Elaborado Por	Aprovado por
Jose Ronaldo Moura Bezerra Junior	Ruan Louzeiro Santos

INDICE

1.0. OBJETIVO

- Definir responsabilidades e orientar a conduta de profissionais e usuários de Tecnologia da Informação (TI) da Empresa Maranhense de Administração Portuária - EMAP na utilização dos recursos computacionais, visando proteger a integridade e a confidencialidade das informações, assim como manter a continuidade operacional dos serviços prestados pela instituição
- Implementar as melhores práticas de segurança da informação sugeridas pela norma homologada pela ABNT, através da NBR ISO/IEC 27.002:2022
- Proteger os recursos de informação de propriedade ou sob custódia da EMAP.
- Garantir confiabilidade a parceiros comerciais nos relacionamentos que implicam a troca de informações confidenciais
- Disponibilizar, sempre que necessário, os ativos de informação para acessos legítimos e proteger os mesmos contra modificações não autorizadas, observando os três pilares da segurança de informação: confidencialidade, integridade e disponibilidade
- Estabelecer que toda e qualquer violação de segurança da informação eventualmente detectada na infraestrutura e nos ativos deverá ser imediatamente reportada e investigada, e que serão estabelecidas ações sistemáticas de controle, monitoramento e prevenção de incidentes de segurança da informação.

2.0. DOCUMENTOS DE REFERÊNCIA

Os documentos de referência podem ser consultados através do link abaixo:

- Abrir

3.0. DEFINIÇÕES

- **CONFIDENCIALIDADE:** Garantia de que a informação é acessível somente por pessoas autorizadas a ter acesso à mesma.
- **DISPONIBILIDADE:** Garantia de acesso da informação aos usuários autorizados, sempre que necessário.
- **INTEGRIDADE:** Garantia da inviolabilidade da informação durante seu ciclo de vida, preservando suas características e dados originais.
- **INFORMAÇÃO:** É um ativo, um bem corporativo que deve ter garantido a sua confidencialidade, integridade e disponibilidade.
- **RISCO:** Resultado da equação que demonstra a vulnerabilidade versus a importância de um ativo de informação.
- **TI:** Tecnologia da Informação.
- **SI:** Segurança da Informação
- **PSI:** Política de Segurança da Informação
- **VULNERABILIDADE:** Resultado da equação que demonstra o grau de exposição de um ativo versus a probabilidade de ocorrência de um incidente de segurança da informação.
- **PRINCÍPIO DE PRIVILÉGIO MÍNIMO:** Permissões limitadas, utilizada para o dia-a-dia. Com este acesso, o utilizador não terá permissão para manipular a configuração do computador, nem instalar software.
- **FTP *File Transfer Protocol***: Protocolo de Transferência de Arquivos.
- **CONEXÃO PROXY:** é um servidor intermediário que atende a requisições repassando os dados do cliente à frente: um usuário (cliente) conecta-se a um servidor proxy, requisitando algum serviço, como um arquivo, conexão, página web, ou qualquer outro recurso disponível no outro servidor.
- **REDE LOCAL:** Dois ou mais computadores interconectados por meio de placas, cabos “Leia Cabos Lógicos”. Se o número for superior a dois, utilizam-se equipamentos de interconexão *hub* e/ou *switch* para se comunicarem.

- **SERVIDOR:** Computador principal de grande porte que dele provém alguns serviços essenciais, assim como o serviço de internet, e-mail, entre outros.
- **HUB:** Aparelho de interconexão utilizado em redes de dados *Ethernet* e outros. O *hub* é responsável pelo recebimento das informações que chegam de várias direções e passar adiante, até o seu endereço “IP” de destino.
- **SWITCH:** Um *switch* é o nó central de uma rede. Ele tem como função o chaveamento entre as estações que desejam se comunicar.
- **ROTEADOR:** É o aparelho utilizado para conectar-se à *Internet Service Provider,* na Internet. Ele consiste em módulo responsável pelo controle de tráfego de pacotes entre a rede do Provedor de Acesso à Internet.
- **CABOS LÓGICOS:** São cabos utilizados para conexão entre computadores a serem aplicados a uma rede local. Ex: cabos coaxial e par trançado.
- **ESTABILIZADOR:** São equipamentos utilizados para estabilizar a voltagem local.
- **NOBREAK:** São equipamentos utilizados para a segurança dos equipamentos eletroeletrônicos. Na falta de energia elétrica o *Nobreak* dá uma sobrevida na alimentação elétrica, por alguns minutos.
- **BACKUP:** É o procedimento que realiza uma segunda cópia dos dados originais como segurança. Serve principalmente para uma eventual perda de dados, onde a segunda cópia repõe a perda da primeira. Esse tipo de procedimento de salvaguarda de arquivos e base de dados pode ser manual ou automatizado.
- **FIREWALL:** Um *firewall* é uma barreira inteligente entre a rede local e a Internet, através da qual só passa tráfego autorizado. Este tráfego é examinado em tempo real e a seleção é feita de acordo com a regra "o que não foi expressamente permitido, é proibido".
- **ACCESS POINT:** Equipamento que proporciona a conexão das estações Wireless (sem fio) até a rede local cabeada.
- **SISTEMA DE CHAMADOS:** módulo de software da Central de Serviços da GETIN responsável pelo gerenciamento de solicitações dos funcionários da EMAP.
- **PRESTADORES DE SERVIÇOS:** todo e qualquer funcionário de empresa contratada pela EMAP que utiliza um ou mais ativos de informação de propriedade da EMAP, ou sob sua responsabilidade, para realização de suas atividades.

