Datasheet

CG//One

Portfólio CG One X NIST®
Cybersecurity Framework

Conheça as soluções de segurança alinhadas ao principal framework do mercado para elevar sua maturidade em cibersegurança

Índice

O cenário

À medida que o cenário digital evolui e as ameaças cibernéticas se tornam mais sofisticadas, a cibersegurança tornou-se uma preocupação crítica para empresas em todo o mundo. Proteger ativos digitais, dados sensíveis e garantir a continuidade operacional são imperativos que não podem ser negligenciados.

No Brasil, assim como em outras partes do mundo, a cibersegurança enfrenta desafios complexos. A rápida adoção de tecnologias digitais, o aumento do uso de dispositivos conectados e a sofisticação crescente de ataques cibernéticos têm desafiado as estruturas tradicionais de defesa.

Além disso, a falta de conscientização sobre segurança cibernética e a escassez de profissionais qualificados têm contribuído para a vulnerabilidade nas empresas.

Esse cenário altamente desafiador torna cada vez mais difícil medir a eficácia das ações de cibersegurança nas organizações.

Neste material, exploraremos os principais desafios da cibersegurança e como o NIST® Cybersecurity Framework pode ser um aliado na luta contra os ataques cibernéticos. Também mostraremos, na prática, como o portólio da CG One, orientado pelo NIST, pode ajudar a sua empresa a elevar a maturidade cibernética.

Medindo a eficácia da cibersegurança: um desafio complexo

Avaliar a eficácia das estratégias de cibersegurança é um desafio constante. A natureza dinâmica das ameaças cibernéticas torna difícil medir o sucesso de ações preventivas e reativas. Além disso, as organizações muitas vezes carecem de métricas claras e padronizadas para avaliar seu nível de segurança digital.

Empresas utilizam uma variedade de tecnologias e ferramentas de segurança. Integrar e correlacionar todos os dados dessas diferentes fontes pode ser complexo. A conformidade com regulamentações adiciona uma camada adicional de complexidade.

Medir a eficácia da cibersegurança também envolve avaliar o custo-benefício das soluções implementadas, considerando o investimento necessário em comparação com os riscos mitigados.

Qual a importância das regulamentações?

Os padrões e regulamentações relevantes desempenham um papel fundamental na medição da eficácia da cibersegurança, fornecendo diretrizes específicas, critérios e requisitos que as organizações devem seguir para proteger seus sistemas e dados.

Esses padrões ajudam a estabelecer uma base sólida para a avaliação da cibersegurança e oferecem uma estrutura para medir o seu desempenho.

Continue a leitura para se aprofundar em um dos frameworks mais importantes para medir a eficácia da cibersegurança na sua organização.

NIST® Cybersecurity Framework: um aliado poderoso para melhorar o gerenciamento de riscos cibernéticos das organizações

O **NIST®** (National Institute of Standards and Technology) é uma **agência governamental dos Estados Unidos** que fornece diretrizes e padrões técnicos para diversas áreas, incluindo cibersegurança.

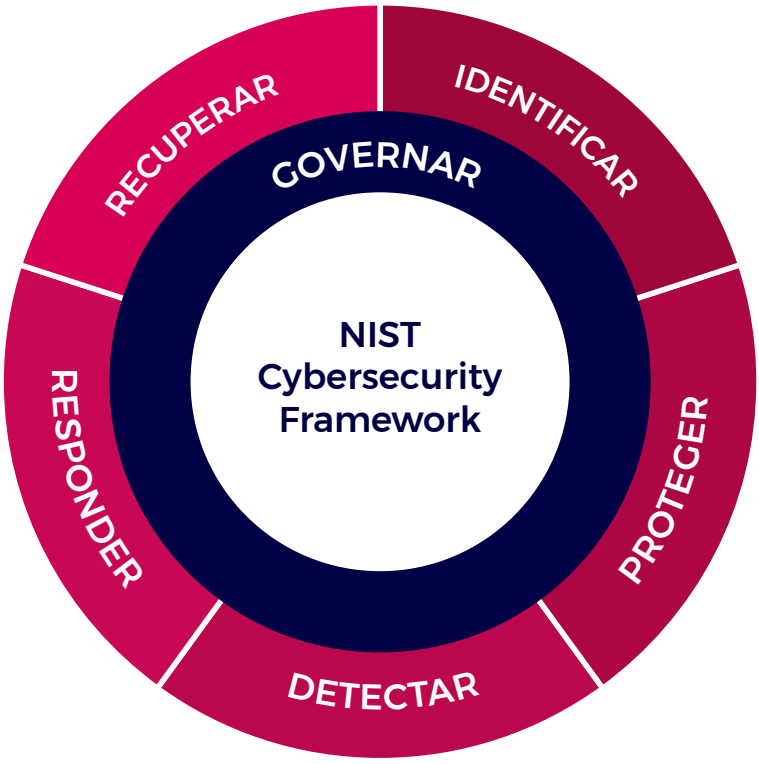
O Instituto tem desempenhado um papel crucial no **estabelecimento de padrões para a segurança cibernética.** Os seis pilares do framework de Cibersegurança do NIST®, por exemplo, oferecem uma abordagem abrangente e completa para **entender, organizar e melhorar as práticas de segurança.**

