

Segurança cibernética em 2027

resiliência por meio de governança estratégica e autonomia

forvis mazars

Prefácio

A segurança cibernética enfrenta uma convergência de tecnologias em rápida mudança, regulamentos em evolução e ameaças avançadas. Para se preparar para o que vem a seguir, as organizações precisarão adotar a governança estratégica e a inovação intencional.

O relatório deste ano explora como as organizações podem aproveitar a tecnologia e lidar com questões globais complexas — como regulamentação, instabilidade geopolítica e questões de soberania digital — para melhorar a resiliência e a autonomia organizacionais.

Para avançar, as organizações devem integrar a segurança cibernética em suas estratégias de inovação e implementação, mantendo-se ágeis para se adaptar às ameaças em constante evolução. Aquelas que o fizerem protegerão seus ativos e obterão uma vantagem competitiva na economia digital.

À medida que as organizações olham para 2027, a segurança cibernética torna-se cada vez mais indissociável da transformação digital. A IA está remodelando o panorama das ameaças, enquanto mudanças operacionais, regulamentação e soberania digital acrescentam ainda mais complexidade. Juntas, essas pressões estão criando novos riscos e requisitos que exigem uma tomada de decisão mais estratégica.



"As ameaças cibernéticas estão evoluindo mais rápido do que nunca, impulsionadas pela IA, ecossistemas interconectados, tensões geopolíticas e um ambiente regulatório cada vez mais complexo. No entanto, a resposta permanece a mesma: uma abordagem baseada em risco que protege o que mais importa e trata a resiliência, não simplesmente a conformidade, como a verdadeira medida de segurança cibernética"

Wadi Mseddi,
Líder do Grupo de Consultoria em Segurança Cibernética, Forvis Mazars

Principais insights

As principais organizações estão indo além da segurança cibernética como um centro de custos e encontrando maneiras estratégicas de aproveitá-la como uma vantagem competitiva

A soberania digital é um foco cada vez maior, mas a autonomia é um objetivo mais útil para as organizações globais

Uma infinidade de regulamentações digitais e de segurança na Europa e contrasta com um movimento de desregulamentação nos EUA, o que significa que uma abordagem baseada em risco continua a ser a resposta para a fadiga de conformidade

A tecnologia operacional está sendo cada vez mais integrada aos ecossistemas corporativos de TI, criando riscos e recompensas

A IA criou uma corrida armamentista entre atacantes e defensores, exigindo combater a IA com IA e implantar uma governança proporcional

A governança de dados ainda é a pedra angular de estratégias eficazes de segurança cibernética, mas deve ser aplicada proporcionalmente

As equipes de segurança cibernética devem receber investimento contínuo para equilibrar a estabilidade com a agilidade e o avanço das posturas de segurança

Estado global da segurança cibernética

Por que a segurança cibernética está se tornando uma prioridade na cadeia de suprimentos

Organizações com fortes posturas de segurança cibernética estão ganhando cada vez mais contratos e parcerias em relação aos concorrentes, já que as RFPs e licitações agora rotineiramente excluem fornecedores que não conseguem demonstrar que atendem aos padrões cibernéticos prescritos.

Com a infraestrutura tecnológica e a cadeia de suprimentos de cada organização cada vez mais complexas, as organizações com fortes posturas cibernéticas estão cada vez mais se beneficiando de vantagens de reputação e preferências da cadeia de suprimentos. Essa tendência é particularmente pronunciada nos mercados B2B, onde RFPs e licitações agora incluem rotineiramente requisitos substanciais de segurança cibernética, removendo fornecedores em potencial de consideração cujas medidas cibernéticas não atendem ao padrão prescrito.

A complexidade das cadeias de suprimentos modernas significa que as organizações muitas vezes não entendem completamente onde seus dados residem ou como estão sendo processados. Essa falta de visibilidade cria vulnerabilidades significativas, particularmente à medida que tecnologias como a IA introduzem novas formas de compartilhamento e processamento de dados. Além disso, a crescente interconexão entre os principais sistemas corporativos, plataformas em nuvem e serviços de terceiros está expandindo as superfícies de ataque e tornando a resiliência dependente da visibilidade em todo o ecossistema de tecnologia.

