INDICE

1.0 OBJETIVO

- Definir responsabilidades e orientar a conduta de profissionais 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 27.002:2013
- 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

2.0 DOCUMENTOS DE REFERÊNCIA

- ABNT NBR ISO/IEC 27001:2013 - Tecnologia da informação
- ABNT NBR ISO/IEC 27002:2013 - Tecnologia da informação
- Decreto nº 7.845, de 14 de novembro de 2012
- Decreto nº 9.637 de 26 e dezembro de 2018
- Instrução Normativa GSI nº 1 de 13 de junho de 2008
- Lei nº 9.609/98
- Lei nº 9.610, de 18 de fevereiro de 1998
- Lei nº 9.279, de 14 de maio de 1996
- Lei nº 9.983, de 14 de julho de 2000
- Lei nº 12.527, de 18 de novembro de 2011
- Lei nº 12.965, de 23 de abril de 2014
- Norma Complementar nº 02/IN01/DSIC/GSIPR
- Norma Complementar nº 03/IN01/DSIC/GSIPR
- Norma Complementar nº 05/IN01/DSIC/GSIPR, e seu anexo
- Norma Complementar nº 07/IN01/DSIC/GSIPR
- Norma Complementar nº 08/IN01/DSIC/GSIPR
- Norma Complementar nº 09/IN01/DSIC/GSIPR
- Norma Complementar nº 10/IN01/DSIC/GSIPR
- Norma Complementar nº 11/IN01/DSIC/GSIPR
- Norma Complementar nº 12/IN01/DSIC/GSIPR
- Norma Complementar nº 13/IN01/DSIC/GSIPR
- Norma Complementar nº 14/IN01/DSIC/GSIPR

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.
- **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:

4.1.1 EQUIPAMENTOS:

- Access Point
- Cabos Lógicos
- Central Telefônica
- Estabilizador
- Hub
- Impressora
- Microcomputador
- NoBreak
- 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

4.1.2 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)
- WebProxy (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).

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 da Gerência de Tecnologia da Informação – GETIN, tendo como premissa básica do seu cumprimento, o comprometimento de todos.

5.1 SISTEMA DE CONTROLE DE CHAMADOS

- A GETIN deve implantar uma ferramenta para controle de chamados (solicitações) feitos pelos colaboradores e prestadores de serviços da EMAP, o **Sistema de Chamados da Central de Serviços da GETIN**.
- Os funcionários da GETIN também poderão acessar diretamente o Sistema de Chamados da Central de Serviços da GETIN e registrar um novo chamado.
- Ao criar um novo chamado, a ferramenta deverá registrar automaticamente pelo menos as seguintes informações (que pode ser extraídas do e-mail): número do chamado (identificador), usuário solicitante, assunto, data de criação e resumo da solicitação.
- Assim que o chamado for criado pelo sistema, o usuário solicitante deverá notificado automaticamente a respeito do número do chamado, de forma que

seja possível enviar novas informações para o chamado apenas respondendo o e-mail recebido.

- A ferramenta também deverá ter funcionalidades para controlar as seguintes informações: responsável pelo atendimento, categoria, tempo para resolução da solicitação e prioridade.
- Todos os técnicos da GETIN ou prestadores de serviços, com a devida autorização, responsáveis por atendimento às solicitações deverão ser acesso ao sistema através de credenciais individuais, tendo acesso a todos os chamados do sistema, seja para atendimento a um chamado em aberto seja para consulta do histórico de chamados.
- Ao final do atendimento de cada chamado, o sistema deverá enviar um e-mail ao usuário que fez a solicitação informando encerramento do mesmo e solicitando que seja feita uma avaliação do atendimento através de um formulário eletrônico (link para o mesmo deverá ser enviado nesse e-mail) onde deverão ser avaliados aspectos relacionados à qualidade e tempo do atendimento.
- O sistema deverá fornecer relatórios customizáveis que utilizem as informações listadas acima, permitindo análise por parte dos gestores a respeito dos atendimentos.

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

- Preferencialmente, os logins de acesso aos sistemas de informação e serviços de TI deverão ser integrados ao Active Directory da EMAP.
- Senhas de acesso aos recursos de informática baseados no Active Directory da EMAP 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.
- É recomendado que o controle de acesso aos recursos de TI não baseados no Active Directory possuam funcionalidade para obrigar o usuário a alterar a senha a cada 3 meses.
- O acesso (conta) aos recursos de TI cujo controle de acesso seja baseado no Active Directory da EMAP será bloqueado após 5 (cinco) tentativas com erro.

