Documento: **Política de Segurança da Informação – PSI**	Data Emissão:13/06/2023

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E DAS COMUNICAÇÕES DO MPMT

1 – ESCOPO

A Política de Segurança da Informação (PSI) tem por finalidade de estabelecer as diretrizes para a segurança do manuseio, tratamento e controle e para a proteção dos dados, informações e conhecimentos produzidos, armazenados ou transmitidos, por qualquer meio, pelos sistemas de informação e serem, obrigatoriamente, observadas na definição de regras operacionais e procedimentos no âmbito Institucional;

O objetivo é estabelecer mecanismos e controles para garantir a efetiva proteção dos dados, informações e conhecimentos gerados, bem como a redução dos riscos de ocorrência de perdas, alterações e acessos indevidos, preservando a disponibilidade, integridade, confidencialidade e autenticidade das informações no MPMT;

Essa Política aplica-se a todos os membros, servidores, estagiários, terceirizados e voluntários do MP e demais agentes públicos ou particulares que, oficialmente, executem atividade vinculada à atuação institucional do MPMT.

2 – PRINCÍPIOS

A garantia ao direito pessoal e coletivo à intimidade e ao sigilo da correspondência e das comunicações individuais;

A proteção dos dados Pessoais coletados e processados no MPMT, conforme sua finalidade e classificação;

A proteção das informações e conhecimentos produzidos no MPMT, conforme sua classificação;

O Estabelecimento de diretrizes de segurança da informação, visando à adoção de procedimentos e mecanismos relacionados à proteção de dados e das informações de sua propriedade e sob sua guarda;

A garantia de atendimento às regulamentações da lei 13.709/18, conhecida como Lei Geral de Proteção de Dados Pessoais – LGPD, em relação ao tratamento de dados pessoais.

Documento: **Política de Segurança da Informação – PSI**	Data Emissão:13/06/2023

3. DIRETRIZES GERAIS

Preservação da disponibilidade, integridade, confidencialidade e autenticidade dos dados, informações e conhecimentos que compõem o ativo da informação do MPMT;

Responsabilidade pela realização e acompanhamento das manutenções preventivas periódicas dos equipamentos e instalações de tecnologia da informação, visando à preservação do patrimônio institucional, buscando economicidade na proteção dos ativos de acesso, operação e armazenamento da informação;

Continuidade das atividades de negócio;

Pessoalidade e utilidade do acesso aos ativos de informação;

O não repúdio e responsabilização do usuário pelos atos que comprometam a segurança dos processos e sistemas da informação.

3.1 Organização da Segurança da Informação

A Política de Segurança da Informação é o instrumento que regula a proteção dos dados, informações e conhecimentos da Instituição, com vistas à garantia de integridade, disponibilidade, confidencialidade e conformidade;

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

O gerenciamento dos ativos de informação deverá observar normas operacionais (Norma Complementar da Política de Segurança da Informação - NCSI) e Manuais e Procedimentos Operacionais Padrão;

O cumprimento dessa Política, bem como das normas complementares e procedimentos de Segurança da Informação no MPMT, será auditado periodicamente, de acordo com os critérios definidos pelo Comitê Estratégico de Tecnologia da Informação (CETI) e pelo Comitê Gestor de Dados Pessoais (CGDP);

As medidas de proteção devem ser planejadas e os custos na aplicação de controles devem ser compatíveis com valor do ativo protegido;

O acesso às informações, sistemas e instalações dependem da apresentação de identificador único, pessoal, intransferível e com validade estabelecida, que permita de maneira clara e indiscutível o seu reconhecimento;

A aquisição, contratação de serviços de desenvolvimento, instalação e uso de sistemas e equipamentos de infraestrutura devem ser homologados e/ou autorizados pela administração;

Para garantir o cumprimento das normas, os responsáveis pelas unidades deverão

auxiliar no controle do uso dos recursos computacionais;
Os requisitos de segurança da informação e privacidade de dados pessoais devem estar explicitamente citados em todos os termos de compromisso celebrados entre o órgão e terceiros;
Todos os membros, servidores, estagiários, terceirizados e voluntários do MPMT e demais agentes públicos ou particulares que, oficialmente, executem atividade vinculada à atuação institucional do MPMT e sejam usuários dos ativos, devem assinar Termo de Compromisso quanto ao sigilo dos dados, informações e conhecimentos do MPMT.