Em última análise, espera-se que cada organização gerencie e monitore os riscos de segurança cibernética em todo o seu ecossistema. Isso se reflete no Regulamento de Resiliência Operacional Digital (DORA) da UE e na Diretiva NIS2, que fortalecem os requisitos para o gerenciamento de riscos cibernéticos de terceiros e da cadeia de suprimentos.

Essa mudança para a responsabilidade compartilhada está impulsionando a adoção de estruturas mais sofisticadas de gerenciamento de riscos de terceiros (TPRM). O surgimento de ferramentas de monitoramento de terceiros que classificam as organizações em métricas de segurança cibernética criou uma nova forma de pressão do mercado. As empresas estão descobrindo que sua maturidade cibernética pode afetar diretamente sua capacidade de conquistar contratos, garantir parcerias e manter a confiança do cliente.



Soberania versus autonomia: a nova geopolítica da segurança cibernética

A segurança cibernética é cada vez mais uma questão de soberania nacional. Os governos agora examinam onde os dados críticos são armazenados, quem opera os principais serviços digitais e de quais tecnologias as organizações dependem, porque os ataques cibernéticos se tornaram instrumentos de ação estatal. Grupos como o Volt Typhoon se incorporaram à infraestrutura civil para alavancagem futura, e interrupções como a interrupção da CrowdStrike em 2024 expuseram a fragilidade da dependência excessiva de provedores externos, especialmente aqueles subordinados a outras jurisdições.

A resposta política tem sido rápida, particularmente na Europa: requisitos de residência de dados, iniciativas soberanas de nuvem e uma rede cada vez mais rígida de regulamentação, com NIS2 e DORA enfatizando a resiliência operacional e a segurança da cadeia de suprimentos. A tendência vai muito além da Europa, no entanto, e o padrão para uma segurança cibernética eficaz está mudando junto. Desde a comprovação da conformidade até a comprovação da resiliência, é vital demonstrar que as operações essenciais podem continuar e se recuperar após um incidente cibernético.

No entanto, a soberania por si só não é uma estratégia de resiliência. Perseguida ao extremo, a soberania pode fragmentar as paisagens dos fornecedores, duplicar a infraestrutura e limitar o acesso à tecnologia eficaz, e pode até concentrar o risco, permitindo que um único governo mantenha a continuidade como refém.

O que as organizações devem buscar é a autonomia – a capacidade de entender, controlar e, quando necessário, mudar suas dependências digitais.

As organizações devem:



Saiba onde os dados confidenciais são armazenados e processados: incluindo backups e funções de suporte, não apenas o que o contrato diz.



Entenda a exposição geopolítica dos fornecedores: as dependências ocultas no fundo da cadeia de suprimentos podem importar tanto quanto os contratos principais.



Considere a localização e jurisdição do provedor durante as compras: a exposição legal e geopolítica de um provedor crítico é agora um fator de risco legítimo.



Demonstrar resiliência, não apenas conformidade: incorporar a soberania a um programa de resiliência mais amplo como um dos vários insumos.

Enquadrada dessa forma, a autonomia – não a soberania – é o objetivo estratégico, e um marcador mais verdadeiro da resiliência que reguladores, clientes e investidores estão realmente pedindo.

“As organizações que tratam a soberania digital como uma consideração dentro de uma busca deliberada de autonomia – conhecendo suas dependências, escolhendo parceiros confiáveis e provando que podem resistir à ruptura – se estarão não apenas em conformidade, mas genuinamente resilientes”



Jakob Haesler
Líder Global de Consultoria,
Forvis Mazars

“As fronteiras entre paz e conflito estão se apagando no ciberespaço. Os atores estatais estão se posicionando dentro da infraestrutura civil – não para ganho imediato, mas para alavancagem futura – e isso muda o cálculo de risco para todas as organizações que dependem de serviços digitais.”



George Lagarias
Economista-Chefe,
Forvis Mazars

Como a DORA e o NIS2 estão mudando a regulamentação de segurança cibernética?

A DORA e a NIS2 estão reformulando a conformidade com a segurança cibernética em toda a Europa, mudando o padrão de fornecer conformidade no papel para demonstrar resiliência operacional. Para as organizações multinacionais, navegar em ambos simultaneamente tornou-se um dos desafios regulatórios mais complexos de 2027.