4.0. RESPONSABILIDADES

4.1. A GERÊNCIA DE TECNOLOGIA DA INFORMAÇÃO – GETIN

- Facilitar a implementação desta política através da elaboração e divulgação de normas e procedimentos apropriados
- Analisar, autorizar ou não as solicitações das outras áreas aos itens que estão descritos na Política de Segurança da Informação.
- Monitorar as mudanças significativas na exposição dos ativos das informações às principais ameaças e adequar a avaliação de riscos a tais condições.
- Analisar criticamente as causas de incidentes de segurança da informação e suportar planos de ação para a melhoria da Segurança da Informação.
- Alocar os recursos cabíveis para iniciativas que visam aumentar o nível de segurança da informação na organização.
- Difundir a cultura de segurança da informação na empresa.
- Garantir a correta e consistente execução dos controles estabelecidos.
- Gerenciar a atualização periódica da Política de Segurança da Informação.
- Manutenção da rede (local e externa) de computadores, provendo o uso contínuo deste recurso, livre de interrupções prolongadas.
- Prover a EMAP de segurança da informação, de modo a prevenir perda de dados ou acesso por pessoas não autorizadas;
- Dar suporte técnico ao parque computacional instalado na EMAP;
- Os equipamentos e softwares de responsabilidade da GETIN são:

a) Equipamentos

- Access Point
- Cabos Lógicos
- Central Telefônica
- Estabilizador
- Hub
- Impressora
- Microcomputador
- No-breaks
- Notebook
- Projetor Multimídia
- Roteador
- Servidor
- Servidores Blades

- Servidores em lâmina com rack
- Storage
- Switch
- Telefonia móvel
- Rádios Digitais
- Coletores de Dados
- Equipamentos de Controle de Acesso

b) Softwares:

- Adobe Cloud
- Active Directory
- AutoCAD
- Banco de Dados Oracle
- BDE Administrator – RM Sistemas
- Domain Name System
- Emplac
- Exchange Mail
- Internet Information Service – IIS
- Jboss
- Kaspersky Anti vírus
- Linux
- Microsoft Office
- Microsoft Project
- Microsoft SQL Server
- Microsoft Visual Studio
- Microsoft Windows 10 Pro
- Microsoft Windows 2008 Server
- Microsoft Windows 2012 Server
- Microsoft Windows 7 Pro
- Microsoft Windows 8.1 Pro
- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2012 R2
- Networker (sistema de backup de dados)
- Painel do Terminal - Monitoramento

- Painel PRC – Monitoramento
- PRC - Chamadas (comando de voz)
- RM Corpore, Labore, Núcleos, Saldos, Fluxos
- S2GPI
- S2GPI - Balança
- SGQ - Sistema de Gestão da Qualidade
- Sistema de Mídia de TV
- Terminal Ferry Boat
- TOMCAT Apache 5.5, 6.0. (Executando GCA, GLA, GLB, GED, SCI, e-Docs)
- TOS+
- Vmware (virtualização de servidores)
- VSFTPD (File Transfer Protocol)
- Web Proxy (Mcafee)
- Windows Server Update Services – WSUS
- W-Access

4.2. TODOS OS COLABORADORES E PRESTADORES DE SERVIÇOS

- É responsabilidade de todos os empregados e prestadores de serviço proteger os ativos de informação e relatar qualquer situação que represente desvio ou violação de segurança dos mesmos, bem como atender às recomendações pertinentes constantes na Política de Segurança da Informação da EMAP.
- Todo usuário é responsável pelo equipamento que utiliza e deve solicitar chamados junto a GETIN em caso de defeito utilizando para isso o Sistema de Chamados da Central de Serviços da GETIN.
- O equipamento deverá ser devolvido à GETIN em perfeitas condições.
- Em caso de roubo/furto de aparelhos eletrônicos o usuário deverá levar até a GETIN uma cópia do B.O (Boletim de ocorrência).
- Todos os funcionários da EMAP devem assinar o EMAP-RSGSI-01 Termo de Compromisso, Confidencialidade e Sigilo (Anexo I) em duas vias, sendo uma para o funcionário e outra arquivada no dossiê do funcionário na Gerência de Recursos Humanos – GEREH.
- É obrigação de todos os colaboradores e prestadores de serviços comunicar, imediatamente, à GETIN, incidentes de segurança da informação que tomem conhecimento.

5.0. DESCRIÇÃO DO PROCEDIMENTO

- A Política de Segurança da Informação contém princípios legais e éticos a serem atendidos no que diz respeito à informática, sendo alguns desses princípios os direitos de propriedade de toda e qualquer produção intelectual; direito sobre software e normas legais correlatas que envolvam os sistemas desenvolvidos; políticas de controle de acesso a recursos e sistemas computacionais, bem como o princípio de supervisão constante das tentativas de violação da segurança de informações
- Este procedimento é aplicável a todos os empregados e prestadores de serviço que utilizem recursos de informação de propriedade da EMAP, tendo como premissa básica do seu cumprimento, o comprometimento de todos os empregados e prestadores de serviço

5.1. SISTEMA DE CONTROLE DE CHAMADOS

- Para o gerenciamento de chamados (solicitações) feitos pelos colaboradores e prestadores de serviços da EMAP, a GETIN utiliza o Sistema de Chamados da Central de Serviços da GETIN.
- Para registrar um novo chamado, o sistema permite que os usuários o façam através do envio de um novo e-mail para o endereço eletrônico servicedesk@emap.ma.gov.br ou acessando a Central de Serviços da GETIN na Intranet (http://centraldeservicos.emap.ma.gov.br/).
- Excepcionalmente, os chamados poderão ser abertos pelos ramais 6011 e 6029 para chamados relativos à rede e infraestrutura e 6512 ou 6012 para chamados relativos a sistemas.
- Os chamados para os quais um técnico da GETIN tenha solicitado informações adicionais há mais de 48 horas úteis sem resposta do solicitante serão encerrados por falta de interatividade.
- O prazo para atendimento das solicitações varia de acordo com a classificação recebida pela equipe da GETIN. Essas classificações, assim como os prazos estimados para atendimento, podem ser consultados no documento EMAP-DCSGSI-15 Catálogo de Serviços de TI.
- Para os clientes externos, os serviços disponíveis, assim como o prazo de atendimento estimado das solicitações referentes a esses serviços, podem ser

consultados no documento EMAP-DCSGSI-23 Catálogo de Serviços de TI - Clientes Externos.

- A comunicação de incidentes de segurança da informação poderá ser feito através do e-mail ou Central de Serviços da GETIN, da mesma forma que a abertura de chamados ou, caso esteja fora do horário administrativo de trabalho (segunda-feira à sexta-feira, das 8:00 às 17:00), ligando para um dos números de plantão da GETIN. A escala de plantão, assim como lista de telefones está disponível na intranet (Plantão da GETIN).

