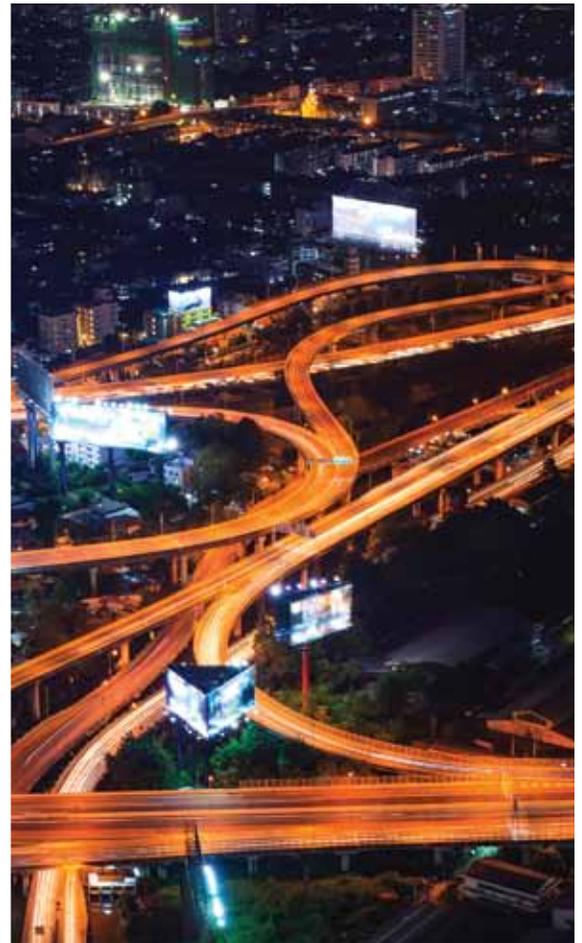




# CONHEÇA QUAIS SÃO OS SEUS RISCOS ANTES DE QUE SE TORNEM REALIDADE



## SERVIÇOS PROFISSIONAIS DE SEGURANÇA CIBERNÉTICA UM ENFOQUE SISTEMÁTICO E INTEGRAL DO GERENCIAMENTO DE RISCOS E DA PROTEÇÃO DE SEU SISTEMA DE MISSÃO CRÍTICA

### CONSTRUINDO REDES MAIS RESILIENTES EM UMA ERA DE CRESCENTES ATAQUES CIBERNÉTICOS

O mundo digital tem introduzido inéditas maneiras de aumentar a produtividade, maximizar o valor e, finalmente, melhorar a vida de bilhões de pessoas. Ao mesmo tempo, uma série de incidentes de segurança cibernética tem trazido desafios únicos tanto para as empresas como para os órgãos governamentais. Na atualidade, ataques variados capazes de modificar-se a cada execução estão em todos os lugares. Enquanto muitas organizações gostariam de pensar que as suas informações mais sensíveis de missão crítica estão protegidas, fica cada vez mais evidente que ninguém está imune. A segurança cibernética vai para além dos ataques de hackers e dos controles técnicos.

O cenário de aplicação e execução das normas de segurança cibernética também é um cenário dinâmico e de rápida evolução, no qual vão aparecendo cada vez mais desafios no esforço por atender aos inúmeros padrões industriais e administrar os controles de segurança adequados. À medida que as redes de missão crítica vão evoluindo em sistemas dinâmicos de redes interconectadas com mais plataformas de código aberto e soluções baseadas na nuvem, é preciso governar e supervisionar todo o ciclo de vida do sistema. Isto inclui uma reavaliação coordenada e regular de pessoas, processos e tecnologias para assegurar a prontidão organizacional para proteger, detectar e responder às ameaças em constante evolução.



## ENTENDENDO SUA POSTURA EM RELAÇÃO AOS RISCOS DA SEGURANÇA CIBERNÉTICA

Os Serviços Profissionais de segurança cibernética da Motorola proporcionam um processo sistemático e integral para a identificação, avaliação e gerenciamento de riscos de segurança cibernética em todos os sistemas empresariais. Com os Serviços Profissionais de segurança cibernética, você poderá entender perfeitamente qual é a sua posição em relação aos riscos de segurança cibernética relacionados com o ambiente operacional da sua empresa. A Motorola oferece uma análise integral do seu perfil exposto a ataques, além de uma avaliação de custo-benefício e recomendações detalhadas de correção. Com processos empresariais e tecnologias em constante mudança, as ameaças contra a segurança mudam permanentemente e a posição da sua organização nunca é estática. A avaliação periódica da posição de segurança ajuda a manter um registro atualizado das vulnerabilidades e a priorizar as ações de correção necessárias com base nos riscos para as suas operações.