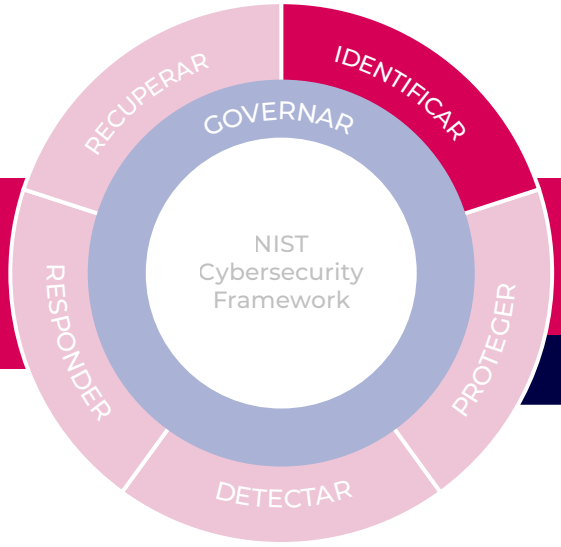
Ao adotar essas diretrizes, as organizações podem criar um ambiente mais seguro, identificando e gerenciando riscos de maneira eficaz, promovendo a padronização e a consistência nas práticas de cibersegurança, seja em empresas iniciantes na implementação de cibersegurança ou com práticas já robustas de proteção.

NIST® Capabilities X Portfólio CG One

O framework se concentra em seis pilares principais para fortalecer a postura de segurança de uma organização.

Abaixo, vamos explorar cada um deles e você também verá como o nosso portfólio foi pensado para abranger as capabilities do NIST® Cybersecurity Framework. Cada solução foi criada para atender às necessidades específicas, garantindo que estamos cobrindo as bases necessárias para uma segurança cibernética sólida.





Identificar

Conheça **as soluções**

Este pilar ajuda a determinar o atual risco de segurança cibernética da organização, identificando e gerenciando de maneira consistente os ativos e sistemas.

Frentes de atuação:

- **Avaliação de riscos**
- **Gestão de ativos**
- **Melhorias nos processos de gestão de riscos**

Conheça as soluções da CG One que se enquadram na categoria "Identificar" do NIST:

Application Security

- DAST
- IAST
- SAST
- SCA

Gerenciamento e Análise

- Cloud Management
- Network Management
- Security Manager

Serviços

- Gestão da Infraestrutura de Segurança
- SOC as a Service / MDR

Cloud Security

- Posture Management (CSPM)

Privacy

- Automação de Avaliações
- Data Discovery
- Data Mapping
- Policy Management
- Privacy Jurisdiction Database

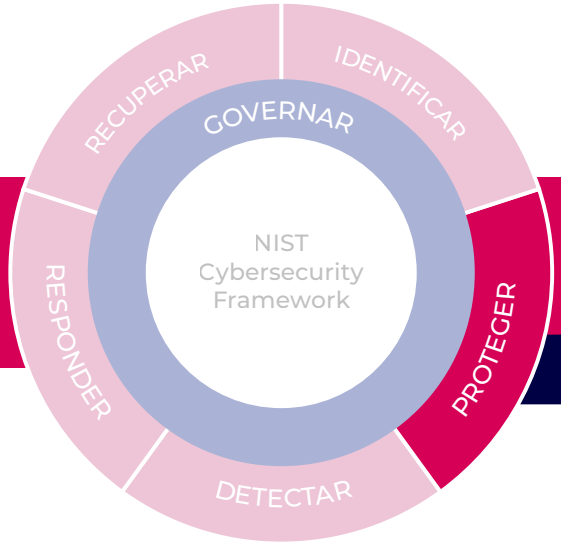
Simuladores e Testes

- Gerador de Tráfego
- Simulador de Ameaças

Secure Access & Endpoint

- CASB

Conheça **as soluções**



Proteger

Conheça **as soluções**

A organização deve desenvolver e implementar as proteções apropriadas para garantir a entrega de serviços de infraestrutura crítica.

