

SICHERGUARD

RYAN
MARCELLO
JULLIA
EDUARDO

2025



contato@sicherguard.com.br



www.sicherguard.com.br





SOBRE-NÓS

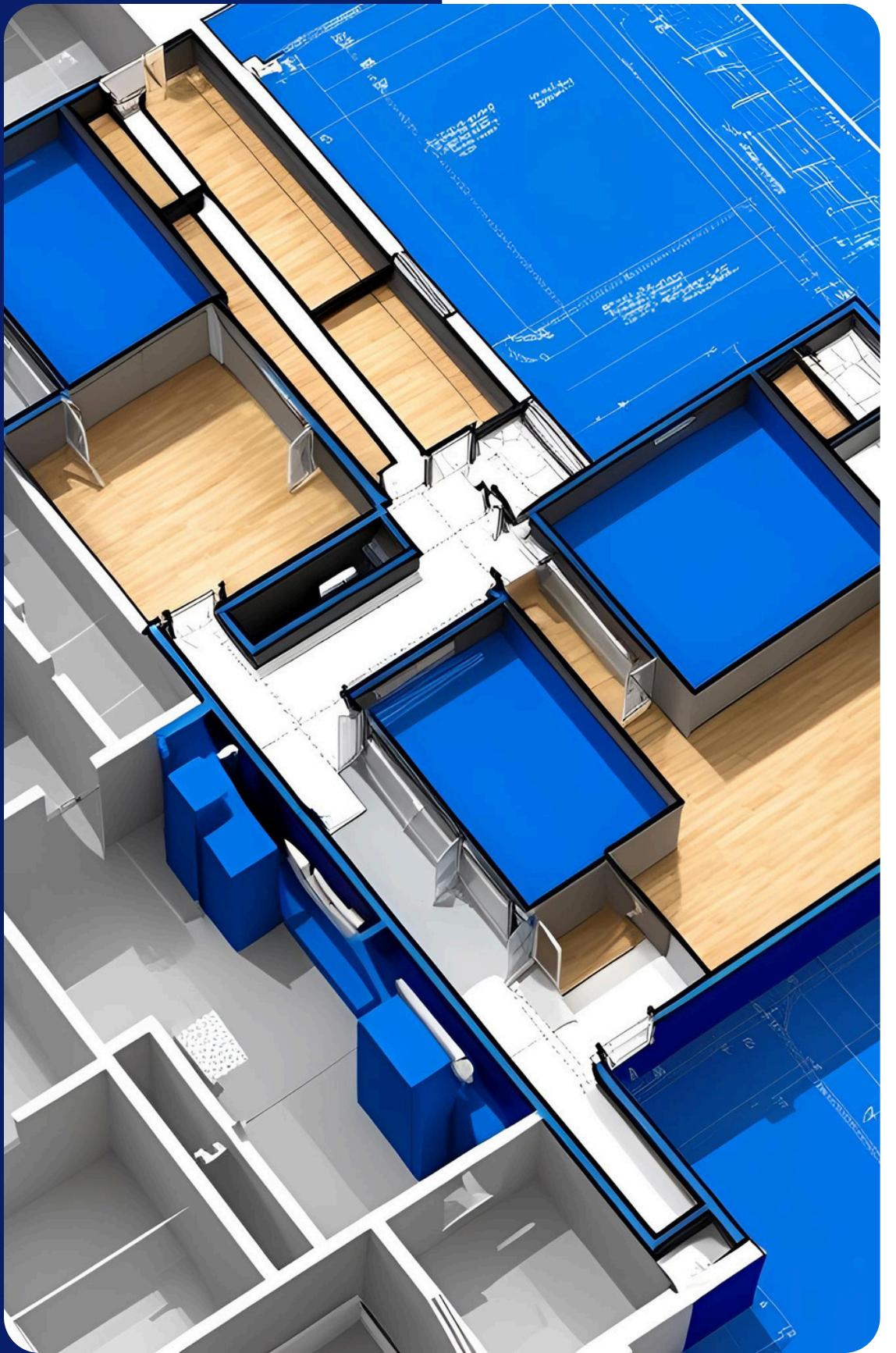
A SicherGuard é uma empresa de tecnologia avançada em segurança, especializada em soluções inovadoras para proteção física e cibernética. Inspirada no legado de segurança de Fort Knox, mas com uma abordagem voltada para a era digital, a SicherGuard utiliza tecnologias de ponta para oferecer sistemas de vigilância, monitoramento e análise de risco, garantindo proteção total para seus clientes.