Na UE, o desafio é em grande parte volumoso: bem mais de uma centena de atos e diretivas relacionados ao digital em vigor, cada uma contribuindo para uma teia densa e interligada de obrigações. O NIS2 está finalmente sendo aplicado após vários adiamentos, e a próxima Lei de Resiliência Cibernética exigirá que produtos com elementos digitais atendam aos controles de segurança cibernética. Uma vez que a NIS2 é uma diretiva, os Estados-Membros transpõem seus princípios para a legislação nacional de formas sutilmente diferentes, pelo que as organizações não podem simplesmente transferir e reutilizar o trabalho de conformidade de uma jurisdição para outra. O omnibus digital proposto visa estratificar a regulamentação de forma mais sensata e adaptá-la ao tamanho e perfil de risco de cada organização, embora ainda não tenha sido plenamente implementado.

Do outro lado do Atlântico, o problema se inverte. Os Estados Unidos estão caminhando para uma desregulamentação significativa, sem nada que se assemelhe a uma estrutura federal abrangente para a segurança cibernética. O que existe é principalmente focado na indústria e no governo, mais notavelmente o Certificação do Modelo de Maturidade em Segurança Cibernética (CMMC) para aqueles que trabalham com o Departamento de Guerra. Embora, mesmo isso tenha sido adiado, sua aplicação efetivamente pausou e os efeitos se espalharam para áreas adjacentes, como TI em serviços financeiros. Não há lei federal de privacidade; a proteção é tratada estado por estado, e o clima político atual aponta para longe da legislação nacional, e não para ela. Contraintuitivamente, esse ambiente menos intervencionista traz sua própria fadiga: onde algumas estruturas são altamente prescritivas e outras deixam as organizações adivinhando. Enquanto isso, as empresas globais enfrentam a tensão de reconciliar abordagens abordagens extremamente dispares de uma só vez.

Como uma abordagem baseada em risco apoia a continuidade sem custos indevidos

Essa complexidade regulatória criou o que muitos profissionais do setor descrevem como um fardo e uma oportunidade. Embora muitas novas regulamentações visem ajudar a melhorar a resiliência e a continuidade dos negócios, o ônus que a conformidade cria também pode ser um grande peso para equipes já restritas.

À medida que a teia de requisitos de conformidade se torna mais complexa, as organizações que adotam uma abordagem de cumprir tabela podem ter dificuldade em lidar com requisitos díspares e áreas complicadas de sobreposição. Para manter a relação custo-benefício em seus esforços de conformidade, as empresas devem priorizar avaliações baseadas em risco. Uma abordagem de segurança cibernética baseada em risco pode ajudar as equipes de segurança cibernética a se concentrarem nos riscos que mais importam, para que a conformidade ofereça suporte à segurança em vez de impulsioná-la.

"As medidas de conformidade são apenas uma variável em um programa de segurança cibernética baseado em risco. Um regulamento ou uma estrutura específica pode afetar o perfil de risco de um aspecto do negócio, mas não deve definir toda a estratégia."



Tom Tollerton
Diretor, CMMC Practice Lead,
Forvis Mazars US

Estado global da segurança cibernética

O que é segurança de tecnologia operacional e por que ela está sob ataque?

A tecnologia operacional (TO) sustenta a infraestrutura crítica e as operações industriais em todo o mundo. À medida que esses sistemas se tornam mais conectados digitalmente, as ameaças cibernéticas estão crescendo, expondo ambientes que historicamente receberam menos atenção de segurança do que os sistemas de TI convencionais.

A TO tem sido tratada há muito tempo como uma preocupação de engenharia, e não de segurança cibernética, protegida menos por defesas sofisticadas do que por puro isolamento. No entanto, os ataques a ambientes de TO estão aumentando acentuadamente, especialmente em infraestruturas críticas, e esses sistemas historicamente subprotegidos estão se mostrando um alvo atraente para adversários com bons recursos e geopoliticamente motivados; somente em dezembro de 2025 houve tentativas de ataques à infraestrutura na Venezuela e na Polônia. Ao lado de incidentes como os da M&S e da Jaguar Land Rover, onde a continuidade dos negócios foi significativamente interrompida por ataques cibernéticos, a expectativa de visibilidade só aumenta.

