SYSADMIN-T.I, LDA.

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO (PSI)_v1.0.1

SUMÁRIO

1. PREÂMBULO

A **segurança da informação** constitui um pilar estratégico para a **SYSADMIN – TECNOLOGIA DE INFORMAÇÃO, LDA.**, sendo essencial para garantir a continuidade dos serviços, a protecção dos dados, a confiança dos clientes e o cumprimento rigoroso da legislação aplicável da República de Angola.

Num contexto marcado pelo crescimento das ameaças cibernéticas, ataques informáticos, fugas de informação e actos de sabotagem digital, torna-se indispensável a adopção de um **sistema estruturado de governação da segurança da informação**, alinhado com a **Lei da Cibersegurança**, a **Lei da Protecção de Dados Pessoais** e as **melhores práticas internacionais** em matéria de segurança da informação. A presente Política estabelece os **princípios, normas, responsabilidades, controlos técnicos e organizacionais**, bem como os **procedimentos de prevenção e resposta a incidentes de segurança da informação**, que orientam a actuação da SYSADMIN na protecção dos seus activos de informação.

A presente Política é elaborada e aplicada em estrita conformidade com o **ordenamento jurídico da República de Angola**, designadamente com os diplomas legais e regulamentares aplicáveis, nomeadamente:

- **Constituição da República de Angola** – Direito à segurança, privacidade e proteção da informação.
- **Lei n.º 22/11 – Lei de Proteção de Dados Pessoais** – Obrigações de segurança, confidencialidade e integridade da informação.
- **Lei n.º 23/11 – Lei das Transações Electrónicas** – Segurança das comunicações e sistemas eletrónicos.
- **Lei n.º 7/17 – Lei da Proteção das Redes e Sistemas Informáticos** – Proteção de infraestruturas tecnológicas e sistemas críticos.
- **Lei n.º 38/20 – Lei da Cibersegurança** – Estabelece obrigações de prevenção, deteção e resposta a incidentes cibernéticos.
- **Estratégia Nacional de Cibersegurança de Angola** – Diretrizes estratégicas nacionais de proteção do ciberespaço.
- **Normas ISO/IEC 27001 e 27002** e **NIST CSF** como boas práticas internacionais de referência.

2. OBJECTIVO

A definição do objectivo da presente Política tem como finalidade clarificar e formalizar o **compromisso institucional da SYSADMIN** com a segurança da informação, a protecção dos dados e o cumprimento rigoroso das **obrigações legais e regulamentares nacionais** aplicáveis.

Garantir a proteção integral dos ativos de informação da SYSADMIN contra:

- Acessos não autorizados
- Divulgação indevida de informação
- Alteração, destruição ou perda de dados
- Interrupção de serviços
- Ataques cibernéticos e incidentes tecnológicos

Esta Política visa ainda:

- Assegurar conformidade com a **Lei n.º 7/17**, **Lei n.º 38/20** e **Lei n.º 22/11**;
- Preservar a reputação e a confiança dos clientes;
- Garantir a continuidade operacional do negócio;
- Estabelecer uma cultura organizacional de segurança.

3. INTRODUÇÃO AO ÂMBITO

A segurança da informação deve abranger toda a organização e toda a cadeia tecnológica.

Esta Política aplica-se a:

- Todos os colaboradores, diretores, estagiários e consultores;
- Todos os fornecedores, parceiros e terceiros com acesso a informação;
- Todos os sistemas, redes, aplicações, infraestruturas, serviços cloud, dispositivos móveis e estações de trabalho;
- Toda a informação em formato digital, físico ou verbal, produzida, armazenada ou processada pela SYSADMIN.

4. PRINCÍPIOS E À CLASSIFICAÇÃO DA INFORMAÇÃO

A Lei de Proteção de Dados Pessoais e a Lei da Cibersegurança exigem que a informação seja tratada conforme o seu nível de sensibilidade e risco.

