AUTAQUIA MUNICIPAL DE PREVIDÊNCIA E ASSISTÊNCIA À SAÚDE DOS SERVIDORES

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

(PSI AMPASS)

RECI SAÚDE PREV RECIFE

WWW.RECIPREV.RECIFE.PE.GOV.BR

MANOEL CARNEIRO SOARES CARDOSO
Diretor-Presidente

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DA AUTARQUIA MUNICIPAL DE PREVIDÊNCIA E ASSISTÊNCIA À SAÚDE DOS SERVIDORES (PSI AMPASS)

CAPÍTULO I
DISPOSIÇÕES PRELIMINARES

Art. 1º A Política de Segurança da Informação da Autarquia Municipal de Previdência e Assistência à Saúde dos Servidores (PSI Ampass) visa estabelecer os conceitos e diretrizes no que diz respeito à adoção de normas e procedimentos para garantir a segurança da informação, assegurando a continuidade dos serviços prestados com a redução dos riscos que possam interferir no alcance dos objetivos da Autarquia.

Art. 2º A PSI Ampass têm por finalidade:

I - estabelecer as estratégias e as definições de responsabilidades e competências para a implantação da gestão de segurança da informação;

II - 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;

III - fomentar o gerenciamento de riscos, prevenir e minimizar os impactos dos incidentes de segurança para que seja preservado o patrimônio não físico desta entidade;

e IV - 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 Autarquia.

Art. 3º Esta Política se aplica a todos os agentes públicos, colaboradores e visitantes que tenham acesso às instalações ou ambientes computacionais e a ativos de informação pertencentes ou sob custódia da Ampass, bem como a todos os sistemas de informação, processos corporativos e relacionamentos firmados entre a Autarquia e outros órgãos ou entidades, sejam públicas ou privadas.

Art. 4º Todas as medidas cabíveis devem ser tomadas para preservar a integridade e confidencialidade da informação, a fim de protegêlas de alteração, destruição ou divulgação não autorizada.

Art. 5º Para fins da PSI Ampass, considera-se:

I - 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;

II - alta administração: diretor-presidente, vice diretor-presidente e os gerentes imediatamente subordinados ao diretor-presidente e ao vice diretor-presidente;

III - ameaça: fatores externos ou causa potencial de um incidente de segurança da informação indesejado, que pode resultar em dano para um sistema ou organização;

IV - arquivo: local físico no qual fica armazenada a documentação da Ampass em fase intermediária;

V - ativos de informação: os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;

VI - autenticidade: garantia de que a informação é proveniente da fonte anunciada e que não foi alvo de mutações ao longo de um processo;

VII - autoridade classificadora: pessoa responsável por classificar, desclassificar, reclassificar e reavaliar informação classificada em qualquer grau de sigilo, de ofício ou sob demanda;

VIII - autoridade hierarquicamente superior: pessoa responsável, juntamente com a autoridade classificadora, por reavaliar informação classificada em qualquer grau de sigilo, de ofício ou sob demanda;

IX - classificação da informação: níveis e critérios estabelecidos para proteção das informações, com tabela de temporalidade para a guarda, de acordo com a importância da informação definida no Código de Classificação e Tabela de Temporalidade e Destinação de Documentos do Arquivo da Ampass;

X - Código de Classificação de Documentos da Ampass: é o esquema de distribuição de documentos em classes, de acordo com métodos de arquivamento específicos, elaborado a partir do estudo das estruturas e funções de uma instituição e da análise do arquivo por ela produzido;

XI - 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 Autarquia;

XII - confidencialidade: garantia de que a informação seja acessível somente pelas pessoas autorizadas;

XIII - disponibilidade: garantia de que a informação esteja disponível para as pessoas autorizadas sempre que se fizer necessária;

XIV - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD), segundo disposições da Lei Federal n.º 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados - LGPD), em especial o artigo 41;