Aqui reside um paradoxo difícil: a maioria dos líderes de tecnologia relata uma séria falta de visibilidade em sua rede de TO, e uma organização não pode governar o que não pode ver. A resposta natural é alcançar e conectar sistemas, dados e outras ferramentas para que o risco se torne compreensível e reportável. No entanto, essa conexão é precisamente o que cria a nova exposição. Os ambientes de TO estão cada vez mais ligados à TI corporativa, plataformas de nuvem e ferramentas de manutenção remota, e cada novo caminho corrói o isolamento que pode estar protegendo esses ativos. A busca pela transparência, tratada sem disciplina, pode fabricar a própria vulnerabilidade que deveria expor – um risco agravado pelos longos ciclos de vida da OT, pelo parque tecnológico legado por padrão e pelas janelas de manutenção amplas.

No entanto, a proteção desses ativos está se tornando cada vez mais obrigatória pela regulamentação digital, especialmente no que diz respeito à infraestrutura crítica.

> “O impulso para a visibilidade da TO é necessário, mas tem que ser disciplinado. Quando sistemas isolados há muito tempo são colocados ainda mais on-line sem governança e controles proporcionais, as organizações podem aumentar o risco operacional que estão tentando entender e evitar”



Paul Truitt
Diretor, Líder de Práticas de Segurança Cibernética, Forvis Mazars US

Como a IA está mudando a segurança cibernética?

A IA está mudando a natureza da segurança cibernética em ambos os lados da batalha. Os atacantes estão usando-a para lançar ameaças mais sofisticadas e direcionadas em escala, enquanto os defensores estão aproveitando-a para fortalecer a detecção, automatizar as respostas e melhorar a resiliência.

Até agora, a IA tem sido frequentemente enquadrada como oportunidade versus risco, mas esse enquadramento não é mais válido. A IA é uma disrupção estrutural que transforma todo o cenário e, em ambos os lados da fronteira cibernética, estão surgindo ecossistemas orientados por IA: desde a descoberta autônoma de vulnerabilidades até cadeias de ataques totalmente automatizadas. O resultado é uma corrida armamentista em que a distância entre atacantes e defensores está aumentando.

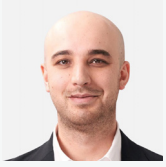
Uma disputa assimétrica

É uma lacuna de possibilidade tanto quanto de capacidade; atacantes e defensores podem comandar uma tecnologia semelhante, mas os atacantes ágeis, por natureza, geralmente têm a vantagem sobre os defensores vinculados a processos. Os invasores não têm nada a manter: nenhum ônus de continuidade de negócios, nenhuma gestão de mudanças, nenhuma obrigação regulatória e nenhum conselho de administração a quem prestar contas. Os defensores estão vinculados por camadas de política, processo e ética – com razão, porque têm uma organização para proteger –, mas cada camada acrescenta atrito, e o atrito é precisamente o que os invasores capacitados por IA exploram. A evidência de aceleração está em toda parte

- **Aumento do volume e realismo:** O volume geral de ataques está aumentando, com a fraude potencializada por IA se destacando como área de crescimento. Os deepfakes passaram da novidade para a ameaça da sala de reuniões – em um caso de alto perfil, a empresa de engenharia Arup perdeu cerca de US$ 25 milhões depois que um funcionário foi enganado por uma videochamada deepfake representando executivos seniores.
- **Malware que se reescreve:** O malware metamórfico – código malicioso que se reescreve para evitar a detecção – está tornando obsoletos os controles tradicionais baseados em assinaturas, forçando os defensores a adotar indicadores comportamentais de comprometimento, em vez de impressões digitais conhecidas.
- **Cadeias de ataque totalmente automatizadas:** Com a IA agêntica agora capaz de automatizar sequências de ataque inteiras, nenhuma equipe humana pode igualar o ritmo,por mais fortes que sejam suas defesas. As organizações precisam corrigir proativamente, monitorar continuamente e se concentrar primeiro nos sistemas e dados que causariam mais danos se comprometidos.

Se os atacantes estão usando IA, os defensores também devem – e a boa notícia é que funciona.