4.1 Princípios

A PSI baseia-se nos seguintes pilares fundamentais:

- **Confidencialidade:** Apenas pessoas autorizadas podem aceder à informação.
- **Integridade:** A informação deve manter-se completa, correta e protegida contra alterações indevidas.
- **Disponibilidade:** A informação deve estar acessível sempre que necessária às operações.
- **Autenticidade:** Garantia de identidade legítima de utilizadores e sistemas.
- **Responsabilização:** Todas as ações devem ser rastreáveis e auditáveis.

4.2 Classificação da Informação

Toda a informação deve ser classificada conforme o impacto potencial:

- **Pública**
- **Interna**
- **Confidencial**
- **Secreta / Crítica**

Cada classe possui requisitos mínimos de proteção, acesso, armazenamento e transmissão.

5. CONTROLES TÉCNICOS E ORGANIZACIONAIS

Os controlos materializam as exigências da Lei da Cibersegurança e da Lei da Proteção de Redes e Sistemas Informáticos.

5.1 Gestão de Identidade e Acesso (IAM)

- Autenticação multifator (MFA) obrigatória para acessos críticos;

- Princípio do menor privilégio;
- Contas individuais e intransmissíveis;
- Desativação imediata após desligamento;
- Revisão semestral e auditoria de acessos.

5.2 Segurança de Rede

- Firewalls, segmentação de rede e isolamento de ambientes críticos;
- IDS/IPS para deteção de intrusões;
- VPN segura para acessos remotos;
- Criptografia TLS 1.2+.

5.3 Gestão de Vulnerabilidades

- Scans periódicos;
- Correção prioritária de vulnerabilidades críticas;
- Hardening de sistemas e aplicações.

5.4 Criptografia

- Proteção de dados confidenciais com algoritmos fortes (ex.: AES-256);
- Gestão segura de chaves e rotação periódica.

5.5 Segurança em Dispositivos Móveis

- MDM obrigatório;
- Bloqueio remoto;
- Criptografia total dos dispositivos.

5.6 Segurança Física

- Controlo de acesso a salas técnicas e datacenter;
- CCTV;
- Registo de entradas e saídas;
- Inventário de equipamentos.

5.7 Logging e Monitorização

- SIEM centralizado;
- Retenção mínima de logs de 12 meses;
- Alertas automáticos para eventos suspeitos.

6. GESTÃO DE INCIDENTES DE SEGURANÇA

Em conformidade com a Lei n.º 38/20 – Lei da Cibersegurança, a **SYSADMIN** deve dispor de **capacidade organizacional, técnica e operacional** adequada para **prevenir, detectar, responder, mitigar e recuperar** de incidentes de segurança da informação e de cibersegurança suscetíveis de comprometer a **confidencialidade, integridade, disponibilidade e autenticidade** dos seus sistemas de informação e dos dados por si tratados.

Um **incidente de segurança da informação** é considerado qualquer evento, de natureza **acidental ou intencional**, que:

- Comprometa ou possa comprometer sistemas informáticos, redes, serviços ou dados;
- Afete a continuidade dos serviços;
- Envolva acesso não autorizado, fuga de informação, destruição de dados, indisponibilidade de sistemas, ataque cibernético, malware, ransomware, intrusão, sabotagem ou fraude digital.

A SYSADMIN mantém um **Processo Formal de Gestão de Incidentes**, com responsabilidades, procedimentos e registos obrigatórios, estruturado nas seguintes fases:

6.1. Deteção e Identificação

Esta fase tem como objectivo **identificar, com a maior brevidade possível, a ocorrência de um incidente de segurança da informação**, permitindo a adopção de medidas imediatas que visem **minimizar o seu impacto**, conter a propagação e preservar a integridade dos sistemas e da informação.

A deteção pode ocorrer por:

- Sistemas de monitorização e segurança (SIEM, EDR, IDS/IPS, firewalls);
- Alertas automáticos;
- Auditorias internas;
- Relatos de colaboradores, clientes ou parceiros;
- Alertas de fornecedores ou entidades externas.

