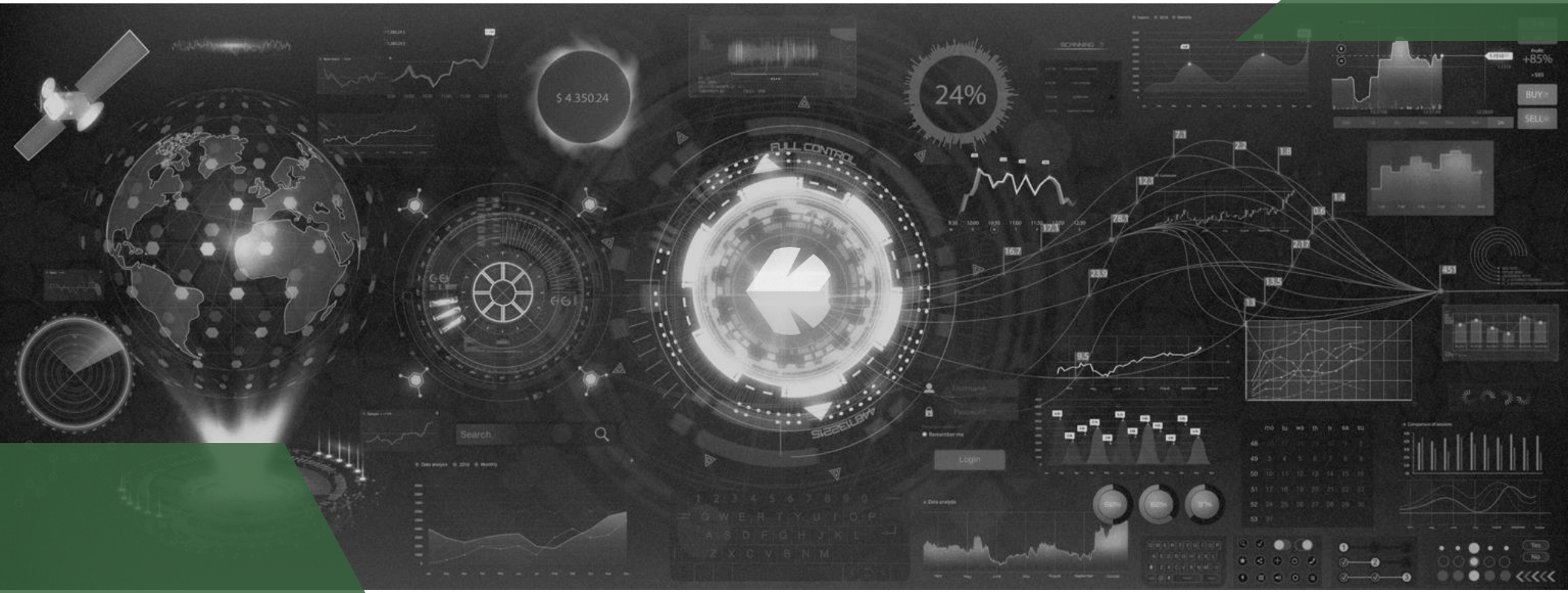


Apresentação Institucional

Cherokee

Segurança em todos os níveis

QUEM SOMOS

A Cherokee foi criada em 2016 por profissionais com mais de 20 anos de atuação nas áreas de Tecnologia e Segurança da Informação. Ao apoiarem empresas de diversos portes, eles observaram que, não importa o tamanho, todas têm suas vulnerabilidades e necessidades na proteção de dados e em garantir a continuidade das operações, seja o incidente causado por um ataque cibernético, uma falha no sistema, uma epidemia mundial ou outro motivo.

NOSSA MISSÃO

Ser o parceiro que toda empresa precisa para atingir a maturidade na proteção de suas informações e no uso eficiente das tecnologias, por meio de serviços e soluções de alta qualidade.

