PREFEITURA DE

CARUARU

PSI

2019 - 2020

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

PREFEITURA DE
CARUARU

SECRETARIA DE ADMINISTRAÇÃO

PORTARIA SAD Nº 79/2019

O Secretário de Administração do Município de Caruaru, Estado de Pernambuco, no uso das atribuições, RESOLVE:

Publicar a Política de Segurança da Informação (PSI) para o biênio 2019/2020.

Caruaru/PE, em 26 de abril de 2019

PSI - POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

DOCUMENTO DE DIRETRIZES E NORMAS

Versão 1.0

PREFEITURA MUNICIPAL DE CARUARU SECRETARIA DE ADMINISTRAÇÃO
COORDENADORIA GERAL DE PROCESSAMENTO DE DADOS

CARUARU

SUMÁRIO

1. OBJETIVOS

A PSI (Política de Segurança da Informação) é um documento que estabelece as diretrizes e normas de segurança que visa proteger a integridade, disponibilidade, conformidade e autenticidade dos dados e informações de uma instituição pública ou privada. Consiste num conjunto de ações técnicas e boas práticas relacionadas ao uso seguro de dados. Trata-se de um documento que determina ações importantes para garantir a segurança da informação. As melhores práticas relacionadas à governança de TI recomendam a implantação de uma política de segurança como um dos instrumentos para realizar uma gestão eficiente dos recursos da área de TI.

Esta PSI fundamenta-se nas recomendações da norma ABNT NBR ISO/IEC 27002:2005, reconhecida mundialmente como um código de prática para a gestão da segurança da informação, bem como está de acordo com as leis vigentes em nosso país.

Tem por objetivo:

1. Estabelecer diretrizes que permitam aos Servidores e Colaboradores da Prefeitura Municipal de Caruaru seguirem padrões de comportamento que contribua com à segurança da informação preservando as informações quanto a:

    - **Integridade:** garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais.
    - **Confidencialidade:** garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.
    - **Disponibilidade:** garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

2. Desenvolver um comportamento ético/profissional quanto a utilização das ferramentas de TI e as informações por elas geradas visando reduzir ameaças através da adoção de medidas preventivas para evitar possíveis incidentes que podem trazer prejuízos à Prefeitura Municipal de Caruaru.

2. TERMOS E DEFINIÇÕES

Ação de evitar o risco – Decisão de não se envolver ou agir de forma a se retirar de uma situação de risco. (NBR ISO/IEC 27005, 2008)

Aceitar/Reter o risco - Aceitação do ônus da perda ou do benefício do ganho associado a um determinado risco. (NBR ISO/IEC 27005, 2008)

Ameaça – Causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização. (ISO/IEC 27000, 2014)

Ativo - Qualquer coisa que tenha valor para a organização. (NBR ISO/IEC 27002, 2005)

Ativos Críticos de Tecnologia da Informação – São os Ativos de Tecnologia da Informação indispensáveis aos processos diretamente relacionados aos objetivos estratégicos da Instituição.

Ativo de Informação – Dados, informações e conhecimentos obtidos, gerados, tratados e/ou armazenados como por exemplos base de dados, arquivos, contratos, acordos, documentação de sistema, informações sobre pesquisa, manuais de usuário, material de treinamento, procedimentos e planos institucionais, processos de trabalho entre outros.

Ativo de Tecnologia da Informação – Composto por ativos de software e ativos físicos, permitindo o armazenamento, a transmissão e processamento das informações. Como exemplo: ativos de software - aplicativos, sistemas, ferramentas de desenvolvimento e utilitários. Exemplo Ativos físicos - os equipamentos computacionais fixos e móveis, equipamentos utilizados Política de Segurança da Informação e Comunicações para comunicação de dados e mídias removíveis.

Conformidade - Estar de acordo com determinadas normas, regras ou preceitos.

Contas de Serviço - Contas de acesso à rede corporativa de computadores necessários a um procedimento automático (aplicação, script, etc.), sem qualquer intervenção humana no seu uso.