Em 2014, o Instituto Nacional de Padrões e Tecnologia (NIST) apresentou o quadro para aperfeiçoar a Segurança Cibernética de Infraestrutura Crítica para ajudar as organizações a conseguir resultados específicos a respeito da Segurança Cibernética. O quadro inclui as principais práticas de vários órgãos de normatização que foram implementadas com sucesso. A Motorola Solutions participou no desenvolvimento deste quadro juntamente com seus parceiros da indústria e do governo. Isto permite à Motorola basear a sua avaliação nas recomendações do NIST fazendo um mapeamento do quadro de Segurança Cibernética do NIST para os processos e procedimentos de gestão de riscos atuais de sua organização a fim de determinar os níveis de risco de seu perfil de Segurança Cibernética atual e as recomendações futuras.

### QUADRO DE SEGURANÇA CIBERNÉTICA DO NIST

 <b>IDENTIFICAÇÃO</b>	 <b>PROTEÇÃO</b>	 <b>DETECÇÃO</b>	 <b>RESPOSTA</b>	 <b>RECUPERAÇÃO</b>
Ambiente empresarial Gestão de riscos Gerenciamento de ativos Avaliação de riscos Gerenciamento de riscos	Políticas Processos Segurança de dados Controle de acesso Tecnologia de proteção Conscientização e capacitação	Anormalidades e eventos Processos de detecção Monitoramento contínuo	Planejamento de resposta Comunicações Análise Mitigação Aperfeiçoamentos	Planejamento de recuperação Aperfeiçoamentos Comunicações

A infraestrutura dos sistemas de missão crítica é variada e complexa; estes sistemas devem ser seguros e devem poder se recuperar rapidamente de qualquer perigo, incluindo eventos físicos e cibernéticos. Os nossos esforços para reduzir os riscos e efetuar atividades de gerenciamento são baseados na identificação de ativos, na avaliação de riscos com base nas consequências, nas vulnerabilidades e ameaças, na proteção, e na medição da efetividade.

# OTIMIZAÇÃO DO GERENCIAMENTO DE RISCOS MEDIANTE A IDENTIFICAÇÃO E REDUÇÃO DE AMEAÇAS

Após muitos anos de trabalho com clientes governamentais, empresariais e de segurança pública, a equipe de Serviços Profissionais de Segurança Cibernética da Motorola desenvolveu um enfoque abrangente e metodológico para o gerenciamento de riscos que oferece um resultado verdadeiramente integral e com priorização baseada em riscos. Os responsáveis pela análise de riscos e os tomadores de decisões recebem uma análise objetiva e cuidadosamente calculada dos fatores de risco aplicáveis.

## ALCANCE

São selecionados só os controles aplicáveis que abrangem as categorias Técnica, Operacional e de Gestão para executar uma análise de riscos personalizada. Os procedimentos para minimizar as mudanças na arquitetura de segurança, integração de produtos específicos ou implementação de controle de procedimentos são sugeridos e discutidos com os interessados somente após o ambiente ter sido metodicamente avaliado, os riscos terem sido identificados, analisados e compreendidos claramente e serem designadas as respectivas prioridades.

## FOCO

Utilizando observação física, entrevistas pessoais, ferramentas personalizadas manuais, computadorizadas e comerciais atualmente disponíveis no mercado, a Motorola avaliará os diferentes cenários de potenciais ameaças e as possíveis implicações dos riscos na confidencialidade, integridade e disponibilidade da missão da organização.

## METODOLOGIA

Todos os fatores de risco aplicáveis são considerados e levados em conta antes e durante a avaliação. Depois de coletar todos os dados necessários relativos ao alcance da avaliação, um perfil de ameaças é desenvolvido e preparado em forma de Scorecard de Riscos, indicando um valor baixo, moderado, alto ou crítico para cada resultado/incidente identificado. Uma recomendação de correção ou de aceitação do risco vão acompanhar cada resultado/incidente.

## ÁREAS DOS SERVIÇOS PROFISSIONAIS DE SEGURANÇA CIBERNÉTICA

### GERENCIAMENTO

- Análise de Impacto Comercial
- Identificação/Classificação de Ativos
- Avaliação do Grau de Preparação do Quadro do NIST
- Estrutura de Gestão do Quadro e Institucionalização
- Indicadores-chave de Desempenho (KPI) Organizacional e Scorecard de Riscos Cibernéticos
- Desenvolvimento de Padrões e Políticas Organizacionais
- Eficácia Operacional dos Processos
- Modelagem de ameaças/Inteligência de Ameaças
- Avaliação de Riscos de Propriedade Intelectual
- Avaliação de Riscos Relacionados com o Desenvolvimento de Software e a Manufatura Off-shore
- Ciclo de Desenvolvimento Seguro
- Pesquisa/Análise de Ameaças
- Avaliação do Impacto do Cumprimento Regulamentar
- Processo de Políticas de Gestão de outros provedores
- Treinamento e Conscientização