MISSÃO

Garantir segurança completa e inteligente para pessoas, infraestruturas e dados, unindo proteção física e cibernética em soluções integradas. Combinamos tecnologia de ponta, monitoramento proativo e respostas rápidas para neutralizar ameaças antes que elas se tornem riscos reais, assegurando que nossos clientes operem com confiança em qualquer ambiente.

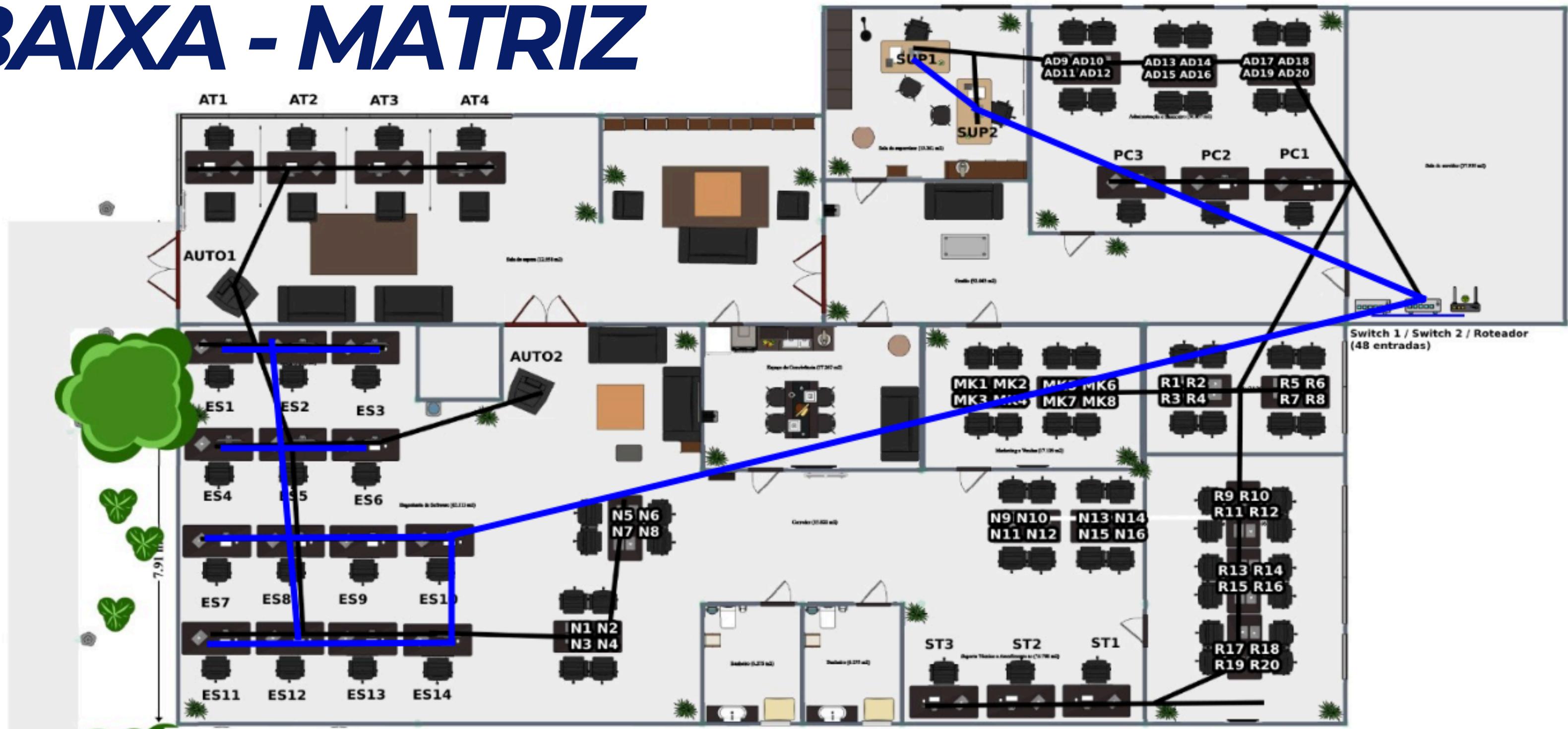
MATRIZ E FILIAIS



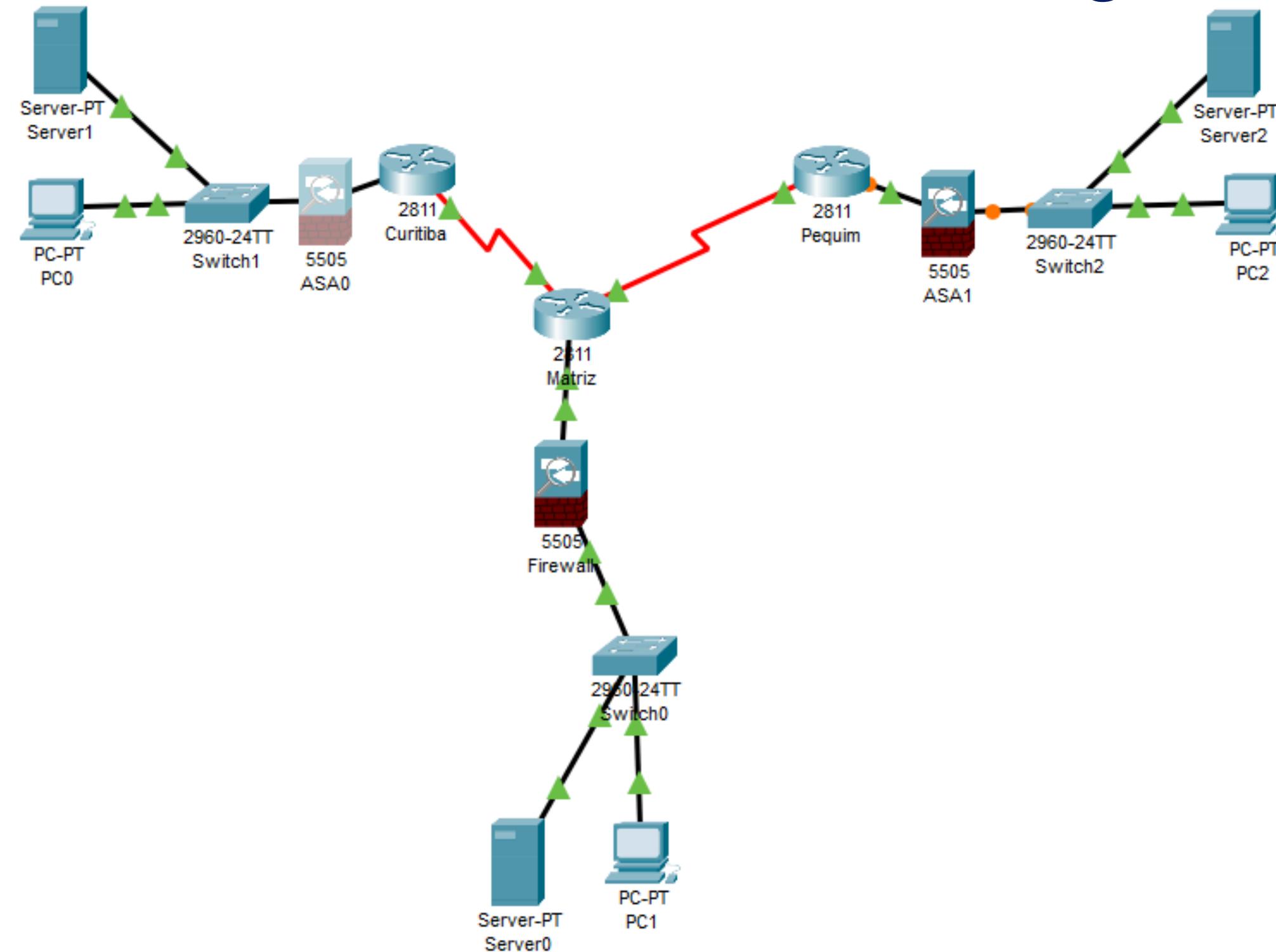
A SicherGuard possui uma matriz em São Paulo, SP, e filias em Curitiba e Pequim.