Todo evento suspeito deve ser:

- Registado imediatamente;
- Classificado preliminarmente;
- Comunicado ao Responsável de Segurança da Informação.

6.2. Classificação e Avaliação de Impacto

Após a deteção, o incidente deve ser **avaliado e classificado** de acordo com:

- Tipo de incidente (ex.: fuga de dados, ataque ransomware, indisponibilidade de serviço, intrusão, fraude);
- Sistemas e dados afetados;
- Número de utilizadores impactados;
- Impacto operacional, financeiro, legal e reputacional;
- Nível de criticidade (Baixo, Médio, Alto, Crítico).

Esta classificação determina:

- A prioridade de resposta;
- Os recursos a mobilizar;
- A necessidade de escalonamento à Direção Executiva.

6.3. Contenção Imediata

O objectivo da contenção é **impedir a propagação do incidente e limitar os danos**.

As ações podem incluir:

- Isolamento de sistemas ou redes afetadas;
- Bloqueio de contas comprometidas;
- Interrupção temporária de serviços;
- Aplicação de regras de firewall de emergência;
- Preservação de evidências digitais para análise forense.

A contenção deve ser feita **com rapidez e controlo**, evitando agravar o impacto.

6.4. Erradicação da Causa Raiz

Após a contenção, deve-se proceder à **eliminação completa da origem do incidente**, garantindo que a ameaça não volte a ocorrer.

Inclui:

- Remoção de malware, ransomware ou código malicioso;
- Correção de vulnerabilidades exploradas;
- Aplicação de patches de segurança;
- Reconfiguração segura de sistemas;
- Revisão de permissões e credenciais comprometidas.

Sempre que necessário, deve ser realizada **análise forense digital** para identificar a causa raiz.

6.5. Recuperação Segura dos Serviços

Nesta fase, os sistemas e serviços são **restaurados de forma controlada e segura**, garantindo:

- Integridade dos dados restaurados;
- Funcionamento normal dos sistemas;
- Monitorização reforçada após a recuperação;
- Validação técnica antes do retorno completo à operação.

A recuperação pode envolver:

- Restauração a partir de backups verificados;
- Reinstalação de sistemas;
- Migração temporária para ambientes de contingência.

6.6. Notificação Interna e Externa

Em conformidade com a **Lei da Cibersegurança** e, quando aplicável, com a **Lei de Proteção de Dados Pessoais**, devem ser avaliadas as obrigações legais de comunicação.

Pode ser necessário notificar:

- Direção Executiva;

- Clientes afetados;
- Parceiros;
- Autoridades competentes;
- Entidades reguladoras.

A decisão de notificação deve considerar:

- Gravidade do incidente;
- Tipo de dados envolvidos;
- Impacto para terceiros;
- Obrigações legais e contratuais.

6.7. Relatório Final e Lições Aprendidas

Após a resolução, deve ser elaborado um **Relatório Formal de Incidente**, contendo:

- Descrição do ocorrido;
- Linha do tempo dos eventos;
- Sistemas e dados afetados;
- Medidas adotadas;
- Impactos apurados;
- Custos estimados;
- Ações corretivas e preventivas.

Este relatório deve servir para:

- Melhorar os controlos de segurança;
- Atualizar políticas e procedimentos;
- Reforçar formações;
- Prevenir recorrência de incidentes semelhantes.

Nos termos da **Lei da Cibersegurança da República de Angola**, os incidentes de segurança da informação classificados como **graves ou críticos**, bem como aqueles que afectem **infra-estruturas relevantes, dados sensíveis ou serviços essenciais**, podem implicar a **obrigatoriedade de notificação às autoridades competentes**, a adopção de medidas correctivas imediatas e a implementação

de acções adicionais de mitigação, nos prazos e condições legalmente estabelecidos:

- Comunicação obrigatória às autoridades competentes;
- Cooperação com entidades governamentais;
- Preservação de provas digitais.