> “Com a IA agêntica agora capaz de automatizar sequências de ataque inteiras, o resultado é claro: nenhuma equipe humana pode igualar o ritmo, por mais fortes que sejam suas defesas. Portanto, embora os defensores não consigam adotar a mesma abordagem totalmente desenfreada para o uso da IA, alavancar a tecnologia para ampliar suas capacidades humanas é essencial para avançar”



Ali-Sultan Kirgizbaev
Sócio, Líder do Centro de Excelência em Dados e IA, Forvis Mazars

Estado global da segurança cibernética

De acordo com o relatório "Cost of a Data Breach" da IBM de 2026, as organizações que usam detecção e resposta assistida por IA viram o custo médio de uma violação cair em quase 40%, com cerca de US$ 1,93 milhão economizados por incidente, e as mesmas técnicas que os invasores usam podem ser usadas para testar as próprias defesas de uma organização.

A ambição, cada vez mais, é agêntica: IA que não apenas detecta uma ameaça, mas a isola e a aborda, com supervisão humana para decisões críticas. A IA agêntica pode ajudar a resolver um paradoxo fundamental dessa corrida armamentista: implantar a IA com segurança requer proteções claras, mas a segurança cibernética existe precisamente porque os invasores exploram o desconhecido; os defensores não podem pré-estabelecer proteções para cada resposta que um agente defensivo possa enfrentar. Os atacantes, por outro lado, não enfrentam essa restrição. A IA agêntica, adequadamente aproveitada, pode responder a ataques de forma semi-autônoma, sem a necessidade de uma bola de cristal.

Dito isso, os ganhos de eficiência são reais, mas também o risco; o agente de um invasor não precisa de estrutura de permissões, enquanto o de um defensor deve trabalhar dentro de barreiras justificáveis.

> "Remover completamente a intervenção humana é uma grande preocupação. Um agente deve realizar uma validação completa em qualquer entrada e estabelecer grades de proteção contra uso indevido em todo o sistema"



Sean Andrews
Gerente de Risco de TI e Conformidade, Forvis Mazars US

A IA também expande o campo de batalha: cada ferramenta de IA cria outra superfície de ataque, com injeção de prompt agora mainstream – como o DPD descobriu quando os clientes manipularam seu chatbot para xingá-los, e o McDonald's quando um chatbot de recrutamento expôs os dados de milhões de candidatos. É por isso que a governança de IA e a privacidade de dados, há muito tratadas como disciplinas separadas e tangenciais, agora precisam urgentemente de consolidação em uma política unificada, biblioteca de controles e estratégia de supervisão de fornecedores.



Estado global da segurança cibernética

Desafios da IA e estratégias práticas de implementação

Os principais desafios da IA agêntica estão em confirmar a validação adequada dos insumos e preservar uma supervisão humana significativa, sem deixar que ela se torne um freio em todas as ações.

Tal como acontece com toda a segurança cibernética, a governança da IA deve permanecer baseada no risco e proporcional; nunca foi possível defender completamente, e os ataques automatizados só tornam isso mais claro. A segurança desde a concepção, o padrão-ouro da mitigação de riscos, envolve compromissos com a usabilidade e o tempo de lançamento no mercado, e exigir a perfeição é autodestrutivo.

"Exija perfeição e você não terá segurança perfeita. Você recebe uma função de segurança que se torna um obstáculo para fazer negócios, soluções alternativas que criam risco oculto e defensores tão sobrecarregados pela conformidade que não podem fazer seu trabalho real."



Anton Yunussov
Líder de Prática de Segurança Cibernética, Forvis Mazars no Reino Unido

O objetivo não é eliminar o risco, mas identificar as "joias da coroa" e protegê-las proporcionalmente. As equipes cibernéticas devem atuar como parceiras de negócios, permitindo que a organização adote a IA com segurança e ritmo. Na prática, isso significa:

- **Governar proporcionalmente:** aplicar a mesma metodologia de avaliação de risco usada para outras tecnologias, combinando controles com o risco que cada caso de uso de IA acarreta. Nem todas as implantações merecem o mesmo escrutínio, e tratá-las como se o fizessem torna o fracasso mais provável.
- **Manter a supervisão humana:** defina o que um agente pode fazer por conta própria – identificar, isolar e até mesmo desligar certos sistemas – e onde uma decisão deve ser encaminhada para uma pessoa, com validação de entrada robusta.
- **Consolidar governança e privacidade:** gerenciar a governança de IA e a privacidade de dados em conjunto – política compartilhada, biblioteca de controles e estratégias de supervisão de fornecedores – em vez de disciplinas separadas com métricas separadas.
- **Investir na equipe:** capacitar as equipes cibernéticas para acompanhar as novas técnicas de ataque e ferramentas defensivas é crucial; a lacuna de capacidade diz respeito tanto às pessoas quanto à tecnologia.