NOSSA VISÃO

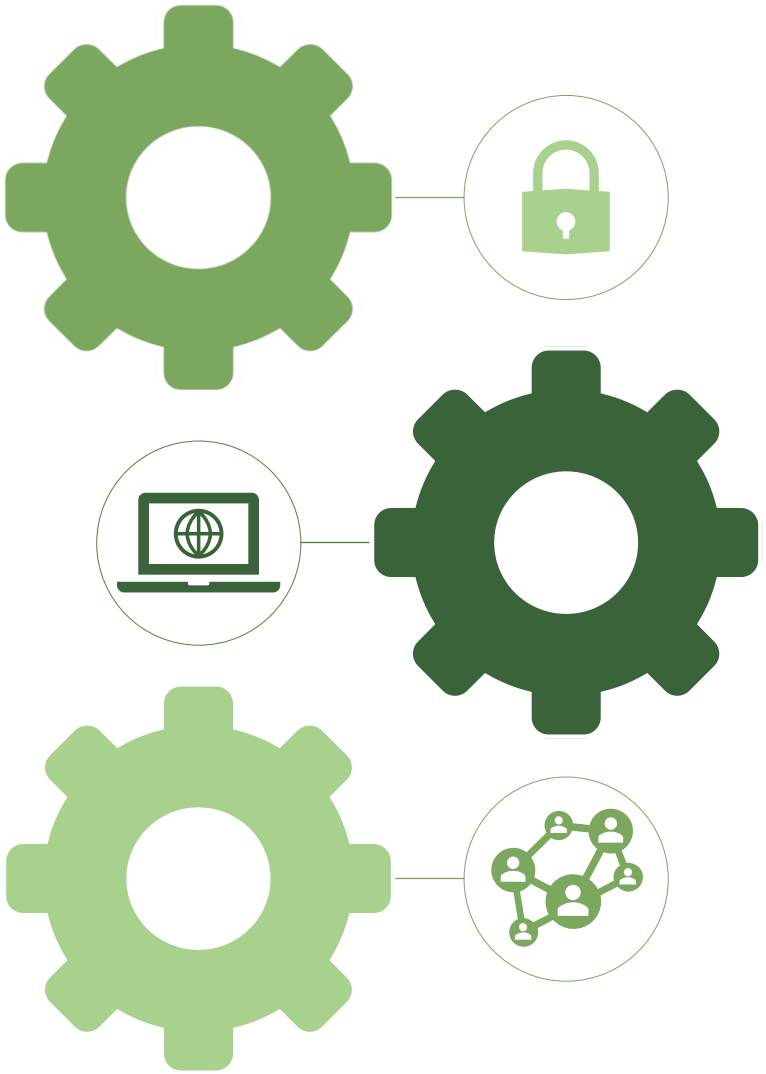
Ser referência de mercado por oferecer serviços e soluções de ponta, com qualidade, assertividade e foco nas necessidades dos clientes, construindo relações duradoras e sustentáveis.

NOSSOS VALORES

Nossos seis valores refletem quem somos, como trabalhamos e o que consideramos nas tomadas de decisões. São eles:

- Foco no cliente
- Respeito aos colaboradores
- Inovação
- Precisão nas soluções
- Rapidez nas decisões
- Ética como valor inegociável

ÁREAS DE ATUAÇÃO



CONSULTORIA

AUDITORIA

ASSESSMENT

CENTRO OPERAÇÕES E MONITORAMENTO

SOLUÇÕES

TREINAMENTOS E CONSCIENTIZAÇÃO

OUTSOURCING

TECNOLOGIA DA INFORMAÇÃO

SEGURANÇA DA INFORMAÇÃO

CONTINUIDADE DE NEGÓCIOS

PRIVACIDADE

PREVENÇÃO

ASSESSMENT, CONSULTORIA E AUDITORIA

***Assessment* -** É importante para avaliar os processos de Tecnologia, Segurança da Informação, Privacidade, Prevenção e Continuidade de Negócios, para identificar as vulnerabilidades e os pontos fortes e os que precisam ser melhorados.

Consultoria - Conte com a Cherokee como seu braço estratégico para avaliar seu ambiente tecnológico, mapear os riscos e aperfeiçoar seus controles de proteção em Tecnologia, Segurança da Informação, Privacidade, Prevenção e Continuidade de Negócios.

Auditoria - Verificação cuidadosa e sistemática das atividades, processos e operação, para averiguar se estão conforme com as leis, normas, *frameworks e* melhores práticas de mercado.

CONTINUIDADE DE NEGÓCIOS

Identifica, prioriza e documenta os serviços e ações essenciais para manter a sua empresa operacional em momentos de crise, minimizando impactos aos clientes e à imagem da empresa

Política de Continuidade de Negócios – Diretrizes para o sistema de Gestão de Continuidade de Negócios.

Norma de Resposta a Incidentes de Segurança - Estabelece as regras para o tratamento do Incidente.

Plano de Continuidade de Negócio (PCN) - Contempla a visão geral do sistema de continuidade de negócios

Plano de Gestão de Crise (PGC) - Contempla o processo para comunicação, lista de contatos, responsabilidades, critérios pré-estabelecidos de crise, resposta, tomada de decisões em crises e retorno à normalidade.

Plano de Continuidade Operacional (PCO) - Contempla os processos de continuidade do escritório, mapeamento dos processos críticos - BIA, avaliação da segurança física do prédio – RIA, local alternativo, etc.

Plano de Recuperação de Desastres (PRD) - Contempla os cenários possíveis de crise no ambiente tecnológico e processos alternativos adotados para restabelecimento do ambiente.

