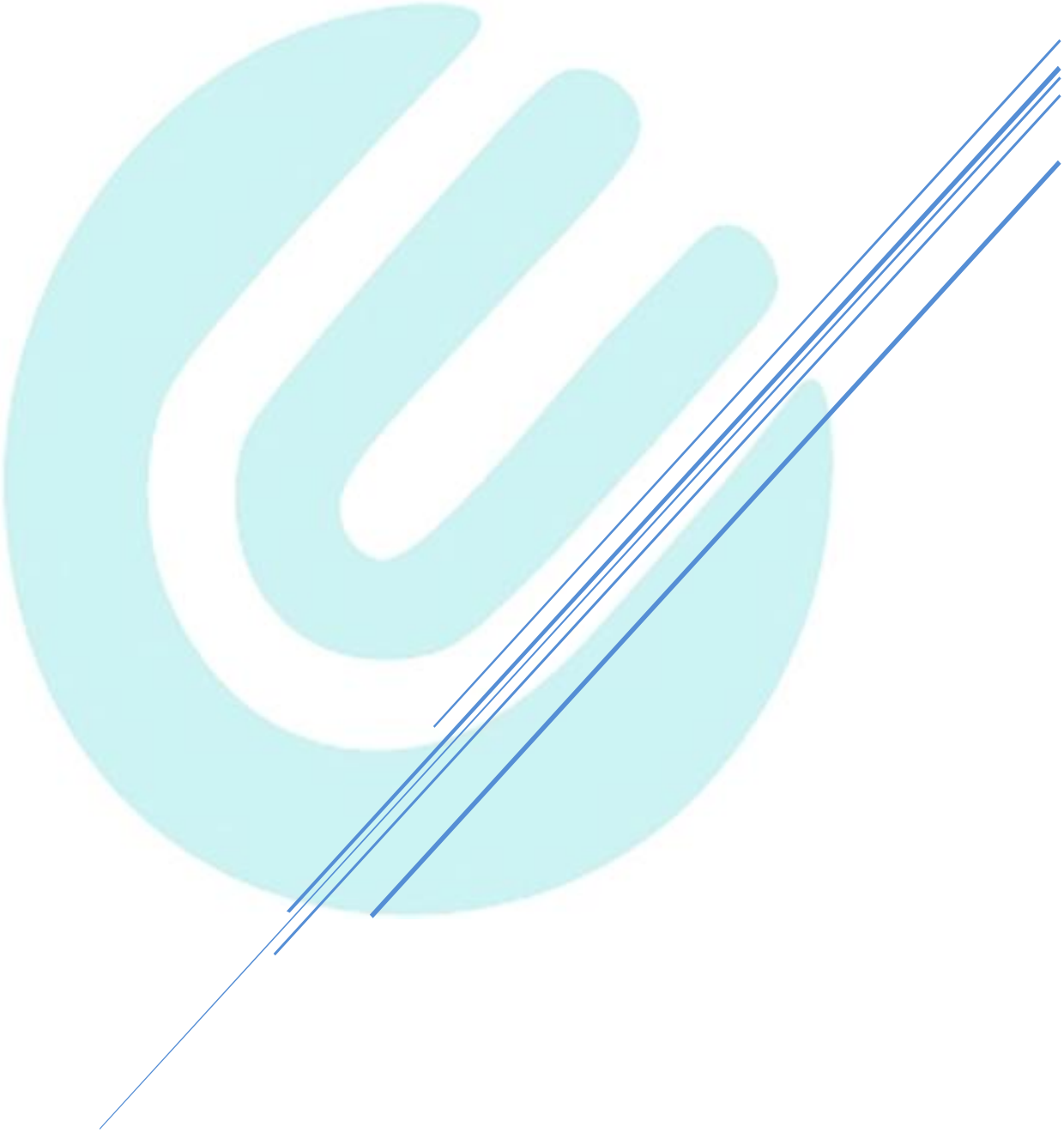
POLÍTICA DE PROCEDIMENTOS DE TI E SEGURANÇA DA INFORMAÇÃO



CODIGO TROPICAL PREST SERV C G SU LDA
NIF: **5417616885 *** Telf. +244 226 434 750**
financeiro@codigotropical.com .::. www.codigotropical-ao.com

CÓDIGO TROPICAL - PRESTAÇÃO DE SERVIÇOS E COMÉRCIO GERAL (SU), LDA

Headquarters: Condomínio Cajueiro, Rua Kwanza, Casa n.º 0-01, Talatona, Luanda, Angola
Tax ID (NIF): 5417616885 **| Contact:** financeiro@codigotropical

1. OBJECTIVO E ÂMBITO DE APLICAÇÃO

A presente **Política de Procedimentos de TI e Segurança da Informação** estabelece as normas técnicas, controlos operativos e diretrizes de segurança que governam a gestão de ativos tecnológicos, a proteção de dados e a administração de redes pela **Código Tropical.**
Esta política aplica-se a todos os sistemas informáticos, redes estruturadas, ambientes de virtualização e infraestruturas de servidores controlados ou operados pela Código Tropical, sendo de cumprimento obrigatório para todo o corpo técnico, engenheiros de sistemas, colaboradores e terceiros com acesso aos recursos de informação da empresa ou de clientes por esta assistidos.

