORPORATIVA, por meio de conexão à internet não fornecida pela AMPASS;
XVII - Autenticação: processo de validação da identidade do usuário, que pode ser feito por diversos meios, tais como: combinação de usuário/senha, biometria ou utilização de certificado digital;
XX - Conexão à REDE: ligação de equipamento à REDE CORPORATIVA por meio de cabeamento físico (telefônico, elétrico, óptico ou coaxial), de equipamentos de radiofrequência ou de comunicação via infravermelho ou micro-ondas (rede sem fio);
XXI - DIVISÃO DE SISTEMAS DA INFORMAÇÃO - DSI: setor vinculado à USI que têm a atribuição de atender, ou providenciar para que sejam atendidas, solicitações de usuários relativas aos serviços e soluções de TI corporativos.
XXII - UNIDADE DE SISTEMAS DA INFORMAÇÃO - USI: setor que têm a atribuição de Junto com as DIRETORIA EXECUTIVA E O Comitê Gestor de Segurança da Informação, criar e implantar as diretrizes e normas com relação a Política de Segurança da Informação.
Parágrafo único. Para os fins desta norma, dispositivo portátil de propriedade da AMPASS tem tratamento equivalente ao de estação de trabalho.
Art. 4 São usuários da REDE CORPORATIVA:
Usuário interno: autoridade ou servidor ativo, contratado, terceirizado e estagiário da AMPASS que tenha acesso, de forma autorizada, a informações produzidas ou custodiadas pela AMPASS;

CAPÍTULO II
DA IDENTIFICAÇÃO DE USUÁRIOS E DO TRATAMENTO DE SENHAS

Art. 5 Cada usuário deve possuir uma conta única, pessoal e intransferível, para acesso à REDE CORPORATIVA, exceto nos casos explicitamente definidos e autorizados pela USI.

Art. 6 A criação e a atualização de conta de usuário, login para acesso à REDE CORPORATIVA e SISTEMAS INFORMATIZADS devem ser realizadas pela USI com base nos registros contidos no sistema informatizado de gestão de pessoas e solicitação de acesso da chefia imediata.

Art. 7 As permissões devem ser concedidas de forma que o usuário tenha somente o privilégio necessário para desempenhar suas funções

Art. 8 O usuário é responsável pelas atividades realizadas por meio da utilização de sua conta, login para acesso à REDE CORPORATIVA e SISTEMAS INFORMATIZADOS.

Art. 9. A senha associada à conta de usuário para acesso à sistemas da AMPASS é pessoal, intransferível e o devido sigilo é de responsabilidade exclusiva do titular da conta.
§ 1º A USI é responsável pela definição e pela divulgação das regras de formação da conta de usuário e da senha.

Art. 10. Cabe as gerências da AMPASS comunicar o desligamento do servidor ou de usuário colaborador, para que as permissões que foram concedidas em razão das atividades realizadas na AMPASS sejam revogadas;

CAPÍTULO III
DO ARMAZENAMENTO DE ARQUIVOS NA REDE CORPORATIVA

Art. 11. A REDE CORPORATIVA deve prover ambiente seguro para armazenamento de arquivos.

Art. 12. Gerências, Unidades, e Divisões pode ter diretório específico na REDE CORPORATIVA.
§ 1º A definição das permissões dos diretórios das Gerências, Unidades e Divisões é responsabilidade do administrador de TI.
§ 2º O Gerente ou Gestor deve solicitar à DSI a concessão, a alteração ou a revogação de permissões sobre o diretório.
§ 3º O disposto no parágrafo anterior não se aplica aos casos de diretórios com conteúdo sigiloso, para os quais a concessão, a alteração ou a revogação de permissões deve ser feita exclusivamente pela USI.

Art. 13. É vedado o armazenamento das seguintes informações nos diretórios da REDE CORPORATIVA:
I - Arquivo em desacordo com o definido na Política de Segurança da Informação da AMPASS, tais como arquivos de imagem, apresentação, áudio ou vídeo que não sejam de interesse do serviço;
II - Programa não homologado ou licenciado pela AMPASS;
III - Programa de conteúdo potencialmente prejudicial à segurança da REDE CORPORATIVA;
IV - Programa em desacordo com demais critérios e requisitos de segurança de que trata a Política de Segurança da Informação da AMPASS;
V - Cópia de segurança de diretório de usuário ou cópia-imagem de estação de trabalho.
Parágrafo único. A USI deve definir parâmetros para armazenamento de arquivos nos equipamentos servidores, incluindo requisitos como tamanho máximo e tipos de arquivo permitidos, com vistas a não comprometer o desempenho e a segurança dos serviços de TI.
Art. 14. As informações armazenadas nos diretórios da REDE CORPORATIVA podem ser inspecionadas pela DSI, por meio de programa ou procedimento automatizado da DSI, quando houver indícios de armazenamento de informações em desacordo com o disposto no artigo anterior.
§ 1º Os procedimentos citados no caput também se aplicam aos diretórios residentes nas estações de trabalho existentes na AMPASS no curso de sindicâncias ou de procedimentos investigativos preliminares, mediante prévia autorização da DIRETORIA DA PRESIDÊNCIA.

