

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

VERSÃO 1.0



Sumário

CAPÍTULO I	03
DISPOSIÇÕES INICIAIS E DEFINIÇÕES	03
CAPÍTULO II	03
DEFINIÇÕES	03
CAPÍTULO III	07
ORIENTAÇÕES GERAIS DE SEGURANÇA DA INFORMAÇÃO	07
CAPÍTULO IV	10
ACESSO	10
CAPÍTULO V	12
DISPONIBILIDADE	12

Estabelece a Política de Segurança da Informação da Prefeitura Municipal de Arraial do Cabo e dá outras providências.

A Prefeitura Municipal de Arraial do Cabo, por meio da presente Política da Segurança da Informação, estabelece diretrizes e normas para assegurar a proteção e integridade das informações no ambiente corporativo, incluindo dados, sistemas e recursos tecnológicos. A segurança da informação é fundamental para a continuidade dos negócios e para a conformidade com regulamentações legais e normativas.

CAPÍTULO I

DISPOSIÇÕES INICIAIS E DEFINIÇÕES

Art. 1º Regulamentar a Política de Segurança da Informação que tem por finalidade estabelecer critérios que permitam aos servidores da Prefeitura Municipal de Arraial do Cabo (PMAC) e empresas prestadoras de serviços seguir padrões de comportamento no tocante à Segurança da Informação, adequados às necessidades de negócio e de proteção legal da PMAC.

Art. 2º Todos os processos de contratação de produtos e serviços devem ser analisados quanto aos aspectos relacionados à Segurança da Informação de forma que, sempre que pertinente, estejam sujeitos aos requisitos de conformidade à política de segurança da informação e às suas normas complementares.

CAPÍTULO II

DEFINIÇÕES

DADOS	Trata-se da informação não processada
INFORMAÇÃO	É um ativo composto por um conjunto de dados ou elementos que tem valor relevante e, conseqüentemente, necessita ser adequadamente protegido de alteração, destruição e divulgação não autorizadas, quer seja acidental ou intencional

<p>CONFIDENCIALIDADE</p>	<p>Propriedade que garante que a informação só está disponível a indivíduos ou processos autorizados</p>
<p>GRAU DE SENSIBILIDADE</p>	<p>É a classificação adotada para limitar o acesso à Informação de acordo com sua natureza e importância para o negócio da PMAC. A Informação poderá ser identificada e classificada como:</p> <ul style="list-style-type: none"> ✓ Crítica - Informação restrita que, caso seja divulgada erroneamente, afetará a continuidade de um ou mais processos de negócio dos órgãos/entidades da PMN; ✓ Média - Informação interna que, caso seja divulgada erroneamente, poderá difamar a imagem da instituição ou causar prejuízos indiretos; ✓ Normal - Informação irrestrita em termos de divulgação e que poderá ser de conhecimento público.
<p>SETOR DE TECNOLOGIA DA INFORMAÇÃO</p>	<p>É a área responsável pela administração da infraestrutura de TIC dentro do órgão/entidade da PMAC, cumprindo as regras especificadas pelo Gestor da Informação</p>
<p>GESTOR DA INFORMAÇÃO</p>	<p>É o servidor ou entidade da hierarquia da PMAC responsável pelo teor e pela classificação da Informação</p>

<p>SERVIDOR</p>	<p>É todo servidor que, por uma finalidade específica, venha a ter acesso a Informações da PMAC. Servidor de outras instituições a serviço da PMAC - Parceiro, estagiário ou outra pessoa que terá acesso a Informações da PMAC, desde que comprovada à necessidade e conveniência para a PMAC, após análise e aprovação da Área de Tecnologia da Informação.</p>
<p>TECNOLOGIA DA INFORMAÇÃO</p>	<p>É o patrimônio composto por elementos de hardwares, softwares, licenças e demais componentes necessários para a execução dos sistemas e processos do órgão/entidade.</p>
<p>SETOR DE TECNOLOGIA DA INFORMAÇÃO</p>	<p>É a área responsável pela administração da infraestrutura de TIC dentro do órgão/entidade da PMAC, cumprindo as regras especificadas pelo Gestor da Informação.</p>
<p>REDE CORPORATIVA</p>	<p>É o conjunto de recursos de infraestrutura, serviços e aplicações de Tecnologia da Informação, mantidos pela Área de Tecnologia da Informação e que tem por objetivo prover interconexão e disponibilizar informações para que sejam suportados os processos organizacionais do órgão/entidade.</p>
<p>EQUIPAMENTO</p>	<p>É o conjunto de instrumentos necessários ao desenvolvimento de atividades informatizadas (micro, impressora, periférico, acessórios).</p>