- É recomendado que o acesso (conta) aos recursos de TI cujo controle de acesso não seja baseado no Active Directory da EMAP também sejam bloqueados após 5 (cinco) tentativas com erro.
- Os colaboradores da GETIN são responsáveis por atribuir aos demais colaboradores da EMAP e prestadores de serviços permissões de acesso a recursos compartilhados da rede local e sistemas de informação.
- Os colaboradores da GETIN devem possuir perfis de acesso diferenciados para executar as atividades de administração da infraestrutura e para realização de tarefas não relacionadas a administração.
- Os colaboradores da GETIN também poderão ter conhecimento da senha de Administrador da rede interna da EMAP para poder atribuir os corretos perfis de acesso aos demais funcionários e prestadores de serviços
- As contas de acesso com perfil de administrador devem ter nomenclatura de fácil associação ao Administrador.
- As contas de acesso impessoais, tais como: *guest*, visitante, backup, operador super etc. não podem ser utilizadas pelos empregados do setor de TI, exceto aqueles utilizados para execução de serviços essenciais e que por limitação técnica não podem ser substituídos.
- O acesso à sala da GETIN, assim como ao datacenter da EMAP, é restrito aos colaboradores desse setor, colaboradores da GESEP e bombeiros, sendo o acesso controlado e registrado por meio de Sistema de Controle de Acesso.
- O acesso outras pessoas (colaboradores da EMAP ou prestadores de serviço) a qualquer um desses ambientes só poderá ocorrer mediante autorização de um dos colaboradores da GETIN e acompanhados por este.
- A GETIN deve analisar e revisar os diretos de acessos aos sistemas de informação e à infraestrutura interna da EMAP de todos os usuários da EMAP, pelo menos, anualmente.
- Toda análise e revisão dos direitos de acesso deve ser deve ser documentada, utilizando o RELATÓRIO DE REVISÃO DE PERMISSÕES E DIREITOS DE ACESSO DE USUÁRIOS ANEXO I (EMAP-RSGSI-15), e armazenada na Central de Serviços da GETIN.

5.3 SUPORTE A INFRAESTRUTURA INTERNA E USUÁRIOS DE TI

- Os colaboradores da GETIN são responsáveis pela administração, manutenção e auditoria de toda infraestrutura de TI e gerenciamento de controle de acesso a sistemas e serviços de TI.

- Os colaboradores da GETIN não podem arbitrariamente acessar, ler, apagar, utilizar ou transferir informações de usuários sem a devida autorização e formalização da atividade.

5.3.1 ATIVIDADES DE ADMINISTRAÇÃO DA INFRAESTRUTURA INTERNA

As seguintes atividades de **administração** da infraestrutura interna devem ser executadas:

- Manter a infraestrutura interna em perfeitas condições de funcionamento, certificando a qualidade, disponibilidade e integridade dos serviços.
- Avaliar os impactos de novas tecnologias antes de sua aquisição e implantação na infraestrutura interna.
- Certificar que os ativos de informação possuem somente sistemas de informações homologados.
- Desinstalar ou desabilitar serviços e sistemas desnecessários ao funcionamento dos ativos.
- Elaborar e manter atualizada uma lista de sistemas de informações homologados.
- Desinstalar das estações de trabalho dos empregados e prestadores de serviço os sistemas de informações não homologado, devendo informar tanto ao usuário quanto ao superior imediato a atividade.
- Atualizar os ativos sempre que for detectado a disponibilização de atualizações e/ou patches de correções por parte dos fabricantes.
- Preferencialmente, as atualizações devem ocorrer em horário que não comprometam o funcionamento da infraestrutura interna.
- Orientar os usuários em relação a eventuais falhas de segurança que possam ocorrer por conta de alterações nos ativos de informação.
- Toda e qualquer alteração de tecnologia na infraestrutura interna da EMAP deve ser comunicada aos usuários afetados pela alteração.
- As estações de trabalho da EMAP devem possuir mecanismos de segurança que impeçam sua abertura por pessoas não autorizadas.
- Os servidores da infraestrutura interna da EMAP não devem ser ligados em tomadas elétricas não estabilizada, bem como ligados em conjunto com outros ativos elétricos que não sejam de TI.
- As estações de trabalho da EMAP devem ser configuradas seguindo os padrões de segurança estabelecidos pelo setor de TI.