7. GESTÃO DE FORNECEDORES E TERCEIROS

A utilização de **fornecedores, parceiros tecnológicos e prestadores de serviços** é essencial para a operação da **SYSADMIN**. Contudo, estes terceiros representam **riscos indirectos relevantes** para a segurança da informação, na medida em que podem ter acesso a **sistemas, dados, infra-estruturas ou processos críticos** da organização.

Em conformidade com a **Lei da Cibersegurança (Lei n.º 38/20)**, a **Lei da Protecção das Redes e Sistemas Informáticos (Lei n.º 7/17)** e a **Lei da Protecção de Dados Pessoais (Lei n.º 22/11)**, a SYSADMIN estabelece um **processo formal de Gestão de Risco de Terceiros**, assente nos seguintes princípios fundamentais:

7.1. Due Diligence de Segurança

Antes da contratação de qualquer fornecedor, parceiro ou prestador de serviços que tenha acesso a:

- Sistemas informáticos;
- Redes;
- Infraestruturas;
- Dados da SYSADMIN ou de clientes;

deve ser realizada uma **avaliação prévia de segurança (due diligence)**, que inclui, entre outros:

- Avaliação da maturidade de segurança da informação do fornecedor;
- Verificação de histórico de incidentes relevantes;
- Avaliação de conformidade com leis e normas aplicáveis;
- Análise do tipo de acesso que será concedido;
- Classificação do fornecedor quanto ao nível de risco.

A contratação só pode prosseguir após **aprovação formal do risco**.

7.2. Cláusulas Contratuais Obrigatórias de Segurança

Todos os contratos com terceiros que envolvam acesso a informação, sistemas ou infraestruturas da SYSADMIN devem conter, obrigatoriamente, cláusulas específicas sobre:

- Confidencialidade e sigilo profissional;
- Proteção de dados pessoais (conformidade com a Lei 22/11);
- Obrigação de adoção de medidas técnicas e organizacionais adequadas;
- Obrigação de notificação imediata de incidentes de segurança;
- Direito de auditoria pela SYSADMIN;
- Responsabilidade por danos causados por falhas de segurança;
- Penalidades e rescisão contratual em caso de incumprimento.

7.3. Auditorias e Monitorização Contínua

A SYSADMIN reserva-se o direito de:

- Realizar auditorias periódicas aos fornecedores críticos;
- Solicitar evidências de controlo de segurança;
- Avaliar relatórios de conformidade e testes de segurança;
- Monitorizar continuamente o cumprimento das obrigações contratuais de segurança.

Fornecedores que apresentem **não conformidades graves** podem ter o acesso suspenso ou o contrato rescindido.

7.4. Classificação de Risco por Fornecedor

Todos os terceiros devem ser **classificados conforme o nível de risco**, considerando:

- Tipo de acesso concedido (dados sensíveis, sistemas críticos, infraestrutura);
- Impacto potencial em caso de incidente;
- Dependência operacional da SYSADMIN;

- Histórico de segurança e conformidade.

Exemplo de classificação:

- **Baixo Risco**
- **Médio Risco**
- **Alto Risco**
- **Crítico**

O nível de controlo, auditoria e exigência contratual será proporcional ao risco.

7.5. Proibição de Subcontratação sem Autorização Formal

É **expressamente proibido** que qualquer fornecedor:

- Subcontrate total ou parcialmente os serviços;
- Transfira acesso a dados ou sistemas;
- Partilhe informação da SYSADMIN;

sem **autorização formal, prévia e escrita** da SYSADMIN.

Caso a subcontratação seja autorizada:

- O subcontratado deve passar pelo mesmo processo de due diligence;
- Deve assumir exatamente as mesmas obrigações contratuais de segurança;
- O fornecedor principal continua integralmente responsável.

7.6. Responsabilidade Solidária e Consequências

O fornecedor é:

- Totalmente responsável por atos e omissões dos seus colaboradores e subcontratados;
- Responsável por quaisquer danos causados à SYSADMIN, clientes ou terceiros por falhas de segurança.

