

# POLÍTICA DE SEGURANÇA DA INFORMAÇÃO



## SUMÁRIO

---

1. INTRODUÇÃO.....	3
2. PROPÓSITOS .....	4
3. ESCOPO.....	4
4. DIRETRIZES.....	4
5. PAPÉIS E RESPONSABILIDADES.....	5
6. SANÇÕES E PUNIÇÕES .....	7
7. CASOS OMISSOS .....	8
8. GLOSSÁRIO .....	8
9. REVISÕES .....	10
10. GESTÃO DA POLÍTICA.....	10



## 1. INTRODUÇÃO

---

O Ministério Público de Contas do Estado do Pará – MPC-PA entende que as informações geradas no cumprimento de sua missão constitucional, na qual deve zelar pelos interesses da sociedade, são um bem essencial para resguardar a qualidade e garantia dos seus serviços.

Neste sentido, a instituição compreende que a manipulação de informações passa por diferentes meios de suporte, armazenamento e comunicação, sendo estes vulneráveis a fatores externos e internos que podem comprometer a segurança de seus ativos de informação.

Dessa forma, o MPC-PA estabelece sua Política de Segurança da Informação (PSINF), como parte integrante do seu sistema de gestão institucional, alinhada à Política de Segurança Institucional (PSI), às boas práticas e normas internacionalmente aceitas, com o objetivo de garantir níveis adequados de controle, confidencialidade, disponibilidade e integridade da informação.



## 2. PROPÓSITOS

---

- a) Estabelecer diretrizes e normas de Segurança da Informação que permitam adotar padrões de comportamento seguro, adequados às metas e necessidades da Instituição;
- b) Orientar a adoção de controles e processos para atendimento dos requisitos para Segurança da Informação;
- c) Resguardar as informações do MPC-PA, garantindo requisitos básicos de confidencialidade, autenticidade, integridade e disponibilidade;
- d) Prevenir possíveis causas de incidentes e responsabilidade legal da instituição, membros, servidores, jurisdicionados e parceiros;
- e) Minimizar os riscos de perdas ou alterações indevidas de informações que comprometam a imagem do Órgão.

## 3. ESCOPO

---

Esta política se aplica a todos os usuários da informação do MPC-PA, incluindo qualquer indivíduo ou organização que possui ou possuiu vínculo com o Órgão, tais como: servidores ativos e inativos, ex-servidores, estagiários, ex-estagiários, prestadores de serviço, ex-prestadores de serviço e qualquer pessoas que detenha informações do MPC-PA mediante acesso à infraestrutura, processos ou à rede de computadores e sistemas deste *Parquet* Especializado de Contas.

## 4. DIRETRIZES

---

O objetivo geral da gestão de Segurança da Informação do Ministério Público de Contas do Estado do Pará é garantir a gestão sistemática e efetiva de todos os aspectos relacionados à



segurança da informação, provendo suporte às operações críticas da instituição e minimizando riscos identificados e seus eventuais impactos.

Os objetivos específicos são:

- Elaborar, implantar e seguir normas e procedimentos de segurança da informação, garantindo que os requisitos básicos de confidencialidade, autenticidade, integridade e disponibilidade da informação sejam atingidos através da adoção de controles contra ameaças provenientes de fontes tanto externas quanto internas;
- Disponibilizar normas e procedimentos de segurança a todas as partes interessadas e autorizadas, tais como: servidores ativos e inativos, ex-servidores, estagiários, ex-estagiários, prestadores e ex-prestadores de serviço.
- Garantir a educação e conscientização sobre as práticas adotadas pelo MPC-PA de segurança da informação para servidores, estagiários e prestadores de serviço.
- Atender integralmente requisitos de segurança da informação aplicáveis ou exigidos por normas ou regulamentações do Órgão;
- Tratar integralmente incidentes de segurança da informação, garantindo que os mesmos sejam adequadamente registrados, classificados, investigados, corrigidos, documentados e, quando necessário, comunicando às autoridades apropriadas;
- Garantir a continuidade do serviço público através da adoção, implantação, teste e melhoria contínua de planos de continuidade e recuperação de desastres;
- Melhorar continuamente a Gestão de Segurança da Informação através da definição e revisão sistemática de objetivos de segurança em todos os níveis da instituição.

## 5. PAPÉIS E RESPONSABILIDADES

---

É responsabilidade do:



PROCURADOR-GERAL DE CONTAS - PGC

- Garantir a disponibilidade dos recursos necessários para uma efetiva Gestão de Segurança da Informação;



- Garantir que as atividades de segurança da informação sejam executadas em conformidade com a Política de Segurança da Informação (PSINF);



#### DEPARTAMENTO DE TECNOLOGIA DA INFORMAÇÃO E TELECOMUNICAÇÕES (DTIT)

- Formular e propor a aprovação de políticas e normas relacionadas à segurança da informação;
- Promover a divulgação da PSINF e tomar as ações necessárias para disseminar uma cultura de segurança da informação no ambiente do MPC-PA;
- Conduzir a Gestão e Operação da segurança da informação, tendo como base esta política e demais normas correlacionadas;
- Elaborar e/ou analisar normas e procedimentos de segurança da informação, necessários para se fazer cumprir a PSINF, para posterior aprovação do Procurador-Geral de Contas;
- Identificar e avaliar as principais ameaças à segurança da informação, bem como propor e, quando aprovado, implantar medidas corretivas para reduzir o risco;
- Realizar a gestão dos incidentes de segurança da informação, garantindo tratamento adequado.



