APD Agência de Protecção de Dados

# SEGURANÇA DA INFORMAÇÃO PARA AS ORGANIZAÇÕES/INSTITUIÇÕES

Última actualização

Julho de 2022

# GUIA DE ORIENTAÇÕES DE SEGURANÇA DA INFORMAÇÃO PARA AS ORGANIZAÇÕES/INSTITUIÇÕES

Versão 1.0

Julho de 2022

# *Índice*





Rua do MAT, Complexo Administrativo Clássicos de Talatona, 3.º edifício, 7.º andar. Luanda/Angola
**Tel.:** 937930788 **E-mail:** geral@apd.ao **Site:** www.apd.ao

# 1. APRESENTAÇÃO

Por forma a assegurar o direito a reserva da vida privada dos cidadãos consagrados na Constituição da República de Angola de 2010, o Estado angolano aprovou em 2011 a Lei n.º 22/11 de 17 de Junho – Lei da Protecção de Dados Pessoais (LPDP), que estabelece as regras jurídicas e de segurança da informação que devem ser observadas no tratamento dos dados pessoais.

A LPDP criou a Agência de Protecção de Dados (APD), como sendo a autoridade competente para fiscalizar o cumprimento das regras para o tratamento de dados pessoais, e dentre as suas atribuições, cabe a esta orientar a aplicação das medidas técnicas e de segurança necessárias e adequadas para a protecção de dados pessoais.

Com base nessa atribuição legal, a APD elaborou esta guia de boas práticas para as organizações que tratam dados pessoais, atendendo os requisitos estabelecidos nos artigos 30.º e 31.º da LPDP.

Importa realçar que as empresas e demais instituições não devem limitar-se as medidas aqui elencadas, pois essas medidas devem ser entendidas como boas práticas, devendo serem complementadas com outras que possam ser identificadas como necessárias para promover a segurança no fluxo informacional da organização. Uma boa referência para o efeito são os requisitos do Sistema de Gestão da Segurança da Informação com base na Norma ISO/IEC 27001, cujos controlos de implementação estão referenciados na Norma ISO/IEC 27002.

# 2. SEGURANÇA DA INFORMAÇÃO NO ÂMBITO DO TRATAMENTO DE DADOS PESSOAIS

## 2.1. Segurança da informação

A segurança da informação é um conjunto de acções e mecanismos que visam alcançar a preservação da Confidencialidade, Integridade e Disponibilidade da Informação (CID).

Para se alcançar esse objectivo é importante a definição de um bom programa de gestão da segurança da informação com base no PDCA (Plan, Do, Check, Action) precedido da realização de gestão de riscos, que consiste em identificar, quantificar e gerir os riscos relacionados à segurança da informação dentro da instituição (Norma ISO/IEC 27005) e esse procedimento (gestão de riscos) deve ser feito pelo menos uma vez por ano.

## 2.2. Tratamento de dados pessoais

**Conceitos:**

A LPDP define o tratamento de dados pessoais como qualquer operação ou conjunto de operações efetuada sobre dados pessoais, com ou sem meios autonomizados, tais como a recolha, o registo, a organização, a conservação, a adaptação ou alteração, a recuperação, a



Rua do MAT, Complexo Administrativo Clássicos de Talatona, 3.º edifício, 7.º andar. Luanda/Angola
**Tel.:** 937930788 **E-mail:** geral@apd.ao **Site:** www.apd.ao

consulta, a utilização, a comunicação por transmissão, por difusão ou por qualquer outra forma de colocação a disposição, com comparação ou interconexão, bem como o bloqueio ou destruição.

Quanto ao conceito de dados pessoais, é qualquer informação, seja qual for a sua natureza ou suporte, incluindo imagem e som, relativa a uma pessoa singular identificada ou identificável a pessoa que possa ser identificada, direta ou indiretamente, designadamente por referência a um número de identificação ou à combinação de elementos específicos da sua identidade física, fisiológica, psíquica económica, cultural ou social.

Dados sensíveis, são os dados pessoais referentes a convicções filosóficas, ou políticas, filiação partidária ou sindical, fé, religiosa, vida privada, origem racial ou étnica, saúde e vida sexual, incluindo os dados genéticos.

Responsável pelo tratamento é a pessoa singular ou coletiva, a autoridade pública ou qualquer outro organismo que, individualmente ou em conjunto com outrem, determine as finalidades e os meios de tratamentos de dados pessoais. Sempre que as finalidades e os meios de tratamento sejam determinados por disposição legislativa, regulamentares ou outras, o responsável pelo tratamento deve ser indicado no respectivo diploma.