- Filial em Pequim tem como objetivo expandir nossos serviços para Ásia afim de alcançar novos mercados e aumentar nossa base de clientes.
- Filial em Curitiba tem como objetivo desenvolver novas tecnologias e segurança devido a cidade ser polo tecnológico em crescimento com forte presença de universidades.
- A matriz é responsável por ser o Hub central da rede com todas filiais conectadas a ela, com a comunicação sendo por MPLS garantindo criptografia e baixa latência.

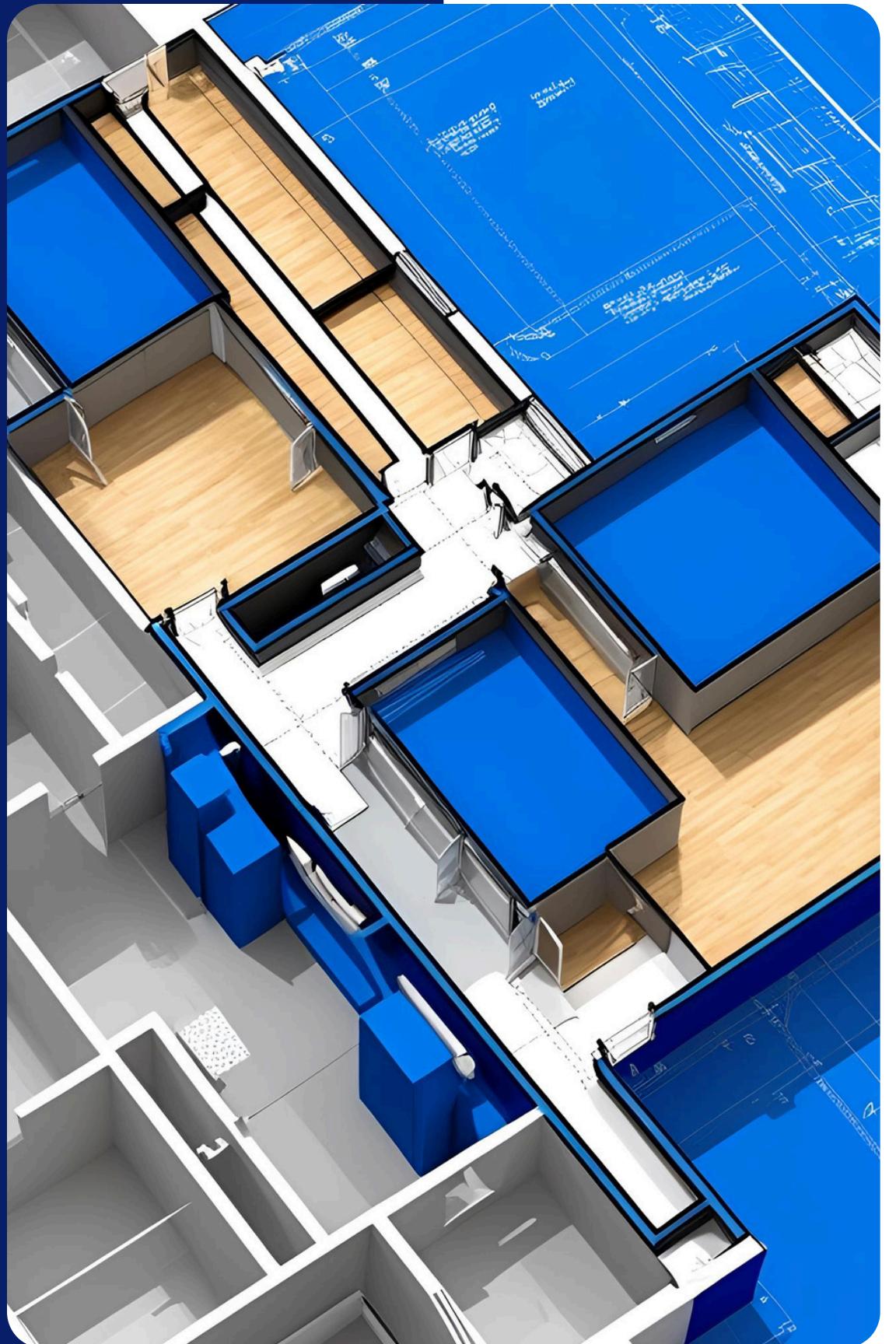
PLANTA BAIXA - MATRIZ



TOPOLOGIA - COMUNICAÇÃO



PLANTA BAIXA - INFRAESTRUTURA



Infraestrutura de Rede SicherGuard

Cabeamento Cat6 (Fio preto):

- Suporta altas velocidades e largura de banda; instalado com ventilação para evitar superaquecimento e garantir estabilidade. (O Cat6 suporta velocidades maiores (até 10Gbps)

Cabeamento Fibra Óptica (Fio azul):

- Usado em áreas críticas que demandam alta velocidade e baixa latência, para aplicações de alta demanda.

Identificação e Proteção:

- Cada dispositivo tem identificação única (nome + IP) para facilitar o controle e a segurança da rede.

Zonas de Segurança e Acesso Controlado:

- Áreas críticas: Pesquisa e Desenvolvimento, Engenharia (Hardware e Software), Qualidade, Logística, Marketing, Suporte Técnico e Financeiro.

Áreas Críticas com Alta Demanda de Banda:

- Desenvolvimento, testes, logística, marketing, suporte, financeiro e servidores/backups em nuvem.

Cabeamento Estruturado:

- Topologia estrela com Cat6 para alta velocidade; fibra óptica para longas distâncias; VLANs para segmentação e segurança; gerenciamento otimizado.