### OPERACIONAL

- Consultas de Clientes Ad-hoc
- Assistência em Segurança Operacional
- Assistência em Resposta a Incidentes
- Investigação Forense Digital
- Monitoramento de Segurança Personalizado
- Monitoramento Personalizado para Detecção de Anomalias
- Testes de Engenharia Social

### TÉCNICO

- Avaliação de Segurança Cibernética de Riscos Técnicos
  - Varredura de Vulnerabilidades
  - Segurança de Aplicativos Web
  - Testes de Penetração sem fio e LAN
  - Testes de Penetração Física
  - Avaliação de Implementação de Nuvem
- Avaliação de Cumprimento
- Revisão de Arquitetura de Rede
- Soluções de Gerenciamento de Acesso e Identidades
- Avaliação de Conectividade de outros provedores
- Avaliação de Riscos de Ambiente SCADA
- Inventário de Ativos/Detecção de Redes
- Revisão de Código/Auditoria de Aplicativos
- Arquitetura de Referência de Segurança
- Segurança de Arquitetura Empresarial
- Serviços Criptográficos
- Adoção de Tecnologia Móvel Segura
- Implementação e Monitoramento de Honey Pot
- Cumprimento de Licença de Software de Código Aberto

## OPÇÕES DE ENTREGA DE SERVIÇOS PROFISSIONAIS DE SEGURANÇA CIBERNÉTICA

A equipe de Serviços Profissionais de Segurança Cibernética da Motorola está integrada por profissionais de segurança certificados e devidamente capacitados para manter-se devidamente informados sobre o cenário de ameaças de segurança em constante mudança e as tecnologias relacionadas. Trabalharemos com você para estabelecer a melhor metodologia de avaliação para que você possa atingir os seus objetivos empresariais. As opções incluem:

### EXECUÇÃO A CARGO DA MOTOROLA

El equipo de Servicios Profesionales de Seguridad Cibernética de Motorola ejecuta la evaluación integral y propone sugerencias con prioridades basadas en los riesgos encontrados.

### PARTICIPAÇÃO CONJUNTA

Trabajo conjunto entre Motorola y su propio personal de TI a fin de garantizar la sostenibilidad del programa, la posibilidad de compartir información y la colaboración de expertos.

### COORDENAÇÃO COM TERCEIROS INDEPENDENTES

Entidade terceira de confiança designada para executar uma avaliação imparcial com a supervisão da Motorola a fim de garantir a que a execução seja bem sucedida para atingir os seus objetivos.

## CONFIE NA MOTOROLA SOLUTIONS E OBTENHA SERVIÇOS PROATIVOS PARA A GESTÃO DE RISCOS RELACIONADOS COM A SEGURANÇA CIBERNÉTICA

Como líder mundial no fornecimento de tecnologias seguras para operações de missão crítica em mais de 100 países, entendemos perfeitamente a importância de projetar, desenvolver e implantar tecnologias inovadoras mais efetivas e seguras.

As expectativas demandam um enfoque cada vez mais integral da Segurança Cibernética através dos ciclos operacionais e de desenvolvimento e implementação. Os avanços tecnológicos nas comunicações de missão crítica resultam em maior vulnerabilidade a falhas na segurança.

Os seus sistemas críticos são vistos como alvos de grande valor pelos criminosos da informática, que cada vez são mais entendidos em tecnologia. Estas tendências exacerbadas aumentam os riscos contra a disponibilidade, a confidencialidade e a integridade dos seus aplicativos de voz e dados de missão crítica. A adoção de um enfoque abrangente com respeito à segurança do sistema com detecção proativa de ameaças, resposta em tempo real e ações corretivas que proporciona a tranquilidade de contar com um sistema seguro e flexível.

Para mais informações sobre os Serviços de Segurança, entre em contato com o seu representante local da Motorola ou visite [motorolasolutions.com/services](https://motorolasolutions.com/services)

Motorola Solutions, Inc. 1301 E. Algonquin Road, Schaumburg, Illinois 60196 EE.UU. [motorolasolutions.com](https://motorolasolutions.com)

MOTOROLA, MOTO, MOTOROLA SOLUTIONS e o logotipo M estilizado são marcas comerciais ou marcas comerciais registradas da Motorola Trademark Holdings, LLC e são utilizadas sob licença. Todas as outras marcas comerciais pertencem a seus respectivos proprietários. © 2015 Motorola Solutions, Inc. Todos os direitos reservados. GC-21-165