3.2 Segurança em Recursos Humanos

As responsabilidades pela segurança da informação devem ser definidas nas descrições de cargos e funções, bem como nos termos e condições das contratações que envolvam o manuseio de dados, informações ou conhecimentos do MPMT;
Todos os usuários devem ser conscientizados e treinados nos procedimentos de segurança da informação e privacidade de dados pessoais;
O controle operacional de uma atividade crítica não pode ser atribuição exclusiva de uma única pessoa;
Quando do afastamento, mudança de cargo e/ou de lotação ou atribuições dentro da organização, faz-se necessária a revisão imediata dos direitos de acesso e de permissões autorizadas anteriormente por outros departamentos, ficando apenas autorizado o acesso conforme o perfil da atual função/localidade e uso dos ativos;
Quando do desligamento de usuário, deverão ser extintos todos os direitos de acesso e uso dos ativos a ele atribuído;
Todos os servidores, membros, estagiários, terceirizados, voluntários, fornecedores e partes externas que tenham acesso a informações sensíveis ou dados pessoais, devem assinar um termo de confidencialidade e de não divulgação, antes de lhes ser dado o acesso aos recursos de processamento da informação;
Ações de bloqueio temporário de acesso, isolamento de equipamento da rede institucional e auditoria, a serem tomadas no caso de o integrante do MPMT ou partes externas desrespeitarem os requisitos de segurança da informação da organização, serão de responsabilidade do Departamento de Tecnologia da Informação (DTI) e do Centro de Apoio Operacional do Conhecimento e Segurança da Informação (CAOP/CSI), uma vez detectadas, e comunicadas à área de competência e gestão dos envolvidos, sem prejuízo de outras ações;
Todo ativo produzido pelo usuário desligado da Instituição deverá ser mantido pelo MPMT, garantindo o reconhecimento e o esclarecimento da propriedade do acervo

para Instituição de acordo com as regras de “classificação da informação” e critérios de temporalidade.

3.3 COMPETÊNCIAS E RESPONSABILIDADES

Essa Política, as normas complementares e os procedimentos de segurança se aplicam a todos os membros, servidores, estagiários, terceirizados e voluntários, do MPMT e demais agentes públicos ou particulares que, oficialmente, executem atividade vinculada à atuação institucional do MPMT.

3.3.1 Compete ao Gabinete do PGJ

Definir padrões de funcionamento, integração, qualidade e segurança dos serviços e sistemas de tecnologia da informação;

Assegurar os recursos necessários para a implementação e gestão da PSI do MPMT;

Definir processos de governança para aplicação de melhoria contínua e auditoria nos processos desta PSI.

3.3.2 Compete ao Comitê Estratégico de Tecnologia da Informação

Definir critérios para auditoria periódica destinada a aferir o cumprimento da PSI do MPMT, suas Normas Complementares e Procedimentos;

Manifestar-se sobre a PSI, com posterior encaminhamento ao PGJ, para aprovação;

3.3.3 Compete a Gerência de Segurança da Informação e ao CAOP/CSI

Assessorar na implementação das ações de segurança da informação;

Constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação;

Propor alterações na PSI;

Propor normas relativas à segurança da informação;

Manter um canal de notificação disponível, de forma anônima, para reporte de violações às políticas e procedimentos de segurança da informação;

Propor ao encarregado de dados a edição ou atualização de normas relativas à proteção de dados pessoais na organização;