5.2. CONTROLE DE ACESSO A SISTEMAS E SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO

- As normas implementadas pela GETIN para controle de acesso de usuários a sistemas de informação e serviços de TI consistem em:
    a) **Política contra invasões externas:** A GETIN implantou o firewall que previne de modo eficaz, que usuários externos não autorizados, acessem a rede local sem a devida permissão
    b) **Política contra acessos internos não autorizados:** Os acessos internos a recursos compartilhados da rede local da EMAP são restringidos por meio de senhas de acessos e permissões de uso, de modo que determinado recurso, somente estará disponível ao usuário que possuir permissões mínimas a estes. Essas permissões possuem para arquivos, três níveis de segurança: somente leitura ao arquivo, permissões de criar/alterar arquivos e permissões de exclusão de arquivos, garantindo assim, que os arquivos e recursos sejam manipulados somente por usuários devidamente autorizados
- A liberação do acesso aos recursos de TI do empregado deve ser solicitada via Sistema de Chamados da Central de Serviços da GETIN, imediatamente após sua admissão ou remanejamento, pela Gerência de Recursos Humanos – GEREH. No caso de liberações para acesso de terceirizados, a solicitação deverá ser realizada pelo gestor da área interessada
- Todo usuário de sistemas e serviços de TI deverá ser identificado através de uma conta composta por identificação de usuário e senha ou por identificação biométrica ou por certificados digitais
- O detentor da conta e senha deve assumir a responsabilidade pela guarda, discrição ou sigilo das operações decorrentes do seu uso

- A implantação de perfis de acesso deve ser realizada com base no princípio de privilégio mínimo
- O padrão de configuração, plano de fundo, barra de tarefas, configurações de *proxy*, definido para estações de trabalho deve ser mantido, a fim de minimizar riscos de segurança da informação
- Caso haja necessidade de acesso do empregado a recursos além dos direitos básicos de perfil, o colaborador deverá solicitar ao Gestor da área e este deverá informar a GETIN – Gerência de Tecnologia da Informação via Sistema de Chamados da Central de Serviços da GETIN quais recursos adicionais devem ser liberados
- Nos casos de demissão, a Gerência de Recursos Humanos – GEREH deve solicitar à Gerência de Tecnologia da Informação, via Sistema de Chamados da Central de Serviços da GETIN, o bloqueio do usuário (acesso lógico) e correio eletrônico do empregado. A GEREH irá orientar o funcionário desligado, para que entregue os equipamentos de informática que estiverem sob sua responsabilidade para a GETIN
- A GETIN tomará as providências necessárias para o bloqueio e posterior cancelamento da conta, e receberá se houver, os equipamentos de informática de propriedade da empresa, que estiverem sob responsabilidade do funcionário desligado. A GETIN irá preencher o EMAP-RSGSI-12 Termo de Devolução (Anexo II) em duas vias a serem assinadas, sendo que uma entregue para o funcionário e outra arquivada na Central de Serviços da GETIN
- Sempre que um colaborador da EMAP for contratado, remanejado de setor ou desligado da EMAP, a CORET – Coordenadoria de Relações Trabalhistas deverá informar à GETIN, via Sistema de Chamados da Central de Serviços da GETIN, para revisão dos acessos aos recursos de TI
- Caso a solicitação não possa ser resolvida pela equipe interna, seja por causa de garantia do equipamento ou sistema, ou porque o equipamento ou ferramenta, está sob cobertura do contrato de manutenção, é feito um chamado externo, junto à empresa parceira, para a realização do serviço solicitado
- **Nota 1:** Nesses casos, a GETIN é responsável por acompanhar o chamado externo e informar ao usuário solicitando o andamento do chamado

5.3. SELEÇÃO E USO DE SENHAS

- Senhas são de uso pessoal e intransferível, sendo sua manutenção e confidencialidade responsabilidade de seu proprietário

- Senhas não devem ser registradas em papel, ou em qualquer meio sem controle ou caracterizado como de acesso público
- As senhas devem conter o padrão mínimo de 6 (seis) caracteres, atendendo ao menos 3 critérios, sendo eles: letra maiúscula, letra minúscula, números e símbolos
- Senhas temporárias ou iniciais devem ser alteradas pelo usuário no primeiro acesso, conforme regras estabelecidas nesta norma
- Senhas de acesso aos recursos de informática devem ser alteradas periodicamente, evitando a reutilização de senhas antigas. Caso esse procedimento não seja realizado pelo usuário, o sistema automaticamente solicitará a cada 3 meses, uma nova senha ao usuário
- O acesso (conta) aos recursos de TI será bloqueado após 5 (cinco) tentativas com erro
- Senhas devem ser alteradas pelos usuários, sempre que existir qualquer indicação de possível comprometimento do sistema, ou das próprias senhas
- Na criação e alteração da senha de acesso à rede e aos sistemas de informação deve-se evitar a utilização de:
    c) Nome próprio ou sobrenome do usuário;
    d) Nome de parentes ou time de preferência;
    e) Datas comemorativas;
    f) Sequência de números e letras;
    g) Conjunto de caracteres totalmente iguais;
    h) Conjunto de caracteres iguais à conta;
    i) Informações que possam ser obtidas do próprio usuário, tais como: telefone, número da identidade, número do CPF, placa de carro, etc.

5.4. USO DE ATIVOS DE INFORMAÇÃO

- Os funcionários da EMAP, para executar suas atividades, poderão utilizar ativos de informação, fixos e móveis, como celular, notebook, modem 3G/4G, tabletes, entre outros.
- Para todo ativo de informação, haverá um responsável e esse necessariamente deverá ser um funcionário da EMAP.
- **Nota 2:** Prestadores de serviço também poderão receber e utilizar ativos de informação da EMAP, porém a responsabilidade pelos ativos utilizados por eles é gestor da área a qual o prestador está vinculado.