Controle de Acesso - Conjunto de procedimentos, recursos e meios utilizados com a finalidade de garantir que os acessos aos ativos só ocorrerão após autorização e serão restritos, baseados nos requisitos de segurança e nas atividades do usuário. (ISO/IEC 27000, 2014)

Credenciais ou Contas de Acesso - Identificação única, concedida de forma pessoale intransferível a uma pessoa, em conjunto com um método de autenticação. Esse par de informações habilita o seu dono a acessar equipamentos, sistemas e aplicações específicas, de acordo com o perfil definido.

Classificação da Informação – Identificação do nível de proteção requerido pela informação, atribuído por autoridade competente.

Confidencialidade – Nenhuma informação estará disponível ou será divulgada a entidades (pessoas, sistemas ou órgãos) não autorizadas.

Colaborador – Servidores, empregados, contratados por tempo determinado, estagiários e prestadores de serviços que exercem atividades no âmbito da Prefeitura Municipal de Caruaru.

Criticidade – Medida de risco obtida da combinação entre o possível impacto na Instituição ou em um projeto e a probabilidade de ocorrência de um evento que afete o mesmo.

Custodiante do Ativo - Unidade administrativa responsável pelo armazenamento, operação, administração e preservação de ativos.

Custodiante da Informação – Servidor e/ou Colaborador responsável pela guarda adequada do dado.

Divulgação - Ato de tornar público o resultado de uma pesquisa.

Equipe de Tratamento de Incidentes - Grupo de pessoas com a responsabilidade de analisar, tratar e documentar os incidentes de segurança nas redes de computadores, e o tratamento aplicado.

Gestor - Unidade administrativa responsável por gerenciar determinado segmento de dados e todos os ativos relacionados.

Incidente - Um ou mais eventos indesejados ou inesperados que podem causar algum dano, colocando em risco os ativo(s) de informação do IBGE, com probabilidade de interromper ou afetar a qualidade dos serviços e/ou atividades da Instituição.

Infraestrutura de TI - Instalações prediais, equipamentos, computadores, software, redes, telecomunicações, sistemas de armazenamento e recuperação de dados, aplicações computacionais, cabeamento e rede telefônica.

Mitigar/Reduzir o risco – Efetuar ações que reduzam a probabilidade, consequências negativas, ou ambas, associadas a um risco. (NBR ISO/IEC 27005, 2008)

Política – Intenções e diretrizes da organização, formalmente expressas pela direção da Instituição. (ISO/IEC 27000, 2014)

Risco – Efeito da incerteza sobre os objetivos de segurança da informação e é associado com o potencial que as ameaças explorarão vulnerabilidades de um ativo de informação ou grupo de ativos de informação e, assim, causar danos a uma organização. (ISO/IEC 27000, 2014)

Segurança da Informação - Preservação da confidencialidade, da integridade e da disponibilidade das informações. (ISO/IEC 27000, 2014)

Sigilo – Confidencialidade, segredo.

Transferir o risco – Compartilhamento com uma outra entidade do ônus da perda ou do benefício do ganho associado a um risco. (NBR ISO/IEC 27005, 2008)

Vulnerabilidade – Fragilidade de um ativo ou controle que pode ser explorada por uma ou mais ameaças. (ISO/IEC 27000, 2014)

3. PRINCÍPIOS

Este PSI considerou alguns conceitos de Segurança da Informação definidos na Norma ISO/IEC 27000, de 15.01.2014.

3.1 Atualidade – As normas e procedimentos devem ser constantemente atualizados, de modo a refletir as mudanças legais, sociais e tecnológicas que interferem na sua aplicabilidade;

3.2 Aplicabilidade – Os processos de segurança devem ser coordenados e integrados entre si e incorporados nos processos de trabalho e práticas de todas as unidades da Prefeitura Municipal de Caruaru;

3.3 Autenticidade – Toda informação terá sua origem certificada;

3.4 Clareza – Todas as normas e procedimentos de segurança produzidos devem ser claros o suficiente para que todos os envolvidos com a informação entendam suas responsabilidades, seus direitos e limites;

3.5 Conhecimento – Os Servidores devem ser continuamente capacitados para o desenvolvimento da cultura de segurança da informação;

3.6 Confidencialidade – Nenhuma informação estará disponível ou será divulgada a entidades (pessoas, sistemas ou órgãos) não autorizadas;

3.7 Disponibilidade – Toda informação estará disponível e poderá ser utilizada sob demanda por entidade autorizada (pessoa, sistema ou órgão);

3.8 Integridade – Os ativos de informação deverão ser protegidos garantindo que os mesmos só serão alterados de forma autorizada e não acidental.