§ 2º A informação armazenada em diretório da REDE CORPORATIVA em desacordo com o disposto no artigo anterior será excluída pela DSI, e o fato caracterizado como incidente de segurança da informação, com prévia comunicação à USI, à sua chefia imediata e ao titular da Gerência, unidade em que está lotado.

CAPÍTULO IV
DA INSTALAÇÃO E EXECUÇÃO DE PROGRAMAS, E DAS ESTAÇÕES DE TRABALHO

Art. 15. A identificação de cada estação de trabalho da AMPASS é realizada pela DSI e deve estar de acordo com padrões por ela definidos.

Art. 16. A instalação de programas em estações de trabalho ou na REDE CORPORATIVA é atribuição exclusiva da DSI ou de pessoa ou empresa por ela expressamente autorizada.
§ 1º É vedado ao usuário o privilégio de administração e o acesso à senha do administrador local da estação de trabalho, exceto nos casos autorizados pela USI, em que seja estritamente necessário para o desempenho das funções.
§ 2º É vedado ao usuário modificar a configuração da estação de trabalho, desabilitar ou desinstalar programas de segurança.

Art. 17. Cabe à USI elaborar, manter atualizada e divulgar relação de programas homologados para utilização na REDE CORPORATIVA.

Art. 18. Compete à USI definir os critérios e requisitos de segurança para a instalação ou a execução de programas em estações de trabalho da REDE CORPORATIVA.
Parágrafo único. Programa instalado ou executado em desacordo com os critérios e requisitos de segurança de que trata o caput será desinstalado pela DSI, e o fato caracterizado como incidente de segurança da informação e previamente comunicado à USI e ao Gerente da respectiva unidade em que se encontra a estação de trabalho para que sejam tomadas as providências pertinentes.

Art. 19. Caso haja necessidade de a Gerência utilizar programa de computador não homologado ou licenciado para a AMPASS. Deve ser encaminhada solicitação de instalação ou aquisição à USI, acompanhada de justificativa e, quando for o caso, dos requisitos necessários.

Art. 20. É vedada a abertura física ou a desmontagem de equipamento de informática de propriedade da AMPASS, exceto se realizada pela DSI ou por pessoa ou empresa autorizada pela USI.

Art. 21. É vedada a conexão de mais de um equipamento a um ponto de rede, exceto nos casos expressamente autorizados pela USI.

Art. 22. É vedada a conexão à REDE CORPORATIVA, por meio de cabeamento físico, de computador de mesa ou dispositivo portátil que não sejam fornecidos pela AMPASS, exceto nos casos expressamente autorizados pela USI.
§ 1º A autorização da USI depende de solicitação justificada do motivo e do período da conexão, bem como da verificação da segurança do computador.
§ 2º No caso de necessidade de conexão à REDE CORPORATIVA de computador de organização que utilize as dependências da AMPASS, cabe à USI autorizar e definir os critérios e requisitos de segurança necessários.

Art. 23. É vedada a instalação de programa licenciado para a AMPASS em computador de mesa ou dispositivo portátil que não sejam de propriedade da AMPASS, excetuando-se programa específico para acesso à REDE CORPORATIVA.

CAPÍTULO V
DOS DISPOSITIVOS PORTÁTEIS E DA REDE SEM FIO

Art. 24. A conexão de dispositivo portátil à REDE CORPORATIVA deve seguir procedimentos específicos definidos pela USI.
Parágrafo único. No caso de dispositivo portátil particular, a conexão direta à REDE CORPORATIVA fica restrita ao acesso à internet por meio de rede sem fio.

Art. 25. Em caso de extravio ou roubo de dispositivo portátil de propriedade da AMPASS, a ocorrência deve ser imediatamente registrada junto à USI como incidente de segurança da informação, sem prejuízo das demais providências necessárias.

Art. 26. A USI deve divulgar os requisitos de compatibilidade e de configuração de dispositivo portátil para conexão à rede sem fio da AMPASS
Parágrafo único. A configuração de dispositivo portátil particular para acesso à rede sem fio da AMPASS é responsabilidade da DSI.

