Sumário Executivo 2025

Carta do Chair da Conferência

Esperamos vê-lo na Conferência Gartner de Segurança e Gestão de Riscos de 2026.

Atenciosamente,
Paul Furtado
Chair da Conferência e Vice-Presidente Analista, Gartner

Principais conclusões

1 Transformar o hype em oportunidade para cibersegurança

Comece reformulando as conversas executivas para enfatizar exposições críticas e impulsionar a cibersegurança orientada por missão. Desenvolva acordos de nível de proteção para manter um foco claro na segurança cibernética e nos resultados de negócio. Garanta que seu programa de segurança esteja pronto para inovação investindo em gestão de mudanças, agilidade de aprendizado e resiliência pessoal. Com comunicação clara e forte tomada de decisões, uma liderança excepcional pode guiar sua organização em meio à complexidade.

"O hype gera disrupção e confusão, mas podemos transformar isso em uma oportunidade para a cibersegurança e nossas organizações. Aproveite o momento!"

Oscar Isaka,
Diretor Analista Sênior,
Gartner

2 Refinar sua visão de segurança para atender aos principais imperativos

Alinhe sua visão com seu programa de cibersegurança, enfatizando a transformação e a resiliência. O desempenho será otimizado ao se avaliar capacidades, aprimorar a tecnologia, explorar a IA e apoiar o bem-estar da equipe. Aumente a resiliência por meio da conscientização, responsabilização por riscos de terceiros, integração de dissuasão e julgamento cibernético. Em seguida, implemente a gestão de riscos colaborativa, adapte sua estratégia, refine a gestão de políticas e redefina a segurança dos dados.

"CISOs bem-sucedidos se concentram em otimizar o desempenho, a resiliência e a agilidade de seus programas de segurança cibernética."

Pedro Pablo Perea
de Duenas,
Sr Principal Analista,
Gartner

3 Fechar lacunas de resiliência cibernética e fortalecer a segurança

Para desenvolver uma estratégia de resiliência cibernética, comece abordando o foco dos stakeholders e reguladores na disponibilidade do sistema e dos dados. Avalie a profundidade e a precisão de suas Análises de Impacto nos Negócios (BIAs - Business Impact Analyses) atuais para aproveitar os insights existentes. Aumente a resiliência cibernética colaborando entre equipes com foco no impacto nos negócios. Com recursos avançados integrados, como detecção e resposta automatizadas a ameaças, você pode efetivamente incorporar a resiliência ao seu programa.

"A resiliência cibernética não é apenas uma vantagem estratégica; é uma necessidade crítica para a sobrevivência."

Arthur Sivanathan,
Diretor Analista Sênior,
Gartner

4 Foco nas tendências de segurança e escolhas estratégicas

Elabore estratégias para seus planos de cibersegurança abordando tendências como geopolítica, criptografia pós-quântica e IA tática, ao mesmo tempo em que alinha iniciativas de zero trust com objetivos estratégicos. Combata o esgotamento profissional em segurança cibernética equilibrando as cargas de trabalho e promovendo a saúde mental por meio de suporte de RH e programas de bem-estar. Utilize uma estrutura de consolidação de plataforma para otimizar os esforços, mas tenha cuidado com escopos inadequados e influências de fornecedores que podem levar a estouros de custos. Aceite uma mudança cultural promovendo a adaptabilidade e a abertura à mudança, o que pode ajudar a superar a resistência e se adaptar à complexidade de zero trust.

"É bem sabido que temos pouco controle sobre influências externas, como reguladores, agentes de ameaças e trajetórias de negócios. No entanto, temos controle sobre nossas respostas aesses desafios."

Fadeen Davis,
Sr Principal Analista,
Gartner

5 Navegar pela incerteza da IA com estratégias acionáveis

Transição da exploração da GenAI (IA Generativa) para a implementação de estratégias acionáveis, protegendo a IA de terceiros, aplicações corporativas e aprimorando a segurança cibernética. Priorize melhorias táticas que ofereçam benefícios claros e colabore com líderes funcionais e usuários finais para garantir que as políticas da GenAI estejam alinhadas às demandas do negócio. Aborde o risco expandido da superfície de ataque avaliando ferramentas de segurança novas e existentes. Por fim, defina e implemente métricas orientadas por resultados para medir efetivamente o impacto e o sucesso de suas iniciativas de GenAI, garantindo que elas atendam às metas organizacionais.

"CISOs bem-sucedidos não buscam "a melhor IA", eles avaliam melhorias testando-as em casos de uso reais."

Katell Thielemann,
Vice-presidente
Analista Distinto,
Gartner

6 Desenvolver e compartilhar uma estratégia adaptável de risco cibernético

Adotar uma estrutura de risco estratégico que integre a cibersegurança às operações comerciais ajudará a equilibrar as disrupções e incertezas. Identifique se você é um modelador ou respondedor de disrupções e crie uma estratégia adaptável de risco cibernético. Compartilhe isso com sua equipe para evitar a gestão isolada de riscos e aumentar a resiliência. Garanta que todos saibam seu papel na gestão de riscos cibernéticos para fortalecer a segurança. Estabeleça um RACI com os líderes e atualize seu conselho sobre os riscos cibernéticos para tomar decisões informadas. Em seguida, use o CyberGRC para melhorar a visibilidade e concentrar os investimentos nos problemas certos, demonstrando valor em seus esforços de segurança cibernética.

"À medida que as ameaças cibernéticas evoluem com nova sofisticação, a questão não é se sua organização será alvo, mas quando."

Arthur Sivanathan,
Diretor Analista Sênior,
Gartner

7 Ampliar uma gestão de risco cibernético de terceiros

Com disrupções frequentes de terceiros, o Gartner prevê que o desempenho de TPCRM (Third-Party Cyber Risk Management - Gestão de Riscos Cibernéticos de Terceiros) será um item importante na agenda do Conselho até 2026. Use o ciclo de vida de TPCRM do Gartner para avaliar a integralidade e a transparência do programa na divisão de trabalho. Facilite o envolvimento do parceiro na gestão de riscos cibernéticos esclarecendo funções e focando em atividades críticas. Mantenha seu conselho atualizado sobre o desempenho de TPCRM, garantindo que os relatórios e o orçamento estejam alinhados com os ODMs e PLAs.

"Para sermos eficazes na gestão de riscos cibernéticos de terceiros, precisamos mudar da prevenção de riscos puros para ajudar a empresa a assumir esses riscos de forma inteligente."

Oscar Isaka,
Diretor Analista Sênior,
Gartner

8 Priorizar o fator humano

É essencial reconhecer que, embora a maioria dos investimentos em segurança cibernética se concentre em soluções técnicas, o erro humano costuma ser a causa raiz dos incidentes. Adote uma mentalidade de resiliência humana desde o primeiro dia, mudando o foco da prevenção para a resiliência, e mude a linguagem usada na cibersegurança para evitar que tenhamos uma narrativa "nós vs. eles". Primeiro, desenvolva métricas para medir a resiliência humana e afaste-se de métricas focadas em falhas. Em seguida, faça a transição do treinamento de compliance tradicional para incentivos dinâmicos que incentivem hábitos mais seguros e adapte sua estratégia de segurança cibernética para uma resiliência cibernética mais ampla.

"A segurança deve ser um componente central, não uma reflexão tardia."

Oscar Isaka,
Diretor Analista Sênior,
Gartner

Save the date!

Confira nossa agenda para explorar a variedade de conferências que realizamos para encontrar aquelas que sejam mais relevantes para você e para os seus negócios.