4. DIRETRIZES

As diretrizes da PSI (Política de Segurança da Informação) estão alinhadas com as seguintes diretrizes do PDTI (Plano Diretor de Tecnologia da Informação) da Prefeitura Municipal de Caruaru.

D1 - Promover a governança de TI.

D7 - Promover a melhoria dos sistemas de informação.

D11 - Garantir a segurança da informação e comunicações.

D13 - Manter os processos internos de TI mapeados, formalizados, mensurados e otimizados.

As diretrizes da PSI deverão ser seguidas por todos os servidores públicos da Prefeitura Municipal de Caruaru no exercício de suas ou qualquer pessoa ou empresa que venha a ter acesso a dados ou informações em qualquer meio ou suporte.

4.1 Toda informação gerada pelos Servidores e/ou Colaboradores, utilizando integralmente ou parcialmente recursos da Prefeitura Municipal de Caruaru, é de propriedade do órgão;

4.2 Todos os mecanismos de proteção utilizados para a segurança da informação devem ser mantidos para preservar a continuidade do negócio;

4.3 Ameaças e riscos devem ser reavaliados periodicamente para garantir que a organização esteja efetivamente protegida.

4.4 O acesso às informações, produzidas ou recebidas deve ser limitado às atribuições necessárias ao desempenho das respectivas atividades dos usuários internos;

4.5 Os processos de aquisição ou contratação de bens e serviços de tecnologia da informação, devem refletir esta PSI, sem prejuízo da observância da legislação em vigor;

4.6 Os equipamentos de informática e comunicação, sistemas e informações deverão ser utilizados para a realização das atividades profissionais.

4.7 Esta política de Segurança da Informação pode ser revisada periodicamente e eventualmente revista sempre que eventos ou fatos relevantes ocorram;

4.8 Os Servidores e/ou Colaboradores devem evitar a circulação das informações e/ou mídias consideradas confidenciais e/ou restritas, como também não deixar relatórios nas impressoras, e mídias em locais de fácil acesso;

4.9 Esta política dá ciência a cada colaborador de que os ambientes, sistemas, computadores e redes do órgão poderão ser monitorados e gravados conforme previsto nas leis brasileiras.

4.10 É também obrigação de cada colaborador se manter atualizado em relação a esta PSI e aos procedimentos e normas relacionadas, buscando orientação do seu gestor ou da área de tecnologia da informação sempre que não estiver absolutamente seguro quanto à aquisição, uso e/ou descarte de informações.

5. RESPONSABILIDADES

5.1 Dos Servidores e Colaboradores

5.1.1 É de inteira responsabilidade de cada Servidor/Colaborador, todo prejuízo ou dano que vier a sofrer ou causar a Prefeitura Municipal de Caruaru ou a terceiros, em decorrência da não obediência às diretrizes e normas aqui referidas.

5.2 Dos Gestores de Pessoas e/ou Processos

5.2.1 É responsabilidade dos Gestores de Pessoas e/ou Processo ter postura exemplar em relação à segurança da informação, servindo como modelo de conduta para os colaboradores sob a sua gestão.

5.2.2 É responsável por atribuir aos colaboradores, na fase de contratação e de formalização dos contratos individuais de trabalho, de prestação de serviços ou de parceria, a responsabilidade do cumprimento da PSI da Prefeitura Municipal de Caruaru.

5.2.3 O Gestor deve exigir dos colaboradores a assinatura do Termo de Compromisso e Ciência, assumindo o dever de seguir as normas estabelecidas.

5.2.4 Antes de conceder acesso às informações restritas da instituição, exigir a assinatura do Acordo de Confidencialidade dos colaboradores casuais e prestadores de serviços.

