DECRETO Nº 157, DE 21 DE NOVEMBRO DE 2017

INSTITUI A POLÍTICA DE SEGURANÇA DA INFORMAÇÃO NO ÂMBITO DA ADMINISTRAÇÃO MUNICIPAL E DÁ OUTRAS PROVIDÊNCIAS

O **PREFEITO MUNICIPAL DE CARIACICA - ESTADO DO ESPÍRITO SANTO**, no uso das atribuições que lhe confere o art. 90, IX da Lei Orgânica do Município de Cariacica,

DECRETA:

Art. 1º Fica instituída a Política de Segurança da Informação no âmbito da Administração Municipal, tornando a utilização dos recursos de Tecnologia da Informação e Comunicações existentes sujeita às normas do presente Decreto, independentemente da respectiva propriedade.

Parágrafo único: Para efeito do disposto neste Decreto, consideram-se:

I. TIC: Tecnologia da Informação e Comunicações;

II. Segurança da Informação: Conjunto de processos e procedimentos de proteção dos ativos da informação contra a intrusão, a negação de serviço a usuários autorizados, modificação desautorizada de dados ou informações, armazenados, em processamento ou em trânsito, abrangendo, inclusive, a segurança dos recursos humanos, a documentação, as áreas e instalações de comunicações e computacional, bem como prevenir, detectar, deter e documentar eventuais ameaças;

III. Equipamento de Informática: Dispositivo de processamento e armazenamento eletrônico de informações, incluindo microcomputadores, respectivos componentes, acessórios e periféricos, como: impressoras, scanners, servidores de rede, switches, roteadores, celulares, smartphones, tablets, appliances e Pendrive, etc.;

IV. Rede local: Conjunto dos equipamentos de informática conectados entre si, com um escopo de funcionamento limitado a uma área geográfica pequena, utilizada pelos órgãos da Administração Municipal;

V. Rede Municipal de Dados: Equipamentos de Informática que interligam todas as redes locais utilizadas pela Administração Municipal. Todas as redes locais se interconectam com o nó concentrador;

VI. Internet: Rede externa à Prefeitura Municipal, integrada por equipamentos de informática conectados entre si;

VII. Intranet: Conjunto das redes locais de conexão entre os equipamentos de informática da Administração Municipal;

VIII. Site (ou Sítio): Conjunto articulado de informações, identificado por um domínio e como tal acessível por meio da Internet;

IX. Correio Eletrônico: Serviço de envio e recebimento de mensagens em meio digital, compreendendo softwares e equipamentos centrais de processamento e de manutenção de caixas postais;

X. Área de Trabalho: Espaço lógico da rede local destinado ao armazenamento exclusivo de arquivos de trabalho;

XI. Arquivo: Conjunto de informações concatenadas e passível de armazenamento em meio digital;

XII. Software: Conjunto de comandos lógicos, escritos em linguagem específica, para execução em equipamento de informática;

XIII. Programa com código malicioso: Software projetado especificamente para atentar contra a segurança de equipamento de informática, normalmente por meio de exploração de alguma vulnerabilidade do equipamento ou respectivos softwares (ex: vírus, worms, spyware, trojan, etc);

XIV. Sistemas Corporativos: São sistemas de uso coletivo da Administração Municipal;

XV. Download: é a transferência de dados de um computador remoto para um computador local;

XVI. Upload: Processo inverso a Download, ou seja, o envio de arquivos de um computador local para um computador remoto;

XVII. SUB-TI: Subsecretaria de Tecnologia da Informação;

XVIII. SEMGEPLAN: Secretaria Municipal de Gestão e Planejamento;

XIX. Usuário: Pessoa autorizada a operar equipamento de informática;

XX. Login: Conjunto de caracteres solicitado para os usuários que necessitam acessar algum sistema computacional. Geralmente os sistemas computacionais solicitam um login e uma senha para a liberação do acesso;

XXI. Criptografia: processo de escrita à base de métodos lógicos e controlados por chaves, cifras ou códigos, de forma que somente os usuários autorizados possam reestabelecer sua forma original;

XXII. Salvaguarda: Cópia segura de Dados e informações, classificadas ou não, com o objetivo preservar ou proteger por determinado período de tempo;

XXIII. Logon: É o evento de acessar um sistema computacional para opera-lo, sendo necessário o fornecimento de credenciais de acesso, como Login e uma Senha ou autenticação multifator;

XXIV. Logoff: Evento inverso ao Logon, nesse evento o usuário indica ao sistema que está terminando a sessão ativa, finalizando qualquer atividade que estiver ativa no momento de logoff;

XXV. Informação Classificada: informação em poder dos órgãos e entidades públicas, observado o seu teor e em razão de sua imprescindibilidade à segurança da sociedade, pode ser classificada como Restrita, Interna ou Pública;

XXVI. Informação sigilosa: informação submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da Sociedade e do Estado, e aquelas abrangidas pelas demais hipóteses legais de sigilo;

XXVII. Tratamento da informação: conjunto de ações que compõem o ciclo de vida da informação, referentes à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação;

XXVIII. Dados processados: dados submetidos a qualquer operação ou tratamento por meio de processamento eletrônico ou por meio automatizado com o emprego de tecnologia da informação;

XXIX. Informação: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

XXX. Ativos da Informação: A informação propriamente dita, os sistemas e equipamentos utilizados na transmissão, processamento e armazenamento da informação, locais físicos onde estão localizados esses ativos e também os recursos humanos que possuem alguma forma de acesso a informação;

XXXI. Recurso Criptográfico: sistema, programa, processo, equipamento isolado ou em rede que utiliza algoritmo simétrico ou assimétrico para realizar cifração ou decifração;

XXXII. Disponibilidade: característica da informação que pode ser conhecida e utilizada por indivíduos, equipamentos ou sistemas autorizados;

XXXIII. Autenticidade: característica da informação que tenha sido produzida, expedida, recebida ou modificada por determinado indivíduo, equipamento ou sistema;

8

XXXIV. Integridade: característica da informação não modificada, inclusive quanto à origem, trânsito e destino.

Art. 2º Os recursos de Tecnologia da Informação e Comunicações de propriedade da Administração Pública Municipal de Cariacica devem ser utilizados exclusivamente para o desempenho de atividades administrativas.

§1º - A realização de inspeções mais detalhadas, no sentido de avaliar uma situação de uso indevido dos recursos, depende de autorização expressa do Prefeito ou Secretário Municipal, aos quais será dada a ciência do procedimento. Não configurando quebra de sigilo a realização de inspeções ou manutenções preventivas e corretivas efetuadas SUB-TI.

§2º - Constatada a utilização inadequada do recurso que trata o art. 2º será de pronto notificado ao Prefeito ou Secretário da pasta que deverá adotar os procedimentos administrativos cabíveis.

Art. 3º Compete exclusivamente a SUB-TI:

I - Administrar os recursos de Tecnologia de Informação e Comunicações;

II - Empregar mecanismos de segurança e contingência, visando garantir a disponibilidade, confidencialidade e integridade dos ativos da informação.

III - Manter sob custódia os Ativos da Informação da Administração Municipal;

IV - Contratar e avaliar a aquisição de Soluções de TIC, decorrentes de projetos de implementação no âmbito da Administração Pública Municipal;

V - Orientar, supervisionar e auxiliar os Servidores Municipais (Prefeito, Secretários, Efetivos, Cargos em Comissão e outros), visando o uso adequado dos recursos de Tecnologia da Informação e Comunicações da Administração Municipal de Cariacica;

VI - Planejar, implantar, aperfeiçoar e manter mecanismos que possibilitem filtrar, detectar, registrar, restringir e bloquear o tratamento inadequado dos Ativos da Informação e Serviços de TIC;

VII - Definir o uso de equipamentos, sistemas de produção, guarda de documentos, dados e informações sigilosas ligados a redes de comunicação de dados que possuam sistemas de proteção e segurança adequados;

VIII - Armazenar informações referentes aos ativos da informação e serviços de TIC, para fins de inspeção, estatísticas de utilização e otimização dos recursos da rede local;

IX - Implantação de mecanismos de controle que evitem à propagação de código malicioso e ataques internos e externos no âmbito da Administração Pública Municipal;

X - Manter um canal de Gerenciamento de Incidentes onde os usuários possam reportar imediatamente qualquer suspeita ou problema relativo a Segurança da Informação;

XI - Planejar e executar a Gestão de Risco de Segurança da Informação em toda a Administração Pública Municipal, com o objetivo de identificar as vulnerabilidades que uma ameaça possa explorar e implementar controles e medidas de proteção para minimizar ou eliminar os riscos que estão sujeitos os ativos da informação;

XII - Definir regras e pré-requisitos para a inserção de dispositivos particulares na rede local e Rede Municipal de Dados, disponibilizada exclusivamente para esse tipo de dispositivo por meio de norma complementar.

XIII - Cadastramento ou exclusão das contas de usuário de Tecnologia da Informação e dos Sistemas Corporativos da Administração Pública Municipal;

XIV - Alteração ou revogação de permissões de usuário nos recursos de TIC;

XV - Empregar mecanismos para controle e bloqueio de: licenças de uso; instalação de softwares não licenciados e alterações da configuração dos equipamentos de informática;

XVI - Integração, fusão ou a ampliação de sistemas legados que ensejarem novos ou reformulados sistemas;

XVII - Desenvolver programas de conscientização e treinamentos de segurança da informação e comunicações, fomentando as melhores práticas na utilização dos recursos de TIC.

XVIII - Promover a capacitação de recursos humanos para o desenvolvimento de competência em segurança da informação.

DOS USUÁRIOS

Art. 4º São usuários dos recursos de Tecnologia da Informação da Administração Municipal: prefeito, vice-prefeito, secretários municipais, servidores efetivos, cargos em comissão, contratados, estagiários e outros prestadores de serviço e demais colaboradores, de acordo com as necessidades do serviço.

§ 1º - A autorização de uso é pessoal e intransferível; toda e qualquer ação, executada por meio de um determinado login, será de responsabilidade daquele a quem lhe for atribuído, cabendo, portanto, zelar pela confidencialidade de sua senha.

§ 2º - A criação de contas de acesso aos ativos de informação requer procedimentos prévios de credenciamento para qualquer usuário.

§ 3º - Utilizar conta de acesso no perfil de administrador de ativos da informação somente para usuários cadastrados para execução de tarefas específicas na administração desses ativos.