Frentes de atuação:

- **Gestão de identidade, autenticação e controle de acesso**
- **Conscientização e treinamentos**
- **Segurança de dados e das plataformas**
- **Resiliência da infraestrutura tecnológica**

Conheça as soluções da CG One que se enquadram na categoria "Proteger" do NIST:

Application Delivery Controller

- Global Network
- Local Network

Secure Access & Endpoint

- Mobile Access
- NAC
- VPN
- ZTNA
- MFA
- Identity & Access Management
- Security Mobile
- Security Browser
- SASE

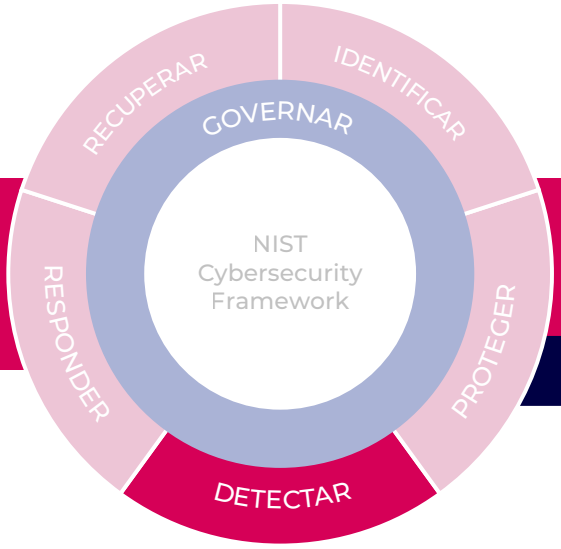
Conheça **as soluções**

Cloud Security

- Advanced WAF
- Cloud Firewall
- DDoS
- API Security
- Email & Office Security
- CNAPP

Secure Network

- ADC e GSLB
- Advanced WAF
- CPS (Cyber Physical Systems)
- Gestão e Automação de Políticas
- IPS
- Microssegmentação com Visibilidade
- Inspeção de Tráfego Criptografado
- SD-WAN
- Switch
- Wi-Fi
- Next Generation Firewall
- PAM
- Workload Container Security



Detectar

Conheça **as soluções**

É crucial desenvolver e implementar as atividades apropriadas para identificar a ocorrência de um evento de segurança cibernética. Aqui, os ativos são constantemente monitorados para buscar anomalias e eventos adversos, visando identificar e mitigar potenciais problemas.

Frentes de atuação:

- **Análise de eventos adversos**
- **Monitoramento contínuo**

Conheça as soluções da CG One que se enquadram na categoria "Detectar" do NIST:

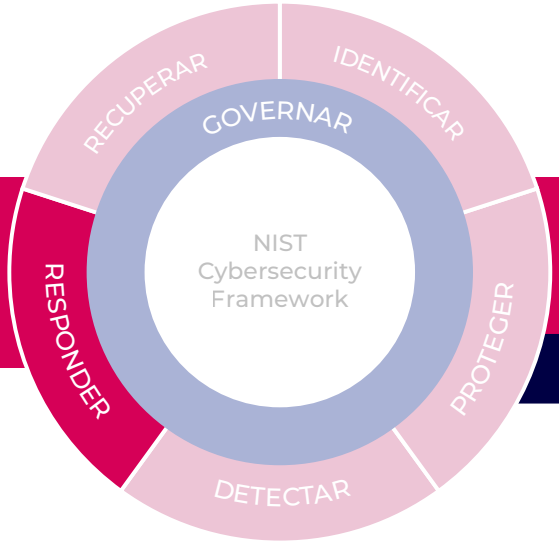
Gerenciamento e Análise
· Analyser

Secure Access & Endpoint
· EDR

Secure Network
· DLP · Sandbox Solution · XIoT/OT

Security Operation
· SIEM

Conheça **as soluções**



Responder

Conheça **as soluções**

A empresa deve desenvolver e implementar as atividades apropriadas para tomar medidas em relação a um evento de segurança cibernética detectado.