5.2.5 Adaptar as normas, os processos, procedimentos e sistemas sob sua responsabilidade para atender a esta PSI.

5.3 Do Núcleo de Gestão de Pessoas da PMC

5.3.1 Informar ao setor de tecnologia da informação todos os desligamentos, afastamentos, retornos e modificações no quadro funcional da PMC.

5.4 Dos Custodiantes da Informação (Área de Tecnologia da Informação)

5.4.1 Configurar os equipamentos, ferramentas e sistemas concedidos aos Servidores com todos os controles necessários para cumprir os requerimentos de segurança estabelecidos por esta PSI.

5.4.2 Garantir que as informações de um usuário não serão removidas de forma irrecuperável antes de disponibilizar o ativo para outro usuário no caso de movimentação interna dos ativos de TI.

5.4.3 Promover cultura de segurança da informação e comunicações;

5.4.4 Supervisionar, analisar e avaliar a eficácia dos controles de segurança utilizados e informar aos gestores os riscos residuais.

5.4.5 Acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;

5.4.6 Implantar controles que gerem registros auditáveis que permitam a rastreabilidade para fins de auditoria ou investigação.

5.4.7 Administrar, proteger e testar as cópias de segurança dos programas e dados relacionados aos processos críticos e relevantes para o Prefeitura Municipal de Caruaru.

5.4.8 Realizar e acompanhar estudos de novas tecnologias, quanto a possíveis impactos na segurança da informação e comunicações;

5.4.9 Planejar e coordenar a execução dos programas, planos, projetos e ações de segurança da informação;

5.4.10 Planejar, implantar e monitorar a capacidade de armazenagem, processamento e transmissão necessários para garantir a segurança requerida pelas áreas de negócio.

5.4.11 Atribuir a cada servidor/colaborar conta de acesso (individual) a computadores, dispositivo, sistemas, bases de dados ou a qualquer outro ativo de informação que se fizer necessário para realização de suas atividades, tornando possível identifica-lo como responsável por suas ações.

5.4.12 Realizar analise para mitigação do risco;

5.4.13 Criar perfis de acesso a fim de restringir ao mínimo necessário os poderes de cada indivíduo.

5.4.14 Garantir segurança especial para sistemas com acesso público, fazendo guarda de evidências que permitam a rastreabilidade para fins de auditoria ou investigação.

5.4.15 Proteger continuamente todos os ativos de informação da empresa contra código malicioso, e garantir que todos os novos ativos só entrem para o ambiente de produção após estarem livres de código malicioso e/ou indesejado.

5.4.16 Definir as regras para instalação de software e hardware em ambiente de produção corporativo.

5.4.17 Monitorar o ambiente de TI registrando incidentes de segurança (vírus, trojans, furtos, acessos indevidos, e assim por diante);

5.4.18 Garantir que todos os servidores e estações de trabalho tenham instalados políticas de segurança e antivírus corporativo atualizados.

5.4.19 Garantir, da forma mais rápida possível, com solicitação formal, o bloqueio de acesso de usuários por motivo de desligamento da empresa, incidente, investigação ou outra situação que exija medida restritiva para fins de salvaguardar os ativos de informação da PMC.

6. POLÍTICAS

6.1 Controle de Acesso Lógico

6.4.1 A conta de acesso é o instrumento para identificação do usuário na rede da PMC sendo individual e o seu compartilhamento não permitido. O responsável pela conta de acesso responde por toda e qualquer ação realizada mediante utilização de sua conta de acesso.

6.4.2 A concessão de privilégios de acesso deve ser realizada em conformidade com o princípio do privilégio mínimo, ou seja, cada credencial de acesso deve possuir apenas o conjunto de privilégios estritamente necessários ao desempenho das suas atribuições profissionais.

6.4.3 A concessão de acesso remoto a ativos de tecnologia da informação, deve ser precedida de autorização do custodiante do ativo, após análise da justificativa fornecida pelo gestor explicitando a necessidade do acesso. Este acesso deve contemplar somente os ativos necessários à realização do serviço, utilizar canal seguro e ser concedido em caráter provisório.