CONECTIVIDADE DA ESTRUTURA

A empresa possui uma rede eficiente, segura e escalável, com redes locais (LAN) segmentadas por VLANs em cada unidade (matriz e filiais), conectadas por links de operadoras.

Equipamentos:

- Roteadores: Cada unidade tem um roteador que conecta LAN à rede externa. Na matriz, o roteador centraliza o tráfego das filiais.
- Switches: Switches gerenciáveis de acesso conectam usuários, e switches de distribuição agregam as VLANs e ligam ao roteador.

Segmentação por VLANs:

Redes separadas por setor, como Administrativo (VLAN 10), Financeiro (VLAN 20), Suporte Técnico (VLAN 30), Wi-Fi Corporativo (VLAN 40), Diretoria (VLAN 50), Recursos Humanos (VLAN 60), Tecnologia (VLAN 70), Comercial (VLAN 80), Segurança (VLAN 90) e Convidados (VLAN 100). VLANs são gerenciadas via switches e roteadores com trunking 802.1Q.

Links de Comunicação:

Conexão entre matriz e filiais via MPLS dedicado da Vivo (Para interligar a matriz e as filiais), garantindo segurança e qualidade. Internet banda larga com VPN IPsec (Para garantir segurança na transmissão de dados pela internet pública e comunicação) serve como redundância.

Topologia:

Topologia em estrela, matriz atua como hub central, roteando o tráfego entre filiais. QoS prioriza aplicações críticas (VoIP, ERP).

Endereçamento IP (IPv4):

Cada VLAN possui sub-rede própria com máscara adequada ao número de dispositivos, reservando espaços para gateways, servidores e DHCP. O planejamento garante expansão futura sem desperdício de endereços ou conflitos.