XV - gestão documental: conjunto de procedimentos e operações técnicas referentes à produção, tramitação, uso, avaliação e arquivamento dos documentos em fase corrente e intermediária, visando a sua eliminação ou o seu recolhimento para guarda permanente;

XVI - informação: conjunto de dados organizados, processados ou não, que apresentam um conteúdo de valor e podem ser utilizados para produzir ou repassar conhecimento, contidos em qualquer meio, suporte ou formato;

XVII - integridade: garantia 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;

XVIII - legalidade: garantia de que as ações sejam realizadas em conformidade com os preceitos legais vigentes e que seus produtos sejam válidos juridicamente;

XIX - princípio do menor privilégio: limitação dos direitos de acesso dos usuários apenas ao que é estritamente necessário para a realização dos seus trabalhos;

XX - recursos de tecnologia da informação: microcomputadores, notebooks, tablets, servidores, celulares e smartphones, periféricos associados aos computadores (câmeras, mouse, teclado, caixa de som, microfones, etc.) e demais acessórios (scanners, impressoras a laser, jato de tinta, matriciais e térmicas, etc.), redes de comunicação de dados e voz e os equipamentos relacionados, câmeras de monitoramento e os equipamentos de controle de acesso, equipamentos de projeção e painel de chamada, os softwares desenvolvidos e disponibilizados pela Ampass, dados armazenados em equipamentos, dispositivos e periféricos e demais equipamentos relacionados à tecnologia da informação que venham a integrar o patrimônio da Ampass;

XXI - segurança da informação: conjunto de medidas eficazes para resguardar os recursos tecnológicos e viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações, garantindo que somente sejam acessadas por aqueles que devem conhecê-las, evitando seu uso indevido, inadequado, ilegal, ou em desconformidade com esta Política;

XXII - tabela de temporalidade: determina prazos e condições de guarda tendo em vista a transferência, recolhimento, descarte ou eliminação de documentos.

XXIII - usuário externo: pessoa física ou jurídica que tenha acesso concedido a informações produzidas ou recebidas pela Ampass e que não seja caracterizada como usuário interno;

e XXIV - usuário interno: empregado público, servidor público, contratado, estagiário ou conveniado da administração municipal que, no exercício de suas funções, tenham acesso a informações produzidas ou recebidas pelo Ampass.

CAPÍTULO II
DAS REGRAS GERAIS E DAS VEDAÇÕES

Art. 6º As informações, em formato físico ou lógico, e os recursos de tecnologia da informação utilizados pelos usuários são de exclusiva propriedade da Ampass ou da Prefeitura da Cidade do Recife, não podendo ser interpretados como de uso pessoal.

Art. 7º Todos os usuários internos e externos devem ter ciência de que o uso das informações e dos sistemas de informação da Ampass pode ser monitorado e que os registros assim obtidos poderão ser utilizados para detecção de violações desta Política e das Normas de Segurança da Informação, podendo servir de evidência para a aplicação de medidas disciplinares cabíveis, bem como para processos administrativos ou judiciais. Parágrafo único. Os usuários internos e os externos estão sujeitos a esta Política e às normas de segurança da informação.

Art. 8º Todo processo durante seu ciclo de vida, deve garantir, sempre que possível, a segregação de funções, por meio da participação de mais de uma pessoa ou equipe. Parágrafo único. 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.

Art. 9º O acesso às informações e o uso dos sistemas e aplicativos deverão ser feitos mediante identificação do usuário único, pessoal e intransferível, com utilização de senha de acesso.

§ 1º As informações devem ser utilizadas de forma transparente e apenas para a finalidade para a qual foi coletada.

§ 2º Cabe ao usuário a responsabilidade quanto ao sigilo das suas senhas de acesso aos recursos de tecnologia da informação e comunicação da Ampass.