6.4.4 Cabe ao gestor responsável por pessoas ou processos, solicitar por ofício ou e-mail corporativo ao setor de TI, a concessão de permissão de acesso ao sistema em questão, bem como informar alterações de atribuições dos colaboradores imediatamente para adequação dos privilégios de acesso.

6.4.5 Todas as senhas, de usuários comuns, para autenticação na rede da PMC devem seguir os seguintes critérios mínimos:

6.4.6 A senha deve ser constituída de, no mínimo, 8 caracteres sendo obrigatório o uso de caracteres alfanuméricos (letras e números), utilizando caracteres especiais (@ # $ %) e variação entre caixa-alta e caixa-baixa (maiúsculo e minúsculo) sempre que possível;

6.4.7 A senha não deve ser baseada em informações pessoais, como próprio nome, data de nascimento, etc.

6.4.8 A data de expiração da senha deve ser de no máximo 90 dias, caso não seja alterada, esta será bloqueada;

6.4.9 Será obrigatória a troca de senha ao efetuar o primeiro logon;

6.4.10 A base de dados de senhas deve ser armazenada com criptografia;

6.4.11 Caso o colaborador esqueça sua senha, ele deverá requisitar formalmente a troca ou comparecer pessoalmente à área técnica responsável para cadastrar uma nova.

6.4.12 Qualquer anormalidade percebida pelo usuário quanto ao privilégio de seu acesso aos recursos de tecnologia da informação deve ser imediatamente comunicada a Gerência de Tecnologia da Informação;

6.4.13 As contas com privilégio de administração de rede devem ser utilizadas somente para execução das atividades correspondentes à administração do ambiente conforme as responsabilidades atribuídas. As variáveis necessárias para acesso e administração devem ser de conhecimento restrito aos administradores dos equipamentos de rede.

6.4.14 Em caso de comprometimento comprovado da segurança do ambiente de TI por algum evento não previsto, todas as senhas de acesso deverão ser modificadas.

6.2 Acesso à Internet

A Política de Acesso à Internet estabelece princípios, direitos, deveres, regras e procedimentos para o uso dos recursos corporativos de Internet, disponibilizados como ferramenta de trabalho para a produção dos serviços institucionais, para a realização de consultas, pesquisas, intercâmbio de dados, ideias e informações em apoio aos projetos, atividades e eventos de interesse da Instituição.

Tem como princípio assegurar que seu uso não viole os aspectos éticos e legais e que seja efetuado de forma segura para assegurar a devida proteção contra riscos à segurança das informações institucionais. Este acesso pode ser revogado nos casos de ameaça iminente a qualquer ativo, por desrespeito Política de Segurança da Informação e por necessidade de serviço.

Fica assim estabelecido que:

6.2.1 É vedado acessar páginas de conteúdo considerado ofensivo, ilegal ou impróprio, tais como: Pornografia, pedofilia, preconceitos, vandalismo, entre outros;

6.2.2 É vedado acessar ou obter na Internet arquivos que apresentem vulnerabilidade de segurança ou possam comprometer, de alguma forma, a segurança e a integridade da rede da PMC;

6.2.3 Utilizar os recursos da PMC para fazer o *download* ou instalação de software ou dados não legalizados;

6.2.4 É vedado também:

- 6.2.4.1 O uso recreativo da internet em horário de expediente;
- 6.2.4.2 Uso de proxy anônimo;
- 6.2.4.3 Acesso a rádio e TV em tempo real, exceto os canais corporativos em horário de expediente;
- 6.2.4.4 Acesso a jogos;
- 6.2.4.5 Acesso a outros conteúdos notadamente fora do contexto do trabalho desenvolvido;
- 6.2.4.6 Envio a destino externo de qualquer software licenciado à PMC;
- 6.2.4.7 Tentar burlar às políticas de bloqueios automaticamente aplicadas pelas ferramentas sistêmicas da PMC;
- 6.2.4.8 Utilização de softwares de compartilhamento de conteúdo na modalidade peer-to-peer (P2P);

6.2.5 Haverá bloqueios de acesso a arquivos e sites não autorizados que comprometam o uso de banda da rede, o desempenho e produtividade das atividades, bem como, que exponham a rede a riscos de segurança;

6.2.6 Caso a PMC julgue necessário haverá auditoria dos sites acessados por usuário para verificação da adequação à política vigente, comprovada a utilização irregular, o usuário envolvido poderá ter o seu acesso à Internet bloqueado, sendo comunicado o fato à chefia imediata, podendo incorrer em processo administrativo disciplinar e nas sanções legalmente previstas, assegurados o contraditório e a ampla defesa.