Art. 27. A USI não é responsável pela resolução de problemas na utilização da rede sem fio da AMPASS por dispositivos portáteis particulares nem pela resolução de problemas relativos a acesso de dispositivos portáteis da AMPASS à rede de terceiros.

CAPÍTULO VI
USO DO E-MAIL CORPORATIVO

Art. 28 Cada usuário que necessitar realizar comunicação através de e-mail, deve possuir uma conta de e-mail corporativo única, pessoal e intransferível.

Art. 29 A criação e a atualização de conta de usuário, deve ser providenciada pela USI com base em solicitação de acesso da chefia imediata.

Art. 30 O usuário é responsável pelas atividades realizadas por meio da utilização do seu e-mail corporativo.

Art. 31. A senha associada à conta de usuário para utilização do e-mail corporativo é pessoal, intransferível e o devido sigilo é de responsabilidade exclusiva do titular da conta.

Art. 32. Cabe as gerências da Autarquia comunicar o desligamento do servidor ou de usuário colaborador, para que o e-mail seja encerrado ou atualizado caso o usuário seja servidor de outros órgãos do Município do Recife;

Art. 33. O uso do e-mail corporativo deve ser apenas para assuntos profissionais;

Art. 34. Todas as mensagens distribuídas pelo E-mail da empresa, até emails pessoais, se ocorrer, são de propriedade da AMPASS.

Art. 35. Os e-mails podem ser monitorados sem prévia notificação.

Art. 36. É terminantemente proibido enviar ou encaminhar qualquer mensagem, seja entre usuários da empresa ou externos, com conteúdo difamatório, ofensivo, racista, especulativo, obsceno, bullying, Spams, correntes ou de qualquer natureza similar, indução religiosa, comércio, propaganda e incentivo a atos de terrorismo, ou que visem instigar, ameaçar, invadir a privacidade ou prejudicar pessoas e/ou organizações;

Art. 37. É terminantemente proibido utilizar o e-mail corporativo e demais recursos de TI para executar quaisquer tipos de fraudes;

Art. 38. Delete imediatamente aqueles assuntos que não lhe dizem respeito, quer seja verificando pelo assunto ou na leitura das primeiras linhas;

Art. 39. Não envie e-mails com informações confidenciais pois eventualmente podem ser interceptadas.

CAPÍTULO VII
ACESSO A CONTAS DE EMAIL PARTICULAR (WEBMAIL)

Art. 40 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 AMPASS, motivo pelo qual tais acessos devem ser extremamente cautelosos e feitos de forma moderada.
§ 1º Além disso, considerando que os e-mails pessoais acessados através da infraestrutura tecnológica da AMPASS, 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 e-mails pessoais poderá gerar responsabilidades à AUTARQUIA, o que justifica a necessidade de maior cautela por parte dos usuários.
§ 2º Neste sentido, caso o acesso à conta de e-mail do usuário cause qualquer tipo de dano à AMPASS este será integralmente responsável por seus atos, respondendo civil e criminalmente.
§ 3º É absolutamente vedado o envio de informações, dados ou arquivos relacionados, direta ou indiretamente, aos interesses da AMPASS via e-mail pessoal.

CAPÍTULO VIII
DO ACESSO À INTERNET

Art. 41 Todos os usuários internos poderão ter acesso à internet, identificados pela sua conta, de uso pessoal. Cabe à USI implantar os controles de acesso e mecanismos de auditoria que garantam o monitoramento do acesso à internet pela rede corporativa da AMPASS

§ 1º Será bloqueado o acesso a sites de conteúdo considerado ofensivo, ilegal ou impróprio a exemplo de sites pornográficos, de jogos ou apostas.

§ 2º Os Gerentes/gestores da AMPASS poderão solicitar à USI restrição de acesso a sites para os usuários das respectivas Gerências/Unidades.

CAPÍTULO IX
CÂMERAS DE FILMAGEM E CONTROLE DE ACESSO FÍSICO
CONTROLE DE ACESSO (FÍSICO E LÓGICO) AOS SERVIDORES DE SISTEMAS

Art. 42 A AMPASS 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.

Art. 43 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.

Art. 44 As imagens captadas dentro das dependências da AMPASS serão arquivadas pelo prazo de 30 (trinta) dias 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.

Art. 45 O acesso físico dos servidores/colaboradores e visitantes as dependências da A AMPASS se darão por meio de cartão de acesso devidamente identificado.

Art. 46 Cabe a Gerência Administrava e Financeira (GAF) solicitar a USI a solicitação de cartão de acesso para novos servidores/colaboradores.