ENDEREÇAMENTO

Endereços

Setor	Vlan	IP	Quantidade	Notas
Administrativo	Vlan 10	192.168.10.X/28	Diretoria + Financeiro	Acessada pelo Administrativo, Financeiro e RH.
Departamento Financeiro	Vlan 20	192.168.20.X/28	4	
Suporte ao cliente	Vlan 30	192.168.30.X/28	5	
Wifi	Vlan 40	192.168.40.X/25	Váriavel	Rede sem fio para funcionários, separada para proteger os dados críticos da rede interna.
Diretoria Executiva	Vlan 50	192.168.50.X/25	3	
Recursos Humanos	Vlan 60	192.168.60.X/27	Diretoria + Financeiro	Diretoria e Financeiro acessam essa rede com controle para garantir segurança e privacidade.
Departamento de Tecnologia e Inovação	Vlan 70	192.168.70.X/28	5	
Comercial e marketing	Vlan 80	192.168.80.X/28	4	
Departamento de Operações:	Vlan 90	192.168.90.X/24	5	

ENDERECAMENTO DE REDE E PROTOCOLOS



Padrão de IP:

A infraestrutura utiliza IPv4 como padrão, por sua ampla compatibilidade e simplicidade. O IPv6 será adotado gradualmente, conforme os dispositivos e sistemas se tornem compatíveis.

Para evitar vulnerabilidades nos IPs livres da rede, vamos bloquear o tráfego para esses endereços no firewall, desativar respostas a ping, manter um controle rigoroso dos IPs usados e reservar os restantes para usos futuros (expansão em 1 mês) ou redes separadas, além de monitorar continuamente para detectar acessos suspeitos.

Justificativa:

O IPv4 é mais prático, amplamente suportado por data centers e ferramentas, além de facilitar a memorização e configuração.

Protocolos de Rede Utilizados:

- **DHCP:** Distribuição automática de IPs
- **DNS:** Resolução de nomes
- **HTTP/HTTPS:** Comunicação web segura
- **TCP:** Transmissão confiável de dados
- **ICMP:** Diagnóstico de rede (ex: ping)
- **VPN (IPSec):** Conexão segura entre redes como China e Brasil.
- **SFTP:** Transferência segura de arquivos
- **NTP:** Sincronização de horário
- **VoIP (SIP/RTP):** Voz e vídeo por IP
- **LDAP:** Autenticação centralizada
- **RADIUS/TACACS+:** Controle de acesso
- **ARP:** Mapeamento IP-MAC na LAN

INFRAESTRUTURA DE REDE

A SicherGuard investe continuamente em tecnologia para garantir eficiência, qualidade e proteção em todas as etapas de seus processos.

01

A infraestrutura é protegida por firewalls avançados, VPNs IPsec, criptografia de ponta a ponta, autenticação multifator e sistemas de prevenção contra intrusões. VLANs segmentam o tráfego e ferramentas de monitoramento garantem resposta rápida a ameaças.

02

A rede em topologia estrela usa Cat6 e fibra óptica para alto desempenho. Conta com roteadores, switches, firewalls e monitoramento inteligente, garantindo escalabilidade e segurança.

03

A rede é segmentada por VLANs: Administrativo (VLAN 10), Financeiro (VLAN 20) e Suporte Técnico (VLAN 30) e outras, com sub-redes IPv4 dedicadas a cada setor. Há planejamento para adoção gradual do IPv6 visando futuras expansões.

04

A comunicação entre matriz e filiais é feita por MPLS dedicado, garantindo alta segurança e desempenho, com redundância assegurada por conexões VPN IPsec.