5.3.2 ATIVIDADES DE MANUTENÇÃO DA INFRAESTRUTURA INTERNA

As seguintes atividades de **manutenção** da infraestrutura interna devem ser executadas:

- Os ativos de informações que suportam processos de negócios críticos da EMAP devem ser priorizados no atendimento e manutenção.
- As manutenções das estações de trabalho devem ser realizadas somente com a autorização do usuário solicitante.
- Os colaboradores da GETIN poderão realizar as manutenções remotamente.
- Os prestadores de serviço também poderão realizar manutenções remotamente, porém, para tal, deve existir uma formalização da necessidade via Sistema de Chamados da Central da de Serviços da GETIN.
- Os ativos de informações que suportam processos de negócios críticos da EMAP (como racks, dispositivos de rede, servidores etc.) devem ser providos de rotinas de manutenção preventiva, pelo menos, a cada 6 meses.

5.3.3 ATIVIDADES DE AUDITORIA DE INFRAESTRUTURA INTERNA

As seguintes atividades de **auditoria** da infraestrutura interna devem ser executadas:

- A GETIN, a seu critério e quando possível, poderá habilitar e desabilitar funcionalidades de geração de logs de auditoria nos ativos de informação e nos sistemas de informações da EMAP.
- Quando possível, os logs deverão contemplar as seguintes informações:
    - Identificação do usuário
    - Evento-chave
    - Data e hora do evento-chave
    - Registro de tentativa de acesso ao ativo / sistema (com e sem sucesso)
- Os colaboradores da GETIN podem realizar periodicamente auditoria nos referidos logs, se necessário.
- Os arquivos de log devem fazer parte do processo de cópias de segurança, seguindo a Política Técnica de Cópias de Segurança.
- As informações existentes nos logs de auditoria dos ativos da EMAP não devem ser divulgadas sem autorização prévia do gestor da GETIN.
- Os sistemas de informação podem possuir usuários com permissão somente leitura com o objetivo de auditar funcionalidades e/ou registros dos sistemas.

5.4 CONTROLE OPERACIONAL DOS ATIVOS DE INFORMAÇÃO

5.4.1 INVENTÁRIO DOS ATIVOS DE INFORMAÇÃO

- Todos os ativos de informação da EMAP, assim como os ativos de informação que não são de sua propriedade, mas que estão sob sua custódia, devem ser inventariados e identificados de forma única.
- Esses ativos de informação devem funcionar somente com softwares regularmente adquiridos e licenciados junto a seus fornecedores ou representantes.
- Um sistema de informação deve ser utilizado para gerenciar os ativos de informação da EMAP e os seus responsáveis.
- O inventário dos ativos de informações deve incluir todas as informações necessárias de forma a permitir a sua recuperação ou substituição efetiva.
- O inventário deve prover as seguintes informações dos ativos de informações:
    - Identificação do ativo
    - Localização do ativo
    - Responsável
    - Descrição de hardware e/ou software
    - Tipo do ativo
    - Identificação de licenças de uso (se for o caso)
    - Valor do ativo para a organização (se for o caso)
- O inventário de ativos de informações deve ser dinâmico, estruturado e com atualização periódica de forma a manter uma base dados dos ativos da EMAP.
- Sempre que um ativo de informação for entregue/desenvolvido a um usuário, as informações do ativo de informação deverão ser atualizadas no sistema de informação de inventários e o Termo de Responsabilidade (ou Termo de Devolução ou Termo de Empréstimo) deverá ser digitalizado e anexado ao sistema
- Os ativos de informações devem ser classificados de forma a assegurar o manuseio e a proteção adequada.
- A segregação de funções (desenvolvimento, homologação e produção) deve ser definida para reduzir o mau uso ou uso doloso dos sistemas de informação da empresa.