3.3.4 Compete ao DTI e ao CAOP/CSI do MPMT

Promover cultura de segurança da informação, comunicações e proteção de dados pessoais;
Propor recursos necessários às ações de segurança da informação, comunicações e atendimento as legislações de proteção de dados;
Coordenar as ações de Segurança da Informação e a Equipe de Tratamento e Resposta a Incidentes em Segurança da Informação;
Realizar e acompanhar estudos de novas tecnologias, quanto a possíveis impactos na segurança da informação, comunicações e proteção de dados pessoais;
Manter contato direto com o CETI e com o CGDP para o trato de assuntos relativos à segurança da informação, comunicações e proteção de dados pessoais;
Propor normas relativas à segurança da informação, comunicações e proteção de dados pessoais;
Propor modificações à PSI;
Definir estratégias para a implantação da PSI;
Editar Normas Complementares e Procedimentos de Segurança da Informação, cabendo ao CETI a recomendação de alteração normativa;
Planejar e coordenar a execução dos programas, planos, projetos e ações de segurança;
Apurar e sanear os incidentes de segurança críticos e, após, encaminhar os fatos apurados às instâncias competentes, para eventual aplicação das sanções previstas;
Supervisionar, analisar e avaliar a efetividade dos processos, procedimentos, sistemas e dispositivos de segurança da informação;
Manter a análise de risco de segurança da informação atualizada, refletindo o estado corrente da organização;
Identificar controles físicos, administrativos e tecnológicos para mitigação do risco;
Recepcionar, organizar, armazenar e tratar adequadamente as informações de eventos e incidentes de segurança da informação, determinando aos respectivos gestores as ações corretivas ou de contingência em cada caso;

Produzir relatórios síntese de incidentes de segurança da informação para o CETI e CGDP;

3.3.5 NORMAS COMPLEMENTARES DE SEGURANÇA DA INFORMAÇÃO.

O regimento da PSI no âmbito do MPMT está estruturado com Normas Complementares que tratam especificamente da gestão dos recursos de tecnologia da informação, e que, portanto, devem ser expressamente cumpridas.
As Normas já previstas na PSI.

Em nenhuma hipótese será permitido o descumprimento das Normas Complementares pela alegação de desconhecimento delas por parte do usuário.

Documento: **Política de Segurança da Informação – PSI**	Data Emissão:13/06/2023

CONCEITOS

1. **Ameaça –** agente ou ação, espontânea ou proposital, que afeta um sistema através de suas vulnerabilidades, causando prejuízos e/ou redução de disponibilidade.
2. **Acesso Lógico –** acesso a redes de computadores, sistemas e estações de trabalho por meio de autenticação;
3. **Appliance –** Dispositivo de hardware com Software embarcado dedicado a uma função específica;
4. **Acesso Remoto –** ingresso, por meio de uma rede, aos dados de um computador fisicamente distante da máquina do usuário;
5. **Ativos de tecnologia da informação –** estações de trabalho, Ativos de Rede e automação, servidores, *software*, mídias e quaisquer equipamentos eletrônicos relacionados à tecnologia da informação, bem como conexões com a internet, *hardware* e software.
6. **Ativo da Informação** – os meios de armazenamento (backups locais ou em nuvem), transmissão (links dedicados ou não, VPNs) e processamento, os sistemas de informação (Banco de dados, BI, etc), bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;
7. **Ativo Sigiloso –** qualquer bem tangível ou intangível que possa conter informações sigilosas que, se acessadas por pessoas não autorizadas, podem causar danos significativos à organização;
8. **Auditoria** - Auditoria de TI é uma ferramenta para avaliar a conformidade, a qualidade, a eficácia, a transferência e a efetividade da área de TI.
9. **Autenticação –** é o ato de confirmar que algo ou alguém é autêntico, ou seja, uma garantia de que qualquer alegação de ou sobre um objeto é verdadeira;
10. **Autenticidade –** propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade;
11. **Backup –** cópia de segurança gerada para possibilitar o acesso e recuperação futura das informações.
12. **Banco de Dados (ou Base de Dados) –** é um sistema de armazenamento de dados, ou seja, um conjunto de registros que tem como objetivo organizar e guardar as informações;
13. **Biometria –** características biológicas e comportamentais mensuráveis da pessoa natural que podem ser coletadas para reconhecimento automatizado, tais como a palma da mão, as digitais dos dedos, a retina ou a íris dos olhos, o formato da face, a voz e a maneira de andar;