§ 4º - Recomenda-se a utilização de autenticação multifator quando possível, para o controle de acesso lógico, a fim de autenticar a identidade de um usuário e vinculá-lo a uma conta de acesso a ativos de informação.

Art. 5º O cadastramento de usuários visando acesso aos recursos de TI será realizado pela SUB-TI, à vista de autorização por escrito do respectivo Secretário Municipal ao qual o servidor esteja subordinado.

§ 1º A autorização de uso contempla o acesso somente aos equipamentos de informática e softwares necessários para a consecução das tarefas do usuário.

§ 2º O departamento pessoal deve comunicar imediatamente à SUB-TI sobre a entrada, afastamento, mudança de lotação de servidores dos quadros funcionais da Administração Municipal, para liberar acesso/cancelamento da autorização de uso de todos os acessos dos recursos de TI.

§ 3º A solicitação de acesso aos sistemas corporativos deverá ser feita de maneira formal pelo interessado, justificando a sua necessidade, sendo que a mesma deverá ser assinada pelo Secretário imediato à qual o usuário esteja subordinado ou vinculado, e depois encaminhada a SUB-TI.

§ 4º As mudanças de autorização de acesso aos sistemas corporativos/recursos de TI devem ser comunicadas de maneira formal pelo Secretário da pasta.

Art. 6º Aos usuários compete:

I - Zelar pelo sigilo de sua senha;

II – Alterar suas senhas periodicamente;

III - Zelar pela segurança das informações, fechando ou bloqueando as telas de equipamentos de informática ou softwares, quando não os estiver utilizando;

IV - Comunicar imediatamente à SUB-TI, qualquer suspeita de que estejam sendo executados atos em seu nome, por meio de recursos de TIC;

V – Comunicar qualquer ato ou suspeita cometidos, que sejam configurados como uso inadequado dos recursos computacionais e informações da Administração Municipal;

VI - Zelar pela segurança da infraestrutura tecnológica da Administração Pública Municipal, não utilizando dispositivos, que possam conter programas com código malicioso;

VII - Zelar pela integridade física dos equipamentos de informática colocados à sua disposição, evitando submetê-los a condições de risco; mantendo-os afastados de líquidos, alimentos ou qualquer material ou utensílio que possam danificá-los, comunicando imediatamente a SUB-TI qualquer anormalidade ou defeito;

VIII - Zelar pela segurança das informações de propriedade da Administração Municipal, que estejam sob sua custódia, em qualquer formato digital ou impresso;

IX – Não divulgação de Informações sigilosas e de uso restrito a Administração Municipal;

X – Efetuar os procedimentos de logon e logoff no sistema adequadamente;

XI – Participar dos Programas periódicos de sensibilização e conscientização em conformidade com a Política de Segurança da Informação e comunicações;

XII – Difundir e cumprir a Política de Segurança da Informação e Comunicações, das normas de segurança e da legislação vigente acerca do tema;

XIII – Adotar comportamento favorável à disponibilidade, à integridade, à confidencialidade e à autenticidade das informações;

XIV – Desligar adequadamente os equipamentos de TIC após o uso.

Art. 7º É considerado uso inadequado dos recursos TIC da Administração Municipal de Cariacica:

I - Fornecer, por qualquer motivo, seu login e senha de acesso para outrem;

II - Fazer uso do login e da senha de outrem;

III - Utilizar arquivos que impliquem violação de direitos autorais, de propriedade intelectual ou de qualquer material protegido;

IV - Inclusão ou execução de programas com código malicioso nos equipamentos de propriedade da Administração Municipal;

V – Divulgar ou utilizar informação pessoal própria ou de outrem na rede local da Prefeitura Municipal de Cariacica ou na internet.

DA SEGURANÇA AOS ATIVOS DA INFORMAÇÃO

Art. 8º Os ativos da informação devem ser protegidos adequadamente, contra ameaças externas e internas.

8

§ 1º - O uso de ativo de informação que não guarde relação com o exercício do cargo, função, emprego ou atividade pública será considerado indevido e passível de imediato bloqueio de acesso, sem prejuízo da apuração da responsabilidade administrativa, penal e civil.

§ 2º - O acesso de prestadores de serviços aos ativos da informação, devem ser estabelecidas contratualmente para que se assegure o cumprimento das diretrizes de segurança da informação previstas neste decreto, bem como em legislações vigentes.

§ 3º - Os ativos de informação classificados como sigilosos requerem procedimentos especiais de controles de acesso físico em conformidade com as diretrizes de acesso físico deste decreto.

Art. 9º Para proteção adequada dos ativos deve-se:

I - Conter ferramentas de proteção contra acesso não autorizado aos ativos de informação que favoreça, preferencialmente, a administração de forma centralizada;

II - Respeitar o princípio do menor privilégio para configurar as credenciais ou contas de acesso dos usuários aos ativos de informação;

III - Utilizar ativo de informação homologado nas aplicações de controle de acesso, de tratamento das informações sigilosas e criptografia;

IV - Registrar eventos relevantes previamente definidos, para a segurança e rastreamento de acesso às informações sigilosas;

V - Criar mecanismos para garantir a exatidão dos registros de auditoria nos ativos de informação;

VI - Classificar os ativos de informação em níveis de criticidade, considerando o tipo de ativo de informação, o provável impacto no caso de quebra de segurança, tomando como base a gestão de risco e a gestão de continuidade de negócios, relativa aos aspectos da segurança da informação e comunicações da Administração Pública Municipal;

VII - Os projetos de TIC para aquisição de ativos da informação classificados como críticos devem considerar como requisitos, a utilização de mecanismos redundantes para garantir a alta disponibilidade dos serviços.

DO CONTROLE DE ACESSO FÍSICO

Art. 10 É de responsabilidade dos Órgãos e da Administração Pública Municipal:

I - Estabelecer regras para o uso de credenciais físicas, que se destinam ao controle de acesso dos usuários às áreas e instalações sob suas responsabilidades;

II - Orientar na instalação de sistemas de detecção de intrusos nas áreas e instalações sob suas responsabilidades;

III - Classificar as áreas e instalações como ativos de informação de acordo com o valor, a criticidade, o tipo de ativo de informação e o grau de sigilo das informações que podem ser tratadas em tais áreas e instalações, mapeando aquelas áreas e instalações consideradas críticas;

IV - Orientar o uso de barreiras físicas de segurança, bem como equipamentos ou mecanismos de controle de entrada e saída;

V- Proteger os ativos de informação contra ações de vandalismo e sabotagem, especialmente em relação àqueles considerados críticos;

VI - Implementar área de recepção com regras claras para a entrada e saída de pessoas, equipamentos e materiais;

VII - Definir pontos de entrega e carregamento de material com acesso exclusivo ao pessoal credenciado;

VIII - Intensificar os controles para as áreas e instalações consideradas críticas em conformidade com a legislação vigente;

IX - Utilizar controle de acesso físico por meio de sistema biométrico são requeridos procedimentos prévios para o credenciamento do usuário. Esse recurso deve ser utilizado em conjunto com outro sistema de identificação (cartão, crachá, senha, chave, dentre outros), a fim de atender os conceitos da autenticação de multifator.

DA CRIPTOGRAFIA

Art. 11 Fica autorizado o uso de código, cifra ou sistema de criptografia no âmbito da Administração Pública Municipal para assegurar o sigilo de documentos, dados e informações.

§ 1º Para circularem fora das instalações da Prefeitura Municipal de Cariacica os documentos, dados e informações sigilosas, produzidos em qualquer tipo de mídia móvel, devem necessariamente estar criptografados.

§ 2º Uma cópia dos documentos, dados e informações sigilosas devem ser mantidas nas áreas e instalações sigilosas da Prefeitura Municipal de Cariacica.

Art. 12 Aplicam-se aos programas, aplicativos, sistemas e equipamentos de criptografia todas as medidas de segurança previstas neste decreto para os documentos, dados e informações sigilosas e também os seguintes procedimentos:

I - Realização de vistorias periódicas, com a finalidade de assegurar uma perfeita execução das operações criptográficas;

II - Elaboração de inventários completos e atualizados do material de criptografia existente;

III - Escolha de sistemas criptográficos adequados a cada destinatário, quando necessário;

IV - Comunicação, ao superior hierárquico ou à autoridade competente, de qualquer anormalidade relativa ao sigilo, à inviolabilidade, à integridade, à autenticidade, à legitimidade e à disponibilidade de documentos, dados e informações sigilosos criptografados;

V - Identificação e registro de indícios de violação ou interceptação ou de irregularidades na transmissão ou recebimento de documentos, dados e informações criptografados.

§ 1º - O Agente Responsável pela cifração ou decifração, no exercício do cargo, função, emprego ou atividade, utilizará recurso criptográfico baseado em algoritmo adotado pela Administração Pública Municipal.
§ 2º - O agente público referido no § 1º deste artigo deverá providenciar as condições de segurança necessárias ao resguardo do sigilo de documentos, dados e informações durante sua produção, tramitação e guarda, bem como a segurança dos equipamentos e sistemas utilizados.

§ 3º - As cópias de segurança de documentos, dados e informações sigilosos deverão ser criptografados, observadas as disposições dos §§ 1º e 2º deste artigo.

Art. 13 Um canal de comunicação seguro (Rede Privada Virtual) que interligue redes de órgãos e entidades da Administração Pública Municipal, objetivando a troca de informações classificadas, deve utilizar recursos criptográficos baseado em algoritmo adotado pela Administração Pública Municipal;

DO USO E CLASSIFICAÇÃO DA INFORMAÇÃO

Art. 14 As informações institucionais geradas pelos órgãos e entidades em qualquer suporte, materiais, áreas, comunicações e sistemas de informação dessa Administração Pública, devem ser classificadas.

§ 1º - As informações institucionais da Administração Pública Municipal deverão ser classificadas visando suas funções administrativas, informativas, probatórias e comunicativas, considerando os princípios do acesso a informação dispostos pela Lei 12.527/2011.

§ 2º - As Informações Institucionais devem ser classificadas em: Restrita (R), Interna (I) ou pública (P).

§ 3º - As Secretarias e órgãos da Administração Municipal devem promover ações para conscientização dos agentes públicos visando à disseminação das diretrizes de tratamento da informação.

Art. 15 Qualquer dado ou informação desenvolvido ou processado eletronicamente utilizando equipamentos de TIC da Prefeitura Municipal de Cariacica é de propriedade da Administração Pública Municipal.