Art. 47 Os servidores/colaboradores serão cadastrados no sistema de controle de acesso de acordo com os níveis de acesso preestabelecidos pela USI.

Art. 48 Na Autarquia o controle de acesso físico é feito primeiramente no térreo através de seguranças armados e porta com controle de acesso de cartão por aproximação.

Art. 49 Os servidores/colaboradores serão cadastrados no sistema de controle de acesso de acordo com os níveis de acesso preestabelecidos pela USI.

Art. 50 O acesso lógico aos sistemas é feito mediante senha individual de cada servidor.

Art. 51 O acesso físico ao ambiente de servidores e backups é exclusivo para os operadores e analistas de suporte da EMPRESA MUNICIPAL DE PROCESSAMENTOS DE DADOS - EMPREL, através de controle eletrônico de acesso por digital. Não é permitida a entrada de pessoas estranhas a área.

CAPÍTULO X
BACKUP

Art. 52 O serviço de backup compreende a realização de cópias de segurança dos arquivos com o objetivo de restaurá-los no menor tempo possível caso haja necessidade.
Parágrafo único. A EMPRESA MUNICIPAL DE PROCESSAMENTOS DE DADOS - EMPREL é responsável pela realização de backups dos sistemas utilizados pela AMPASS.

Orientações Gerais:
1.Cabe aos administradores prever a realização de testes periódicos de restauração, no intuito de averiguar os processos de backup e estabelecer melhorias.
2.A administração dos backups também deve ser orientada para que seus trabalhos respeitem as janelas para execução, inclusive realizando previsão para a ampliação da capacidade dos dispositivos envolvidos no armazenamento.
3.As mídias (ou dispositivos de armazenamento) deverão ser armazenados em cofre corta-fogo, ou em localidade diversa da origem dos dados (backup off-site).
4.As mídias defeituosas ou inservíveis serão encaminhadas para picotamento, incineração, procedimentos de sobrescrita de dados remanescentes (disco rígido) ou outro procedimento que impossibilite a recuperação dos dados por terceiros.
5.As solicitações de restauração de arquivos deverão ser abertas formalmente através de ferramentas de abertura de chamados e / ou formulário que deverá conter os nomes dos arquivos e pastas que deverão ser recuperados e, principalmente, a data do arquivo que se pretende ter acesso.

Por padrão será adotada o seguinte esquema de realização de backups (exceto se especificada necessidade especial no item 5):

CLASSE	RETENÇÃO	DISCRIMINAÇÃO
MC-ARQUIVOS_	15 15 DIAS	Arquivos com pouco acesso
MC-ARQUIVOS_	30 30 DIAS	Arquivos das maquinas Linux
MC BANCOS	90 DIAS	Para todos os Bancos (mysql e Post)
MC-DB2	90 DIAS	Retencao feita pelo DB2
MC-DB2-ARCH01	90 DIAS	Retencao feita pelo DB2
MC-DB2-ARCH02	90 DIAS	Retencao feita pelo DB2
MC-PADRAO	40 Dias	Retencao de 40 dias (DEFAULT)
MC-ORACLE	90 DIAS	Retencao feita pelo Oracle (RMAN)
MC_ARCH_DB2_ANUAL	90 DIAS	Retencao feita pelo DB2
MC_ARCH_DB2_DIARIO	90 DIAS	Retencao feita pelo DB2
MC_ARCH_ORA_ANUAL	90 DIAS	Retencao feita pelo DB2

Procedimentos de contingência
A contingência de equipamentos para atendimento ao público é a Prefeitura da Cidade do Recife, Cais do Apolo.
A contingência de equipamentos é na EMPREL

CAPÍTULO XI
DAS DISPOSIÇÕES FINAIS

Art. 53. Cabe ao usuário, como custodiante nos termos da Política de Segurança da Informação da AMPASS, garantir a segurança das informações sob sua guarda, armazenadas tanto em computadores de mesa como em dispositivos portáteis, independentemente de a AMPASS ser proprietária desses equipamentos.

Art. 54. Cabe à USI junto com a EMPREL, como administradora do serviço de rede:
I - Garantir a disponibilidade dos serviços, de acordo com níveis de serviço definidos;
II - Implantar e manter atualizados mecanismos e procedimentos de monitoramento e proteção da rede contra-ataques externos e internos; e
III - Implantar e manter atualizados sistemas operacionais e mecanismos de proteção das estações de trabalho, servidores e equipamentos de rede.