14. **Bloqueio de acesso -** processo que tem por finalidade suspender temporariamente o acesso;
15. **Bluetooth -** tecnologia de transmissão de dados via sinais de rádio de alta frequência, entre dispositivos eletrônicos próximos;
16. **Classificação da informação -** atribuição, pela autoridade competente, de grau de sigilo dado à informação, documento, material, área ou instalação;
17. **Caixa corporativa do correio eletrônico –** identifica, de forma não pessoal, um único órgão, unidade administrativa, grupo de trabalho, projeto, evento ou serviço do Ministério Público do Estado de Mato Grosso, o mesmo que e-mail institucional.
18. **Compliance -** trata da apresentação de um conjunto de recomendações em conformidade e auditoria que devem ser aplicadas conforme o contexto institucional e legal.
19. **Confidencialidade –** propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade autorizados;
20. **Contingência -** descrição de medidas a serem tomadas, incluindo a ativação de processos manuais, para fazer com que seus processos vitais voltem a funcionar plenamente, ou num estado minimamente aceitável, o mais rápido possível, evitando assim uma paralisação prolongada que possa gerar maiores prejuízos à corporação;
21. **Conta individual do correio eletrônico –** Caixa postal que identifica um único usuário, pessoa física, conforme padrão estabelecido pelo Ministério Público do Estado de Mato Grosso, o mesmo que e-mail individual.
22. **Criptografia –** Princípios e técnicas pelas quais a informação pode ser transformada da sua forma original para outra ilegível, de forma que possa ser conhecida apenas por seu destinatário (detentor da "chave secreta");
23. **Disponibilidade –** garantir que o serviço esteja funcionando conforme especificado e os acessos às informações estejam disponíveis somente a usuários autorizados.
24. **Download -** (Baixar) copiar arquivos de um servidor (site) na internet para um computador pessoal;
25. **Espelhamento –** Sistema de proteção de dados onde o conteúdo é espelhado em tempo real. Todos os dados são duplicados entre as áreas de armazenamento disponíveis.
26. **FTP (File Transfer Protocol) –** (Protocolo de Transferência de Arquivo) é um protocolo da Internet para transferência de arquivos;
27. **Firewall –** sistema de segurança de computadores usado para restringir acesso de/para em uma rede, além de realizar a filtragem de pacotes com base em regras previamente configuradas.

Documento: **Política de Segurança da Informação – PSI**	Data Emissão:13/06/2023

28. **Gestão de risco –** atividades coordenadas para direcionar e controlar uma organização no que se refere a riscos, incluindo análise e avaliação, tratamento, aceitação e comunicação dos riscos.

29. **Gestão de Continuidade de Negócios -** Processo de gestão global que identifica as potenciais ameaças para uma organização e os impactos nas operações da instituição que essas ameaças, se concretizando, poderiam causar, e fornecendo e mantendo um nível aceitável de serviço face a rupturas e desafios à operação normal do dia-a-dia;

30. **Gestão de Segurança da Informação e Comunicação –** conjunto de processos articulados, que busca a proteção da informação de vários tipos de ameaças, para garantir a continuidade do negócio, minimizar o risco e maximizar o retorno sobre os investimentos.

31. **Hiperconvergencia:** Appliance de infraestrutura combina todos os componentes de um Data Center (armazenamento, processamento, rede e gerenciamento)

32. **Incidente de segurança da informação –** representado por um simples ou por uma série de eventos de segurança da informação que tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a Segurança da Informação.

33. **Integridade –** toda informação trafegada ou armazenada deve ter garantias quanto à sua integridade, assegurando que ela não seja indevidamente alterada ou eliminada.

34. **IP Internet Protocolo** – (Protocolo de Internet) é um protocolo de comunicação usado entre duas ou mais máquinas em rede para encaminhamento dos dados;

35. **Intranet –** rede de computadores privada que faz uso dos mesmos protocolos da Internet. Pode ser entendida como rede interna de alguma instituição em que geralmente o acesso ao seu conteúdo é restrito;

36. **Invadir ou Invasão** - Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita;

37. **Listas de destinatários –** grupos de usuários do correio eletrônico corporativo (restrito aos endereços do Ministério Público do Estado de Mato Grosso), criados mediante solicitação dos responsáveis por órgãos, projetos, eventos e serviços institucionais, para o envio de mensagens.

38. **Log -** é o termo utilizado para descrever o processo de registro de eventos relevantes num sistema computacional. Esse registro pode ser utilizado para reestabelecer o estado original de um sistema ou para que um administrador conheça o seu comportamento no passado. Um arquivo de log pode ser utilizado para auditoria e

diagnóstico de problemas em sistemas computacionais;

39. **Logon -** Procedimento de identificação e autenticação do usuário nos Recursos de Tecnologia da Informação. É pessoal e intransferível;

40. **Nuvem (cloud) -** refere-se a um ambiente distinto de TI projetado com o propósito de provisionar recursos de TI escaláveis e mensuráveis, com fronteiras delimitadas e acessados remotamente.