SERVIDOR CORPORATIVO	É o equipamento centralizador, destinado ao armazenamento de Informações Corporativas.
SISTEMA/APLICATIVO	É todo o sistema de computação e software que abrange procedimentos e documentação relativa à sua operação.
CRIPTOGRAFIA	É a aplicação de um sistema/aplicativo para tornar incompreensível um conjunto de dados, voz ou imagem, com observância de normas especiais consignadas numa cifra ou num código.
PLANO DE CONTINGÊNCIA E CONTINUIDADE	É o plano que tem o objetivo de não permitir a interrupção das atividades do negócio e proteger os processos críticos contra efeitos de falhas ou desastres significativos.
SENHA	É o meio de validação da identidade e, conseqüentemente, de estabelecimento dos direitos de acesso para os recursos ou serviços de processamento da informação dentro de um sistema ou ambiente.

Para os fins do disposto nesta Política de Segurança da Informação abrange:

- ✓ A segurança cibernética;
- ✓ A defesa cibernética;
- ✓ A segurança física e a proteção de dados organizacionais;
- ✓ As ações destinadas a assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação.

CAPÍTULO III

ORIENTAÇÕES GERAIS DE SEGURANÇA DA INFORMAÇÃO

Artº 3 Os mecanismos, procedimentos e equipamentos de segurança adotados pelos órgãos e entidades da PMAC deverão ser praticados e/ou operados quando da utilização dos recursos de Tecnologia da Informação.

Artº 4 O Setor de Tecnologia da Informação deverá manter equipamentos/sistemas/aplicativos de segurança para controlar o acesso aos recursos de Tecnologia da Informação e para interligar a Rede Corporativa a outras redes.

Artº 5 Serão aplicados recursos de segurança de grau de complexidade compatível com o nível de importância definido para a Informação.

Artº 6 A identificação e a classificação do nível de importância da Informação para o órgão/entidade serão definidas pelo gestor da Informação, responsável por gerar e/ou armazenar a Informação.

Artº 7 O Gestor da Informação deverá analisar periodicamente a classificação da Informação em termos de valor e impacto para o órgão/entidade, pois a aquisição de novos ativos e a manipulação de novas Informações poderão mudar a prioridade de implementação dos controles de segurança

Artº 8 Na classificação da Informação, deverá se buscar, sempre que possível, o grau de segurança menos restritivo que não comprometa a Informação, visando otimizar e agilizar o processo de tratamento da Informação e, ao mesmo tempo, reduzir os seus custos de proteção.

Artº 9 Para a Informação classificada como "crítica", deverá ser preservado o seu registro histórico, com a identificação inequívoca do usuário que a acessou, de forma a permitir a execução do processo de Auditoria Interna, a ser viabilizada pelo Comitê Gestor de Tecnologia da Informação e Comunicação (CGTIC), caso necessária

Artº 10 Ao classificar uma Informação como "crítica" ou "média", deverão ser indicados as pessoas, os grupos de trabalho, os órgãos e as organizações que têm permissão de acesso a ela.

Artº 11 A Informação que não possuir uma classificação explícita quanto a sua confidencialidade deverá ser considerada como “normal”.

Artº 12 A implantação de sistema/aplicativo e/ou Informação Corporativa deverá ser precedida da definição de procedimentos de segurança, monitoração e contingência.

Artº 13 A Informação Corporativa será armazenada de forma centralizada pela Área de Tecnologia da Informação, que será responsável por manter mecanismos de segurança com o objetivo de impedir a violação e a quebra de sigilo, garantir sua disponibilidade e proteger contra perda ou dano do original.

Artº 14 Toda Informação gerada, armazenada ou veiculada no órgão/entidade é de propriedade do órgão/entidade, reservando-se a este o direito de monitorar e registrar o uso da mesma.

Artº 15 A divulgação de Informação em nome da PMAC somente poderá ser feita por servidor devidamente autorizado.

Artº 16 O usuário será responsável pela segurança das Informações armazenadas no seu equipamento, arcando com o ônus da perda ou dano dos dados.

Artº 17 A instalação de aplicativos antivírus e sua atualização sistemática nos equipamentos do órgão/entidade serão de responsabilidade do Setor de Tecnologia da Informação.

Artº 18 É vedado o uso de equipamento de informática de propriedade particular, inclusive de armazenamento portátil, no âmbito das instalações dos órgãos/entidades da PMAC.

§ 1º Será permitida a utilização de equipamento particular somente se for comprovada a necessidade e conveniência para a PMAC, após análise e aprovação da Área de Tecnologia da Informação do órgão/entidade.