5.4.2 CONTROLE DE MUDANÇAS OPERACIONAIS

- Todas as mudanças nos ativos de informação da EMAP devem ser previamente avaliadas quanto aos requisitos de segurança da informação pela GETIN e só poderão ocorrer com autorização dos gestores da GETIN.
- O sistema de informação de controle de inventários deve ser capaz de gerenciar as mudanças relacionadas aos ativos de informação e que possibilite a identificação e o registro das alterações operacionais realizadas.
- Para execução das demais atividades referentes a controle de mudanças operacionais, os empregados da GETIN devem observar as regras descritas no **procedimento EMAP-PC-75 Gestão de Mudanças**.

5.4.3 CONTROLE DE CAPACIDADE DOS ATIVOS DE INFORMAÇÃO

- A utilização dos recursos deve ser monitorada através de indicadores, ajustada e as projeções de capacidade futura devem ser feitas para necessidades para garantir o desempenho requerido do sistema.
- As projeções de capacidade futura, assim como eventuais dificuldades identificadas devem ser registradas através dos procedimentos **EMAP-PC-74 Gestão de Problemas** e **EMAP-PC-75 Gestão de Mudanças**.

5.4.4 DESATIVAÇÃO DE ATIVOS DE INFORMAÇÃO E DISPOSITIVOS DE ARMAZENAMENTO MÓVEIS

- 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.
- O processo de descarte das mídias que contenham informações deve ser realizado de forma a impossibilitar recuperação parcial ou total dessas informações.

5.5 COMPUTAÇÃO MÓVEL E TRABALHO REMOTO

5.5.1 DISPOSITIVOS MÓVEIS

- A utilização de dispositivos móveis pelos empregados da EMAP somente será autorizada quando for de estrito interesse da empresa, devendo ser analisada e autorizada pelo gestor da área a qual o funcionário faz parte.
- A EMAP consente na utilização cuidadosa dos dispositivos móveis para interesses particulares, desde que não exceda os limites da razoabilidade, ética e bom senso.

- É vetado o uso dos dispositivos móveis da EMAP para acesso a conteúdos de jogos, crimes, rádios, TVs, apostas, eróticos, pornográficos e blogs.
- A concessão aos empregados da EMAP para portar os dispositivos móveis está condicionada a autorização formal do superior imediato do setor.
- A distribuição somente será concedida pela GETIN caso haja disponibilidade do dispositivo móvel.
- Os dispositivos móveis somente podem ser acessados mediante o uso de uma conta de acesso para proteção e segurança das informações que estão armazenadas neles.
- Nos dispositivos móveis da EMAP devem conter instalações apenas de sistemas de informações homologados pela GETIN.
- Os usuários dos dispositivos móveis são proibidos de instalar/desinstalar softwares nos mesmos.
- Para utilização de sistemas de informações diferentes dos fornecidos no dispositivo móvel, deve-se solicitar, via sistema de chamados, para análise, avaliação e instalação no dispositivo, mediante autorização pelos gestores da GETIN.

5.5.2 TRABALHO REMOTO

- O acesso remoto à infraestrutura interna da EMAP é controlado e monitorado pela GETIN e utiliza mecanismos de criptografia na troca de informações.
- Todos os acessos de trabalhos remotos devem ser monitorados com seus respectivos logs.
- Os logs devem ter no mínimo data e hora, serviço utilizado, usuário de acesso e informações específicas que facilitem o rastreamento e a auditoria posterior.
- O acesso para trabalho remoto somente poderá ser concedido com autorização formal do gestor da área do usuário solicitante e dos gestores da GETIN.

5.6 AQUISIÇÃO, DESENVOLVIMENTO E MANUTENÇÃO SEGURA DE SISTEMAS DE INFORMAÇÃO

5.6.1 REQUISITOS DE SEGURANÇA DE SISTEMAS DE INFORMAÇÃO

- Antes do desenvolvimento de um sistema é necessário um levantamento e documentação de requisitos, quando os requisitos de segurança devem ser identificados e acordados antes do início de desenvolvimento e/ou implementação de sistemas de informação.