Art. 10. É vedado a qualquer usuário da Ampass o uso dos recursos de tecnologia da informação 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 Autarquia ou

do Município do Recife, comprometendo a integridade, a confidencialidade, a confiabilidade, a autenticidade ou a disponibilidade das informações.

CAPÍTULO III
DA GESTÃO DE ACESSOS E DAS IDENTIDADES

Seção I
Normas Gerais

Art. 11. O acesso às informações e aos ambientes tecnológicos da Ampass deve ser controlado de acordo com a sua classificação, de forma a garantir acesso apenas às pessoas autorizadas, mediante aprovação formal do gestor da informação.

Parágrafo único. Os acessos dos usuários internos e dos externos devem ser solicitados e aprovados somente às informações necessárias ao desempenho de suas atividades.

Art. 12. O uso dos recursos de tecnologia da informação da Ampass deve ser passível de monitoramento e auditoria, devendo ser implementados e mantidos mecanismos que permitam sua rastreabilidade, acompanhamento, controle e verificação de acessos aos sistemas corporativos e à rede interna da Prefeitura da Cidade do Recife. Parágrafo único. Caso sejam identificadas mudanças ou fragilidades quanto ao uso de ativos de informações durante o monitoramento ou a auditoria, elas deverão ser reportadas imediatamente ao Comitê Gestor de Segurança da Informação (CGSI) da Ampass

Art. 13. A sistematização da gestão de acessos tem por objetivo garantir que o acesso à informação e aos recursos tecnológicos que a armazenam sejam franqueados exclusivamente a pessoas autorizadas, com base nos requisitos de negócio e de segurança da informação, sendo passível de monitoramento com vistas a garantir a rastreabilidade e a auditoria das ações realizadas.

Art. 14. Os sistemas que tratam informações restritas deverão ter, sempre que possível, mais de um fator de autenticação.

Seção II
Do Controle de Acessos

Art. 15. O controle de acesso, credenciais e perfis dos usuários deverá observar as seguintes operações, dentre outras que se façam necessárias:

I - por ocasião do ingresso dos usuários, mediante:

a) criação de perfis de usuários com nível de autorização adequados às atividades empenhadas;
b) concessão de credenciais de acesso;
c) acesso aos ativos e sistemas necessários à execução de suas atividades, proporcionando a rastreabilidade das ações realizadas;

e d) entrega de compromisso assinado de não divulgação de informações classificadas ou restritas a que venha a ter acesso, ainda que após o seu desligamento ou movimentação.

II - por ocasião do desligamento ou movimentação dos usuários, mediante:
a) exclusão dos respectivos perfis de usuários;
b) revogação das credenciais de acesso;
e c) devolução de todos os ativos de informação e recursos de tecnologia da informação da Ampass que estejam em sua posse.

Parágrafo único. Será considerado o princípio do menor privilégio na configuração das credenciais ou concessão de acesso aos ativos de informação.

Seção III
Da Segurança Física

Art. 16. A segurança física e patrimonial em relação à segurança da informação tem por objetivo prevenir danos e interferências nas instalações da Ampass que possam causar perda, roubo ou comprometimento das informações.

Art. 17. Será assegurado o controle de acesso e a salvaguarda das instalações e dos ativos de informação em que são elaborados, tratados, custodiados, manuseados ou guardados dados e informações críticas ou sensíveis, independentemente do meio em que estão armazenados.

CAPÍTULO IV
DA GESTÃO DE RISCOS E INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

Art. 18. A gestão de riscos de segurança da informação deve ser realizada de forma sistemática e contínua e englobar todos os ativos de informação da Ampass, visando a tratar riscos relacionados à disponibilidade, integridade, confidencialidade e autenticidade.

Art. 19. Aplicam-se à PSI Ampass, no que couber, os princípios e diretrizes de gestão de riscos definidos pela Resolução Ampass nº 03, de 05 de dezembro de 2019.

Art. 20. Em caso de violação desta Política, por ação ou omissão, intencional ou acidental, o CGSI realizará deliberações sobre os incidentes classificados como de alta criticidade.