§ 2º Para evitar a disseminação de vírus, o usuário deverá utilizar os meios de armazenamento portátil (pen drive, CD, DVD, etc...) somente no equipamento instalado no respectivo órgão/entidade de lotação.

I - O meio de armazenamento portátil de origem externa ao ambiente do usuário deverá ser examinado e descontaminado previamente pelo sistema/aplicativo antivírus adotado pelo órgão/entidade.

Artº 19 A responsabilidade pela Segurança da Informação deverá ser atribuída na fase de admissão do servidor no órgão/entidade e prevista no contrato individual de trabalho.

Artº 20 O servidor, em qualquer nível hierárquico, na sua esfera de competência, será responsável em cumprir e fazer cumprir a aplicação eficaz das normas e princípios da Segurança da Informação, no compromisso com os critérios legais e éticos que envolvem o órgão/entidade. É de sua responsabilidade qualquer prejuízo ou dano que vier a sofrer ou causar a PMAC ou a terceiros, em decorrência de não obediência às diretrizes e normas acima referidas.

Artº 21 O servidor será responsável pela confidencialidade de qualquer senha que lhe tenha sido concedida para acesso ou uso da Informação do órgão/entidade, sendo a senha de caráter pessoal e intransferível, não podendo ser compartilhada em nenhuma hipótese.

§ 1º Será também de responsabilidade do servidor o uso de Senha segura, devendo alterá-la conforme periodicidade determinada pelo órgão/entidade.

Artº 22 Quando o servidor tomar atitudes ou ações contrárias às diretrizes da Política de Segurança da Informação ou às normas correlatas, estará sujeito às penalidades estabelecidas em normas disciplinares da PMAC ou em contrato de prestação de serviço específico.

Artº 23 Deverão ser previstas, nos contratos de prestação de serviços de terceiros, cláusulas que contemplem as responsabilidades no cumprimento da Política de Segurança da Informação da PMAC e de suas normas e procedimentos.

Artº 24 O usuário externo, ao executar serviços autorizado pela Setor de Tecnologia da Informação ou pelo órgão/entidade detentor de equipamento de informática, não poderá utilizar os meios de armazenamento portátil de sua propriedade em equipamento instalado no órgão/entidade, conforme §2º do Art. 18.

Artº 25 Será terminantemente proibido ao servidor utilizar a Informação e o Ativo de Tecnologia da Informação para outros fins que não os estritamente profissionais, associados às atribuições de sua contratação específica, e contrários aos critérios estabelecidos na Política de Segurança da Informação e em outros Atos Normativos que tratem do assunto, especialmente em situação de pirataria, pornografia, cassino, incitação à violência ou racismo, estando sujeito a penalidades internas e a responder civil e criminalmente por seus atos.

Artº 26 Todo o Incidente de Segurança que afetar a Informação deverá ser reportado ao Comitê Gestor de Tecnologia da Informação e Comunicação (CGTIC), que tem atribuição de criar normas e padrões técnicos a serem observados pelos órgãos e pelas entidades, validar e aprovar os instrumentos instituídos pela EGD e promover a governança da tecnologia da informação e comunicação, bem como estabelecer diretrizes de segurança da informação no âmbito da Prefeitura Municipal de Arraial do Cabo e suas entidades vinculadas, caracterizando-se como a entidade mais adequada para tratar do assunto.

CAPÍTULO IV

ACESSO

Artº 27 O acesso à Rede Corporativa será disponibilizado pelo Setor de Tecnologia da Informação de acordo com o nível de acesso estabelecido pelo titular de cada órgão de nível mínimo gerencial.

Artº 28 Não será permitido acesso individual a outras redes interligadas à Rede Corporativa.

Artº 29 O acesso será controlado por equipamentos e sistemas/aplicativos com o objetivo de identificar e registrar a solicitação de acesso do usuário aos recursos de Tecnologia da Informação, bem como impedir o acesso não autorizado à rede interna do órgão/entidade em geral e, em especial, aos bancos de dados corporativos.

Artº 30 O usuário dos serviços da Rede Corporativa será cadastrado e terá um identificador individual e único, de acordo com os procedimentos operacionais definidos pela Área de Tecnologia da Informação.

Artº 31 O Acesso à Rede Corporativa do órgão/entidade se dará através de senha pessoal e intransferível, cuja guarda e sigilo é de responsabilidade do usuário.

§ 1º O usuário deverá manter o sigilo da sua senha, sendo de sua responsabilidade o uso indevido, inclusive quando utilizada por terceiros.

Artº 32 Será registrado o acesso à Informação identificada e classificada, quanto ao seu grau de sensibilidade, como “crítica” e “média”.