- O responsável por ativos de informação móveis deverá assinar o EMAP-RSGSI-26 Termo de Responsabilidade no ato de entrega do equipamento (Anexo I). No caso de desligamento da empresa, o funcionário deverá assinar EMAP-RSGSI-12 Termo de Devolução do equipamento (Anexo II) e em caso de entrega temporária do equipamento, o EMAP-RSGSI-11 Termo de Empréstimo (Anexo III). As assinaturas deverão ser feitas em duas vias, sendo uma anexada à Central de Serviços da GETIN e a outra entregue ao usuário.
- **Nota 3:** Em caso de danos ao ativo de informação, o responsável pelo mesmo poderá ser cobrado pela reparação pelo dano.
- Os usuários e administradores de estações de trabalho, ou de outros recursos computacionais, devem acionar as proteções adequadas quando interromperem ou finalizarem suas atividades operacionais (bloqueio, *logoff* ou desligamento da estação).
- A conexão de equipamentos de terceiros (empregados e prestadores de serviço) à rede corporativa da EMAP deve ser solicitada através do Sistema de Chamados da Central de Serviços da GETIN pela Diretoria ou Gerência da área interessada, cabendo a Gerência de Tecnologia da Informação, autorizar ou não esta conexão.
- Somente a Gerência de Tecnologia da Informação é autorizada a executar a conexão de equipamentos de terceiros à rede corporativa da EMAP, não sendo permitido a nenhum outro setor, executar este procedimento.
- Qualquer ocorrência (quebra, falha, mau funcionamento, incidente de segurança da informação, desaparecimento) relacionada aos equipamentos de informática, deverá ser informada à GETIN pelo Sistema de Chamados da Central de Serviços da GETIN, com cópia para o gestor da sua área. Em caso de roubo ou furto, o funcionário deverá apresentar comprovação do fato por meio de Boletim de Ocorrência para a Gerência de Tecnologia da Informação. Depois de apresentado, o Boletim de Ocorrência deverá ficar em poder da GETIN. Um novo equipamento poderá ser entregue ao funcionário, desde que autorizado pelo gestor da área.
- É vedado o uso de modem nas estações de trabalho conectadas à rede corporativa, salvo quando houver um setor que esteja com problemas de conexão. A instalação será feita somente pela equipe GETIN, através de solicitação do Gestor da área pelo Sistema de Chamados da Central de Serviços da GETIN.
- Qualquer movimentação de equipamento de TI demandada pelos usuários, deve ser solicitada à área de Informática, através do Sistema de Chamados da Central de Serviços da GETIN, com anuência do gestor da área, para garantir o correto funcionamento e adequação dos inventários físicos dos mesmos.

- Não é permitida qualquer alteração de hardware nos equipamentos de TI, incluindo cabeamento lógico e elétrico, sem uma prévia análise da GETIN.
- Não é permitido o uso de dispositivos de armazenamento móveis nos ativos de informação da EMAP, salvo situações específicas analisadas, autorizadas e monitorados pela GETIN.
- Não é permitido o uso de dispositivos de armazenamento móveis para transferência de informações entre setores e/ou para fora da empresa, salvo situações específicas analisadas, autorizadas e monitorados pela GETIN.
- Para transferência de informações, deve-se utilizar o e-mail. Na impossibilidade de uso do mesmo, a GETIN deverá ser acionada através do sistema de chamados da Central de Serviços da GETIN.
- Os ativos de informação e dispositivos de armazenamento móveis de propriedade da EMAP só poderão ser desativados após eliminação completa das informações contidas nos mesmos.
- Para os empregados e prestadores que possuem autorização para uso de mídias de armazenamento removíveis, sempre que um desses dispositivos for conectado ao ativo de informação, o antivírus deverá realizar uma varredura automaticamente e o seu uso somente será liberado se nenhuma ameaça for identificada.
- Após o uso, as informações contidas nesses dispositivos deverão ser eliminadas de forma permanente, não permitindo a sua recuperação, total ou parcial.
- Em caso de dúvidas, a respeito de como fazê-lo, a GETIN deverá ser acionada através do sistema de chamados da Central de Serviços da GETIN.

5.5. COMPUTAÇÃO MÓVEL E TRABALHO REMOTO

- O trabalho à distância está restrito aos empregados e prestadores de serviços autorizados diretamente por seus gestores e pela Gerência de Tecnologia da Informação, conforme as regras de acesso definidas por este procedimento.
- Os usuários de computação móvel devem estar cientes dos seguintes riscos e aceitar as seguintes responsabilidades:

    a) A segurança física e lógica existente no local de trabalho à distância deve ser avaliada com o objetivo de minimizar o risco de roubos de informações ou ocorrência de incidentes de segurança que comprometam a segurança dos sistemas da EMAP;
    b) O acesso a informações ou recursos por pessoas não autorizadas, será de responsabilidade do responsável pelo dispositivo móvel em questão.

- Quaisquer incidentes de segurança da informação, que ocorram nas localidades remotas de trabalho, tais como roubos, invasões, ataques por vírus, deverão ser imediatamente comunicadas à Gerência de Tecnologia da Informação, para que as medidas apropriadas sejam tomadas.
- Os dispositivos móveis devem ter suas sessões bloqueadas quando o empregado se afastar do equipamento.
- Os dispositivos móveis devem ser desligados e acondicionados corretamente em local onde somente o empregado tenha acesso, quando não estiver em uso.
- Para os empregados que possuem autorização para uso de mídias de armazenamento removíveis, sempre que um desses dispositivos for conectado ao ativo de informação, o antivírus deverá realizar uma varredura automaticamente e o seu uso somente será liberado se nenhuma ameaça for identificada.
- O empregado deve providenciar a transferência das informações da EMAP manipuladas no dispositivo móvel para o servidor de arquivos, quando necessário.
- Quando da devolução do dispositivo móvel ao setor de TI, as informações da EMAP devem ser transferidas definitivamente para o servidor de arquivos. Se existentes, o empregado da EMAP deve transferir suas informações pessoais para outras mídias de armazenamento.
- O empregado deve apagar todas as informações pessoais que tenha sido armazenada no dispositivo móvel. Em caso de dúvidas, deve solicitar auxílio a GETIN.
- A GETIN não se responsabiliza por nenhuma informação pessoal do usuário contida/deixada nos dispositivos móveis.
- Excepcionalmente, os empregados da EMAP que tenham sob sua responsabilidade computadores móveis poderão ter acesso remoto à infraestrutura interna da EMAP.
- O trabalho remoto à infraestrutura da EMAP somente será autorizado quando for de estrito interesse da empresa, devendo ser precedida de solicitação do gestor do setor do empregado e análise quanto a sua necessidade, viabilidade e autorização formal da GETIN.
- O trabalho remoto à infraestrutura interna deve ser realizado somente a partir de ativos de informações e dispositivos móveis de propriedade da EMAP.
- A GETIN deve providenciar a instalação dos sistemas de informações necessários para o trabalho remoto.
- O trabalho remoto à infraestrutura interna deve ser solicitado, formalizado e justificado pelo superior imediato do empregado a GETIN.