## 2.3 Obrigações dos responsáveis pelo tratamento de dados pessoais

1. O responsável pelo tratamento deve pôr em prática as medidas técnicas e organizativas, e estabelecer níveis de segurança adequada, para proteger os dados pessoais contra a destruição total ou parcial, acidental ou ilícita, a perda acidental, a alteração total ou parcial, a difusão ou o acesso não autorizado, fundamentalmente quando o tratamento implicar a sua transmissão em rede, e contra qualquer outra forma de tratamento ilícito.

2. As medidas de segurança devem assegurar, atendendo aos conhecimentos técnicos disponíveis e aos custos resultantes da sua aplicação, um nível de segurança adequado em relação aos riscos que o tratamento apresenta e à natureza dos dados a proteger.

3. O responsável pelo tratamento deve elaborar um documento com as medidas, normas e procedimentos de segurança aplicáveis ao tratamento de dados pessoais, detalhando os níveis de segurança, os recursos e proteger e as funções e obrigações das pessoas com acesso aos dados de acordo com as regras de segurança.

Uma importante obrigação relacionada à segurança de dados pessoais é tratada no artigo 15.º da Lei 7/17 de 16 de Fevereiro – Lei de Protecção das Redes e Sistemas Informáticos, mormente, os provedores, operadores e prestadores de serviços do Ciberespaço, antes do início de actividades devem apresentar Agência de Protecção de Dados e ao INFOSI um Plano de Gestão de Acidentes e Incidentes em caso de emergência informática.



Rua do MAT, Complexo Administrativo Clássicos de Talatona, 3.º edifício, 7.º andar. Luanda/Angola
**Tel.:** 937930788 **E-mail:** geral@apd.ao **Site:** www.apd.ao

# 3. MEDIDAS DE SEGURANÇA DA INFORMAÇÃO

## 3.1 Medidas administrativas

### 3.1.1 Política de segurança da informação

A APD sugere que seja estabelecida pela organização uma política de segurança da informação, ainda que simplificada, com previsão de revisão pelo menos uma vez por ano e que incorpore controlos relacionados ao tratamento de dados pessoais, como por exemplo, cópias de segurança; uso de senhas; acesso à informação; comunicação e transferência de dados; atualização de softwares; uso de correio electrónico; uso de antivírus, uso de certificados digitais, uso de firewall, manutenção de logs, entre outros.

### 3.1.2 Consciencialização e Treinamento

As pessoas de uma organização são sem sombra de dúvidas factor chave para o sucesso das medidas de segurança da informação e a protecção de dados pessoais, uma vez que efectivamente são elas que trabalham para as instituições, independentemente do seu porte ou tamanho.

Em função disso, recomenda-se que as instituições realizem campanhas de consciencialização periódicas com todos os funcionários e colaboradores sobre as suas obrigações e responsabilidades no que toca ao tratamento de dados pessoais, quer sejam dados de funcionários ou de clientes/utentes.

Essas acções devem ser voltadas para informar claramente e sensibilizar todos os funcionários da organização, especialmente aqueles que lidam diretamente na actividade de tratamento de dados, sobre as obrigações legais existentes na LPDP e outras leis subsidiárias, na Política de Segurança da Informação, bem como no código de conduta.

**A seguir algumas informações úteis que devem ser passadas aos funcionários:**

- Impedir o acesso indevido aos dados pessoais por parte de terceiros, mesmo que sejam colegas de trabalho;
- Manter os documentos físicos que contenham dados pessoais dentro de cofres, armários ou gavetas trancadas, e não por cima de mesas ou armários;
- Bloquear os computadores quando se afastar das estações de trabalho, para evitar que pessoas não autorizadas tenham acesso aos dados (configurar protecção de tela);
- Não compartilhar logins e senhas de acesso das estações de trabalho e outros dispositivos que contenham dados;
- Instrução de como utilizar controlos de segurança dos sistemas de TI relacionados ao trabalho diário;



Rua do MAT, Complexo Administrativo Clássicos de Talatona, 3.º edifício, 7.º andar. Luanda/Angola
**Tel.:** 937930788 **E-mail:** geral@apd.ao **Site:** www.apd.ao

- Como evitar de se tornarem vítimas de incidentes de segurança triviais, tais como contaminação por vírus ou ataques de phishing, que podem ocorrer, por exemplo, ao clicar em links recebidos na forma de pop-up de ofertas promocionais ou em links desconhecidos que chegam por e-mail;
- Cumprir as orientações da política de segurança da informação;
- Usar trituradoras de papel para o descarte seguro de dados;
- Informar os incidentes e vulnerabilidades detectadas.