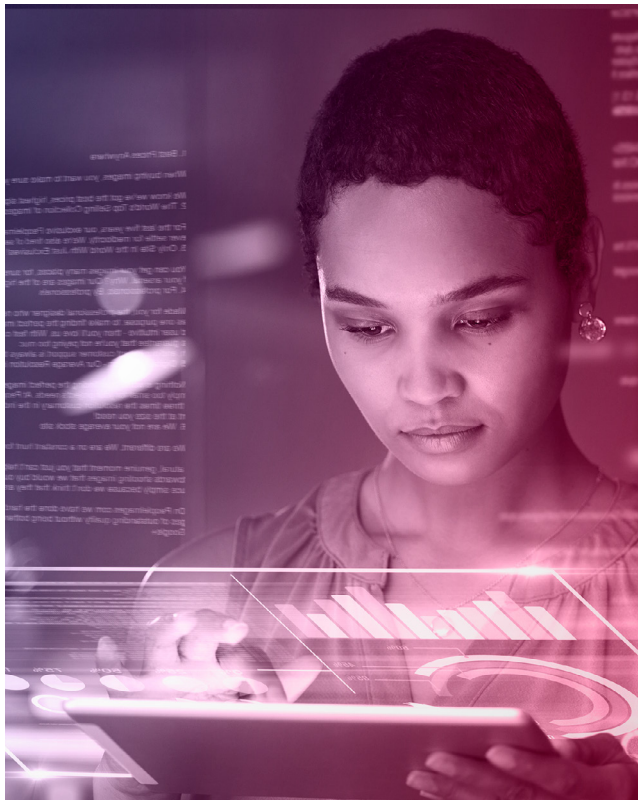
Frentes de atuação:

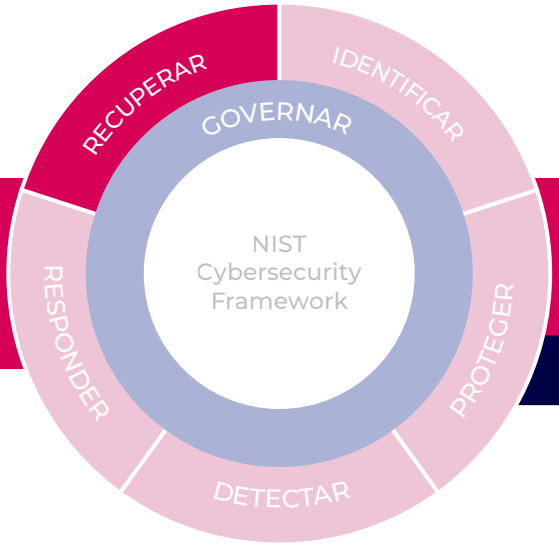
- **Gerenciamento e análise de incidentes**
- **Relatório e comunicação**
- **Plano de resposta a incidentes**
- **Mitigação de incidentes**

Conheça as soluções da CG One que se enquadram na categoria "Responder" do NIST:

Security Operation
• SOAR

Conheça **as soluções**





Recuperar

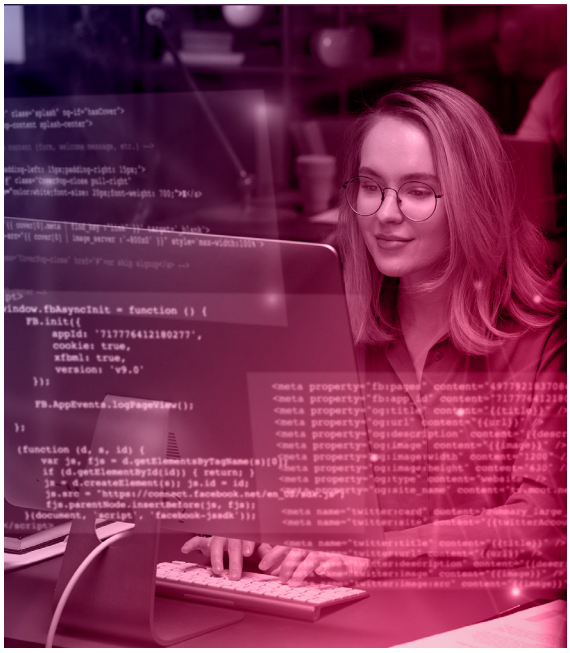
Conheça **as soluções**

As ações de recuperação devem garantir a disponibilidade operacional dos sistemas e serviços afetados por eventuais incidentes de cibersegurança.