- Todos os requisitos de segurança devem ser identificados na fase de levantamento de requisitos dos projetos, sendo justificados, acordados e documentados como parte dos artefatos de negócio dos sistemas de informação.
- Todo o ciclo de desenvolvimento de sistemas deve ter requisitos de segurança da informação definidos desde a definição, projeto, desenvolvimento, implantação e manutenção.
- Os contratos de desenvolvimento de sistemas de informações com prestadores de serviços devem possuir uma cláusula instituindo propriedade exclusiva dos códigos-fonte dos sistemas desenvolvidos para a EMAP, seja desenvolvido interna ou externamente.
- Os contratos de customizações de sistemas de informações desenvolvidas para uso exclusivo da EMAP devem possuir uma cláusula instituindo propriedade da empresa.
- Todos os desenvolvedores que tiverem acesso aos códigos-fonte e base de dados dos sistemas desenvolvidos para ou na EMAP, sejam funcionários, sejam empresas prestadoras de serviços ou funcionários das empresas prestadoras de serviços tem obrigação de manter sigilo e confidencialidade.
- Os processos de aquisição de sistemas de informações devem sempre explicitar os requisitos de segurança que os mesmos devem possuir

5.6.2 CONTROLES CRIPTOGRÁFICOS

- Os sistemas de informações adquiridos ou desenvolvidos pela EMAP devem fazer uso de criptografia, no mínimo, para as senhas dos usuários dos sistemas.

5.6.3 SEGURANÇA NO PROCESSO DE DESENVOLVIMENTO

- Os ativos de informação da GETIN devem ser segregados em diferentes ambientes para promover maior segurança ao processo de desenvolvimento e implantação dos sistemas de informação:
  - Desenvolvimento
  - Homologação
  - Produção
- Os sistemas de informação em desenvolvimento e homologação devem ser processados em ambientes totalmente distintos do ambiente de produção (servidores de aplicação e banco de dados).

- As senhas de acessos aos ativos de informação dos três ambientes devem ser diferentes e, no caso do ambiente de produção, de conhecimento restrito a poucos funcionários da GETIN.
- A massa de dados utilizadas nos testes de desenvolvimento e homologação, preferencialmente, devem ser diferentes da utilizada no ambiente de produção.
- O processo de geração de massa de dados, preferencialmente, deve ser automatizado para criar informações aleatórias e que não reflitam dados de produção.
- O ambiente de homologação deverá ser utilizado para validar os requisitos (inclusive de segurança e vulnerabilidades) dos sistemas de informação desenvolvidos ou modificados pela GETIN (ou por prestadores de serviços) antes de ser implantado no ambiente de produção.
- Novos sistemas de informação adquiridos pela EMAP, assim como novas versões e *patches* de correções desses sistemas, também deverão ser validados no ambiente de homologação antes de implantados no ambiente de produção, inclusive com objetivo de identificar vulnerabilidades técnicas.
- O desenvolvimento de sistemas de informações realizados por prestadores de serviço deve ser supervisionado integralmente pelos empregados da EMAP.
- Sempre que o usuário solicitar o desenvolvimento de uma nova funcionalidade e/ou relatórios, ou mesmo a modificação, um registro de Solicitação de Mudança (procedimento **EMAP-PC-75 Gestão de Mudanças**) deverá ser criado.
- Durante o processo de desenvolvimento do sistema de informação os testes unitários devem validar os requisitos de segurança da informação.
- Sempre que um sistema de informação for validado no ambiente de homologação, os requisitos de processamento definidos na fase de levantamento de requisitos deverão ser validados de modo a reduzir os riscos de falhas de desempenho.
- Cada sistema de informação desenvolvido pela GETIN deve ter um empregado responsável designado.
- A GETIN deverá implantar uma ferramenta para controle de identificação e versionamento de todos os sistemas de informação desenvolvidos.
- A ferramenta deve possuir controle de acesso baseado em perfis permitindo gerenciar as permissões dos desenvolvedores.
- Os acessos aos códigos fontes devem ser concedidos considerando o princípio de privilégio mínimo.

- Também deverá ser registrado um log com as atividades realizadas pelos desenvolvedores, permitindo auditoria das atividades realizadas com os códigos-fonte.
- As ferramentas de desenvolvimento utilizadas na EMAP para a geração de sistemas de informação devem ser especificadas e identificadas claramente, desde a análise de requisitos e modelagem até a programação e testes.
- Todos os sistemas de informações desenvolvidos pela/para EMAP devem possuir documentação dos requisitos, modelagem, programação e ciclo de testes.
- As documentações devem fornecer evidências de quais medidas de segurança foram adotadas durante o processo de desenvolvimento.
- As evidências devem garantir que as medidas são suficientes para manter a integridade e confidencialidade dos sistemas de informação.
- Sempre que uma nova versão de um sistema de informação for validada e estiver pronta para ser implantada em produção, os usuários afetados pelo sistema deverão comunicados.
- A aplicação de *patches* de correções considerados pequenos e sem impacto de indisponibilidade temporária do sistema não necessitam de comunicado.