### 3.1.3. Gestão de contratos

Recomenda-se que os funcionários e colaboradores assinem termos de confidencialidade (non-disclosure agreement - NDA) e que se comprometam a não divulgar informações confidenciais que envolvam dados pessoais, ainda que deixem de trabalhar para a instituição.

Em caso de contratação de serviços de TI terceirizados, recomenda-se que estabeleçam com os fornecedores contratos que incluam dentre outras, cláusulas de segurança da informação que assegurem a adequada protecção de dados pessoais.

**Tais instrumentos poderão conter, por exemplo, cláusulas que tratam de:**

- Regras para fornecedores e parceiros;
- Regras sobre compartilhamentos;
- Relações entre o responsável pelo tratamento e o subcontratado ou terceiro.

## 3.2 Medidas técnicas

### 3.2.1 Controlo de acesso

O controlo de acesso consiste em uma medida técnica para garantir que os dados sejam acessados somente por pessoas autorizadas. Isso pode ser alcançado com processos de autenticação, autorização e auditoria.

- A autenticação identifica quem acessa o sistema ou os dados;
- A autorização determina o que o utilizador identificado pode fazer;
- A auditoria regista o que foi feito pelo utilizador.

Recomenda-se que, caso o responsável pelo tratamento tenha uma rede interna de computadores, seja implementado um sistema de controlo de acesso aplicável a todos os utilizadores, com níveis de permissão na proporção da necessidade de trabalhar com o sistema e de acessar dados pessoais. Esse sistema de controlo de acesso pode, por exemplo, permitir a criação, aprovação, revisão e exclusão de contas de utilizadores.



Rua do MAT, Complexo Administrativo Clássicos de Talatona, 3.º edifício, 7.º andar. Luanda/Angola
**Tel.:** 937930788 **E-mail:** geral@apd.ao **Site:** www.apd.ao

Ademais, é recomendável que o sistema de controlo de acesso seja configurado com funcionalidades que possam detectar e não permitir o uso de senhas que não respeitem um nível mínimo de complexidade. Ou seja, é importante que o sistema tenha capacidade de estabelecer o número de caracteres para se criar uma senha, incluindo caractere especial ou outros elementos que se considere necessários.

É importante, ainda, utilizar uma adequada gestão de senhas, para evitar o uso de senhas padrão disponibilizadas pelos fornecedores de software ou hardware adquiridos, tendo em vista que geralmente os atacantes utilizam estas senhas padronizadas (default) para tentativas de conexão e realizar os seus ataques.

Essas senhas devem ser alteradas por outras com requisitos mais seguros.

Não deve ser permitido o compartilhamento de contas ou de senhas entre funcionários, uma vez que isso é um elemento crítico de vulnerabilidade de segurança da informação.

Considera-se a aplicação do princípio de privilégio mínimo (need to know), ou seja, os utilizadores de um sistema devem ter apenas o nível de acesso necessário para a realização de suas atividades específicas.

Outro mecanismo muito importante é a utilização de autenticação por multi-factores (MFA) para acessar sistemas ou base de dados que contenham dados pessoais. Ela consiste em estabelecer uma camada adicional de segurança para o processo de login da conta, exigindo que o utilizador forneça duas formas de autenticação.

A título de exemplo de autenticação por multi-factores, podemos citar o envio de códigos de segurança por short message service (SMS) ou por e-mail e o uso de aplicativos autenticadores ou tokens de segurança.

### 3.2.2 Segurança dos dados pessoais armazenados

Considerando que os dados pessoais sensíveis gozam de uma protecção especial pela LPDP, recomenda-se que os responsáveis pelo tratamento que armazenam dados dessa natureza implementem soluções que dificultem a identificação do titular, como a criptografia.

Recomenda-se que os funcionários devem ser informados sobre a importância das configurações de segurança nas suas estações de trabalho, para que eles não as desativem ou ignorem, inclusive quanto a restrições de acesso de determinados tipos de sites.