EQUIPAMENTOS



Equipamentos

- 40 computadores (Máquinas eficientes conforme a necessidade de cada função), 2 switches de 24 portas (Catalyst 2960x), 1 roteador de borda (Cisco 2811) e 5 servidores físico.
- Servidor físico para autenticação, arquivos, backup, desenvolvimento e segurança para melhor redundância (Data Center)

O QUE PRODUZIMOS

A SicherGuard desenvolve e integra soluções completas em segurança física e cibernética, incluindo servidores dedicados, redes estruturadas, sistemas de vigilância, controle de acesso e infraestrutura em nuvem. Tudo é planejado para garantir alto desempenho, proteção de dados e conectividade inteligente.

- Servidores físicos personalizados
- Cabeamento estruturado (Cat6 e fibra óptica)
- Sistemas de monitoramento e câmeras inteligentes
- Controle de acesso (biometria, cartões, RFID)
- Serviços em nuvem (e-mail, backup, firewall)
- Infraestrutura de rede com VLANs e segurança avançada

SERVIÇOS EM NÚVEM



E-mail Corporativo – Amazon WorkMail

- **Amazon WorkMail:** E-mail corporativo seguro, integrado a outros serviços AWS, com acesso móvel.
- **Custo:** R\$2.200/mês (40 usuários).

Armazenamento e Compartilhamento – Amazon S3 + WorkDocs

- **Amazon S3 + WorkDocs:** Armazenamento e colaboração em nuvem com controle de acesso e versionamento.
- **Custo:** R\$1.440/mês (40 usuários).

Infraestrutura como Serviço – Amazon EC2

- **Amazon EC2:** Servidores virtuais escaláveis para sistemas internos.
- **Custo:** R\$570/mês (2 servidores).

Backup em Nuvem – AWS Backup

- **AWS Backup:** Backup automatizado e seguro com políticas flexíveis.
- **Custo:** R\$200/mês (até 1TB).

Firewall em Nuvem – AWS Network Firewall

- **AWS Network Firewall:** Firewall em nuvem com VPN e proteção contra ameaças.
- **Custo:** R\$600/mês.

Usamos serviços AWS porque oferecem alta confiabilidade, escalabilidade, segurança e uma ampla gama de soluções prontas para uso, com bom custo-benefício e suporte global.

ARMAZENAMENTO LOCAL E EM NUVEM



Armazenamento Local

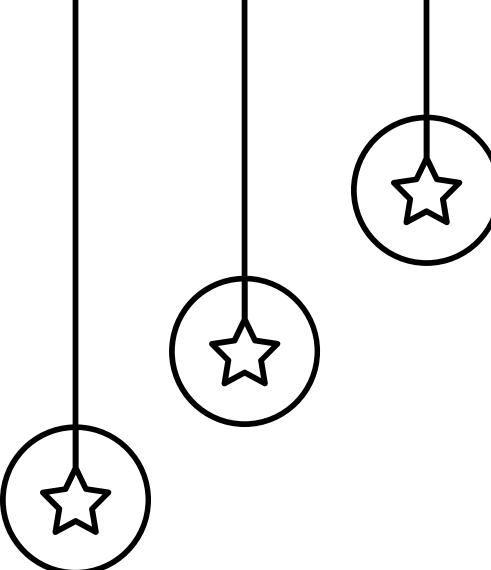
- Autenticação de usuários (ex: **LDAP** - Protocolo para gerenciar um servidor de diretório, **Active Directory** - Serviço de diretório da Microsoft que usa o LDAP como base)
- Arquivos internos e operacionais sensíveis
- Backups recentes (redundância local)
- Ambientes de desenvolvimento e testes internos

Objetivo: Garantir controle direto, segurança e acesso rápido, mesmo sem conexão com a internet.

Armazenamento em Nuvem (AWS)

- Documentos corporativos e compartilhados (WorkDocs)
- Backups automáticos de servidores e estações (AWS Backup)
- Sistemas internos (EC2)
- E-mail e calendário corporativo (WorkMail)

Objetivo: Garantir escalabilidade, colaboração entre filiais e alta disponibilidade com segurança.



OBRIGADO

*Inovação que Conecta o
Futuro.*

CONTATO



São Paulo - 01025-020



(11) 98004-8944



www.sicherguard.com.br