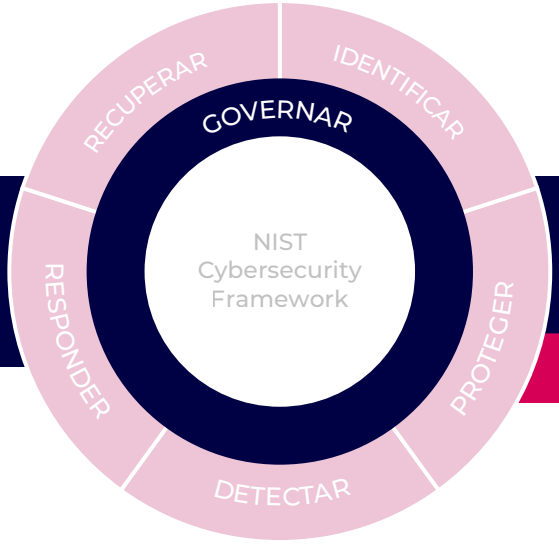
Frentes de atuação:

Planejamento de recuperação

Comunicação coordenada durante e após o incidente de segurança cibernética



Para saber mais sobre a categoria Recuperar, entre em contato com nossos especialistas.



Governar

Conheça **as soluções**

A nova versão 2.0 do framework adicionou um sexto pilar: Governar. Neste pilar, estamos falando de políticas, procedimentos e processos para monitorar os requisitos regulatórios, legais e de risco de segurança cibernética da organização.

Frentes de atuação:

- **Adaptação ao contexto da organização**
- **Estratégia de gestão de risco**
- **Definição de papéis e responsabilidades**
- **Gerenciamento de riscos na cadeia de suprimentos**
- **Políticas e procedimentos**

Conheça as soluções da CG One que se enquadram na categoria "Governar" do NIST:

GRC, Ética e Conscientização

- Awareness Training
- Ethics Management
- Third-Party Risk Management (TPRM)
- Incident Management
- Internal Audit
- Policy Management
- Risk Management

Privacy

- Cookie Compliance
- Data Subject Rights Request Management (DSAR)
- Consent Management
- Maturity Benchmarking

Serviços

- Adequação à LGPD
- DPO as a service
- Privacy Proof

Conheça **as soluções**

Como implementar o NIST Cybersecurity Framework?

O NIST oferece um passo a passo para a criação ou aprimoramento do seu programa de gestão de riscos de segurança da informação. Abaixo, fizemos um resumo dessas diretrizes. Acesse o documento completo aqui.

1. Priorize e defina o escopo

Ao priorizar e definir o escopo do projeto, é fundamental estabelecer uma visão clara do que se pretende alcançar. Isso envolve a criação de um escopo bem definido, delimitando as fronteiras do projeto e identificando suas prioridades. Neste estágio, é crucial estabelecer as missões de alto nível e determinar a tolerância ao risco da empresa. Isso permitirá uma compreensão abrangente das metas e limites do projeto, orientando as decisões e a alocação de recursos de forma eficiente.

2. Oriente

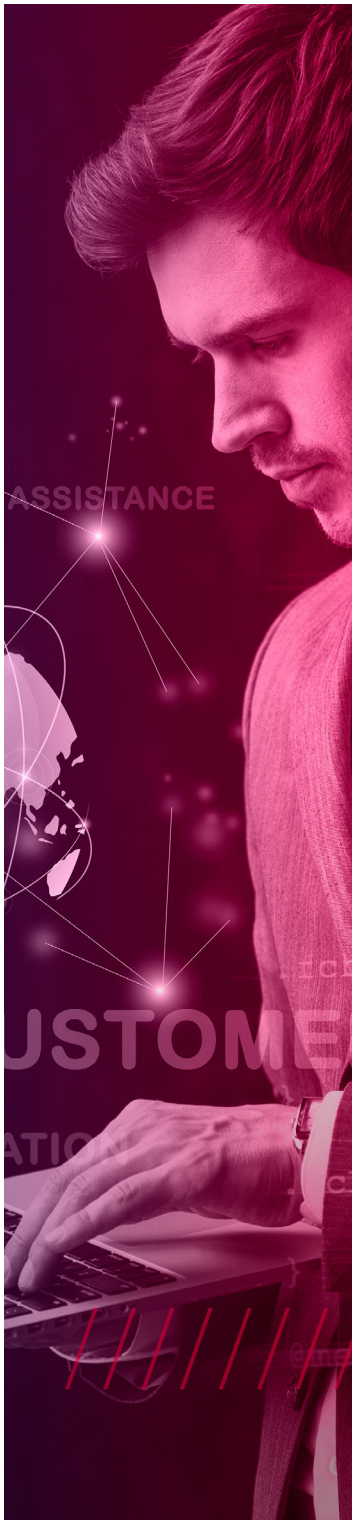
Identifique os ativos, sistemas e as ameaças às quais a organização pode estar exposta. Isso envolve uma análise minuciosa dos recursos críticos da organização, bem como das vulnerabilidades e ameaças potenciais que podem comprometer sua segurança. Ao entender completamente o panorama de ameaças, a organização estará mais bem preparada para implementar medidas eficazes de segurança cibernética e mitigar os riscos identificados.