Artº 33 A Informação classificada como “crítica” será criptografada e protegida por senha de acesso pessoal, de responsabilidade de cada usuário.

Artº 34 As configurações das estações de trabalho não deverão ser alteradas pelo usuário.

Artº 35 Deverá ser desconectado da rede o equipamento que seja definido pelo usuário e/ou pelos padrões do órgão/entidade como detentor de Informações que devam estar protegidas com segurança total e que devam ter acesso físico especial.

Artº 36 As salas dos servidores corporativos deverão ter controle de acesso físico, sendo proibida a entrada de pessoas não autorizadas.

Artº 37 Os serviços de Correio Eletrônico Interno e Internet deverão garantir a identidade do emitente e, quando necessário, deverão ser compactados as mensagens e arquivos enviados.

Artº 38 Ao acessar a Rede Corporativa, internamente ou externamente, o usuário não poderá, em hipótese alguma, deixar sua conexão ativa, seja em que ambiente for. Ao descumprir esta determinação, o usuário implicitamente será responsável pelo uso indevido do acesso à Rede que venha a ser feito a partir de sua chave de acesso.

Artº 39 O acesso externo às Informações de uso restrito por meio da INTERNET, como aplicações específicas a determinadas áreas do órgão/entidade, deverá ser solicitado ao Setor de Tecnologia da Informação pelo titular de cada órgão de nível mínimo gerencial.

Artº 40 Os registros de eventos ocorridos na rede (log) devem ser protegidos adequadamente contra adulteração e destruição, para que não percam sua característica de evidência legal.

Artº 41 A PMAC se reservará ao direito de produzir e manter trilhas de auditoria, registrando o uso de recursos e serviços da Rede Corporativa de maneira geral, bem como as exceções e outros eventos de segurança relevantes, a fim de auxiliar investigações futuras e a monitoração de acesso.

Artº 42 O desligamento de servidores de outras instituições a serviço da PMAC, estagiários ou o encerramento do serviço prestado à PMAC por prestadores de serviço deverá ser comunicado ao Setor de Tecnologia da Informação imediatamente após a sua saída, para que o direito de acesso seja desativado.

Artº 43 A transferência de servidor deverá ser comunicada ao Setor de Tecnologia da Informação imediatamente, para que seu direito de acesso seja revisto.

Artº 44 A validade do acesso dos prestadores de serviço não poderá ultrapassar o limite estabelecido nas instruções operacionais na INTRANET, ocasião em que o acesso será automaticamente suspenso ou renovado, quando necessário.

Artº 45 Toda Informação disponibilizada a um servidor ou grupo de servidores será de uso restrito e confidencial, a menos que o Gestor da Informação a torne disponível explicitamente para outros usuários ou grupos de usuários.

Artº 46 O acesso à Informação deverá ficar restrito aos servidores autorizados para tanto, observando-se a classificação da Informação.

CAPÍTULO V

DISPONIBILIDADE

Artº 48 Será elaborado um Plano de Contingência e Continuidade do negócio, que deverá ser implementado e testado periodicamente e que deve definir, no mínimo:

- ✓ As ações, os procedimentos e a programação de testes com o objetivo de restabelecer o funcionamento dos recursos essenciais de Tecnologia da Informação;
- ✓ Os meios alternativos de funcionamento dos recursos de Tecnologia da Informação;
- ✓ Instruções para manter armazenada a configuração padrão dos equipamentos, com o objetivo de permitir a sua restauração imediata em caso de falhas.

Artº 49 As Informações dos órgãos/entidades da PMAC deverão ser protegidas por uma cópia de segurança, para que possa ser utilizada em caso de perda ou dano do original.

✓ Diariamente deverão ser feitas cópias de segurança de todas as Informações armazenadas nos servidores corporativos.

✓ No primeiro dia útil de cada mês, deverá ser feita uma cópia de segurança de todos os dados dos servidores corporativos, que será guardada em uma instalação distante do local onde estarão guardadas as cópias diárias.

✓ A área detentora de Informações que necessitem de uma agenda específica deverá combinar sua programação especial com O Setor de Tecnologia da Informação do seu órgão/entidade.

✓ A definição da periodicidade para produção de cópia de segurança de Informações não corporativas será do titular do órgão de nível mínimo gerencial, que deverá objetivar uma recuperação de dados que permita a continuidade dos serviços.

Essa Política da Segurança da Informação estabelece as principais diretrizes e responsabilidades para a segurança da informação, cobrindo desde o controle de acesso até a gestão de incidentes, com o objetivo de garantir a proteção dos dados e sistemas da Prefeitura Municipal de Arraial do Cabo. Ela pode ser adaptada conforme a realidade e as necessidades específicas da organização.