- O setor solicitante deve informar o prazo de validade para a realização do trabalho remoto.
- O perfil de acesso e permissões que o usuário possui aos sistemas de informações e recursos da rede interna da EMAP devem ser os mesmos, tanto no trabalho remoto quanto na infraestrutura interna.
- Todo acesso remoto autorizado deverá possuir prazo de expiração que poderá ser renovado mediante solicitação do gestor do setor do empregado e análise quanto a sua necessidade, viabilidade e autorização formal da GETIN.

5.6. INSTALAÇÃO E UTILIZAÇÃO DE SOFTWARES

- Os equipamentos de informática funcionarão somente com softwares regularmente adquiridos e licenciados junto a seus fornecedores ou representantes, ou ainda, aquele fruto de desenvolvimento personalizado para EMAP.
- A aquisição de novos softwares deverá ser solicitada a GETIN, ficando essa Gerência responsável por avaliar e autorizar a aquisição.
- A área de Informática realizará levantamento periódico de inventário, através de ferramenta específica, assim efetuando a verificação das estações de trabalho utilizadas pelos colaboradores da EMAP, objetivando manter o inventário atualizado e as versões dos softwares de atualização operacionais padronizadas.
- São expressamente proibidas as seguintes atividades:
    a) Cópia de softwares adquiridos ou desenvolvidos pela EMAP, seja qual for a finalidade;
    b) Instalação de softwares nos ativos de informação da EMAP;
    c) Modificação ou distribuição de dados ou programas sem autorização.
- Todas as estações de trabalho e servidores corporativos serão protegidos pelo software antivírus homologado, que deve estar sempre ativo e atualizado, seguindo as configurações definidas pela Gerência de Tecnologia da Informação.
- O software de antivírus somente poderá ser removido das estações de trabalho e servidores, pelos técnicos da Gerência de Tecnologia da Informação.
- A instalação de qualquer software nos ativos de informação da EMAP somente poderá realizada pelos técnicos da GETIN e deverá ser solicitada pelo funcionário da EMAP, com anuência de seu gestor, através do Sistema de Chamados da Central de Serviços da GETIN e analisado e autorizado pelos gestores da GETIN.

5.7. PROTEÇÃO DAS INFORMAÇÕES

- Ao usuário, é expressamente proibido:

    a) A transmissão ou posse de informações, que impliquem violação de direitos autorais (pirataria) ou de propriedade da informação;
    b) Divulgação não autorizada de qualquer informação classificada como restrita ou confidencial;
    c) Utilização dos servidores da Empresa, para armazenamento de informações ou arquivos pessoais (fotos, vídeos e músicas);
    d) Armazenar informações confidenciais em diretórios públicos;
    e) Acesso anônimo a qualquer recurso de rede ou sistema da Empresa, a não ser que o mesmo tenha sido criado para este fim.

- Os usuários têm obrigação de bloquear as estações de trabalho quando se afastarem das mesmas para impedir acesso não autorizado. Após 5 (cinco) minutos de inatividade, as estações de trabalho serão bloqueadas automaticamente.
- Em caso de violação às medidas de segurança das informações, a GETIN deve efetuar o bloqueio do acesso do usuário à rede, e comunicar o fato ocorrido, imediatamente ao responsável pela área onde ocorreu a violação, para que sejam aplicadas as advertências ou sanções cabíveis.
- Todo usuário, empregado ou terceiro, deve relatar à área de Informática qualquer violação da Política de Segurança da Informação instituída, ou qualquer problema de segurança tão logo os perceba, para que sejam tomadas as devidas medidas corretivas pela Empresa.
- Os documentos em papéis e mídias eletrônicas não devem permanecer sobre a mesa desnecessariamente, devem ser armazenados em armários ou gavetas trancadas, quando não estiverem em uso, especialmente fora do horário do expediente.
- Informações sensíveis ou críticas para o negócio da EMAP devem ser trancadas em local separado e seguro (um armário ou cofre à prova de fogo).
- Anotações, recados e lembretes não devem ser deixados à mostra sobre a mesa ou colados em paredes, divisórias, murais ou monitor do computador.
- Não anotar informações sensíveis em quadros brancos.
- Não guardar pastas com documentos sensíveis em locais de fácil acesso.
- Destruir os documentos impressos antes de jogá-los fora. Sempre que possível utilizar máquinas desfragmentadoras.
- Não imprimir documentos apenas para lê-los. Leia-os nas telas dos ativos de informações, preferencialmente.

- Informações sensíveis ou confidenciais, quando impressas em local coletivo, devem ser retiradas da impressora imediatamente.
- Devolver todos os documentos obtidos por empréstimos de outros departamentos, quando eles não forem mais necessários.
- Guardar agendas e cadernos de anotações, assim como objetos pessoais, em gavetas ou armários trancados.
- Manter crachá de identificação e/ou chaves junto ao corpo e notificar o setor de segurança patrimonial imediatamente se sumirem.
- Nunca anotar as senhas em papeis ou ativos de informação. As mesmas devem ser memorizadas.
- Preferencialmente, mesas e móveis deverão ser posicionados de forma que dados sensíveis não sejam visíveis de janelas ou corredores.
- Ao final do expediente, ou em caso de ausência prolongada do local de trabalho, a mesa de trabalho deve permanecer limpa, documentos guardados, gavetas e armários trancados e computador desligado.
- Não deixar o local de trabalho aberto sem que haja um colaborador que trabalhe no local presente.