Art. 55. O acesso à internet e a redes de outros órgãos, por meio da REDE CORPORATIVA, deve ser provido exclusivamente pela USI.
Parágrafo único. Enquanto conectado à REDE CORPORATIVA, o computador ou o dispositivo portátil não pode estar conectado à internet por solução diferente daquela provida pela USI.

Art. 56. A utilização dos recursos de TI integrantes da REDE CORPORATIVA pode ser monitorada pela USI, com vistas a identificar inobservâncias às normas definidas na Política de Segurança da Informação da AMPASS e a fornecer evidências, no caso de incidentes de segurança da informação, respeitados os direitos e as garantias individuais previstos em lei, e observados os procedimentos previstos para situações específicas dispostas nesta Portaria.
Art. 57. As seguintes ações indevidas relativas à REDE CORPORATIVA são passíveis de apuração de responsabilidade:
I - Conexão à REDE CORPORATIVA, sem autorização expressa da USI, de dispositivo de comunicação, tais como dispositivo de acesso a rede sem fio ou equipamento de rede que não seja de propriedade da AMPASS;
II - Utilização de programa para captura ou geração de tráfego na rede, exceto pela equipe de administração da rede e segurança da AMPASS;
III - Desenvolvimento, manutenção, utilização ou divulgação de mecanismo que permita ou tente violar os sistemas de segurança da rede da AMPASS;
IV - Tentativas de acesso não autorizado a recursos de TI, com indícios de fraude ou sabotagem;
V - Utilização ou tentativa de utilização, com indícios de fraude ou sabotagem, de conta cujo acesso não seja autorizado ao usuário;
VI - Utilização de recurso tecnológico para burlar dispositivo de segurança ou restrição de acesso implementada na rede;
VII - Utilização, com indícios de fraude ou sabotagem, de mecanismo que provoque congestionamento da rede, sobrecarga ou indisponibilidade de serviço;
VIII - Outras utilizações em desacordo com as normas de segurança estabelecidas pela Política de Segurança da Informação da AMPASS

Art. 58. Ao utilizar rede de computadores externa por meio de dispositivos portáteis de propriedade da AMPASS, o usuário deve obedecer também às normas e às diretrizes daquelas redes.
Parágrafo único. Em caso de divergência entre as normas das redes externas e a Política de Segurança da Informação da AMPASS, prevalece o definido nas normas da AMPASS.

Art. 59. Cabe à USI, por meio da DSI, esclarecer eventuais dúvidas do usuário quanto à conformidade de determinada atitude ou utilização em relação às normas de uso da REDE CORPORATIVA.

Art. 60. A violação a Política de Segurança da Informação da AMPASS, ou a inobservância aos dispositivos desta Portaria, podem acarretar, isolada ou cumulativamente:
I - Limitação do uso da REDE CORPORATIVA, conforme estabelecido nos arts. 41 e 42 desta Portaria; e
II - Nos termos da legislação aplicável, outras sanções administrativas, civis e penais.

Art. 61. Para o servidor ativo, o uso da REDE CORPORATIVA pode ser limitado cautelarmente mediante anuência dos titulares das respectivas unidades e Gerências as quais se encontra vinculado, com posterior comunicação ao usuário envolvido.
§ 1º A limitação cautelar do uso da REDE CORPORATIVA pode ser proposta por iniciativa da USI ou, ainda, mediante solicitação justificada, pelo titular da unidade de lotação do usuário.
§ 2º A liberação da limitação do uso da REDE EMPREL a que se refere o caput deste artigo será realizada pela USI no 1º dia útil após a expiração da medida cautelar.

Art. 62. A limitação do uso da REDE CORPORATIVA por usuários colaboradores, externos e visitantes pode ser realizada pela USI, a qualquer tempo.
Parágrafo único. A limitação de que trata o caput deste artigo deve ser comunicada ao usuário envolvido, e a respectiva liberação realizada no 1º dia útil após o término da limitação.

Art. 63. Os casos omissos serão analisados conjuntamente pela USI, ouvido o administrador do recurso de TI em questão.

Art. 64. Esta Resolução integra a Política de Segurança da Informação da AMPASS.

ANEXO III - Termo de Responsabilização e Sigilo
Pelo presente instrumento, eu_____, CPF _____, identidade _____, expedida pelo _____, em _____, DECLARO, sob pena
das sanções cabíveis, nos termos da legislação vigente, que conheço e estou comprometido com as práticas, responsabilidades e obrigações normativas referentes à Política de Segurança
da Informação da Autarquia Municipal de Previdência e Assistência à Saúde dos Servidores - AMPASS e à sua Regra de Uso dos Recursos de Tecnologia da Informação e Comunicação.

Recife, _____ de _____de 20__

Assinatura
Cargo/Função: _____