Os funcionários devem evitar a transferência de dados pessoais de estações de trabalho para dispositivos de armazenamento externo, como pendrives, discos rígidos externos, dentre outros, tendo em vista o risco de se perder a guarda dos dados pessoais transferidos, ou de transferência de vírus para a estação de trabalho e/ou rede. Caso essa operação seja imprescindível, sugere-se a adoção de mecanismos adicionais de segurança nesses dispositivos externos, como inventariá-los, cifrar os dados e armazená-los em locais seguros.



Rua do MAT, Complexo Administrativo Clássicos de Talatona, 3.º edifício, 7.º andar. Luanda/Angola
**Tel.:** 937930788 **E-mail:** geral@apd.ao **Site:** www.apd.ao

Quanto aos backups, é importante que elas sejam realizadas regularmente de forma completa e armazenadas em locais seguros e distintos dos dispositivos de armazenamento principais. Também é importante que essas cópias não sejam sincronizadas online (em tempo real), para evitar a perda de dados em casos de infecções por códigos maliciosos que sequestram os dados como por exemplo o *Ransomware.*

Recomenda-se igualmente a manutenção de um backup desconectado fisicamente.

**Relativamente a eliminação de dados pessoais:**

Recomenda-se que em todas as mídias que contenham dados pessoais seja executado o método de formatar antes de descartá-las e quando isso não for possível, como em CDs e DVDs, deve ser realizada a destruição física da mídia. Esse método também se aplica para a destruição de papel e de mídia portátil para armazenar dados pessoais.

Para as empresas que fazem uso de serviço terceirizados para o descarte, seja de mídia ou registo em papel, recomenda-se que seja estabelecido um contrato de serviço com cláusulas de registo da destruição que for realizada, incluindo o registo de imagem.

### 3.2.3 Segurança das comunicações

Para garantir a segurança dos dados durante as comunicações um elemento muito importante a considerar é a utilização de conexões cifradas (com uso de TLS/HTTPS) ou aplicativos com criptografia fim a fim, devendo ser extensivo no uso de e-mails.

Os e-mails ou os arquivos para envio de dados devem ser cifrados.

Outra boa prática é o monitoramento do tráfego de rede.

**Eis algumas formas de o fazer:**

- Instalar e manter um sistema de firewall, que monitore, detecte e bloqueie ameaças, impedindo conexões a redes não confiáveis. Caso serviços web sejam utilizados, sugere-se o uso de firewall de aplicação web (Web Application Firewall – WAF).
- Proteger serviços de e-mail, utilizando antivírus integrados, ferramentas anti-spam e filtros de e-mail;
- Remover quaisquer dados sensíveis e outros dados pessoais que estejam desnecessariamente disponibilizados em redes públicas, por exemplo, no site da instituição.
- Caso proceda ao tratamento de dados sensíveis (ex. serviços de saúde) recomenda-se criar um canal de acesso restrito para que o cliente acesse essas informações.

### 3.2.4 Gestão de vulnerabilidades

É altamente recomendável o monitoramento das operações da rede. Devem considerar a implementação de um Security Operation Center (SOC), equipa de segurança da informação



Rua do MAT, Complexo Administrativo Clássicos de Talatona, 3.º edifício, 7.º andar. Luanda/Angola
**Tel.:** 937930788 **E-mail:** geral@apd.ao **Site:** www.apd.ao

responsável por monitorar e analisar continuamente a postura de segurança da organização, com o objectivo de detectar, analisar e responder a incidentes de segurança cibernética usando uma combinação de soluções de tecnologia e um forte conjunto de processos, para garantir que os problemas de segurança sejam resolvidos rapidamente após a descoberta.

Cabe ainda verificar a existência de novas versões e correções disponíveis em todos os sistemas e aplicativos para assegurar-se que os mesmos sejam mantidos em suas últimas versões e instalar todas as correções de segurança disponíveis (patches) lançadas pelos respectivos desenvolvedores.

Recomenda-se a implementação de antivírus nos seus sistemas, especialmente nos computadores e laptops e que esses mecanismos sejam mantidos funcionando ativamente e atualizados e que realizem varreduras periódicas nos dispositivos.

Devem implementar mecanismos que não permitam aos utilizadores procederem a desativação ou alteração dos aplicativos e demais softwares instalados pela área de TI e da Segurança da Informação.

## 3.3 Medidas para protecção de dados no uso de dispositivos móveis

No que tange a dispositivos móveis, como smartphones e laptops e outros endpoints usados para fins corporativos ou institucionais, recomenda-se que estejam sujeitos aos mesmos procedimentos de controlo de acesso a que os outros equipamentos de TI, tais como o uso da autenticação por multi-factor para acesso aos dispositivos e sistemas de informação da organização, devendo serem guardados em locais seguros quando não estiverem em uso.