5.8. RESTAURAÇÃO DE CÓPIAS DE SEGURANÇA

- A GETIN é responsável por efetuar as operações de *Backup* e Restauração das informações armazenadas nos servidores da EMAP.
- Entende-se por *Backup* as operações de cópias realizadas para garantir a recuperação de dados em caso de perda.
- Não será realizado pela Gerência de Tecnologia da Informação, Backup de nenhuma informação ou arquivo armazenado nas estações de trabalho ou documentos pessoais, salvo os que estão armazenados no Active Directory.
- Quando necessário, o proprietário da Informação, deve solicitar formalmente à GETIN a restauração da cópia de segurança da informação armazenada nos servidores, com a aprovação dos superiores imediatos, através do Sistema de Chamados da Central de Serviços da GETIN.
- Os backups são divididos em três categorias:

    a) Backup de imagens de vídeo monitoramento, cujo tempo de retenção será de 180 (cento e oitenta) dias;
    b) Backup de caixas de correio (somente e-mails no servidor), cujo tempo de retenção será de 90 (noventa) dias;

c) Backup dos demais arquivos e documentos, cujo tempo de retenção será de 180 (cento e oitenta) dias

5.9. MANUTENÇÃO E ADMINISTRAÇÃO DO AMBIENTE

- Alterações em locais que afetem ou demandem novos recursos de infraestrutura de rede, devem ser informados à Gerência de Tecnologia da Informação, para as devidas providências. As alterações somente serão feitas após análise da GETIN, sendo que a mesma informará se a mudança pode ou não ocorrer.
- Qualquer remanejamento do usuário entre setores da empresa deverá ser comunicado imediatamente pela Gerência de Recursos Humanos à GETIN, que providenciará as alterações necessárias.
- As permissões referentes ao setor de origem serão retiradas e as novas permissões (referentes ao setor de destino) serão atribuídas.

5.10. USO DE MENSAGENS ELETRÔNICAS (E-MAIL)

- O correio eletrônico é um recurso disponibilizado pela EMAP para uso profissional, sendo passível de auditoria.
- As regras para a segura utilização de correio eletrônico e dos serviços de acesso à Internet devem ser conhecidas e cumpridas por todos os usuários, são elas:
    a) Não enviar sem autorização formal do responsável pela área, quaisquer documentos, contendo material confidencial, ou de uso interno da empresa;
    b) Não utilizar o correio eletrônico da empresa para veicular correntes, filmes, músicas, pornografias, movimentos políticos ou outros conteúdos não relacionados à finalidade de trabalho;
    c) Não utilizar palavras de baixo calão, ou ofensivas a qualquer outro usuário, seja interno ou externo.
    d) Não abrir mensagens de e-mail que contenham assuntos estranhos, ou que tenham sido enviadas por desconhecidos. Tais mensagens podem conter vírus incorporados em seu conteúdo.
    e) Em caso de dúvidas quanto à segurança do conteúdo do e-mail, o mesmo deve ser encaminhado para o Sistema de Chamados da Central de Serviços da GETIN para análise.
- O uso particular do correio eletrônico, de ordem eventual não é permitido.

- As mensagens do correio eletrônico deverão ser armazenadas no servidor corporativo da Empresa, onde estarão devidamente protegidas e salvaguardadas.
- A integridade e o backup de mensagens armazenadas fora dos servidores corporativos serão de responsabilidade do usuário.
- Mensagens de correio eletrônico são consideradas correspondências oficiais. Assim sendo, recomenda-se a identificação do usuário emitente, mediante inserção de informações ao final do texto, contendo:

    a) Nome do remetente
    b) Cargo / Setor
    c) Telefone
- Todo usuário poderá enviar/receber mensagens, desde que não excedam o limite de 20 MB (vinte) Megabytes.
- A caixa postal dos usuários, também terá limite pré-estabelecido pela Gerência de Tecnologia da Informação, sendo este limite, fixado em 50 GB, para colaboradores e 10 GB para prestadores de serviços.
- Para envio/recebimento de arquivos que excedam o limite de 20 MB, o usuário deverá solicitar à GETIN através do Sistema de Chamados da Central de Serviços da GETIN, para que esta possa orientar sobre as melhores formas de realizar este procedimento.
- É expressamente proibida a transmissão de mensagens de correio eletrônico indiscriminadamente para todos os empregados. As exceções serão definidas pela Gerência de Recursos Humanos - GEREH.
- A área de Informática regularmente verifica o uso do correio eletrônico, com o objetivo, de detectar ameaças à segurança ou uso indevido. Para tal, poderão ser utilizados softwares específicos, com funcionalidades de bloqueio proativo de spams.
- A utilização do serviço de e-mail por prestadores de serviço deve ser precedida de solicitação do Gestor da área interessada, devendo a Gerência de Tecnologia da Informação autorizar ou não.
- As contas de e-mail autorizadas para os prestadores de serviços é individual e intransferível, porém na sua identificação, além do nome do prestador de serviços, deve constar o nome da empresa a qual o mesmo está vinculado. Exemplo; empresaxpto.joao@emap.ma.gov.br.
- Reserva-se à EMAP, o direito de auditar a utilização de suas contas de correio eletrônico fornecidas aos usuários, sem se caracterizar invasão de privacidade.

- É terminantemente proibido aos representantes da GETIN, administradores de rede e/ou correio eletrônico ler mensagens de correio eletrônico de qualquer usuário quando estiver realizando serviços de manutenção e suporte, exceto quando em cumprimento de determinações das diretorias para efeitos de auditoria, ou da própria justiça.
- Os usuários são responsáveis pela utilização do e-mail corporativo da EMAP e, portanto, serão identificados e responsabilizados em caso de uso indevido.