5.6.4 GESTÃO DE VULNERABILIDADES TÉCNICAS

- A GETIN deve possuir ferramentas para identificação de vulnerabilidade técnica dos sistemas de informação adquiridos e/ou desenvolvidos pela/para a EMAP.
- Sempre que um sistema de informação for validado no ambiente de homologação, as vulnerabilidades técnicas deverão ser analisadas.
- As vulnerabilidades técnicas identificadas devem ser registradas, avaliadas e medidas apropriadas devem ser tomadas para reduzir os riscos associados, através dos procedimentos **EMAP-PC-74 (Gestão de Problemas)** e **EMAP-PC-75 (Gestão de Mudanças)**.

5.6.5 PROCESSAMENTO CORRETO DE APLICAÇÕES

- Os sistemas de informações devem ter seus dados de entrada validados para garantir que são corretos e apropriados.
- A validação deve ser realizada com vistas a detectar falta de integridade das informações, por erros ou ações intencionais.

- Os sistemas de informações devem ter seus dados de saída validados para garantir que o processamento das informações estão corretos e são apropriados.

5.7 BACKUP E RESTAURAÇÃO

- 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.
- Este procedimento considera dois tipos de cópias de segurança:
  - **Cópias de segurança full:** cópia de todas as informações contidas nos servidores da infraestrutura interna, tais como: servidor de banco de dados, servidor de arquivos, servidor de sistemas de informações e servidor controlador de domínio;
  - **Cópias de segurança diferencial:** cópia que contempla somente as informações que foram alteradas desde a última cópia de segurança full.

5.7.1 REALIZAÇÃO E RESTAURAÇÃO DE CÓPIAS DE SEGURANÇA

- A GETIN deve realizar cópia de segurança dos servidores da infraestrutura do datacenter de forma automatizada, através de software especializado em gestão de cópias de segurança, preferencialmente fora do horário de expediente.
- 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.
- As cópias de segurança realizadas mensalmente devem ser do tipo full e as realizadas diariamente do tipo diferencial.
- A GETIN deve planejar cópias de segurança, considerando o ciclo de vida dos dispositivos de armazenamento das cópias de segurança e suas características, conforme especificação dos fabricantes.
- Em caso de falha na execução do backup, a solução de gerenciamento de cópias de segurança deve enviar alerta o sistema de chamados da GETIN para imediata análise dos logs gerados.
- Em caso de falhas no processo de realização cópias de segurança, a GETIN deve providenciar imediatamente ações corretivas.

- A cópia de segurança dos servidores da infraestrutura interna deve ser provisionada de forma a manter redundância.
    - Uma cópia deve ser armazenada próximo aos servidores da infraestrutura interna.
    - Outra cópia deve ser armazenada em local externo com as mesmas características de segurança da infraestrutura interna.
- A restauração de cópias de segurança contidas deve ser realizada nas seguintes situações:
    - Restabelecer o funcionamento e/ou integridade dos servidores da infraestrutura do datacenter.
    - Restauração de cópias obrigatórias com solicitação formal de setores da EMAP com a aprovação dos superiores imediatos.
- A restauração das cópias de segurança deve ser realizada somente pela GETIN.
- A restauração deve ocorrer em ambiente diferente de sua origem, preferencialmente.
- A GETIN deve instruir o setor solicitante que confirme a autenticidade e integridade das informações restauradas antes do seu uso.
- Pelo menos uma vez por mês, a GETIN realizar testes de restauração de cópia de segurança, por amostragem, de leitura, acesso, recuperação das informações armazenadas nas mídias de cópias de segurança como forma de certificar a recuperação correta das informações quando necessário.
- Os testes de recuperação de cópia de segurança devem ser documentados, utilizando RELATÓRIO DE TESTE DE RESTAURAÇÃO DE BACKUP - ANEXO II (EMAP-RSGSI-14), e armazenados na Central de Serviços da GETIN.
- O prazo de retenção das cópias de segurança obedece aos seguintes critérios:
    - Caixa de correio (e-mail) no servidor: 90(noventa) dias;
    - Demais arquivos, documentos: 180 (cento e oitenta) dias

5.7.2 TRATAMENTO DE CÓPIAS DE SEGURANÇA

- O acesso físico ao local onde as cópias de segurança ficam armazenadas deve ser protegido e controlado.
- Toda infraestrutura de suporte ao funcionamento das cópias de segurança também deve ser protegida e controlada.