#### GESTORES DA INFORMAÇÃO (PROCURADORIAS, ASSESSORIAS E DEPARTAMENTOS);

- Gerenciar as informações produzidas ou sob a responsabilidade da sua área, incluindo a criação, manuseio e descarte conforme as normas estabelecidas pelo MPC-PA.
- Identificar, classificar e rotular as informações geradas ou sob a responsabilidade da sua área conforme normas, critérios e procedimentos adotados por este Órgão;
- Autorizar e revisar os acessos à informação e sistemas de informação sob sua responsabilidade;



- Solicitar a concessão ou revogação de acesso à informação ou sistemas de informação de acordo com os procedimentos adotados pelo MPC-PA.



#### USUÁRIOS DA INFORMAÇÃO;

- Ler, compreender e cumprir integralmente os termos da Política de Segurança da Informação, bem como as demais normas e procedimentos de segurança aplicáveis;
- Encaminhar quaisquer dúvidas e/ou pedidos de esclarecimento sobre a Política de Segurança da Informação, suas normas e procedimentos ao DTIT;
- Comunicar ao DTIT qualquer evento que viole esta Política ou que possa vir a colocar em risco a segurança das informações ou dos recursos computacionais do MPC-PA;
- Assinar o Termo de Uso de Sistemas de Informação do MPC-PA, formalizando a ciência e o aceite integral das disposições da Política de Segurança da Informação, bem como as demais normas e procedimentos de segurança, assumindo responsabilidade pelo seu cumprimento;
- Responder pela inobservância da Política de Segurança da Informação, normas e procedimentos de segurança, conforme definido no item sanções e punições.

## 6. SANÇÕES E PUNIÇÕES

---



As violações desta política, bem como das demais normas e procedimentos de segurança, sujeitarão os responsáveis às penas da lei, nas esferas civil, administrativa e penal, observado o devido processo legal, contraditório e ampla defesa.



As violações serão analisadas pelo DTIT, sendo as sanções e punições aplicadas pelo Procurador-Geral de Contas, devendo-se considerar a gravidade da infração, efeito alcançado, recorrência e as hipóteses previstas na legislação vigente;





- No caso de terceiros contratados ou prestadores de serviço, o DTIT deve analisar a ocorrência e submeter à apreciação do Procurador-Geral de Contas para deliberação acerca da aplicação das sanções e punições, conforme termos previstos em contrato e na legislação vigente.

## 7. CASOS OMISSOS

---

- Os casos omissos serão avaliados pelo DTIT, submetendo sua decisão para posterior apreciação do Procurador-Geral de Contas;
- As diretrizes estabelecidas nesta política e nas demais normas e procedimentos de segurança não se esgotam em razão da contínua evolução tecnológica e constante surgimento de novas ameaças. Desta forma, constitui rol exemplificativo, sendo obrigação do usuário da informação do MPC-PA adotar, sempre que possível, outras medidas de segurança além das aqui previstas, com o objetivo de garantir proteção às informações deste *Parque* Especializado de Contas.

## 8. GLOSSÁRIO

---

- **Segurança da informação:** A preservação das propriedades de confidencialidade, integridade e disponibilidade das informações do MPC-PA;
- **Ativo:** Tudo aquilo que possui valor para o MPC-PA;
- **Ativo de informação:** Patrimônio intangível do MPC-PA, constituído por suas informações de qualquer natureza, incluindo de caráter estratégico, técnico, administrativo, financeiro, de recursos humanos, em como quaisquer informações criadas ou adquiridas por meio de parceria, aquisição, licenciamento, compra ou confiadas ao MPC-PA, servidores, estagiários, prestadores de serviço ou membros da sociedade em formato escrito, verbal, físico ou digitalizado, armazenada, trafegada ou transitando pela infraestrutura computacional do MPC-PA ou por infraestrutura





externa contratada pela organização, além dos documentos em suporte físico, ou mídia eletrônica transitados dentro e fora de sua estrutura física;

- **Gestor da Informação:** Usuário da informação ao qual foi atribuída responsabilidade sob um ou mais ativos de informação criados, adquiridos, manipulados ou colocados sob a responsabilidade de sua área de atuação;
- **Usuário da informação:** Servidores, estagiários ou prestadores de serviço do MPC-PA, assim como outros indivíduos ou organizações devidamente autorizados a utilizar ou manipular qualquer ativo de informação do MPC-PA para o desempenho de suas atividades profissionais;
- **Controle:** Medida de segurança adotada pelo MPC-PA para o tratamento de um risco específico;
- **Confidencialidade:** Propriedade dos ativos da informação do MPC-PA, que não podem ser disponibilizados ou divulgados para indivíduos, processos ou entidades não autorizadas;
- **Disponibilidade:** Propriedade dos ativos da informação do MPC-PA que devem permanecer acessíveis e utilizáveis sob demanda por partes autorizadas;
- **Integridade:** Propriedade dos ativos da informação do MPC-PA que devem permanecer com seu conteúdo exato e completo;
- **Vulnerabilidade:** Causa potencial de um incidente de segurança da informação, que pode vir a prejudicar as operações ou ameaçar as informações do MPC-PA;
- **Ameaça:** Causa potencial de um incidente que pode vir a prejudicar o MPC-PA;
- **Risco de segurança da informação:** Efeito da incerteza sobre os objetivos de segurança da informação do MPC-PA;



**Incidente de Segurança da Informação:** Um evento ou conjunto de eventos indesejados de segurança da informação que tem possibilidade significativa de afetar as operações ou ameaçar as informações do MPC-PA;

## 9. REVISÕES

---



Esta política será revisada com periodicidade bienal ou conforme a proposição do DTIT.

## 10. GESTÃO DA POLÍTICA

---



O DTIT irá propor a normatização e as revisões da PSINF, necessitando posteriormente ser aprovada pelo Procurador-Geral de Contas ou pelo Colégio de Procuradores do MPC-PA quando a matéria for submetida ao mesmo;



A presente política foi aprovada no dia 01/11/2019.