3. Avalie o perfil atual

Fazer uma avaliação do perfil atual da organização envolve uma captura instantânea de como os riscos estão sendo gerenciados no momento. Isso inclui uma análise detalhada dos processos, controles e práticas de segurança existentes. Ao compreender o estado atual de segurança cibernética da organização, é possível identificar áreas de força e fraqueza, fornecendo insights valiosos para orientar as etapas futuras do processo de gerenciamento de riscos.

4. Conduza uma avaliação de risco

Avalie as ameaças para determinar a probabilidade e a gravidade de um evento. Ao entender a natureza e a magnitude das ameaças enfrentadas pela organização, é possível priorizar os riscos e concentrar os esforços de mitigação nos aspectos mais críticos da segurança cibernética.



5. Crie um perfil de destino

Nesta etapa, é importante definir todas as metas de gerenciamento de riscos que a organização deseja alcançar. Isso envolve estabelecer um perfil de destino que represente o estado desejado de segurança cibernética. Ao definir claramente os objetivos e metas, a organização pode direcionar seus esforços de forma eficaz e monitorar seu progresso ao longo do tempo.

6. Determine, analise e priorize lacunas

Ao determinar, analisar e priorizar lacunas, é essencial identificar as diferenças entre o estado atual e o estado desejado de segurança cibernética. Isso envolve uma análise abrangente das deficiências e lacunas existentes nos processos, controles e práticas de segurança.

7. Implemente o plano de ação

Finalmente, é o momento de executar as medidas planejadas para preencher as lacunas identificadas. Isso envolve a implementação de novos processos, controles e tecnologias de segurança, bem como a revisão e melhoria contínua das práticas existentes. Ao executar o plano de ação de forma diligente e eficiente, a organização pode fortalecer sua postura de segurança cibernética e mitigar eficazmente os riscos identificados.

Conclusão

Em resumo, o NIST® emerge como um aliado essencial na busca por um ambiente digital mais seguro e resiliente.

Seu framework oferece uma abordagem abrangente e clara para **avaliar, aprimorar e manter a eficácia das práticas de segurança cibernética.** Ao adotá-lo, as organizações ganham direção na gestão de riscos, promovem padronização e fortalecem suas defesas contra as ameaças digitais.

Por isso, antes de contratar seu próximo fornecedor de cibersegurança, avalie se o portfólio dele está alinhado a esse importante framework de cibersegurança. Isso demonstra maturidade e conhecimento do assunto, o que faz toda a diferença ao escolher seu próximo parceiro no combate às ameaças cibernéticas.

O diferencial CG One

Enquanto você se concentra em impulsionar o seu negócio, nossa equipe de especialistas está pronta para cuidar de todas as complexidades tecnológicas do seu negócio. Conte com a CG One como seu parceiro estratégico de segurança digital e riscos. Protegemos ecossistemas digitais de ponta a ponta das melhores empresas do Brasil, empoderando nossos clientes com soluções inovadoras para que possam focar em seus negócios com tranquilidade.

Network

Configuração, otimização e fortalecimento das infraestruturas de rede.

Security

Proteção de ativos críticos e prevenção de ataques cibernéticos.

Integrated Risk Management

Gerenciamento de riscos para melhorar a visibilidade e o processo de tomada de decisão.

Parceiros:

Akamai · algosec · Checkmarx · CHECK POINT · CLAROTY · CYBERARK · CYREBRO · FORTINET · GetGlobal · KEYSIGHT · netskope · OneTrust · proofpoint.

CG//One

Dê o próximo passo

Com mais de 40 anos de expertise no mercado, sabemos exatamente como proteger o seu negócio das mais avançadas ameaças cibernéticas. Desenvolvemos e gerenciamos soluções de **Redes, Segurança da Informação e Gerenciamento Integrado de Riscos, em conformidade com as práticas e os padrões de segurança do NIST.**

Contamos com um time qualificado e certificado que já proporcionou operações seguras para mais de 500 empresas de diversos portes e setores, em todo o Brasil.

Quer implementar o NIST?

Converse agora
com um especialista