Treinamento e Testes - Treinamento da equipe e execução de testes.

OPERAÇÕES

Gestão de vulnerabilidades - Identifica, monitora e corrige as vulnerabilidades tecnológicas preventivamente, por meio de varreduras e testes de penetração.

***Pentest* -** Simula um ataque controlado ao ambiente tecnológico de sua empresa, para identificar as vulnerabilidades em sua infraestrutura e os riscos potenciais de seus ambientes e sistemas informatizados.

***Threat Intel* (Inteligência cibernética e monitoramento de ameaças) -** Pesquisa, monitoramento e correlacionamento de dados da *surface web*, *deep web* e *darknet* identificando ameaças e ataques que possam comprometer a segurança da empresa.

Prevenção a Perda de Dados (DLP) - Gestão de regras, monitoramento e relatórios gerenciais.

Gestão de incidentes de segurança - Classifica os incidentes, executa as ações de contenção, identifica e trata a causa raiz, atualiza a base de conhecimento e promove medidas de prevenção/reincidência.

Gestão de endpoints - Realiza o inventário de todos esses dispositivos e desenvolve estratégias e mecanismos de acesso para cada um deles.

Gestão de identidades e acessos - Gestão de solicitações no modelo de governança da empresa, aumentando a segurança e conformidade com transparência.

Análise Forense - Identifica todas as ações executadas em equipamentos como *desktops*, *notebooks*, *tablets* e *smartphones* e os respectivos responsáveis.

MONITORAMENTO

Monitoramento de *clouds* - Apresenta todos os indicadores de consumo e disponibilidade de forma clara e completa, em dashboards executivos com diferentes níveis de detalhamento.

Monitoramento de infraestrutura e redes - Faz a gestão de configurações e ativos, correlacionamento de logs, gestão de alerta, identificação de incidentes e indicadores, analise histórica dos eventos, monitoramento de consumo de infraestrutura e rede (exemplo: *autoscale*, ataque de DDoS).

***Cybersecurity* -** Protege e monitora continuamente programas, computadores, redes e dados de danos e invasão, evitando a paralisação parcial ou total das atividades e reagindo rapidamente a incidentes e crises.

Gestão de certificados digitais - Monitoramento dos certificados digitais e mudança de *status*, como exemplo: valido ou revogado, expirado ou em vigor.

Gestão de licenças - Permitem o controle com precisão e confiabilidade de suas quantidades e validades, assegurando a disponibilidade dos softwares aos seus colaboradores.

Monitoramento de sistemas e aplicações - Simula processos reais em aplicações e analisa seus retornos de forma automática e contínua, para identificar anomalias em aplicações.

Monitoramento de home office - Acessos, ativos, geolocalização, conectividade, aplicações e interação do usuário.

SOLUÇÕES

Licenciamento, implementação e sustentação de soluções próprias ou de mercado.

CHEROKEE

Autenticação unificada (SSO) - Permite que diversos sistemas sejam automaticamente autenticados e autorizados a partir de um único conjunto de credenciais.

SOC Security Operations Center - Centro de operações de segurança

Monitoramento – Infraestrutura, Clouds, Redes e Aplicações

***Zero Trust* -** Blinda o acesso aos sistemas da empresa, disponibilizando-os apenas para aqueles que devem acessá-los.

***Threath Intel* ICMA -** Inteligência Cibernética e Monitoramento de ameaças.

***E-Learning* Segurança -** Portal de cursos abordando Segurança, Golpes e Privacidade.

Portal de Segurança - Pílulas, cartilha, filmes e dicas de Segurança para conscientização.

Simulação de *Phishing* - Portal para gestão de campanhas de *Phishing*.

MERCADO

Cofre de senhas - Gestão e proteção de senhas.

IDM - Gestão de identidades, acessos e governança.

***Keycloak* -** Gestão de identidades e acessos.

Microsoft 365 - E-mail, DLP, Classificação da Informação

SIEM – Monitoramento e alertas

ITSM – Ferramenta de gestão de serviços de TI

Orange Testing - Plataforma completa para automatizar testes Web, API e Mobile

OUTSOURCING

Amplie a eficácia de sua equipe com outsourcing ou alocação de profissionais especializados, em operação, processos ou projetos.

Tecnologia da Informação

Governança

Segurança da Informação

Prevenção

Atendimento

Ciso as a Service

CIO as a Service

Necessidades específicas ou sob demanda

NOSSOS CLIENTES

NOSSOS PARCEIROS

NOSSAS IMPLEMENTAÇÕES

CONTATO

cherokee.com.br

Rogério Gomes
rogerio.gomes@cherokee.com.br
fone +55 11 97426-6587

Ulisses Donato
ulisses.donato@cherokee.com.br
fone +55 11 96461-0029