O incumprimento destas obrigações pode resultar em:

- Suspensão imediata de acessos;

- Rescisão contratual;
- Responsabilização civil e, quando aplicável, criminal;
- Comunicação às autoridades competentes.

8. CONFORMIDADE, AUDITORIA E GOVERNANÇA DE SEGURANÇA DA INFORMAÇÃO

A conformidade em matéria de segurança da informação constitui uma **obrigação legal, contratual e estratégica** da SYSADMIN, decorrente, nomeadamente, da **Lei da Cibersegurança (Lei n.º 38/20)**, da **Lei da Proteção das Redes e Sistemas Informáticos (Lei n.º 7/17)**, da **Lei de Proteção de Dados Pessoais (Lei n.º 22/11)**, bem como de compromissos contratuais assumidos com clientes, parceiros e entidades públicas.

A SYSADMIN mantém um **Sistema de Governação e Controlo de Segurança da Informação**, destinado a assegurar:

- O cumprimento permanente das leis e regulamentos aplicáveis;
- A aderência às políticas internas e procedimentos técnicos;
- A eficácia dos controlos de segurança implementados;
- A melhoria contínua do seu Sistema de Gestão de Segurança da Informação (SGSI).

Este sistema de governação assenta nos seguintes pilares:

8.1. Auditorias Internas Semestrais

A SYSADMIN realiza **auditorias internas periódicas**, pelo menos duas vezes por ano, com os seguintes objetivos:

- Verificar o cumprimento da Política de Segurança da Informação e dos procedimentos associados;
- Avaliar a eficácia dos controlos técnicos e organizacionais;
- Identificar não conformidades, fragilidades e oportunidades de melhoria;
- Avaliar o nível de maturidade do SGSI;
- Garantir alinhamento com as exigências legais e normativas (ISO 27001, NIST).

As auditorias internas:

- São planeadas e documentadas;
- Geram relatórios formais;
- Produzem planos de ação obrigatórios com prazos e responsáveis definidos.

8.2. Auditorias Externas (Quando Aplicável)

Sempre que exigido por:

- Clientes institucionais ou governamentais;
- Requisitos contratuais;
- Processos de certificação;
- Ou decisão estratégica da Direção;

a SYSADMIN submeter-se-á a **auditorias externas independentes**, conduzidas por entidades qualificadas, com o objetivo de:

- Validar a conformidade legal e normativa;
- Reforçar a credibilidade institucional;
- Identificar riscos não detetados internamente;
- Demonstrar maturidade e robustez dos controlos de segurança.

8.3. Revisão Anual da Política de Segurança da Informação (PSI)

A presente Política:

- É revista **obrigatoriamente pelo menos uma vez por ano**;
- É atualizada sempre que ocorram:
    - Alterações na legislação angolana;
    - Incidentes graves de segurança;
    - Mudanças significativas na infraestrutura, serviços ou modelo de negócio.

A revisão é:

- Coordenada pelo Responsável de Segurança da Informação;
- Aprovada pela Direção Executiva;
- Formalmente comunicada a todos os colaboradores.

8.4. Monitorização de KPIs e Indicadores de Segurança

A **SYSADMIN** define, acompanha e revê periodicamente **Indicadores-Chave de Desempenho (KPIs)** e **Indicadores-Chave de Risco (KRIs)** de segurança da informação, com o objectivo de avaliar a eficácia dos controlos implementados, identificar tendências, antecipar riscos e apoiar a tomada de decisão, incluindo, designadamente:

- **Número de incidentes de segurança da informação**, por tipologia e severidade;
- **Tempo médio de resposta e de resolução** de incidentes;
- **Percentagem de sistemas e activos de informação actualizados**, incluindo patches e actualizações de segurança;
- **Resultados de auditorias internas e externas**, incluindo não conformidades e recomendações;
- **Grau de conformidade de fornecedores e terceiros**, no âmbito da segurança da informação;
- **Taxa de participação e conclusão** de acções de formação e sensibilização em segurança da informação.