§ 1º- Os dados e informações desenvolvidos ou gerados por agente público no cumprimento de suas atribuições são de propriedade da Administração Pública Municipal e devem ser armazenados apropriadamente nos recursos de TIC disponíveis.

Art. 16 No tratamento, tramitação das informações, deverão ser utilizados sistemas de informação e canais de comunicação seguros que atendam aos padrões mínimos de qualidade, segurança e criptografia;

Art. 17 Os dados e informações presentes em arquivos e sistemas de informação, devem possuir um usuário ou área de negócio proprietário;

§ 1º - Os proprietários da informação devem ser responsáveis pela gestão, classificação e controle de acesso a informação, conforme estabelecidos pelo Prefeito ou Secretário Municipal da respectiva pasta;

§ 2º - A liberação e revogação dos acessos a informação são de responsabilidade dos usuários e áreas de negócio proprietários, devendo seguir as diretrizes de Segurança da Informação, presentes neste Decreto.

Art. 18 São deveres do Agente Público proprietário da informação:

I - Classificar a informação;

II - Armazenar a informação classificada e sigilosa nos meios de armazenamento disponibilizados pela Administração Municipal;

III - Assegurar a publicidade da informação de caráter ostensivo, utilizando-as, exclusivamente, para o exercício das atribuições de cargo, emprego ou função pública, sob pena de responsabilização administrativa, civil e penal;

IV - Efetuar o tratamento das informações ao longo de seu ciclo de vida de modo ético e responsável e com respeito à legislação vigente.

V- As medidas e os procedimentos relacionados ao tratamento da informação a ser realizado com apoio de empresas terceirizadas, em qualquer fase do ciclo de vida da informação, deverão ser estabelecidos contratualmente para que se assegure o

cumprimento das diretrizes previstas nesta norma, bem como em legislações vigentes.

Art. 19 As informações da Administração devem ser armazenadas em cópia salvaguarda, por meio de mecanismos que sejam capazes de garantir a Disponibilidade, Integridade e Confidencialidade.

§ 1º - O tempo de retenção das informações armazenadas em cópias salvaguarda deve seguir a legislação complementar designada pela Administração Municipal.

Art. 20 É considerado inadequado no Tratamento das Informações da Administração Pública Municipal:

I - Armazena-la em serviços de armazenamento remoto privados disponíveis na Internet;

II - Armazena-la em Serviços de correio eletrônicos privados;

III - Transferência por meio de Serviços FTP sem adequada requisitos de segurança;

IV - Envio de Informações Classificadas como restrita, confidencial ou com restrições de sigilo sem o devido tratamento criptográfico;

V- Divulgação de dados ou informações deliberadamente ou inadvertidamente ou sem autorização de seu superior.

DO USO DO E-MAIL INSTITUCIONAL

Art. 21 Administração Pública Municipal adotará o Correio Eletrônico como ferramenta comunicação oficial.

Parágrafo Único - O uso do Correio Eletrônico deverá ser aderente às atividades fim da Administração Municipal.

Art. 22 O armazenamento das mensagens de correio eletrônico deve ocorrer em recurso de TIC adequado que utilize mecanismos de segurança da informação apropriados.

Art. 23 As mensagens de Correio eletrônico enviadas ou recebidas a partir do domínio "cariacica.es.gov.br" e seus subdomínios são de propriedade da Administração Pública Municipal.

Art. 24 É considerado uso inadequado do Correio Eletrônico:

I - Utilizar o Correio Eletrônico provido pela Administração Municipal para envio de arquivos que não estejam relacionados às atividades administrativas;

II - Tentar ou efetivamente burlar as regras definidas para o Correio Eletrônico;

8

III - Tentar ou efetivamente alterar os registros de envio e recebimento de mensagens do correio eletrônico;

IV - Utilizar o Correio Eletrônico para enviar material ofensivo, difamatório, de assédio, de propaganda, etc.;

V - Divulgar informações confidenciais da Administração Municipal em grupos ou listas de correio, dentre outros, não importando se a divulgação foi deliberada ou inadvertida, sob pena de responsabilização administrativa, civil e penal.

DO USO E AQUISIÇÃO DOS EQUIPAMENTOS DE INFORMÁTICA

Art. 25 As solicitações para aquisição ou substituição de recursos de Tecnologia de Informação, devem ser encaminhadas a SUB-TI para análise segundo seus critérios de padronização.

Art. 26 A Administração Municipal proverá rede de dados para atender aos equipamentos de informática.

§ 1º - Somente equipamentos de informática da Prefeitura Municipal de Cariacica, devem ser conectados à Rede Local Corporativa e a Rede Municipal de Dados dos órgãos e secretarias.

§ 2º - Equipamentos particulares dos Agentes Públicos, visitantes, munícipes e contribuintes, devem ser conectados a rede especifica, disponibilizada sob as diretrizes de Segurança da Informação do presente decreto;

§ 3º - Os equipamentos devem atender aos pré-requisitos mínimos de configuração e segurança, definidos pela Administração Municipal;

§ 4º - Nenhum equipamento de informática poderá ser removido ou instalado sem a anuência da SUB-TI.

Art. 27 É considerado uso inadequado dos equipamentos de Informática:

I - Alterar as configurações físicas dos equipamentos, através da inserção ou remoção de peças sem a anuência da Coordenação de Infraestrutura e Tecnologia da SUB-TI;

II - Alterar o local de instalação dos equipamentos, sem a supervisão da SUB-TI;

III - Alterar as configurações lógicas que impeçam, alterem ou possam alterar e regular a administração realizada pela SUB-TI, bem como a segurança deste ou de qualquer outro recurso de Tecnologia da Informação;

IV - Conectar equipamentos que possam tornar a rede local vulnerável a invasões externas e ataques de programas com código malicioso, em suas mais diferentes formas;

V - Conectar equipamentos que tentem ou efetivamente violem os sistemas de segurança da Administração Municipal;

VI - Conectar equipamentos que tentem ou efetivamente realizem ataques ou invasões a computadores, ou ainda, qualquer outra forma de fraude;

VII - Utilizar equipamentos para executar qualquer tipo ou forma de pirataria;

VIII - ligar equipamentos que não sejam de informática em rede elétrica estabilizada, quando esta existir;

IX - Romper lacres e proteções físicas dos equipamentos.

DO USO E AQUISIÇÃO DE SOFTWARES

Art. 28 As solicitações de aquisição e substituição de softwares, devem ser encaminhadas a SUB-TI, para análise controles de segurança da informação e comunicações e critérios de padronização.

Parágrafo Único - A SUB-TI é responsável por estabelecer critérios de segurança da informação e comunicação e padronização para aquisição ou uso de softwares nos equipamentos de informática da Administração Municipal.

Art. 29 É vedado o uso de softwares de propriedade particular nos equipamentos da Administração Municipal.

§ 1º Todos os softwares, aplicativos e sistemas utilizados nos equipamentos de informática da Administração Pública Municipal devem ser homologados e padronizados pela SUB-TI.

§ 2º A Instalação e Regularização de licenças de Softwares por todos os setores devem ser feitas por formalização das solicitações, por meio de requerimento obrigatório endereçado à SUB-TI;

§ 3º É considerado uso inadequado dos softwares de propriedade da Administração Municipal:

I - Instalar, utilizar ou manter cópias de softwares que não atendam aos critérios de padronização estabelecidos pela SUB-TI;

II - Fazer cópias não autorizadas dos softwares desenvolvidos ou adquiridos;

III - Apropriar-se, por quaisquer meios, das chaves de ativação dos softwares.

Art. 30 É de responsabilidade das empresas prestadoras de serviços, colaboradores e demais usuários, a legalidade dos softwares utilizados em seus equipamentos de informática.

§ 1º O uso de equipamentos pelas empresas contratadas, nas dependências da Administração Municipal, depende de autorização prévia da SUB-TI.

§ 2º As empresas contratadas ficam obrigadas a comprovar a legalidade de seus softwares, quando necessário.

DO USO DA INTERNET

Art. 31 A Administração Municipal adotará política interna definida por norma complementar, na inspeção e restrição de acesso à Internet, com a identificação do usuário, por meio de sistema automatizado.

§ 1º O uso da internet deverá ser aderente às atividades fim da Administração Municipal e enquadrado nos seguintes objetivos:

I - Assegurar a garantia do direito individual e coletivo das pessoas, quanto à inviolabilidade da sua intimidade e ao sigilo da correspondência e das comunicações, nos termos previstos na Constituição da República de 1988;

II - Assegurar o cumprimento e a aplicabilidade da legislação corrente quanto ao uso inadequado da internet, como por exemplo, pirataria, pedofilia, ações discriminatórias, dentre outras;

III - Minimizar a ocorrência de danos ou riscos desnecessários ao desenvolvimento das atividades realizadas pela Administração Municipal, bem como o download de programas não permitidos;

IV - Assegurar a proteção de assuntos que mereçam tratamento especial;

V - Dotar a Administração de instrumentos jurídicos, normativos e organizacionais que os capacitem científica, tecnológica e administrativamente a assegurar a confidencialidade, a integridade, a autenticidade, o não-repúdio e a disponibilidade dos dados e das informações tratadas, classificadas e sensíveis;

VI - Estabelecer normas jurídicas necessárias à efetiva implementação da segurança da informação;

VII - Promover as ações necessárias à implementação e manutenção da segurança da informação;

Art. 32 Todas as atividades fim devem ser executadas utilizando o serviço de Internet provido pela Administração Municipal.

Art. 33 É considerado uso inadequado da Internet:

I - Tentar ou efetivamente acessar informações consideradas inadequadas ou não relacionadas às atividades administrativas, especialmente, sites de conteúdo agressivo (racismo, pedofilia, nazismo, etc.), de drogas, de pornografia, etc.;

II - Fazer o download de arquivos e outros que possam tornar a rede local vulnerável a invasões externas e ataques de programas com código malicioso, em suas mais diferentes formas;

III – Tentar ou efetivamente violar os sistemas de segurança da Administração Municipal, burlar as regras definidas, os registros de acesso, realizar ataque ou invasão a computadores, ou ainda, qualquer outra forma de fraude na Internet;

IV - Utilizar acesso à Internet provido pela Administração Municipal para upload de arquivos que não estejam relacionados às atividades administrativas;

V - Utilizar o computador para executar qualquer tipo ou forma de pirataria, envio de material ofensivo, difamatório, de assédio, de propaganda, etc.;

VI - Utilizar serviços de streaming, a não ser que o acesso seja inerente a trabalhos, pesquisas e negócios da Administração Municipal;

VII - divulgar informações confidenciais da Administração Municipal em grupos de discussão, listas, bate-papo, dentre outros, não importando se a divulgação foi deliberada ou inadvertida, sendo possível sofrer as penalidades previstas nas políticas e procedimentos internos e/ou na forma da Lei.