5.11. UTILIZAÇÃO DE INTERNET

- A utilização do acesso à Internet na EMAP deve estar prioritariamente relacionada às tarefas desempenhadas pelo empregado. Uso pessoal, de ordem eventual é permitido, desde que não consuma recursos significativos de tempo, ou interfira na produtividade pessoal, e ainda que não vá de encontro com o disposto nos itens abaixo.
- Todos os acessos à internet serão armazenados em log, para posterior pesquisa, se necessário;

    a) O acesso à Internet na EMAP está direcionado aos serviços de consulta à WEB e correio eletrônico;
    b) É vetado o acesso a sites de conteúdo de jogos, crimes, rádios, TVs, apostas, eróticos, pornográficos e blogs. A EMAP irá restringir os acessos a sites que, considerar alheios aos objetivos da Empresa, e monitorar consultas de usuários com o objetivo de garantir segurança e adequação no uso deste recurso;
    c) A solicitação de liberação de acesso a sites bloqueados deve ser enviada para Gerência de Tecnologia da Informação via Sistema de Chamados da Central de Serviços da GETIN e deve conter o endereço do site, justificativa para liberação e anuência do seu gestor. O acesso será liberado somente após autorização dos gestores da GETIN;
    d) O Acesso ao serviço de FTP deve ser solicitado formalmente pelo responsável da área interessada à GETIN pelo Sistema de Chamados da Central de Serviços da GETIN justificando o pedido. O serviço será liberado somente após autorização dos gestores da GETIN;
    e) É proibido o uso de serviços de troca de mensagens instantâneas *(softwares externos não autorizados ou disponibilizados pela GETIN),* reprodução de músicas on-line ou afins;

f) Sempre que os usuários, utilizando a Internet, tiverem acesso a materiais criminosos como pornografia infantil (arte, textos, figuras, cenas, imagens) e outros, mesmo que de maneira esporádica ou involuntária, deverão entrar em contato imediatamente com a GETIN.

- Nos casos que houver necessidade de o usuário acessar a internet sem restrições, a solicitação deve ser realizada pela Gerência a qual o usuário está ligado. Essa solicitação deve ser enviada via Sistema de Chamados da Central de Serviços da GETIN à Gerência de Tecnologia da Informação, ficando esta responsável por avaliar e liberar ou não este acesso.
- Os usuários que estiverem com liberação total de acesso à internet também terão seus acessos monitorados.
- Os usuários são responsáveis por seus acessos à Internet, e, portanto, serão identificados e responsabilizados em caso de acessos indevidos.

5.12. USO DOS SISTEMAS DE INFORMAÇÃO

- Os empregados autorizados a acessarem os Sistemas de Informação que são utilizados na EMAP têm por obrigação fornecer todos os dados que complementem os cadastros existentes a fim de evitar inconsistência na base de dados.
- A concessão e autorização de perfis de acesso aos sistemas de informação serão solicitadas via Sistema de Chamados da Central de Serviços da GETIN, pelo gestor da área, à Gerência de Tecnologia da Informação:

    a) Perfis de acesso são direitos de acesso a funcionalidades dos sistemas de informação, de acordo com as tarefas executadas pelo empregado;
    b) Cabe ao Gestor do usuário e à Gerência de Tecnologia da Informação definir qual o perfil adequado para acessar cada sistema, devendo este perfil estar documentado na solicitação;
    c) Cabe também ao Gestor do usuário certificar que o nível de acesso concedido está adequado aos propósitos do negócio e não comprometa o desempenho de funções;

- Cabe à área de Informática remover as contas de acesso aos sistemas de informação de usuários que tenham sido desligados, ou revogar os direitos em caso de transferência e conceder as permissões necessárias para a nova função.
- Para prestadores de serviço que necessitam de acesso aos sistemas de informação, é necessário que o gestor da área responsável envie uma solicitação através do

Sistema de Chamados da Central de Serviços da GETIN, informando os dados do usuário.

5.13. USO DE RECURSOS DE TELEFONIA

- A utilização de ramais telefônicos e telefones celulares da EMAP devem estar prioritariamente relacionados às tarefas desempenhadas pelos empregados:
    a) Uso pessoal, de ordem eventual e para ligações locais é permitido, desde que não consuma recursos significativos de tempo, ou interfira na produtividade pessoal;
    b) Uso pessoal para ligações DDD ou DDI não serão permitidas.
- A Gerência de Tecnologia da Informação fica responsável pelas seguintes atividades, mediante solicitação do gestor direto do solicitante e autorização dos gestores da GETIN:
    a) Habilitação de novos ramais telefônicos;
    b) Alterações de categorias de serviços;
    c) Emissão de relatórios de detalhamento de ligações telefônicas (relatório fornecido pela operadora e/ou software de gerenciamento de ligações)
    d) Atendimento a solicitações de aparelhos de telefone celular. Estas solicitações deverão ser efetuadas pelo Gestor da área. A GETIN determinará o valor da franquia que será liberada para a linha.
- A Área de Informática será responsável pela manutenção dos equipamentos de telefonia, visando manter a integridade, disponibilidade e segurança dos serviços.
- É vetado aos usuários dos serviços de telefonia:
    a) Utilizar os serviços de telefonia para acesso a serviços de entretenimento, tais como participação em programas de rádio ou TV;
    b) Utilizar serviços auxiliares das operadoras de telefonia fixa e móvel, tais como salas de bate-papo e serviços de interatividade com os meios de comunicação, tais como votação telefônica.
- Os ramais telefônicos serão programados com categorias de serviço, de acordo com a abrangência de uso do mesmo:
    a) Categoria 0 – Recebe ligações internas e externas e origina ligações locais;
    b) Categoria 2 – Recebe ligações internas e externas e origina ligações locais e DDD;

c) Categoria 4 – Recebe ligações internas e externas e origina ligações locais, DDD e DDI.
d) Categoria 6 – Recebe ligações internas e externas e origina ligações locais e celulares locais;
e) Categoria 8 – Recebe ligações internas e externas e origina ligações locais, celulares e DDD;
f) Categoria 10 – Recebe ligações internas e externas e origina ligações locais, celulares, DDD e DDI.

- A troca de categorias de um determinado ramal deve ser solicitada pelo Gestor da área à Gerencia de Tecnologia da Informação, através do Sistema de Chamados da Central de Serviços da GETIN e autorizada pela GETIN.

5.14. USO DA REDE SEM FIO (WIRELESS)

- O uso da rede corporativa sem fio da EMAP é para uso exclusivo com ativos de informação de propriedade da EMAP ou sob sua responsabilidade.
- Os usuários são responsáveis por toda utilização da Internet via rede sem fio da EMAP, portanto, serão identificados e responsabilizados em caso de acessos indevidos.
- Os ativos de informação que não estão sob responsabilidade da EMAP, poderão ser conectados à rede sem fio para visitantes que pode ser utilizada por funcionários, prestadores de serviços e visitantes por ativos de informação.
- A rede de visitantes não deve ser utilizada para realização das atividades profissionais, uma vez que não é possível acessar a rede interna da EMAP, pasta compartilhada na rede e sistemas de informação de acesso exclusivo pela rede interna.
- Todo o acesso à Internet através da rede wireless da EMAP será monitorado.