§ 1º Os demais casos serão tratados pelo fluxo normal de resposta a incidentes.
§ 2º Após deliberações descritas no caput, o CGSI recomendará ao Diretor-Presidente da Ampass as ações a serem tomadas e este decidirá sobre sua procedência ou não observando o Código de Ética da Ampass, sem prejuízo de outras legislações vigentes.

Art. 21. Os contratos entre a Ampass e as empresas prestadoras de serviços com acesso às informações, aos sistemas e/ou ao ambiente tecnológico da Autarquia 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.

Art. 22. A 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.

CAPÍTULO V
DO TRATAMENTO E DA CLASSIFICAÇÃO DA INFORMAÇÃO

Art. 23. Toda informação institucional no âmbito da Ampass deve ser gerida adequadamente com o objetivo de garantir a sua disponibilidade, integridade, autenticidade e, quando aplicável, confidencialidade, independente do meio de armazenamento, processamento ou transmissão utilizado.

Art. 24. A segurança da informação deve ser prevista e realizada em todo o ciclo de vida dos dados, sendo apoiada pelo desenvolvimento de software seguro e sob governança efetiva dos dados.

Art. 25. Todos que tiverem acesso aos ativos de informação da Ampass devem utilizar preferencialmente as ferramentas de trabalho homologadas pela Unidade de Sistemas e Informações (USI) da Ampass, ainda que fora das dependências da Ampass.

Art. 26. O tratamento das informações pessoais deve considerar o respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais, conforme o disposto na Lei Federal n.º 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados - LGPD), na Lei Federal nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação - LAI) e na Lei Municipal nº 17.866, de 15 de maio de 2013 (Lei de Acesso à Informação do Município do Recife - LAI Recife).

Parágrafo único. O compartilhamento de dados com outros órgãos ou entidades da Administração Pública deve ser pautado na legislação vigente, considerando as restrições de acesso e sigilo, cabendo à Ampass definir os níveis adequados de segurança.

CAPÍTULO VI DO COMITÊ GESTOR DE SEGURANÇA DA INFORMAÇÃO (GCSI)

Art. 27. O Comitê Gestor de Segurança da Informação (CGSI) será composto por 03 (três) membros e seus respectivos suplentes, com mandato de 3 (três) anos, prorrogável por igual período. Parágrafo único. O CGSI será designado por meio de portaria do Diretor-Presidente da Ampass.

Art. 28. O CGSI reunir-se-á, conforme a necessidade, com o objetivo de acompanhar o andamento das ações relativas à segurança, por solicitação de qualquer de seus membros.

§ 1º As reuniões poderão ocorrer com a utilização de recursos de videoconferência ou outros meios similares que permitam a comunicação em tempo real.

§ 2º As votações serão realizadas de forma aberta e nominal e todos os membros titulares, ou suplentes em substituição, terão direito a voz e a voto.

§ 3º As decisões serão tomadas por maioria dos membros presentes à reunião.

§ 4º As deliberações do Comitê serão lavradas em atas, que devem ser redigidas com clareza.

§ 5º O CGSI proporá soluções ao Diretor-Presidente da Ampass, que decidirá.

CAPÍTULO VII
DOS DEVERES

Seção I
Dos Deveres de Todos os Usuários

Art. 29. São deveres de todos os usuários:

I - cumprir fielmente a política, as normas e os procedimentos de segurança da informação da Ampass;
II - assinar os Termos de Responsabilidade e Sigilo (Anexo III, da Resolução nº 01/2019) e os termos constantes nos anexos da Resolução nº 02, de 20 de agosto de 2020, que regulamentam o teletrabalho no âmbito da Ampass;
III - proteger as informações contra acessos, modificação, destruição ou divulgação não autorizados pela Ampass;
IV - assegurar que os recursos tecnológicos, as informações e sistemas a sua disposição sejam utilizados apenas para as finalidades aprovadas pela Ampass;
V - manter, nas unidades de armazenamento de rede, apenas arquivos que estejam estritamente relacionados às atividades desempenhadas pela Ampass, sendo vedada a gravação de arquivos de músicas, fotos, vídeos e outros, que não atendam a tal finalidade;
VI - tratar os dados dos sistemas informatizados em conformidade com os princípios e práticas dispostos na Lei Federal n.º 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados - LGPD);
VII - cumprir as leis e as normas que regulamentam a propriedade intelectual;
VIII - garantir a segurança das informações da administração municipal a que tenham acesso;
IX - utilizar as senhas utilizadas de acordo com as diretrizes fixadas no Anexo II, da Resolução nº 01/2019;
X - não discutir assuntos confidenciais de trabalho em ambientes públicos ou em áreas expostas, incluindo a emissão de comentários e opiniões em blogs e redes sociais;
XI - não compartilhar informações confidenciais de qualquer tipo;

XII - colaborar com alertas, sugestões e críticas que possam melhorar a segurança da informação;
e XIII - comunicar imediatamente ao CGSI e ao seu superior hierárquico, 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.
Parágrafo único. Após a assinatura dos termos citados no inciso II, o usuário assume formalmente a responsabilidade pelo bom uso dos ativos de informações, o compromisso de seguir a PSI Ampass e de manter o sigilo, em caráter permanente, sobre todos os ativos de informações, mesmo após o seu desligamento ou término de prestação de serviços.

Seção II
Dos Deveres do Comitê Gestor de Segurança da Informação

Art. 30. São deveres do Comitê Gestor de Segurança da Informação (CGSI):
I - assessorar na implementação das ações de segurança da informação e comunicações na Ampass;
II - propor soluções específicas sobre segurança da informação e comunicações;
III - propor normas e procedimentos internos relativos à segurança da informação e comunicações, em conformidade com as legislações existentes sobre o tema;
e IV - realizar deliberações sobre os incidentes classificados como de alta criticidade.

Seção III
Dos Deveres do Setor de Gestão de Segurança da Informação

Art. 31. São deveres do setor de gestão de segurança da informação:
I - promover ações de segurança da informação e comunicações para conscientização da PSI Ampass;
II - promover ampla divulgação da Política e das Normas de Segurança da Informação para todos os usuários internos e externos;
III - propor normas, projetos e iniciativas relativas à segurança da informação e comunicações e ao seu aperfeiçoamento;
IV - definir, implementar e revisar os controles;
V - identificar os riscos inerentes e residuais da segurança da informação;
VI - avaliar os procedimentos de segurança, analisar os seus resultados e discutir as melhorias necessárias em relação a eles;
VII - definir soluções de segurança antes da sua implementação, bem como revisar as soluções durante a sua manutenção;
VIII - elaborar programas de treinamento para capacitação de usuários e proprietários da informação;
IX - desenvolver, implementar e manter planos de continuidade de tecnologia da informação que visam garantir as operações em casos de desastre e indisponibilidade dos sistemas de informação;
X - programar, executar e gerenciar as rotinas de backups;
XI - gerir os ativos da rede;
XII - definir requisitos e especificar instruções para utilização do teletrabalho;

XIII - prestar assessoramento técnico à alta administração da Ampass e ao encarregado em assuntos referentes à Lei Federal n.º 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados - LGPD);
XIV - acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;
e XV - gerir a infraestrutura de hardware e software necessária à prestação dos serviços de acesso à rede interna e à internet, sendo vedada a instalação de qualquer equipamento no âmbito da Ampass, salvo prévia autorização.