Art. 34 Quanto a publicações e divulgação via Internet, caberá ao Prefeito Municipal, determinar como será a análise e liberação da forma e conteúdo de quaisquer publicações oficiais via Internet.

DO USO DA REDE LOCAL

Art. 35 A rede local deve possuir os seguintes seguimentos:

I - Rede local corporativa: Rede de local onde os equipamentos da Prefeitura Municipal de Cariacica são conectados para realização das tarefas administrativas, estão disponíveis em todos os órgãos municipais participantes da Rede de Dados Municipal;

II - Rede local de dispositivos móveis: Rede local para equipamentos móveis pessoais dos Servidores municipais, fornecedores, visitantes, contribuintes e munícipes;

Parágrafo único - O tráfego de dados nos segmentos da Rede Local deve ser separado logicamente utilizando recursos, de Segurança da Informação e Criptográficos apropriados nos ativos da Informação.

Art. 36 A rede local deve possuir mecanismos que:

I - Registrem os acessos à rede corporativa de computadores de forma a permitir a rastreabilidade e a identificação do usuário;

II - Evitem que equipamentos externos se conectem na rede corporativa de computadores;

III - Permitam identificar e rastrear os endereços de origem e destino, bem como os serviços utilizados;

IV - Registrem o acesso remoto à rede corporativa em logs para posterior auditoria, contendo informações específicas que facilitem o rastreamento da ação tomada;

V - Os órgãos ou entidades da Administração Pública Municipal, em suas áreas de competência, devem estabelecer regras para o uso de redes sem fio.

Art. 37 É considerado uso inadequado da Rede Local Corporativa:

I - Utilizar os recursos da rede local para transferência de arquivos que não estejam relacionados às atividades administrativas;

II - Tentar ou efetivamente violar os sistemas de segurança da rede local;

III - Tentar ou efetivamente burlar as regras definidas para o acesso à rede local;

IV - Tentar ou efetivamente alterar os registros de acesso à rede local;

V- Tentar ou efetivamente realizar ataque ou invasão a computadores da rede local;

VI - Tentar ou efetivamente negar ou desativar acesso aos serviços de Tecnologia da Informação.

Art. 38 É considerado uso inadequado da Rede Local de Dispositivos Móveis:

I - Conexão de dispositivos infectados por códigos maliciosos;

II - Tentar ou efetivamente violar os sistemas de segurança da rede local;

III - Tentar ou efetivamente burlar as regras definidas para o acesso à rede local;

IV - Divulgação de dados, documentos ou informações pessoais de outrem;

V - Utilizar a rede para roubo de dados ou mesmo se passar por outra pessoa;

VI - Utilizar a rede para tentativas de intrusão na Internet ou em outros dispositivos conectados a mesma rede;

VII - Fazer o download de arquivos e outros que possam tornar a rede local vulnerável a invasões externas e ataques de programas com código malicioso, em suas mais diferentes formas;

VIII – Tentar ou efetivamente violar os sistemas de segurança da Administração Municipal;

IX - Tentar ou efetivamente realizar ataque ou invasão a computadores, ou ainda, qualquer outra forma de fraude;

X - Utilizar a rede local para enviar material ofensivo, difamatório, de assédio, de propaganda, etc.

DO PLANO DE CONTINUIDADE DOS NEGÓCIOS E RECUPERAÇÃO DE DESASTRES

Art. 39 A Administração Municipal deve contar com um Plano de Continuidade dos Negócios, definido por norma complementar, responsável por estabelecer critérios para a Continuidade e Recuperação em caso de Desastres, dos Serviços prestados pela Administração Municipal.

§ 1º - O Plano de Continuidade deve abranger a todos os serviços de TIC da Administração Municipal, permitindo a rápido restabelecimento em caso de desastres.

§ 2º - Devem ser utilizados recurso de redundância e dispersão geográfica dos ativos para evitar indisponibilidades dos Serviços de TIC.

§ 3º - Os Ativos da Informação e Serviços classificados como Críticos e Sigilosos devem ter prioridade em seu restabelecimento no Plano de Continuidade dos Negócios.

§ 4º - Devem ser desenvolvidos procedimentos formais para operacionalização do Plano de Continuidade dos Negócios.

§ 5º - Os usuários, fornecedores e terceiros envolvidos, devem estar devidamente treinados nos procedimentos do Plano de Continuidade de Negócios.

§ 6º - Testes periódicos devem ser executados visando avaliar a capacidade operacional de executar o Plano de Continuidade de Negócios, havendo detecção e falhas as mesmas devem ser relatadas e corrigidas.

DAS PENALIDADES

Art. 40 O descumprimento das disposições contidas neste Decreto caracteriza infração funcional, a ser apurada em Processo Administrativo Disciplinar, conforme legislação vigente.

Art. 41 A autoridade que determinar a instauração de Processo Administrativo Disciplinar contra servidor pode requisitar a SUB-TI a suspensão cautelar da correspondente autorização de uso, mediante bloqueio de recursos de TI.

Parágrafo Único - O usuário identificado como causador de risco imediato aos recursos de tecnologia da informação da Administração Municipal, terá seu login, imediatamente, suspenso pela SUB-TI, com pronta notificação ao Prefeito Municipal, ao respectivo Secretário e à SEMGEPLAN, inclusive podendo ser confiscado o computador utilizado pelo usuário até o fim das investigações.

DAS DISPOSIÇÕES FINAIS

Art. 42 Os casos excepcionais a este Decreto devem ser submetidos para análise e parecer da Secretaria Municipal de Finanças.

Art. 43 Esta política deverá ser parte integrante do Plano Diretor de Informática do Município de Cariacica, podendo ser modificada, quando necessário, pela comissão para elaboração e alteração do mesmo.

Art. 44 Fica revogado o Decreto nº 74, de 18 de setembro de 2009.

Art. 45 Este Decreto entra em vigor na data de sua publicação, ficando revogadas as disposições em contrário.

Cariacica – ES, 21 de novembro de 2017.

GERALDO LUZIA DE OLIVEIRA JUNIOR
Prefeito Municipal

CARLOS RENATO MARTINS
Secretário Municipal de Finanças

DIÁRIO OFICIAL DO MUNICIPIO
Cariacica (ES), quinta-feira, 23 de novembro de 2017.

DECRETOS

DECRETO Nº 157, DE 21 DE NOVEMBRO DE 2017

INSTITUI A POLÍTICA DE SEGURANÇA DA INFORMAÇÃO NO ÂMBITO DA ADMINISTRAÇÃO MUNICIPAL E DÁ OUTRAS PROVIDÊNCIAS

O PREFEITO MUNICIPAL DE CARIACICA - ESTADO DO ESPÍRITO SANTO, no uso das atribuições que lhe confere o art. 90, IX da Lei Orgânica do Município de Cariacica,

DECRETA:

Art. 1º Fica instituída a Política de Segurança da Informação no âmbito da Administração Municipal, tornando a utilização dos recursos de Tecnologia da Informação e Comunicações existentes sujeita às normas do presente Decreto, independentemente da respectiva propriedade.

Parágrafo único: Para efeito do disposto neste Decreto, consideram-se:

I. TIC: Tecnologia da Informação e Comunicações;

II. Segurança da Informação: Conjunto de processos e procedimentos de proteção dos ativos da informação contra a intrusão, a negação de serviço a usuários autorizados, modificação desautorizada de dados ou informações, armazenados, em processamento ou em trânsito, abrangendo, inclusive, a segurança dos recursos humanos, a documentação, as áreas e instalações de comunicações e computacional, bem como prevenir, detectar, deter e documentar eventuais ameaças;

III. Equipamento de Informática: Dispositivo de processamento e armazenamento eletrônico de informações, incluindo microcomputadores, respectivos componentes, acessórios e periféricos, como: impressoras, scanners, servidores de rede, switches, roteadores, celulares, smartphones, tablets, appliances e Pendrive, etc.;

IV. Rede local: Conjunto dos equipamentos de informática conectados entre si, com um escopo de funcionamento limitado a uma área geográfica pequena, utilizada pelos órgãos da Administração Municipal;

V. Rede Municipal de Dados: Equipamentos de Informática que interligam todas as redes locais utilizadas pela Administração Municipal. Todas as redes locais se interconectam com o nó concentrador;

VI. Internet: Rede externa à Prefeitura Municipal, integrada por equipamentos de informática conectados entre si;

VII. Intranet: Conjunto das redes locais de conexão entre os equipamentos de informática da Administração Municipal;

VIII. Site (ou Sítio): Conjunto articulado de informações, identificado por um domínio e como tal acessível por meio da Internet;

IX. Correio Eletrônico: Serviço de envio e recebimento de mensagens em meio digital, compreendendo softwares e equipamentos centrais de processamento e de manutenção de caixas postais;

X. Área de Trabalho: Espaço lógico da rede local destinado ao armazenamento exclusivo de arquivos de trabalho;

XI. Arquivo: Conjunto de informações concatenadas e passível de armazenamento em meio digital;

XII. Software: Conjunto de comandos lógicos, escritos em linguagem específica, para execução em equipamento de informática;

XIII. Programa com código malicioso: Software projetado especificamente para atentar contra a segurança de equipamento de informática, normalmente por meio de exploração de alguma vulnerabilidade do equipamento ou respectivos softwares (ex: vírus, worms, spyware, trojan, etc);

XIV. Sistemas Corporativos: São sistemas de uso coletivo da Administração Municipal;

XV. Download: é a transferência de dados de um computador remoto para um computador local;

XVI. Upload: Processo inverso a Download, ou seja, o envio de arquivos de um computador local para um computador remoto;

XVII. SUB-TI: Subsecretaria de Tecnologia da Informação;

XVIII. SEMGEPLAN: Secretaria Municipal de Gestão e Planejamento;

XIX. Usuário: Pessoa autorizada a operar equipamento de informática;

XX. Login: Conjunto de caracteres solicitado para os usuários que necessitam acessar algum sistema computacional. Geralmente os sistemas computacionais solicitam um login e uma senha para a liberação do acesso;