5.15. SOLICITAÇÃO DE DESENVOLVIMENTO DE SISTEMAS DE INFORMAÇÃO

Toda solicitação de desenvolvimento de sistema deve ser feita conforme procedimento **EMAP-PC-119 Solicitação de Projetos de Tecnologia da Informação**

5.16. INSTALAÇÃO DE CERTIFICADOS DIGITAIS

- Os colaboradores e prestadores de serviços que necessitam de certificado digital para executar suas atividades na EMAP deverão solicitar a instalação do mesmo (ou permissão para utilização de tokens) no ativo de informação da EMAP (ou sob sua responsabilidade).
- Os certificados digitais instalados podem ser de propriedade do próprio colaborador (eCPF) ou de propriedade da EMAP (eCNPJ).
- Quando da solicitação, o colaborador ou prestador de serviços deverá justificar sua solicitação e, caso a solicitação refira-se a um eCNPJ, o gestor da área deverá autorizar a sua instalação e utilização.
- O uso do certificado digital do tipo eCNPJ somente será autorizado quando for de estrito interesse da empresa, devendo ser precedida de autorização do gestor do setor do empregado e análise quanto a sua necessidade, viabilidade e autorização da GETIN.
- Caso o certificado digital seja de propriedade da EMAP (eCNPJ), o responsável pelo seu uso deverá assinar o EMAP-RSGSI-26 Termo de Responsabilidade no ato de entrega da instalação do mesmo (Anexo V). As assinaturas deverão ser feitas em duas vias, sendo uma anexada à Central de Serviços da GETIN e a outra entregue ao usuário.
- Os usuários do certificado digital do tipo eCNPJ devem estar cientes dos riscos e aceitar as responsabilidades contidas no EMAP-RSGSI-26 Termo de Responsabilidade acima citado.
- O uso do certificado digital do tipo eCNPJ deve ser realizado somente em ativos de informações de propriedade da EMAP (ou sob sua responsabilidade) indicados pela GETIN.
- Quaisquer incidentes de segurança da informação envolvendo o certificado digital do tipo eCNPJ deverão ser imediatamente comunicadas à Gerência de Tecnologia da Informação e para o seu gestor, para que as medidas apropriadas sejam tomadas.
- Somente a Gerência de Tecnologia da Informação é autorizada a executar a instalação de certificados digitais em ativos de informação da EMAP, não sendo permitido a nenhum outro setor, executar este procedimento.

5.17. PENALIDADES

- A GETIN alerta a todos os usuários da EMAP que a instalação ou a utilização de *software* não autorizado constitui crime contra a propriedade intelectual, de acordo

com a Lei nº 9.609, de 19/02/1998, sujeitando os infratores à pena de detenção e multa.

- Alerta também que todos os usuários são responsáveis pelo uso correto das ferramentas eletrônicas de propriedade da EMAP e, que todas as práticas que representam ameaça à segurança da informação, serão tratadas com a aplicação de ações disciplinares.
- Na ocorrência de infrações constantes desse documento, ficam os infratores sujeitos às seguintes penalidades:

a) Advertência verbal;
b) Advertência por escrito;
c) Suspensão;
d) Demissão e/ou outras medidas judiciais cabíveis.

Nota: As penalidades serão aplicadas de acordo com a gravidade da infração.

- Os usuários estão sujeitos também às penalidades previstas no Código de Conduta e Ética da EMAP.

6.0. ANEXOS

- Anexo I: EMAP-RSGSI-13 Termo de Responsabilidade
- Anexo II: EMAP-RSGSI-12 Termo de Devolução
- Anexo III: EMAP-RSGSI-11 Termo de Empréstimo
- Anexo IV: EMAP-RSGSI-01 Termo de Compromisso, Confidencialidade e Sigilo
- Anexo V: EMAP-RSGSI-26 Termo de Responsabilidade Certificado Digital

7.0. REGISTROS

Identificação	Local do Arquivo	Armazenamento	Proteção	Disposição e Recuperação	Tempo de Retenção		Descarte
					Tempo	Base legal	
EMAP-RSGSI-13 Termo de Responsabilidade	Servidor	Central de Serviços da GETIN	Usuário e senha. Acesso restrito à GETIN	Ordem cronológica	Permanente	Não há	Não há

Identificação	Local do Arquivo	Armazenamento	Proteção	Disposição e Recuperação	Tempo de Retenção		Descarte
					Tempo	Base legal	
EMAP-RSGSI-12 Termo de Devolução	Servidor	Central de Serviços da GETIN	Usuário e senha. Acesso restrito à GETIN	Ordem cronológica	Permanente	Não há	Não há
EMAP-RSGSI-11 Termo de Empréstimo	Servidor	Central de Serviços da GETIN	Usuário e senha. Acesso restrito à GETIN	Ordem cronológica	Permanente	Não há	Não há
EMAP-RSGSI-26 Termo de Responsabilidade Certificado Digital	Servidor	Central de Serviços da GETIN	Usuário e senha. Acesso restrito à GETIN	Ordem cronológica	Permanente	Não há	Não há
EMAP-RSGSI-01 Termo de Compromisso, Confidencialidade e Sigilo	Sala de GEREH	Dossiê do funcionário	Pasta A/Z	Ordem cronológica	10 anos	Não há	Picotar

8.0. HISTÓRICO DE REVISÃO

Versão	Data	Item	Revisões
20	27/09/2023	2	Documentos de referência foi retirado foi revogado. O Ato Declaratório Executivo Coana/Cotec nº 2, de 26 de setembro de 2003

Versão	Data	Item	Revisões
21	10/06/2024	Todo o procedimento	Alteração: NBR ISO/IEC 27.002:2013 > NBR ISO/IEC 27.002:2022 E NBR ISO/IEC 27.001:2013 > NBR ISO/IEC 27.001:2022
21	14/06/2024	2	Alteração: Documentos Inseridos na intranet