Computação quântica: preparando-se para a mudança de paradigma

Embora a computação quântica possa não representar uma ameaça imediata para a maioria das organizações, o impacto potencial é tão significativo que a preparação deve começar em breve.

Entendendo a ameaça quântica

A ameaça quântica opera em uma linha do tempo diferente dos riscos tradicionais de segurança cibernética. Embora os computadores quânticos capazes de quebrar os padrões atuais de criptografia possam estar a anos de distância da disponibilidade generalizada, os adversários já estão empregando táticas de "roubar agora, descriptografar depois".

> "Os cibercriminosos estão se preparando para a computação quântica agora, então as organizações também deveriam estar. Eles não precisam de um computador quântico para agir. Eles só precisam dos seus dados criptografados e podem roubá-los hoje e descriptografá-los quando o hardware os alcançar. A questão não é quando a computação quântica quebrará sua criptografia, mas por quanto tempo seus dados precisam permanecer confidenciais."



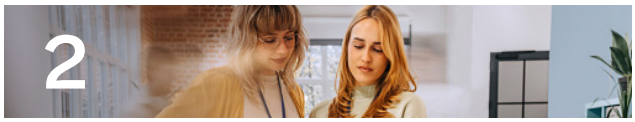
Anton Yunussov
Líder de Prática de Segurança Cibernética, Forvis Mazars no Reino Unido

Essa realidade significa que as organizações devem começar a se preparar para a transição para a criptografia resistente à computação quântica, começando com inventários criptográficos, priorização de riscos e roteiros de fornecedores, antes que a ameaça se torne aguda. O Instituto Nacional de Padrões e Tecnologia (NIST), tendo finalizado seus padrões pós-quânticos em agosto de 2024, começou a lançar ferramentas de criptografia quântica seguras e fornecer às organizações orientações úteis para essa transição.

As organizações podem e devem buscar a preparação quântica agora com o planejamento de descoberta criptográfica e planejamento de migração, começando com as seguintes etapas:



Inventário criptográfico: mapear todos os sistemas e dados que dependem de proteção criptográfica para entender possíveis vulnerabilidades.



Priorização de ativos: identificar quais dados e sistemas seriam mais severamente afetados por uma perda de proteção criptográfica.



Planejamento de transição: desenvolver estratégias de migração para mudar para algoritmos quânticos seguros à medida que estiverem disponíveis.



Avaliação da cadeia de suprimentos: garantir que fornecedores e parceiros também estejam se preparando para a transição quântica.

Estado global da segurança cibernética

Estratégia, transformação e governança de dados

O princípio "lixo entra, lixo sai" precisa ser abordado com mais urgência do que nunca, pois as decisões baseadas em IA dependem de dados de alta qualidade que, consequentemente, tornam a governança central para a segurança cibernética. A má governança de dados cria riscos em cascata que vão muito além das preocupações tradicionais com a proteção de dados. Durante os incidentes, as organizações geralmente descobrem dados anteriormente desconhecidos armazenados em locais não monitorados com controles de acesso pouco claros.

Essa falta de visibilidade não só cria superfícies de ataque desconhecidas – dados que não estão devidamente catalogados não podem ser adequadamente protegidos – mas também pode criar risco de conformidade.