XXI. Criptografia: processo de escrita à base de métodos lógicos e controlados por chaves, cifras ou códigos, de forma que somente os usuários autorizados possam reestabelecer sua forma original;

XXII. Salvaguarda: Cópia segura de Dados e informações, classificadas ou não, com o objetivo preservar ou proteger por determinado período de tempo;

XXIII. Logon: É o evento de acessar um sistema computacional para opera-lo, sendo necessário o fornecimento de credenciais de acesso, como Login e uma Senha ou autenticação multifator;

XXIV. Logoff: Evento inverso ao Logon, nesse evento o usuário indica ao sistema que está terminando a sessão ativa, finalizando qualquer atividade que estiver ativa no momento de logoff;

XXV. Informação Classificada: informação em poder dos órgãos e entidades públicas, observado o seu teor e em razão de sua imprescindibilidade à segurança da sociedade, pode ser classificada como Restrita, Interna ou Pública;

XXVI. Informação sigilosa: informação submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da Sociedade e do Estado, e aquelas abrangidas pelas demais hipóteses legais de sigilo;

XXVII. Tratamento da informação: conjunto de ações que compõem o ciclo de vida da informação, referentes à produção, recepção,

EXPEDIENTE:
Coordenadora de Confecção, Reg. e Exped. de Atos Oficiais – Maria de Lourdes M. Coelho da Silva
Assistente Técnico – Thiago H. Rodrigues de Andrade
Rodovia BR 262, Nº 3.700 - KM 3,0 - Alto Lage, CARIACICA-ES.
CEP: 29.151-570 - End. Eletrônico: atosoficiais@cariacica.es.gov.br
Tel: (27) 3354-5807

classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação;
XXVIII. Dados processados: dados submetidos a qualquer operação ou tratamento por meio de processamento eletrônico ou por meio automatizado com o emprego de tecnologia da informação;
XXIX. Informação: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;
XXX. Ativos da Informação: A informação propriamente dita, os sistemas e equipamentos utilizados na transmissão, processamento e armazenamento da informação, locais físicos onde estão localizados esses ativos e também os recursos humanos que possuem alguma forma de acesso a informação;
XXXI. Recurso Criptográfico: sistema, programa, processo, equipamento isolado ou em rede que utiliza algoritmo simétrico ou assimétrico para realizar cifração ou decifração;
XXXII. Disponibilidade: característica da informação que pode ser conhecida e utilizada por indivíduos, equipamentos ou sistemas autorizados;
XXXIII. Autenticidade: característica da informação que tenha sido produzida, expedida, recebida ou modificada por determinado indivíduo, equipamento ou sistema;
XXXIV. Integridade: característica da informação não modificada, inclusive quanto à origem, trânsito e destino.
Art. 2º Os recursos de Tecnologia da Informação e Comunicações de propriedade da Administração Pública Municipal de Cariacica devem ser utilizados exclusivamente para o desempenho de atividades administrativas.
§1º - A realização de inspeções mais detalhadas, no sentido de avaliar uma situação de uso indevido dos recursos, depende de autorização expressa do Prefeito ou Secretário Municipal, aos quais será dada a ciência do procedimento. Não configurando quebra de sigilo a realização de inspeções ou manutenções preventivas e corretivas efetuadas SUB-TI.
§2º - Constatada a utilização inadequada do recurso que trata o art. 2º será de pronto notificado ao Prefeito ou Secretário da pasta que deverá adotar os procedimentos administrativos cabíveis.
Art. 3º Compete exclusivamente a SUB-TI:
I - Administrar os recursos de Tecnologia de Informação e Comunicações;
II - Empregar mecanismos de segurança e contingência, visando garantir a disponibilidade, confidencialidade e integridade dos ativos da informação.
III - Manter sob custódia os Ativos da Informação da Administração Municipal;
IV - Contratar e avaliar a aquisição de Soluções de TIC, decorrentes de projetos de implementação no âmbito da Administração Pública Municipal;
V - Orientar, supervisionar e auxiliar os Servidores Municipais (Prefeito, Secretários, Efetivos, Cargos em Comissão e outros), visando o uso adequado dos recursos de Tecnologia da Informação e Comunicações da Administração Municipal de Cariacica;
VI - Planejar, implantar, aperfeiçoar e manter mecanismos que possibilitem filtrar, detectar, registrar, restringir e bloquear o tratamento inadequado dos Ativos da Informação e Serviços de TIC;
VII - Definir o uso de equipamentos, sistemas de produção, guarda de documentos, dados e informações sigilosas ligados a redes de comunicação de dados que possuam sistemas de proteção e segurança adequados;
VIII - Armazenar informações referentes aos ativos da informação e serviços de TIC, para fins de inspeção, estatísticas de utilização e otimização dos recursos da rede local;
IX - Implantação de mecanismos de controle que evitem à propagação de código malicioso e ataques internos e externos no âmbito da Administração Pública Municipal;
X - Manter um canal de Gerenciamento de Incidentes onde os usuários possam reportar imediatamente qualquer suspeita ou problema relativo a Segurança da Informação;
XI - Planejar e executar a Gestão de Risco de Segurança da Informação em toda a Administração Pública Municipal, com o objetivo de identificar as vulnerabilidades que uma ameaça possa explorar e implementar controles e medidas de proteção para minimizar ou eliminar os riscos que estão sujeitos os ativos da informação;
XII - Definir regras e pré-requisitos para a inserção de dispositivos particulares na rede local e Rede Municipal de Dados, disponibilizada exclusivamente para esse tipo de dispositivo por meio de norma complementar.
XIII - Cadastramento ou exclusão das contas de usuário de Tecnologia da Informação e dos Sistemas Corporativos da Administração Pública Municipal;
XIV - Alteração ou revogação de permissões de usuário nos recursos de TIC;
XV - Empregar mecanismos para controle e bloqueio de: licenças de uso; instalação de softwares não licenciados e alterações da configuração dos equipamentos de informática;
XVI - Integração, fusão ou a ampliação de sistemas legados que ensejarem novos ou reformulados sistemas;
XVII - Desenvolver programas de conscientização e treinamentos de segurança da informação e comunicações, fomentando as melhores práticas na utilização dos recursos de TIC.
XVIII - Promover a capacitação de recursos humanos para o desenvolvimento de competência em segurança da informação.

DOS USUÁRIOS

Art. 4º São usuários dos recursos de Tecnologia da Informação da Administração Municipal: prefeito, vice-prefeito, secretários municipais, servidores efetivos, cargos em comissão, contratados, estagiários e outros prestadores

EXPEDIENTE:
Coordenadora de Confecção, Reg. e Exped. de Atos Oficiais – Maria de Lourdes M. Coelho da Silva
Assistente Técnico – Thiago H. Rodrigues de Andrade
Rodovia BR 262, Nº 3.700 - KM 3,0 - Alto Lage, CARIACICA-ES.
CEP: 29.151-570 - End. Eletrônico: atosoficiais@cariacica.es.gov.br
Tel: (27) 3354-5807

DIÁRIO OFICIAL DO MUNICIPIO
Cariacica (ES), quinta-feira, 23 de novembro de 2017.

de serviço e demais colaboradores, de acordo com as necessidades do serviço.
§ 1º - A autorização de uso é pessoal e intransferível; toda e qualquer ação, executada por meio de um determinado login, será de responsabilidade daquele a quem lhe for atribuído, cabendo, portanto, zelar pela confidencialidade de sua senha.
§ 2º - A criação de contas de acesso aos ativos de informação requer procedimentos prévios de credenciamento para qualquer usuário.
§ 3º - Utilizar conta de acesso no perfil de administrador de ativos da informação somente para usuários cadastrados para execução de tarefas específicas na administração desses ativos.
§ 4º - Recomenda-se a utilização de autenticação multifator quando possível, para o controle de acesso lógico, a fim de autenticar a identidade de um usuário e vinculá-lo a uma conta de acesso a ativos de informação.
Art. 5º O cadastramento de usuários visando acesso aos recursos de TI será realizado pela SUB-TI, à vista de autorização por escrito do respectivo Secretário Municipal ao qual o servidor esteja subordinado.
§ 1º A autorização de uso contempla o acesso somente aos equipamentos de informática e softwares necessários para a consecução das tarefas do usuário.
§ 2º O departamento pessoal deve comunicar imediatamente à SUB-TI sobre a entrada, afastamento, mudança de lotação de servidores dos quadros funcionais da Administração Municipal, para liberar acesso/cancelamento da autorização de uso de todos os acessos dos recursos de TI.
§ 3º A solicitação de acesso aos sistemas corporativos deverá ser feita de maneira formal pelo interessado, justificando a sua necessidade, sendo que a mesma deverá ser assinada pelo Secretário imediato à qual o usuário esteja subordinado ou vinculado, e depois encaminhada à SUB-TI.
§ 4º As mudanças de autorização de acesso aos sistemas corporativos/recursos de TI devem ser comunicadas de maneira formal pelo Secretário da pasta.
Art. 6º Aos usuários compete:
I - Zelar pelo sigilo de sua senha;
II – Alterar suas senhas periodicamente;
III - Zelar pela segurança das informações, fechando ou bloqueando as telas de equipamentos de informática ou softwares, quando não os estiver utilizando;
IV - Comunicar imediatamente à SUB-TI, qualquer suspeita de que estejam sendo executados atos em seu nome, por meio de recursos de TIC;
V – Comunicar qualquer ato ou suspeita cometidos, que sejam configurados como uso inadequado dos recursos computacionais e informações da Administração Municipal;
VI - Zelar pela segurança da infraestrutura tecnológica da Administração Pública Municipal, não utilizando dispositivos, que possam conter programas com código malicioso;
VII - Zelar pela integridade física dos equipamentos de informática colocados à sua disposição, evitando submetê-los a condições de risco; mantendo-os afastados de líquidos, alimentos ou qualquer material ou utensílio que possam danificá-los, comunicando imediatamente a SUB-TI qualquer anormalidade ou defeito;
VIII - Zelar pela segurança das informações de propriedade da Administração Municipal, que estejam sob sua custódia, em qualquer formato digital ou impresso;
IX – Não divulgação de Informações sigilosas e de uso restrito a Administração Municipal;
X – Efetuar os procedimentos de logon e logoff no sistema adequadamente;
XI – Participar dos Programas periódicos de sensibilização e conscientização em conformidade com a Política de Segurança da Informação e comunicações;
XII – Difundir e cumprir a Política de Segurança da Informação e Comunicações, das normas de segurança e da legislação vigente acerca do tema;
XIII – Adotar comportamento favorável à disponibilidade, à integridade, à confidencialidade e à autenticidade das informações;
XIV – Desligar adequadamente os equipamentos de TIC após o uso.
Art. 7º É considerado uso inadequado dos recursos TIC da Administração Municipal de Cariacica:
I - Fornecer, por qualquer motivo, seu login e senha de acesso para outrem;
II - Fazer uso do login e da senha de outrem;
III - Utilizar arquivos que impliquem violação de direitos autorais, de propriedade intelectual ou de qualquer material protegido;
IV - Inclusão ou execução de programas com código malicioso nos equipamentos de propriedade da Administração Municipal;
V – Divulgar ou utilizar informação pessoal própria ou de outrem na rede local da Prefeitura Municipal de Cariacica ou na internet.
DA SEGURANÇA AOS ATIVOS DA INFORMAÇÃO
Art. 8º Os ativos da informação devem ser protegidos adequadamente, contra ameaças externas e internas.
§ 1º - O uso de ativo de informação que não guarde relação com o exercício do cargo, função, emprego ou atividade pública será considerado indevido e passível de imediato bloqueio de acesso, sem prejuízo da apuração da responsabilidade administrativa, penal e civil.
§ 2º - O acesso de prestadores de serviços aos ativos da informação, devem ser estabelecidas contratualmente para que se assegure o cumprimento das diretrizes de segurança da informação previstas neste decreto, bem como em legislações vigentes.
§ 3º - Os ativos de informação classificados como sigilosos requerem procedimentos especiais de controles de acesso físico em conformidade com as diretrizes de acesso físico deste Decreto.
Art. 9º Para proteção adequada dos ativos deve-se:
I - Conter ferramentas de proteção contra acesso não autorizado aos ativos de informação