2. CONTROLO DE ACESSOS E GESTÃO DE IDENTIDADES

O acesso aos recursos lógicos e servidores rege-se pelo princípio internacional do **Menor Privilégio** (*Least Privilege*), garantindo que cada técnico possui acesso exclusivamente aos dados estritamente necessários para a execução das suas funções.

- **Autenticação Forte:** É obrigatória a implementação de políticas de passwords complexas (mínimo de 12 caracteres, incluindo maiúsculas, minúsculas, números e caracteres especiais) com renovação forçada a cada 90 dias.
- **Autenticação Multi-Factor (MFA):** O acesso a ambientes de administração, hipervisores, consolas de gestão de servidores (ex: Dell iDRAC, Lenovo XClarity) e e-mails corporativos exige obrigatoriamente a validação por MFA.
- **Revogação de Acessos:** Os acessos técnicos e credenciais de colaboradores desligados ou de projetos concluídos são revogados de forma imediata e permanente nos sistemas centrais.

3. SEGURANÇA DE INFRAESTRUTURA E ENGENHARIA DE REDES

As redes estruturadas e os ambientes corporativos projetados ou operados pela Código Tropical devem seguir arquiteturas de **Defesa em Profundidade**:

- **Micro-segmentação:** Isolamento rigoroso de tráfego através de Redes Locais Virtuais (VLANs), separando redes de gestão de servidores, tráfego de dados de utilizadores, redes de armazenamento (SAN) e acessos de visitantes.
- **Segurança Perimetral:** Implementação de Firewalls de Próxima Geração (NGFW) com políticas restritivas de tráfego de entrada (*Inbound*) e monitorização ativa de portas lógicas.
- **Isolamento de Ambientes:** Os laboratórios de teste e ambientes de encenação (*staging*) devem estar logicamente estancados e sem comunicação direta com as redes de produção de clientes ou embaixadas.

4. PROTEÇÃO DE DADOS E PROCEDIMENTOS DE BACKUP

Para assegurar a integridade absoluta da informação contra falhas de hardware, desastres físicos ou ataques de *ransomware*, a Código Tropical adota a **Estratégia de Cópia de Segurança 3-2-1:**

- **Regra dos Três Cópias:** Manutenção de um mínimo de 3 cópias da informação crítica (1 de produção ativa e 2 cópias de segurança).
- **Dois Suportes Diferentes:** Armazenamento das cópias de segurança em pelo menos 2 tipos de suportes físicos ou volumes lógicos distintos (ex: armazenamento local em arrays NAS/SAN e volumes imutáveis).
- **Uma Cópia Fora do Sítio (*Offsite*):** Replicação de pelo menos 1 das cópias de segurança para uma localização geográfica externa ou ambiente cloud blindado.
- **Cifragem de Dados:** Todos os backups de dados confidenciais de clientes, bancos ou embaixadas são obrigatoriamente cifrados na origem (em descanso) e durante o processo de transferência (em trânsito) utilizando algoritmos avançados (AES-256).
- **Testes de Restauro:** Realização de auditorias e testes de recuperação periódicos para garantir a eficácia do plano de continuidade de negócio (BCP).

5. GESTÃO DE VULNERABILIDADES E INTEGRIDADE DE FIRMWARE

A Código Tropical opera exclusivamente com **distribuidores mundiais autorizados**, garantindo a legitimidade física e lógica de todos os componentes de hardware Tier-1 (Dell, Cisco, Lenovo, entre outros).

- **Atualização de Patches:** Definição de uma calendarização regular para a aplicação de patches de segurança críticos em sistemas operativos, bases de dados e plataformas de virtualização empresarial.
- **Verificação de Firmware:** Antes do comissionamento de novos servidores empresariais (como linhas Dell PowerEdge), as equipas de Engenharia de Nível 3 procedem à verificação da assinatura criptográfica e integridade dos firmwares de fábrica, eliminando riscos de vulnerabilidades na cadeia de aprovisionamento internacional.

6. RESPOSTA A INCIDENTES E SUPORTE TÉCNICO L2 / L3

Em caso de deteção de uma anomalia de rede ou violação de segurança, é ativado de imediato o Protocolo de Resposta a Incidentes da Código Tropical:

- **Contenção Imediata:** Isolamento lógico dos ativos afetados para mitigar a propagação do incidente.
- **Análise Forense e Erradicação:** Identificação da causa raiz da falha ou intrusão, remoção da ameaça e reposição dos sistemas através de backups validados.
- **Escalonamento Especializado:** Situações de elevada complexidade que afetem infraestruturas centrais são tratadas diretamente pelas equipas de suporte avançado de Nível 2 (L2) e Nível 3 (L3), garantindo o cumprimento estrito dos Acordos de Nível de Serviço (SLAs) contratados.

CODIGOTROPICAL SU LDA
www.codigotropical.com | info@codigotropical.com
NIF 5417616885 | ANGOLA