Uma vez que os móveis de uso privado estão sujeitos a mais vulnerabilidades, recomenda-se que sempre que possível, as organizações devem separar os dispositivos móveis de uso privado daqueles de uso institucional.

Caso não seja possível implementar medidas de segurança equivalentes às da organização, recomenda-se que dispositivos móveis pessoais não sejam utilizados para fins institucionais.

Tendo em vista que dispositivos móveis podem ser comprometidos mais facilmente em eventual perda ou roubo, e que isso pode colocar em risco a guarda dos dados pessoais, recomenda-se também que as empresas avaliem e implementem funcionalidades que permitam apagar remotamente os dados pessoais relacionados à sua actividade de processamento. Isso poderá diminuir a chance de eventual incidente de segurança com dados pessoais e essas medidas valem tanto para dispositivos móveis de propriedade institucional quanto os pessoais.

## 3.4. Medidas relacionadas ao serviço em nuvem

Serviço em nuvem é o fornecimento de serviços de computação, incluindo servidores, armazenamento, bancos de dados, rede, software, análise e inteligência pela Internet.



Rua do MAT, Complexo Administrativo Clássicos de Talatona, 3.º edifício, 7.º andar. Luanda/Angola
**Tel.:** 937930788 **E-mail:** geral@apd.ao **Site:** www.apd.ao

Espera-se que, devido ao porte dos provedores de serviço de computação em nuvem e à especificidade do trabalho que elas exercem, observem e implementem as recomendações internacionais e as boas práticas de segurança da informação.

No entanto recomenda-se que o responsável pelo tratamento realize um contrato de acordo de nível de serviço, contemplando a segurança dos dados armazenados.

Recomenda-se as empresas a optar por prestador de serviço em nuvem com certificação em segurança da informação, por exemplo, ISO 27001.

O responsável pelo tratamento pode também solicitar uma auditoria em segurança da informação ao prestador de serviço de computação em nuvem.

Também se recomenda que sejam especificados os requisitos para o acesso do utilizador a cada serviço em nuvem utilizado, bem como que sejam usadas técnicas de autenticação por multi factor, como por exemplo, aplicativos autenticadores ou SMS para acesso aos serviços em nuvem relacionados a dados pessoais.

## 4. CONTROLO INTERNO

Recomenda-se que as organizações de médio e grande porte estabeleçam funções de controlo interno, que devem ser exercidas por funcionários altamente treinados em segurança da informação e protecção de dados pessoais para procederem ao controlo da observância das normas da Política de Segurança da Informação, da LPDP e suas subsidiárias, do código de conduta e das demais regras que concorrem para a segurança dos dados pessoais estabelecidas pela organização.

Convém que esses profissionais sejam também treinados para exercer as funções de Data Protection Officer (oficiais de protecção de dados).

## 5. CONSIDERAÇÕES FINAIS

Essa guia de orientação foi elaborada com o objetivo de disseminar boas práticas e medidas básicas de segurança da informação para apoiar os responsáveis pelo tratamento de dados pessoais no desenvolvimento das suas actividades num ambiente mais seguro.

Na sua elaboração tivemos como base as sugestões da guia de segurança da informação para agentes de tratamento de pequeno porte, disponível em https://www.gov.br/anpd/pt-br, bem como as normas ISO/IEC 27001, 27002 e 27005, além das disposições das Leis 22/11 de 17 de Junho e 7/17 de 16 de Fevereiro.

Auguramos, pois, que as medidas aqui elencadas contribuam para promover a protecção de dados pessoais no seio das organizações, bem como da elevação da confiança dos titulares de dados por essas organizações.



Rua do MAT, Complexo Administrativo Clássicos de Talatona, 3.º edifício, 7.º andar. Luanda/Angola
**Tel.:** 937930788 **E-mail:** geral@apd.ao **Site:** www.apd.ao

## 6. REFERÊNCIAS

Guia de segurança da informação para agentes de tratamento de pequeno porte

Norma ISO/IEC 27001

Norma ISO/IEC 27002

Norma ISO/IEC 27005



Rua do MAT, Complexo Administrativo Clássicos de Talatona, 3.º edifício, 7.º andar. Luanda/Angola
**Tel.:** 937930788 **E-mail:** geral@apd.ao **Site:** www.apd.ao