EXPEDIENTE:
Coordenadora de Confecção, Reg. e Exped. de Atos Oficiais – Maria de Lourdes M. Coelho da Silva
Assistente Técnico – Thiago H. Rodrigues de Andrade
Rodovia BR 262, Nº 3.700 - KM 3,0 - Alto Lage, CARIACICA-ES.
CEP: 29.151-570 - End. Eletrônico: atosoficiais@cariacica.es.gov.br
Tel: (27) 3354-5807

DIÁRIO OFICIAL DO MUNICIPIO
Cariacica (ES), quinta-feira, 23 de novembro de 2017.

que favoreça, preferencialmente, a administração de forma centralizada;
II - Respeitar o princípio do menor privilégio para configurar as credenciais ou contas de acesso dos usuários aos ativos de informação;
III - Utilizar ativo de informação homologado nas aplicações de controle de acesso, de tratamento das informações sigilosas e criptografia;
IV - Registrar eventos relevantes previamente definidos, para a segurança e rastreamento de acesso às informações sigilosas;
V - Criar mecanismos para garantir a exatidão dos registros de auditoria nos ativos de informação;
VI - Classificar os ativos de informação em níveis de criticidade, considerando o tipo de ativo de informação, o provável impacto no caso de quebra de segurança, tomando como base a gestão de risco e a gestão de continuidade de negócios, relativa aos aspectos da segurança da informação e comunicações da Administração Pública Municipal;
VII - Os projetos de TIC para aquisição de ativos da informação classificados como críticos devem considerar como requisitos, a utilização de mecanismos redundantes para garantir a alta disponibilidade dos serviços.

DO CONTROLE DE ACESSO FÍSICO

Art. 10 É de responsabilidade dos Órgãos e da Administração Pública Municipal:
I - Estabelecer regras para o uso de credenciais físicas, que se destinam ao controle de acesso dos usuários às áreas e instalações sob suas responsabilidades;
II - Orientar na instalação de sistemas de detecção de intrusos nas áreas e instalações sob suas responsabilidades;
III - Classificar as áreas e instalações como ativos de informação de acordo com o valor, a criticidade, o tipo de ativo de informação e o grau de sigilo das informações que podem ser tratadas em tais áreas e instalações, mapeando aquelas áreas e instalações consideradas críticas;
IV - Orientar o uso de barreiras físicas de segurança, bem como equipamentos ou mecanismos de controle de entrada e saída;
V- Proteger os ativos de informação contra ações de vandalismo e sabotagem, especialmente em relação àqueles considerados críticos;
VI - Implementar área de recepção com regras claras para a entrada e saída de pessoas, equipamentos e materiais;
VII - Definir pontos de entrega e carregamento de material com acesso exclusivo ao pessoal credenciado;
VIII - Intensificar os controles para as áreas e instalações consideradas críticas em conformidade com a legislação vigente;
IX - Utilizar controle de acesso físico por meio de sistema biométrico são requeridos procedimentos prévios para o credenciamento do usuário. Esse recurso deve ser utilizado em conjunto com outro sistema de identificação (cartão, crachá, senha, chave, dentre outros), a fim de atender os conceitos da autenticação de multifator.

DA CRIPTOGRAFIA

Art. 11 Fica autorizado o uso de código, cifra ou sistema de criptografia no âmbito da Administração Pública Municipal para assegurar o sigilo de documentos, dados e informações.
§ 1º Para circularem fora das instalações da Prefeitura Municipal de Cariacica os documentos, dados e informações sigilosas, produzidos em qualquer tipo de mídia móvel, devem necessariamente estar criptografados.
§ 2º Uma cópia dos documentos, dados e informações sigilosas devem ser mantidas nas áreas e instalações sigilosas da Prefeitura Municipal de Cariacica.
Art. 12 Aplicam-se aos programas, aplicativos, sistemas e equipamentos de criptografia todas as medidas de segurança previstas neste decreto para os documentos, dados e informações sigilosas e também os seguintes procedimentos:
I - Realização de vistorias periódicas, com a finalidade de assegurar uma perfeita execução das operações criptográficas;
II - Elaboração de inventários completos e atualizados do material de criptografia existente;
III - Escolha de sistemas criptográficos adequados a cada destinatário, quando necessário;
IV - Comunicação, ao superior hierárquico ou à autoridade competente, de qualquer anormalidade relativa ao sigilo, à inviolabilidade, à integridade, à autenticidade, à legitimidade e à disponibilidade de documentos, dados e informações sigilosos criptografados;
V - Identificação e registro de indícios de violação ou interceptação ou de irregularidades na transmissão ou recebimento de documentos, dados e informações criptografados.
§ 1º - O Agente Responsável pela cifração ou decifração, no exercício do cargo, função, emprego ou atividade, utilizará recurso criptográfico baseado em algoritmo adotado pela Administração Pública Municipal.
§ 2º - O agente público referido no § 1º deste artigo deverá providenciar as condições de segurança necessárias ao resguardo do sigilo de documentos, dados e informações durante sua produção, tramitação e guarda, bem como a segurança dos equipamentos e sistemas utilizados.
§ 3º - As cópias de segurança de documentos, dados e informações sigilosos deverão ser criptografados, observadas as disposições dos §§ 1º e 2º deste artigo.
Art. 13 Um canal de comunicação seguro (Rede Privada Virtual) que interligue redes de órgãos e entidades da Administração Pública Municipal, objetivando a troca de informações classificadas, deve utilizar recursos criptográficos baseado em algoritmo adotado pela Administração Pública Municipal;

DO USO E CLASSIFICAÇÃO DA INFORMAÇÃO

Art. 14 As informações institucionais geradas pelos órgãos e entidades em qualquer suporte, materiais, áreas, comunicações e sistemas de informação dessa Administração Pública, devem ser classificadas.

EXPEDIENTE:
Coordenadora de Confecção, Reg. e Exped. de Atos Oficiais – Maria de Lourdes M. Coelho da Silva
Assistente Técnico – Thiago H. Rodrigues de Andrade
Rodovia BR 262, Nº 3.700 - KM 3,0 - Alto Lage, CARIACICA-ES.
CEP: 29.151-570 - End. Eletrônico: atosoficiais@cariacica.es.gov.br
Tel: (27) 3354-5807

DIÁRIO OFICIAL DO MUNICIPIO
Cariacica (ES), quinta-feira, 23 de novembro de 2017.

§ 1º - As informações institucionais da Administração Pública Municipal deverão ser classificadas visando suas funções administrativas, informativas, probatórias e comunicativas, considerando os princípios do acesso a informação dispostos pela Lei 12.527/2011.
§ 2º - As Informações Institucionais devem ser classificadas em: Restrita (R), Interna (I) ou pública (P).
§ 3º - As Secretarias e órgãos da Administração Municipal devem promover ações para conscientização dos agentes públicos visando à disseminação das diretrizes de tratamento da informação.
Art. 15 Qualquer dado ou informação desenvolvido ou processado eletronicamente utilizando equipamentos de TIC da Prefeitura Municipal de Cariacica é de propriedade da Administração Pública Municipal.
§ 1º- Os dados e informações desenvolvidos ou gerados por agente público no cumprimento de suas atribuições são de propriedade da Administração Pública Municipal e devem ser armazenados apropriadamente nos recursos de TIC disponíveis.
Art. 16 No tratamento, tramitação das informações, deverão ser utilizados sistemas de informação e canais de comunicação seguros que atendam aos padrões mínimos de qualidade, segurança e criptografia;
Art. 17 Os dados e informações presentes em arquivos e sistemas de informação, devem possuir um usuário ou área de negócio proprietário;
§ 1º - Os proprietários da informação devem ser responsáveis pela gestão, classificação e controle de acesso a informação, conforme estabelecidos pelo Prefeito ou Secretário Municipal da respectiva pasta;
§ 2º - A liberação e revogação dos acessos a informação são de responsabilidade dos usuários e áreas de negócio proprietários, devendo seguir as diretrizes de Segurança da Informação, presentes neste Decreto.
Art. 18 São deveres do Agente Público proprietário da informação:
I - Classificar a informação;
II - Armazenar a informação classificada e sigilosa nos meios de armazenamento disponibilizados pela Administração Municipal;
III - Assegurar a publicidade da informação de caráter ostensivo, utilizando-as, exclusivamente, para o exercício das atribuições de cargo, emprego ou função pública, sob pena de responsabilização administrativa, civil e penal;
IV - Efetuar o tratamento das informações ao longo de seu ciclo de vida de modo ético e responsável e com respeito à legislação vigente.
V- As medidas e os procedimentos relacionados ao tratamento da informação a ser realizado com apoio de empresas terceirizadas, em qualquer fase do ciclo de vida da informação, deverão ser estabelecidos contratualmente para que se assegure o cumprimento das diretrizes previstas nesta norma, bem como em legislações vigentes.
Art. 19 As informações da Administração devem ser armazenadas em cópia salvaguarda, por meio de mecanismos que sejam capazes de garantir a Disponibilidade, Integridade e Confidencialidade.
§ 1º - O tempo de retenção das informações armazenadas em cópias salvaguarda deve seguir a legislação complementar designada pela Administração Municipal.
Art. 20 É considerado inadequado no Tratamento das Informações da Administração Pública Municipal:
I - Armazena-la em serviços de armazenamento remoto privados disponíveis na Internet;
II - Armazena-la em Serviços de correio eletrônicos privados;
III - Transferência por meio de Serviços FTP sem adequada requisitos de segurança;
IV - Envio de Informações Classificadas como restrita, confidencial ou com restrições de sigilo sem o devido tratamento criptográfico;
V- Divulgação de dados ou informações deliberadamente ou inadvertidamente ou sem autorização de seu superior.