Estes indicadores:

- São **monitorizados de forma contínua e sistemática**;
- **Suportam decisões estratégicas e operacionais** da Direcção;
- **Permitem medir a eficácia do Sistema de Gestão da Segurança da Informação (SGSI)**;
- **Orientam a definição e implementação de acções de melhoria contínua**, em alinhamento com os objectivos de segurança e conformidade da SYSADMIN.

9. REPORTE REGULAR À DIREÇÃO EXECUTIVA

O Responsável de Segurança da Informação deve:

- Produzir **relatórios periódicos de segurança**;
- Reportar à Direção:
    - Estado da conformidade legal;

- Principais riscos;
- Incidentes relevantes;
- Resultados de auditorias;
- Evolução dos KPIs;
- Necessidades de investimento e melhorias.

Este reporte assegura:

- Envolvimento da gestão de topo;
- Tomada de decisão informada;
- Alocação adequada de recursos;
- Responsabilização e governação eficaz.

8.6. Gestão de Não Conformidades

Sempre que forem identificadas não conformidades:

- São registadas formalmente;
- É elaborado plano de ação corretivo;
- São definidos responsáveis e prazos;
- A implementação é acompanhada e verificada.

10. RESPONSABILIDADES

O A segurança da informação é dever institucional e individual.

- **Direção Executiva:** governação, recursos, decisões estratégicas.
- **Responsável de Segurança:** coordenação do SGSI, incidentes e auditorias.
- **Equipa Técnica:** implementação e operação dos controlos.
- **Colaboradores:** cumprimento integral da política e reporte imediato de incidentes.

11. MELHORIA CONTÍNUA

A **segurança da informação** é um **processo evolutivo e contínuo**, que exige monitorização permanente, adaptação às ameaças emergentes e alinhamento com o enquadramento legal e operacional aplicável.

Neste contexto, a SYSADMIN adopta, designadamente, as seguintes medidas:

- **Realização de testes regulares**, incluindo testes de recuperação de desastre (DR), simulações de incidentes de segurança e verificação periódica de backups;
- **Reavaliação periódica dos riscos** de segurança da informação e de cibersegurança;
- **Actualização contínua dos procedimentos, políticas e controlos** de segurança;
- **Implementação de programas de formação e sensibilização contínua** para colaboradores e partes relevantes;
- **Revisão anual da presente Política**, ou sempre que se justifique face a alterações significativas no contexto tecnológico, operacional ou legal.

▪ SERVIÇOS INCLUÍDOS

A **SYSADMIN-T.I,** monitoriza activamente, de forma contínua, todos os circuitos dos seus clientes, procedendo à detecção atempada de quaisquer anomalias ou incidentes que possam ocorrer. Para o efeito, coloca à disposição do **CLIENTE** ferramentas de gestão e de acesso à informação relativas aos serviços prestados.

O **CLIENTE** será sempre notificado por correio electrónico relativamente às actividades, intervenções ou ocorrências relevantes. Em situações de carácter emergente ou excepcional, a comunicação poderá ser efectuada de forma oral, devendo, nesses casos, ser posteriormente formalizada por correio electrónico.

▪ SUPORTE NOC – 24X7X365

A **SYSADMIN-T.I,** assegura um serviço de Suporte **NOC** permanente, **disponível 24 horas por dia, 7 dias por semana, 365 dias por ano,** que inclui, designadamente:

- **Abertura e acompanhamento de tickets pelo Cliente**, através da plataforma oficial de Suporte HelpDesk: **https://suporte.sysadmin.it.ao**
- **Comunicações e feedback ao Cliente**
  As intervenções de suporte técnico poderão ocorrer através das seguintes modalidades:
  - **Abertura de ticket de NOC/Suporte pelo Cliente**, via plataforma HelpDesk, correio electrónico ou contacto telefónico para o serviço de suporte;
  - **Detecção proactiva de incidentes por monitorização activa**, realizada pelo **NOC (Network Operations Center)**, com comunicação imediata ao Cliente para efeitos de diagnóstico e/ou resolução da situação.
  - **Esclarecimento de dúvidas técnicas e operacionais** relacionadas com os serviços prestados;

- **Verificação, diagnóstico, monitorização e acompanhamento** de questões de conectividade e desempenho;
- **Resolução directa de incidentes de funcionamento**, através de **assistência remota**, sempre que tal seja tecnicamente possível;
- **Prestação de informação regular, clara e actualizada** ao **Cliente** sobre o estado dos incidentes, intervenções e actividades em curso.