- Aos empregados da GETIN é vedada a transferência de informações contidas nas cópias de segurança para mídias de uso pessoal e/ou ativos de informação que não sejam da EMAP.
- As cópias de segurança eventuais devem ser identificadas de forma diferenciada das cópias periódicas, devendo ser incluída a informação do setor solicitante.
- A GETIN deve manter documentação (registro) de todas as operações de cópias de segurança e restaurações.
- A GETIN deve elaborar e manter atualizada documentação referente ao manuseio das cópias de segurança.
- O local de armazenamento da documentação deve estar em ambiente com acesso restrito e controlado.
- O hardware e software utilizados para a realização das cópias de segurança e restauração só devem ser substituídos após certificação de que todas as informações contidas nas mídias antigas foram transferidas para as novas.
- Os antigos hardware e software só devem ser eliminados após verificação completa das informações transferidas.

5.8 COMPUTAÇÃO EM NUVEM

- A EMAP poderá fazer uso de serviços em nuvem pública, privada ou híbrida.
- Os tipos de serviços de nuvem possíveis de serem utilizados pela EMAP são:
    - **IaaS (infraestrutura como serviço):** inclui servidores e máquinas virtuais, armazenamento (VMs), redes e sistemas operacionais
    - **PaaS (plataforma como serviço):** serviços de computação em nuvem que fornecem um ambiente sob demanda para desenvolvimento, teste, fornecimento e gerenciamento de aplicativos de software
    - **SaaS (software como serviço):** aplicativos de software pela Internet sob demanda e, normalmente, baseado em assinaturas
- Independentemente do tipo da nuvem e dos serviços contratados, a GETIN deve manter o controle de acesso utilizando os mesmos critérios de segurança da infraestrutura local.
- A comunicação entre o datacenter da EMAP e a nuvem deve utilizar mecanismos de criptografia na troca de informações, sendo este controlado e monitorado pela GETIN.

6.0 ANEXOS

- Anexo I – EMAP-RSGSI-15 RELATÓRIO DE REVISÃO DE PERMISSÕES E DIREITOS DE ACESSO DE USUÁRIOS
- Anexo II – EMAP-RSGSI-14 RELATÓRIO DE TESTE DE RESTAURAÇÃO DE BACKUP

7.0 REGISTROS

Identificação	Local do Arquivo	Armazenamento	Proteção	Recuperação	Tempo de Retenção		Descarte
					Tempo	Base legal	
EMAP-RSGSI-15 Relatório de Revisão de Permissões/Direitos de Acesso de Usuários	Servidor	Central de Serviços da GETIN	Usuário e senha. Acesso restrito à GETIN	Ordem cronológica	Permanente	Não há	Não há
EMAP-RSGSI-14 Relatório de Teste de Restauração de Backup	Servidor	Central de Serviços da GETIN	Usuário e senha. Acesso restrito à GETIN	Ordem cronológica	Permanente	Não há	Não há

8.0 HISTÓRICO DE REVISÃO

Versão	Data	Item	Revisões
0	25/09/2019		Elaboração do Procedimento
0	29/09/2019	5.2	A GETIN deve analisar e revisar os diretos de acessos aos sistemas de informação e à infraestrutura interna da EMAP de todos os usuários da EMAP, pelo menos, a cada 6 meses
0	29/09/2019	6	Inclusão dos anexos I e II
0	29/09/2019	7	Retirado registro “Relatório de Manutenção Preventiva Ativos de TI”
1	27/01/2020	3	Incluída a definição de PRESTADORES DE SERVIÇOS
2	18/09/2020	2	Documentos de referência atualizados
2	18/09/2020		Corrigido layout dos Anexos I e II