41. **Serviços na nuvem (cloud services) -** São quaisquer serviços e soluções entregues e consumidos em tempo real, localizados na nuvem e acessados remotamente, comumente pela **Internet**, tais como serviços de e-mails, armazenamento, colaboração, compras, bancos, etc.

42. **Serviço de correio eletrônico –** sistema utilizado para criar, enviar, encaminhar, responder, transmitir, arquivar, manter, copiar, mostrar, ler ou imprimir informações, com o propósito de comunicação entre pessoas ou grupos, exclusivamente em concordância com os interesses da Instituição, vedado como meio de armazenamento de informações. O mesmo que e-mail corporativo ou correio institucional.

43. **Perfil de acesso -** conjunto de atributos de cada usuário, definidos previamente como necessários para credencial de acesso;

44. **Plano de Contingência -** Descrever as medidas a serem tomadas por uma empresa, incluindo a ativação de processos manuais, para fazer com que seus processos críticos voltem a funcionar plenamente, ou num estado minimamente aceitável, o mais rápido possível, evitando assim uma paralisação prolongada;

45. **Plano de Continuidade de Negócios -** documentação dos procedimentos e informações necessárias para que os órgãos mantenham seus ativos de informação críticos e a continuidade de suas atividades críticas em local alternativo num nível previamente definido, em casos de incidentes;

46. **Plano de Comunicação -** descreve como os processos de comunicação serão gerenciados desde a identificação das partes interessadas até o encerramento

47. **Procedimento Operacional Padrão -** descrição detalhada de todas as operações necessárias para a realização de uma tarefa, um roteiro padronizado para realizar uma atividade.

48. **Rede Corporativa -** conjunto de todas as redes locais sob a gestão da instituição;

49. **Replicação -** é a manutenção de cópias idênticas de dados em locais diferentes. O objetivo de um mecanismo de replicação de dados é permitir a manutenção de várias cópias idênticas de um mesmo dado em vários sistemas de armazenamento;

50. **Roteador –** equipamento responsável pela troca de informações entre redes;

51. **Servidor de Rede -** recurso de TI com a finalidade de disponibilizar ou gerenciar serviços ou sistemas informáticos;

52. **Spam –** mensagens não solicitadas, geralmente destinadas a grande número de pessoas, por meio do correio eletrônico.

53. **Streaming -** transferência de dados (normalmente áudio e vídeo) em fluxo contínuo por meio da Internet;

54. **Usuário –** qualquer colaborador seja ele membro, servidor, estagiário, parceiro, fornecedor, prestador de serviço ou terceiro em geral que acessa ou utiliza informações custodiadas ou de propriedade, do Ministério Público do Estado de Mato Grosso.

55. **Inventário –** Sistema que coleta contínua de informações, (configuração, localização, responsável e mudanças) de Ativos de rede (Hardware e Software), para um controle rígido, buscando um aproveitamento mais eficiente dos recursos, que elimina desperdícios, gastos futuros e aumenta a eficiência.

56. **Sala Segura -** sala que proporciona um ambiente seguro no **Datacenter**, oferecendo maior garantia no armazenamento de informações eletrônicas. Uma Sala Segura possui gerador próprio, instalação elétrica independente, paredes especiais, piso elevado, ar-condicionado, detecção e combate a incêndios, iluminação, sinalização de emergência e monitoração do ambiente;

57. **Termo de Responsabilidade** - termo assinado pelo usuário concordando em contribuir com a disponibilidade, a integridade, e manter a confidencialidade e a autenticidade das informações que tiver acesso, bem como assumir responsabilidades decorrentes de tal acesso;

58. **Usuário do correio eletrônico –** pessoa física, seja membro ou servidor, e órgão, unidade administrativa, grupo de trabalho, projeto, evento ou serviço do Ministério Público do Estado de Mato Grosso reconhecido e habilitado pela administração do serviço de correio eletrônico para utilizá-lo.

59. **VPN (Virtual Private Network) –** (Rede Privada Virtual) é uma rede de dados privada que faz uso das infraestruturas públicas de telecomunicações, preservando a privacidade, logo é a extensão de uma rede privada que engloba conexões com redes compartilhadas ou públicas. Com uma VPN pode-se enviar dados entre dois computadores através de uma rede compartilhada ou pública de uma maneira que emula uma conexão ponto a ponto privada;

60. **Wireless (rede sem fio) -** rede que permite a conexão entre computadores e outros dispositivos através da transmissão e recepção de sinais de rádio.