DO USO DO E-MAIL INSTITUCIONAL

Art. 21 Administração Pública Municipal adotará o Correio Eletrônico como ferramenta comunicação oficial.
Parágrafo Único - O uso do Correio Eletrônico deverá ser aderente às atividades fim da Administração Municipal.
Art. 22 O armazenamento das mensagens de correio eletrônico deve ocorrer em recurso de TIC adequado que utilize mecanismos de segurança da informação apropriados.
Art. 23 As mensagens de Correio eletrônico enviadas ou recebidas a partir do domínio "cariacica.es.gov.br" e seus subdomínios são de propriedade da Administração Pública Municipal.
Art. 24 É considerado uso inadequado do Correio Eletrônico:
I - Utilizar o Correio Eletrônico provido pela Administração Municipal para envio de arquivos que não estejam relacionados às atividades administrativas;
II - Tentar ou efetivamente burlar as regras definidas para o Correio Eletrônico;
III - Tentar ou efetivamente alterar os registros de envio e recebimento de mensagens do correio eletrônico;
IV - Utilizar o Correio Eletrônico para enviar material ofensivo, difamatório, de assédio, de propaganda, etc.;
V - Divulgar informações confidenciais da Administração Municipal em grupos ou listas de correio, dentre outros, não importando se a divulgação foi deliberada ou inadvertida, sob pena de responsabilização administrativa, civil e penal.

DO USO E AQUISIÇÃO DOS EQUIPAMENTOS DE INFORMÁTICA

Art. 25 As solicitações para aquisição ou substituição de recursos de Tecnologia de Informação, devem ser encaminhadas a SUB-TI para análise segundo seus critérios de padronização.
Art. 26 A Administração Municipal proverá rede de dados para atender aos equipamentos de informática.

EXPEDIENTE:
Coordenadora de Confecção, Reg. e Exped. de Atos Oficiais – Maria de Lourdes M. Coelho da Silva
Assistente Técnico.– Thiago H. Rodrigues de Andrade
Rodovia BR 262, Nº 3.700 - KM 3,0 - Alto Lage, CARIACICA-ES.
CEP: 29.151-570 - End. Eletrônico: atosoficiais@cariacica.es.gov.br
Tel: (27) 3354-5807

§ 1º - Somente equipamentos de informática da Prefeitura Municipal de Cariacica, devem ser conectados à Rede Local Corporativa e a Rede Municipal de Dados dos órgãos e secretarias.
§ 2º - Equipamentos particulares dos Agentes Públicos, visitantes, munícipes e contribuintes, devem ser conectados e rede especifica, disponibilizada sob as diretrizes de Segurança da Informação do presente decreto;
§ 3º - Os equipamentos devem atender aos pré-requisitos mínimos de configuração e segurança, definidos pela Administração Municipal;
§ 4º - Nenhum equipamento de informática poderá ser removido ou instalado sem a anuência da SUB-TI.
Art. 27 É considerado uso inadequado dos equipamentos de Informática:
I - Alterar as configurações físicas dos equipamentos, através da inserção ou remoção de peças sem a anuência da Coordenação de Infraestrutura e Tecnologia da SUB-TI;
II - Alterar o local de instalação dos equipamentos, sem a supervisão da SUB-TI;
III - Alterar as configurações lógicas que impeçam, alterem ou possam alterar e regular a administração realizada pela SUB-TI, bem como a segurança deste ou de qualquer outro recurso de Tecnologia da Informação;
IV - Conectar equipamentos que possam tornar a rede local vulnerável a invasões externas e ataques de programas com código malicioso, em suas mais diferentes formas;
V - Conectar equipamentos que tentem ou efetivamente violem os sistemas de segurança da Administração Municipal;
VI - Conectar equipamentos que tentem ou efetivamente realizem ataques ou invasões a computadores, ou ainda, qualquer outra forma de fraude;
VII - Utilizar equipamentos para executar qualquer tipo ou forma de pirataria;
VIII - ligar equipamentos que não sejam de informática em rede elétrica estabilizada, quando esta existir;
IX - Romper lacres e proteções físicas dos equipamentos.

DO USO E AQUISIÇÃO DE SOFTWARES

Art. 28 As solicitações de aquisição e substituição de softwares, devem ser encaminhadas a SUB-TI, para análise controles de segurança da informação e comunicações e critérios de padronização.
Parágrafo Único - A SUB-TI é responsável por estabelecer critérios de segurança da informação e comunicação e padronização para aquisição ou uso de softwares nos equipamentos de informática da Administração Municipal.
Art. 29 É vedado o uso de softwares de propriedade particular nos equipamentos da Administração Municipal.
§ 1º Todos os softwares, aplicativos e sistemas utilizados nos equipamentos de informática da Administração Pública Municipal devem ser homologados e padronizados pela SUB-TI.
§ 2º A Instalação e Regularização de licenças de Softwares por todos os setores devem ser feitas por formalização das solicitações, por meio de requerimento obrigatório endereçado à SUB-TI;
§ 3º É considerado uso inadequado dos softwares de propriedade da Administração Municipal:
I - Instalar, utilizar ou manter cópias de softwares que não atendam aos critérios de padronização estabelecidos pela SUB-TI;
II - Fazer cópias não autorizadas dos softwares desenvolvidos ou adquiridos;
III - Apropriar-se, por quaisquer meios, das chaves de ativação dos softwares.
Art. 30 É de responsabilidade das empresas prestadoras de serviços, colaboradores e demais usuários, a legalidade dos softwares utilizados em seus equipamentos de informática.
§ 1º O uso de equipamentos pelas empresas contratadas, nas dependências da Administração Municipal, depende de autorização prévia da SUB-TI.
§ 2º As empresas contratadas ficam obrigadas a comprovar a legalidade de seus softwares, quando necessário.

DO USO DA INTERNET

Art. 31 A Administração Municipal adotará política interna definida por norma complementar, na inspeção e restrição de acesso à Internet, com a identificação do usuário, por meio de sistema automatizado.
§ 1º O uso da internet deverá ser aderente às atividades fim da Administração Municipal e enquadrado nos seguintes objetivos:
I - Assegurar a garantia do direito individual e coletivo das pessoas, quanto à inviolabilidade da sua intimidade e ao sigilo da correspondência e das comunicações, nos termos previstos na Constituição da República de 1988;
II - Assegurar o cumprimento e a aplicabilidade da legislação corrente quanto ao uso inadequado da internet, como por exemplo, pirataria, pedofilia, ações discriminatórias, dentre outras;
III - Minimizar a ocorrência de danos ou riscos desnecessários ao desenvolvimento das atividades realizadas pela Administração Municipal, bem como o download de programas não permitidos;
IV - Assegurar a proteção de assuntos que mereçam tratamento especial;
V - Dotar a Administração de instrumentos jurídicos, normativos e organizacionais que os capacitem científica, tecnológica e administrativamente a assegurar a confidencialidade, a integridade, a autenticidade, o não-repúdio e a disponibilidade dos dados e das informações tratadas, classificadas e sensíveis;
VI - Estabelecer normas jurídicas necessárias à efetiva implementação da segurança da informação;
VII - Promover as ações necessárias à implementação e manutenção da segurança da informação;
Art. 32 Todas as atividades fim devem ser executadas utilizando o serviço de Internet provido pela Administração Municipal.

EXPEDIENTE:
Coordenadora de Confecção, Reg. e Exped. de Atos Oficiais – Maria de Lourdes M. Coelho da Silva
Assistente Técnico – Thiago H. Rodrigues de Andrade
Rodovia BR 262, Nº 3.700 - KM 3,0 - Alto Lage, CARIACICA-ES.
CEP: 29.151-570 - End. Eletrônico: atosoficiais@cariacica.es.gov.br
Tel: (27) 3354-5807

DIÁRIO OFICIAL DO MUNICIPIO
Cariacica (ES), quinta-feira, 23 de novembro de 2017.

Art. 33 É considerado uso inadequado da Internet:
I - Tentar ou efetivamente acessar informações consideradas inadequadas ou não relacionadas às atividades administrativas, especialmente, sites de conteúdo agressivo (racismo, pedofilia, nazismo, etc.), de drogas, de pornografia, etc.;
II - Fazer o download de arquivos e outros que possam tornar a rede local vulnerável a invasões externas e ataques de programas com código malicioso, em suas mais diferentes formas;
III – Tentar ou efetivamente violar os sistemas de segurança da Administração Municipal, burlar as regras definidas, os registros de acesso, realizar ataque ou invasão a computadores, ou ainda, qualquer outra forma de fraude na Internet;
IV - Utilizar acesso à Internet provido pela Administração Municipal para upload de arquivos que não estejam relacionados às atividades administrativas;
V - Utilizar o computador para executar qualquer tipo ou forma de pirataria, envio de material ofensivo, difamatório, de assédio, de propaganda, etc.;
VI - Utilizar serviços de streaming, a não ser que o acesso seja inerente a trabalhos, pesquisas e negócios da Administração Municipal;
VII - divulgar informações confidenciais da Administração Municipal em grupos de discussão, listas, bate-papo, dentre outros, não importando se a divulgação foi deliberada ou inadvertida, sendo possível sofrer as penalidades previstas nas políticas e procedimentos internos e/ou na forma da Lei.
Art. 34 Quanto a publicações e divulgação via Internet, caberá ao Prefeito Municipal, determinar como será a análise e liberação da forma e conteúdo de quaisquer publicações oficiais via Internet.