6.3 Uso do e-mail Corporativo

O objetivo desta norma é informar aos colaboradores do Prefeitura Municipal de Caruaru quais são as atividades permitidas e proibidas quanto ao uso do e-mail corporativo.

O e-mail corporativo da Prefeitura Municipal de Caruaru é para uso relacionados às atividades do servidor no desempenho de sua função.

É portanto, vedado aos servidores o uso do serviço de correio eletrônico corporativo com o objetivo de:

6.3.1 Praticar crimes e infrações de qualquer natureza;
6.3.2 Executar ações nocivas contra outros recursos computacionais da PMC ou de redes externas;
6.3.3 Distribuir material obsceno, pornográfico, ofensivo, preconceituoso, discriminatório, ou de qualquer forma contrário à lei e aos bons costumes;
6.3.4 Disseminar anúncios publicitários, mensagens de entretenimento e mensagens do tipo "corrente", vírus ou qualquer outro tipo de programa de computador que não seja destinado ao desempenho de suas funções ou que possam ser considerados nocivos ao ambiente de rede da PMC;
6.3.5 Enviar arquivos de áudio, vídeo ou animações, salvo os que tenham relação com as funções institucionais desempenhadas pela PMC;
6.3.6 Enviar mensagens que inclua material protegido por direitos autorais sem a permissão do detentor dos direitos.
6.3.7 Divulgar, no todo ou em parte, os endereços eletrônicos corporativos constantes do catálogo de endereços do serviço;
6.3.8 Enviar qualquer mensagem por meios eletrônicos que torne seu remetente e/ou o Prefeitura Municipal de Caruaru ou suas unidades vulneráveis a ações civis ou criminais;
6.3.9 Divulgar informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização expressa e formal concedida pelo proprietário desse ativo de informação;
6.3.10 Executar outras atividades lesivas, tendentes a comprometer a intimidade de usuários, a segurança e a disponibilidade do sistema, ou a imagem institucional.

É de responsabilidade do usuário do correio eletrônico:

6.3.11 Manter em sigilo sua senha de acesso ao correio eletrônico;
6.3.12 Fechar o aplicativo de correio (cliente) toda vez que se ausentar, evitando o acesso indevido;
6.3.13 Comunicar imediatamente a Gerência de Tecnologia da Informação, recebimento de mensagens com vírus ou que venham a trazer algum tipo de dano aos sistemas de informática;
6.3.14 Efetuar a manutenção de sua caixa postal, evitando ultrapassar o limite de armazenamento e garantindo o seu funcionamento contínuo.

6.4 Uso de Equipamentos de Informática

O objetivo desta seção é estabelecer critérios na utilização dos equipamentos de informática na Prefeitura Municipal de Caruaru, sendo estas:

6.4.1 Os recursos computacionais somente devem ser utilizados para a execução de atividades de interesse da PMC;

6.4.2 Cada estação de trabalho possui controle de IP (Protocol Internet), os quais permitem que ela seja identificada na rede. Sendo assim, tudo que for executado na estação de trabalho será de responsabilidade do usuário;

6.4.3 Não é permitido gravar nas estações de trabalho e na Rede da PMC: MP3, filmes, fotos e software com direitos autorais ou qualquer outro tipo que possa ser considerado pirataria;

6.4.4 Todos os dados relativos às atividades da Secretaria devem ser mantidos no Servidor de Arquivos, onde existe sistema de backup diário e confiável;

6.4.5 Os arquivos gravados em diretórios temporários (pastas públicas) podem ser acessados por todos os usuários que utilizarem a rede local, portanto não garante sua integridade, podendo ser alterados ou excluídos sem prévio aviso e por qualquer usuário;