61. **Vulnerabilidade –** fragilidade de um software, sistema operacional ou outro componente da infraestrutura de TI que pode ser explorada por uma ou mais ameaças.

REFERÊNCIAS BIBLIOGRÁFICAS, LEGAIS E NORMATIVAS

1. Lei nº 9.983, de 14 de julho de 2000: Altera o Decreto Lei nº 2848/40 – Código Penal, sobre tipificação de crimes por computador contra a Previdência Social e a Administração Pública;
2. 12.737/2012 - Esta Lei dispõe sobre a tipificação criminal de delitos informáticos e dá outras providências; (lei Carolina Dieckmann)
3. Lei Geral de Proteção de Dados 13.709/2018;
4. Lei nº 12.965/2014, Marco Civil da Internet;
5. Lei n° 9.610, de 19 de fevereiro de 1998, que altera, atualiza e consolida a legislação sobre direitos autorais;
6. Lei 12527, de 18 de novembro de 2011 – Lei de acesso a informação;
7. NBR/ISO/IEC 27002/2013, que institui o código de melhores práticas para gestão de segurança da informação;
8. NBR/ISO/IEC 27001/2013, que estabelece os elementos de um Sistema de Gestão de Segurança da Informação;
9. Norma NBR/ISO/IEC 27005:2018 - Diretrizes para o gerenciamento dos riscos de Segurança da Informação (SI);
10. Código Civil, Art. 1.016, que institui que os administradores respondem solidariamente perante a sociedade e os terceiros prejudicados, por culpa no desempenho de suas funções;
11. Cartilha de Segurança para Internet, desenvolvida pelo CERT.br, mantido pelo NIC.br, com inteiro teor em http://cartilha.cert.br/;

Documento: **Política de Segurança da Informação – PSI**	Data Emissão:13/06/2023

ANEXO I

Normas Complementares da Política de Segurança da Informação

Normas	Norma
NCSI 01	**ACESSO FÍSICO E LÓGICO:** Estabelecer controle de acesso físico e lógico dentro do MPMT;
NCSI 02	**ACESSO REMOTO EXTERNO** Critério para disponibilização de acesso remoto à rede corporativa;
NCSI 03	**CONTAS DE ACESSO E SENHAS** Trata especificamente da Norma de uso das contas e senhas utilizadas para obter acesso à rede de dados do MPMT;
NCSI 04	**CORREIO ELETRÔNICO** Trata especificamente da Norma de uso dos recursos de correio eletrônico (e-mail) do MPMT;
NCSI 05	**EQUIPE DE TRATAMENTO E RESPOSTA A INCIDENTES DE SEGURANÇA MPMT – ETIS** Regulamentar o funcionamento da Equipe de Tratamento e Resposta a Incidentes de Segurança (ETIS) computacionais
NCSI 06	**RECURSOS COMPUTACIONAIS** Estabelecer critérios e procedimentos para o uso dos recursos computacionais disponíveis aos usuários da rede do MPMT, assim como o controle, administração e requisitos mínimos desses recursos.
NCSI 07	**CONFORMIDADE E AUDITORIA (*Compliance*)** Trata da apresentação de um conjunto de recomendações em conformidade e auditoria que devem ser aplicadas conforme o contexto e as necessidades do MPMT
NCSI 08	**BACKUP E RESTOTORE** Estabelecer critério e procedimento para a realização de cópia de segurança exata dos ativos de informação do MP-MT
NCSI 09	**NUVEM** Adotar um modelo de Governança da Segurança da Informação com a finalidade de mitigar os riscos inerentes dos modelos de prestação de serviços na Nuvem
NCSI 10	**DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMAS** Adotar um modelo Segurança da Informação com a finalidade de mitigar os riscos no desenvolvimento de softwares, gerando padrão de segurança desde a criação de sistemas e aplicativos.
NCSI 11	**UTILIZAÇÃO DA INTERNET E INTRANET** Trata especificamente da Norma de uso dos recursos de Internet e Intranet através da rede de dados do MPMT
NCSI 12	**BANCO DE DADO** Trata especificamente da Norma de uso dos recursos de Banco de Dados MPMT