DO USO DA REDE LOCAL

Art. 35 A rede local deve possuir os seguintes seguimentos:
I - Rede local corporativa: Rede de local onde os equipamentos da Prefeitura Municipal de Cariacica são conectados para realização das tarefas administrativas, estão disponíveis em todos os órgãos municipais participantes da Rede de Dados Municipal;
II - Rede local de dispositivos móveis: Rede local para equipamentos móveis pessoais dos Servidores municipais, fornecedores, visitantes, contribuintes e munícipes;
Parágrafo único - O tráfego de dados nos segmentos da Rede Local deve ser separado logicamente utilizando recursos de Segurança da Informação e Criptográficos apropriados nos ativos da Informação.
Art. 36 A rede local deve possuir mecanismos que:
I - Registrem os acessos à rede corporativa de computadores de forma a permitir a rastreabilidade e a identificação do usuário;
II - Evitem que equipamentos externos se conectem na rede corporativa de computadores;
III - Permitam identificar e rastrear os endereços de origem e destino, bem como os serviços utilizados;
IV - Registrem o acesso remoto à rede corporativa em logs para posterior auditoria, contendo informações específicas que facilitem o rastreamento da ação tomada;
V - Os órgãos ou entidades da Administração Pública Municipal, em suas áreas de competência, devem estabelecer regras para o uso de redes sem fio.
Art. 37 É considerado uso inadequado da Rede Local Corporativa:
I - Utilizar os recursos da rede local para transferência de arquivos que não estejam relacionados às atividades administrativas;
II - Tentar ou efetivamente violar os sistemas de segurança da rede local;
III - Tentar ou efetivamente burlar as regras definidas para o acesso à rede local;
IV - Tentar ou efetivamente alterar os registros de acesso à rede local;
V- Tentar ou efetivamente realizar ataque ou invasão a computadores da rede local;
VI - Tentar ou efetivamente negar ou desativar acesso aos serviços de Tecnologia da Informação.
Art. 38 É considerado uso inadequado da Rede Local de Dispositivos Móveis:
I - Conexão de dispositivos infectados por códigos maliciosos;
II - Tentar ou efetivamente violar os sistemas de segurança da rede local;
III - Tentar ou efetivamente burlar as regras definidas para o acesso à rede local;
IV - Divulgação de dados, documentos ou informações pessoais de outrem;
V - Utilizar a rede para roubo de dados ou mesmo se passar por outra pessoa;
VI - Utilizar a rede para tentativas de intrusão na Internet ou em outros dispositivos conectados a mesma rede;
VII - Fazer o download de arquivos e outros que possam tornar a rede local vulnerável a invasões externas e ataques de programas com código malicioso, em suas mais diferentes formas;
VIII – Tentar ou efetivamente violar os sistemas de segurança da Administração Municipal;
IX - Tentar ou efetivamente realizar ataque ou invasão a computadores, ou ainda, qualquer outra forma de fraude;
X - Utilizar a rede local para enviar material ofensivo, difamatório, de assédio, de propaganda, etc.

DO PLANO DE CONTINUIDADE DOS NEGÓCIOS E RECUPERAÇÃO DE DESASTRES

Art. 39 A Administração Municipal deve contar com um Plano de Continuidade dos Negócios, definido por norma complementar, responsável por estabelecer critérios para a Continuidade e Recuperação em caso de Desastres, dos Serviços prestados pela Administração Municipal.
§ 1º - O Plano de Continuidade deve abranger a todos os serviços de TIC da Administração Municipal, permitindo a rápido restabelecimento em caso de desastres.

EXPEDIENTE:
Coordenadora de Confecção, Reg. e Exped. de Atos Oficiais – Maria de Lourdes M. Coelho da Silva
Assistente Técnico – Thiago H. Rodrigues de Andrade
Rodovia BR 262, Nº 3.700 - KM 3,0 - Alto Lage, CARIACICA-ES.
CEP: 29.151-570 - End. Eletrônico: atosoficiais@cariacica.es.gov.br
Tel: (27) 3354-5807

§ 2º - Devem ser utilizados recurso de redundância e dispersão geográfica dos ativos para evitar indisponibilidades dos Serviços de TIC.
§ 3º - Os Ativos da Informação e Serviços classificados como Críticos e Sigilosos devem ter prioridade em seu restabelecimento no Plano de Continuidade dos Negócios.
§ 4º - Devem ser desenvolvidos procedimentos formais para operacionalização do Plano de Continuidade dos Negócios.
§ 5º - Os usuários, fornecedores e terceiros envolvidos, devem estar devidamente treinados nos procedimentos do Plano de Continuidade de Negócios.
§ 6º - Testes periódicos devem ser executados visando avaliar a capacidade operacional de executar o Plano de Continuidade de Negócios, havendo detecção e falhas as mesmas devem ser relatadas e corrigidas.

DAS PENALIDADES

Art. 40 O descumprimento das disposições contidas neste Decreto caracteriza infração funcional, a ser apurada em Processo Administrativo Disciplinar, conforme legislação vigente.
Art. 41 A autoridade que determinar a instauração de Processo Administrativo Disciplinar contra servidor pode requisitar a SUB-TI a suspensão cautelar da correspondente autorização de uso, mediante bloqueio de recursos de TI.
Parágrafo Único - O usuário identificado como causador de risco imediato aos recursos de tecnologia da informação da Administração Municipal, terá seu login, imediatamente, suspenso pela SUB-TI, com pronta notificação ao Prefeito Municipal, ao respectivo Secretário e à SEMGEPLAN, inclusive podendo ser confiscado o computador utilizado pelo usuário até o fim das investigações.

DAS DISPOSIÇÕES FINAIS

Art. 42 Os casos excepcionais a este Decreto devem ser submetidos para análise e parecer da Secretaria Municipal de Finanças.
Art. 43 Esta política deverá ser parte integrante do Plano Diretor de Informática do Município de Cariacica, podendo ser modificada, quando necessário, pela comissão para elaboração e alteração do mesmo.
Art. 44 Fica revogado o Decreto nº 74, de 18 de setembro de 2009.
Art. 45 Este Decreto entra em vigor na data de sua publicação, ficando revogadas as disposições em contrário.
Cariacica – ES, 21 de novembro de 2017.

GERALDO LUZIA DE OLIVEIRA JUNIOR
Prefeito Municipal
CARLOS RENATO MARTINS
Secretário Municipal de Finanças

DECRETO Nº 159, DE 22 DE NOVEMBRO DE 2017

INSTITUI A COMISSÃO TEMPORÁRIA DE ORGANIZAÇÃO DAS ATIVIDADES DE MOBILIZAÇÃO SOCIAL PARA A FORMAÇÃO DO GRUPO GESTOR DA PRAÇA CEU – CENTRO DE ARTES E ESPORTES UNIFICADOS – DE NOVA ROSA DA PENHA E DÁ OUTRAS PROVIDÊNCIAS.

O PREFEITO MUNICIPAL DE CARIACICA - ESTADO DO ESPÍRITO SANTO, no uso das atribuições que lhe são conferidas pelo Art. 90, Inciso XI, da Lei Orgânica do Município de Cariacica e com base no disposto no §1º do Art. 216 da Constituição Federal,

DECRETA:

Art. 1º Fica instituído, a comissão temporária de organização das atividades de mobilização social para a formação do Grupo Gestor da Praça CEU – Centro de Artes e Esportes Unificados de Nova Rosa da Penha.
Art. 2º São atribuições da Comissão:
I – Elaborar o Estatuto do Grupo Gestor da Praça CEU;
II – Elaborar o Regimento da Comissão Eleitoral que implementará e fiscalizará a eleição do Grupo Gestor;
III – Elaborar cronograma com a previsão das ações a serem realizadas até a eleição do Grupo Gestor;
IV – Realizar reuniões e oficinas de mobilização social na comunidade para capacitar candidatos e eleitores;
V - Acompanhar junto à Comissão Eleitoral o processo de eleição para a composição do Grupo Gestor.
Art. 3º O prazo de vigência dessa comissão será de 02 (dois) meses podendo ser prorrogada até a consecução do seu objeto.
Art. 4º Este Decreto entra em vigor na data de sua publicação.
Art. 5º Revogam-se todas as disposições em contrário.
Cariacica-ES, 22 de novembro de 2017.

GERALDO LUZIA DE OLIVEIRA JÚNIOR
Prefeito Municipal

PORTARIAS

PORTARIA/SEMCULT/Nº01, DE 20 DE SETEMBRO DE 2017

ALTERA A COMPOSIÇÃO DA COMISSÃO PERMANENTE DE DESCARTE DE OBRAS BIBLIOGRÁFICAS E DÁ OUTRAS PROVIDÊNCIAS.

O SECRETÁRIO MUNICIPAL DE CULTURA da PREFEITURA MUNICIPAL DE CARIACICA, no uso das suas atribuições legais que lhe são conferidas pela Artigo 58 da Lei Municipal nº 5283/2014 e c/c Art. 138 do Decreto Municipal nº. 166/2015,

RESOLVE:

Art. 1º Alterar a composição da Comissão Permanente de Descarte de Obras Bibliográficas da Biblioteca Pública Municipal, que passa a vigorar com os seguintes membros:
I. Presidente: Marcelle da Silva Coelho Queiroz – matrícula nº 111917;
II. Membro: Júlive Argentina Santos Serra – matrícula nº 115722;
III. Membro: Silvani Silva de Almeida – matrícula nº 112078;
IV. Membro: Marcos Prado Rabelo – matrícula nº 113355;
V. Membro: Evelyn Reis Bergamim – matrícula nº 114174.

EXPEDIENTE:
Coordenadora de Confecção, Reg. e Exped. de Atos Oficiais – Maria de Lourdes M. Coelho da Silva
Assistente Técnico – Thiago H. Rodrigues de Andrade
Rodovia BR 262, Nº 3.760 - KM 3,0 - Alto Lage, CARIACICA-ES.
CEP: 29.151-570 - End. Eletrônico: atosoficiais@cariacica.es.gov.br
Tel: (27) 3354-5807