6.4.6 Não será feito cópia de segurança dos arquivos criados no computador local dos colaboradores. O próprio usuário deve fazer cópia de segurança dos arquivos locais e verificar o que pode ser eliminado, evitando acumulo de dados desnecessários;

6.4.7 É proibida a abertura de computadores para qualquer tipo de reparo, caso seja necessário o reparo deverá ocorrer pelo suporte técnico de TI da PMC;

6.4.8 Quanto à utilização de equipamentos de informática particulares (celulares, notebooks, tablets e/ou qualquer dispositivos móveis que venham acessar a rede sem fio ou rede estruturada) o colaborador deverá comunicar a chefia imediata, que solicitará sua liberação de acesso através da Gerência de Tecnologia da Informação;

6.4.9 Em caso de dano, inutilização ou extravio do equipamento o colaborador deverá comunicar imediatamente à Gerência de Tecnologia da Informação que deverá adotar as providências cabíveis;

6.4.10 Em caso de furto ou roubo, providenciar Boletim de Ocorrência junto à Polícia Civil e entregá-lo na Gerência de Tecnologia da Informação, que deverá adotar as providências cabíveis;

6.4.11 É proibida a colocação de adesivos com imãs nos equipamentos;

6.4.12 É dever do colaborador zelar pela integridade do equipamento estritamente como instrumento de trabalho, juntamente com os acessórios que foram utilizados;

6.4.13 É de inteira responsabilidade do colaborador ao receber o Termo de Responsabilidade, verificar as informações nele contidas como Tombamento, série, além dos seus dados pessoais, matrícula e unidade de trabalho;

6.4.14 Não é permitido alterar as configurações de rede e da BIOS das máquinas, bem como, efetuar qualquer modificação que possa causar algum problema futuro;

6.4.15 Fica proibida a utilização, sem devido consentimento, da utilização de equipamentos de informática por pessoas sem vínculo com a Prefeitura Municipal de Caruaru;

6.4.16 É vedado retirar e/ou danificar placas identificadoras de patrimônio, travas e lacres de segurança dos equipamentos de informática;

6.4.17 Não é permitido conectar e/ou configurar equipamento à rede, sem a prévia liberação da Gerência de Tecnologia da Informação;

6.4.18 O antivírus deve estar atualizado e com a autoproteção ativa na estação de trabalho;

6.4.19 Os equipamentos considerados críticos ao desempenho das atividades da PMC devem ser armazenados em áreas apropriadas, com acesso restrito e, sempre que possível, controlado por dispositivos de identificação.

6.4.20 O acesso de colaboradores/visitantes às áreas que hospedam equipamentos críticos deverá ser autorizado pelo custodiante e acompanhado de um servidor público. A restrição de acesso deve estar alinhada aos riscos identificados.

7. MONITORAMENTO E AUDITORIA

O monitoramento e auditoria consiste na verificação e avaliação dos sistemas e procedimentos internos com o objetivo de garantir a segurança da informação e a imagem da instituição.

A Prefeitura Municipal por intermédio da Coordenadoria Geral de Processamento de Dados tem o direito de monitorar e registrar o acesso e utilização dos dados armazenados ou em trânsito sob sua custódia, bem como o uso dos equipamentos, com o objetivo de zelar pelo fiel cumprimento da Política de Segurança da Informação.

8. CONSIDERAÇÕES FINAIS

O PSI da Prefeitura Municipal de Caruaru se aplica a todos os servidores e colaboradores que utilizam os recursos tecnológicos da PMC e abrange toda a infraestrutura TI de todas as unidades municipais.

As politicas de segurança definidas nesta PSI devem ser publicadas e amplamente promovida visando garantir a integridade dos dados e informações, e o comprometimento dos servidores quanto ao uso correto dos recursos de TI disponibilizados pela Prefeitura Municipal de Caruaru.

A PSI será revisada anualmente pela Coordenadoria Geral de Processamento de Dados e submetida à aprovação da Secretaria de Administração.

Cabe a Coordenadoria Geral de Processamento de Dados dar suporte as diligencias relativas a segurança da informação providas por auditorias internas ou externas.