Seção IV
Dos Deveres do Encarregado

Art. 32. São deveres do encarregado:

I - garantir o cumprimento da LGPD na Ampass;
II - informar ao CGSI e a alta administração da Autarquia acerca de qualquer ocorrência referente ao descumprimento de norma da LGPD;
III - tomar as medidas adequadas, dentro de sua esfera de competência, para cessar qualquer descumprimento à LGPD;
IV - informar à alta administração da Autarquia sobre atualizações e outras informações pertinentes referentes à LGPD;
e V - intermediar a comunicação entre a Autoridade Nacional de Proteção de Dados (ANPD), os usuários dos serviços e a Ampass na qualidade de controladora de dados.

Seção V
Dos Deveres Da Alta Administração

Art. 33. São deveres da alta administração da Ampass:
I - definir as responsabilidades pela segurança da informação, nas descrições dos cargos e funções, bem como nos termos e condições das contratações que envolvam o manuseio de dados, informações ou conhecimentos da Ampass;
II - promover ações para que todos os usuários sejam conscientizados e treinados nos procedimentos de segurança da informação;
III - assegurar que o controle operacional de uma atividade crítica não seja de atribuição exclusiva de uma única pessoa;
IV - assegurar que quando houver afastamento, mudança de responsabilidades e de lotação ou, ainda, mudança de atribuições dentro da Autarquia ocorra imediata revisão dos direitos de acesso e uso dos ativos;
V - assegurar que quando da efetivação do desligamento de usuário, deverão ser extintos todos os direitos de acesso e uso dos ativos a ele atribuído;
e VI - assegurar que todo o ativo produzido por um usuário desligado seja mantido pela Ampass, garantindo o reconhecimento e o esclarecimento da propriedade do acervo para a Instituição.

Seção VI
Dos Deveres Do Setor de Gestão Documental

Art. 34. São deveres do setor de gestão documental da Ampass:

I - realizar a gestão documental da Autarquia, bem como orientar os setores internos acerca de procedimentos para acesso à documentação, empréstimos, consultas, arquivamentos, acondicionamentos e classificação da informação dos documentos em meios físicos e digitais, observados os dispostos no Diagnóstico da Massa Documental e no Código de Classificação e Tabela de Temporalidade da Ampass;
II - garantir, por meio da criação e implantação de procedimentos, a integridade, autenticidade, disponibilidade, não repúdio e a confidencialidade dos documentos/processos físicos, digitais e híbridos, produzidos ou recebidos pela Ampass, desde a sua entrada até o seu arquivamento e acondicionamento;
III - opinar sobre a informação produzida no âmbito de sua atuação para fins de classificação em qualquer grau de sigilo;
IV - assessorar a autoridade classificadora ou a autoridade hierarquicamente superior quanto à classificação, desclassificação, reclassificação ou reavaliação de informação classificada em qualquer grau de sigilo, conforme Código de Classificação e Tabela de Temporalidade da Ampass;
e V - propor o destino final das informações desclassificadas, indicando os documentos para a guarda permanente, conforme Código de Classificação e Tabela de Temporalidade da Ampass.

CAPÍTULO VIII
DISPOSIÇÕES FINAIS

Art. 35. Na ocorrência de violação desta Política ou das normas de segurança da informação, o Diretor-Presidente da Ampass poderá adotar, com o apoio da alta administração, sanções administrativas e/ou legais.
Art. 36. A Ampass se reserva ao direito de revisar, adicionar, modificar ou atualizar a Política de Segurança da Informação, periodicamente, no máximo a cada 2 (anos), para aprimorar e garantir o perfeito funcionamento das normas e regras.
Art. 37. Os casos omissos serão analisados pelo setor de segurança da informação, que deverá propor solução ao Diretor-Presidente da Ampass.
Art. 38. As normas e procedimentos da PSI Ampass 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.
Art. 39. A implementação da PSI Ampass será feita de forma gradual, de acordo com a disponibilidade técnica, recursos humanos, tecnológicos e financeiros, cujas ações serão priorizadas em virtude de seu grau de relevância, criticidade e impacto e em função dos investimentos envolvidos.

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: _____