▪ NOSSO DIFERENCIAL

- As soluções da **SYSADMIN-T.I,** vão além do fornecimento de recursos tecnológicos, assegurando um **processo contínuo de conformidade legal e regulamentar**, em estrita observância do disposto na **Lei n.º 22/11, de 17 de Junho**, **Lei n.º 23/11, de 20 de Junho**, **Lei n.º 7/17, de 16 de Fevereiro**, **Lei n.º 2/20, de 22 de Janeiro**, bem como no **Decreto Presidencial n.º 308/21, de 21 de Dezembro**, com vista à mitigação de riscos e à prevenção de sanções e multas aplicáveis pela **Agência de Protecção de Dados (APD)**.
- Com profissionais **certificadas Microsoft**, a **SYSADMIN-T.I,** garante aos seus clientes **condições comerciais vantajosas**, incluindo **redução de custos na aquisição de licenças** para clientes fidelizados, com descontos estimados entre **10% e 15%** na aquisição de licenças perpétuas do **Microsoft Office 2021**, bem como do **Windows 11 Pro** e **Windows Server 2022 e 2025**, nos termos aplicáveis.
- Adicionalmente, os clientes da **SYSADMIN-T.I,** beneficiam de **vantagens comerciais complementares**, decorrentes do nível de parceria estabelecido com outras empresas **nacionais e internacionais**, conforme detalhado na **carta de apresentação anexa ao dossiê**, revertendo em benefícios directos para os nossos clientes.
- A **parceria estratégica com a Acronis**, estabelecida em 2023, permitiu a implementação de **upgrades tecnológicos** para os nossos clientes, incluindo a atribuição de **50 GB gratuitos de armazenamento em cloud**, no âmbito do serviço **Backup-as-a-Service (BaaS)**, com **funcionalidades reforçadas de cibersegurança**.

- A **parceria com a VMware** possibilitou à **SYSADMIN-T.I,** a **revenda de licenças com condições comerciais competitivas**, ajustadas à realidade e às exigências do mercado angolano.
- A **SYSADMIN-T.I,** disponibiliza **modalidades de pagamento flexíveis**, ajustadas às necessidades e à capacidade financeira dos seus clientes.
- A **SYSADMIN-T.I, cumpre rigorosamente as suas obrigações fiscais e tributárias**, contribuindo de forma activa para o crescimento económico do país, facto comprovável através das **declarações e cartas emitidas pelas entidades estatais competentes**, anexas ao presente dossiê.

▪ SOLICITAÇÃO DE SUPORTE (PORTAL DO CLIENTE)

A **solicitação de suporte** deverá, preferencialmente, ser efectuada através do **Portal do Cliente**.

Sempre que o pedido seja realizado por **correio electrónico, contacto telefónico ou qualquer outro meio**, é **obrigatória a abertura de um ticket**, o qual será registado no sistema de suporte e associado ao Cliente.

- **Acesso ao Portal de Chamados (HelpDesk): https://suporte.sysadmin.it.ao**
- Para efeitos de acesso ao Portal, o **Cliente deverá indicar um endereço de correio electrónico válido**, que será utilizado para autenticação, acompanhamento e recepção de notificações relativas aos tickets.
- **Canais de contacto para suporte:**
  - E-mail: **suporte@sysadmin.it.ao**
  - Telefones: (+244) **933 108 370 - 222 734 118**

FALE CONNOSCO

Última actualização: Luanda, 12 de janeiro de 2026