Gestão de riscos de terceiros e compartilhamento de dados

À medida que o compartilhamento de dados se torna mais complexo, o TPRM se tornou essencial para gerenciar o risco cibernético. As cadeias de suprimentos multicamadas muitas vezes obscurecem a forma como os dados são processados e protegidos, aumentando a exposição. O TPRM eficaz requer vários componentes-chave:

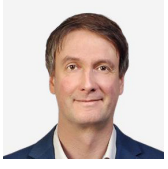
- **Acordos de nível de serviço (SLAs) com controles de segurança:** os contratos devem definir explicitamente os requisitos de segurança e conformidade, com o direito de auditar incluído sempre que possível, em vez de depender de relatórios próprios.
- **Avaliação e monitoramento regulares:** Os programas de TPRM podem ser mais eficazes quando incluem monitoramento contínuo e reavaliação regular dos riscos do fornecedor, e o direito de auditar só tem valor quando é exercido.
- **Gerenciamento de fornecedores em camadas:** nem todos os fornecedores representam o mesmo risco. As organizações devem implementar abordagens em camadas que concentrem a supervisão intensiva nos relacionamentos mais críticos.

Implementação prática de segurança e governança de dados

As organizações que procuram melhorar sua governança de dados devem considerar começar com exercícios práticos, em vez de desenvolver políticas abstratas. Os exercícios de continuidade de negócios podem começar em torno de uma mesa com líderes, técnicos e não técnicos, abrindo com uma pergunta simples como: "o que acontece se seu telefone e computador não funcionarem?" Essa discussão mais casual pode evoluir naturalmente para diálogos mais sofisticados sobre dependências de dados e requisitos de proteção.

Essa abordagem conversacional também se estende às políticas oficiais. As equipes cibernéticas devem considerar se as políticas são simples o suficiente para os usuários não técnicos entenderem e implementarem. A educação e a parceria podem ajudar a capacitar a força de trabalho a defender essas políticas e capacitar as equipes de governança com o conhecimento de negócios de que precisam para projetar medidas eficazes.

"As equipes de segurança devem trabalhar em estreita colaboração com as unidades de negócios para entender suas necessidades de dados, desenvolver soluções adequadas e explicar as políticas. Quando as pessoas entendem o "porquê" e confiam que as equipes cibernéticas também entendem o que estão tentando alcançar, é mais provável que cumpram as medidas de segurança."



Christopher Hock
Diretor,
Forvis Mazars na Alemanha

Esse equilíbrio entre segurança de dados e capacitação de negócios é um desafio central de governança. Políticas excessivamente rígidas geralmente levam a soluções alternativas arriscadas, alimentando a ascensão da TI paralela. Uma abordagem eficaz para capacitação da força de trabalho combina controles técnicos com iniciativas culturais. A estreita parceria com as unidades de negócios pode criar entendimento mútuo e os controles compensatórios, como o monitoramento, podem manter as equipes cibernéticas informadas sobre o comportamento do usuário.

Equipes cibernéticas e experiência

A força de trabalho de segurança cibernética enfrenta desafios sem precedentes à medida que o campo evolui rapidamente e a lacuna de habilidades continua a aumentar. As organizações precisam de profissionais que entendam os princípios tradicionais de segurança e as tecnologias emergentes, mas esse conhecimento é cada vez mais raro.

O papel do Diretor de Segurança da Informação (CISO), em particular, evoluiu significativamente nos últimos anos. Espera-se cada vez mais que os CISOs funcionem como líderes de negócios em vez de especialistas técnicos, com responsabilidades que se estendem à conformidade regulatória, relatórios do conselho e planejamento estratégico. Essa evolução reflete a transição da segurança cibernética de uma função técnica para um facilitador de negócios.

A remuneração para as funções de CISO aumentou de acordo, refletindo tanto as responsabilidades expandidas quanto a importância da função. No entanto, essa tendência também destaca o desafio de desenvolver um pipeline de candidatos qualificados que possuam o conhecimento técnico e a visão de negócios necessários para a liderança moderna em segurança cibernética. Muitas organizações estão recorrendo aos CISOs virtuais como uma solução para ajudar a preencher as lacunas dentro de seu grupo de talentos existente e fornecer um contexto mais amplo de experiência.

O desafio da inovação

Um dos desafios mais significativos da força de trabalho está em encontrar profissionais que possam inovar e gerenciar, especialmente em organizações de médio porte. O ritmo acelerado das mudanças tecnológicas significa que os profissionais de segurança cibernética devem aprender continuamente novas tecnologias, mantendo a experiência em princípios fundamentais de segurança.

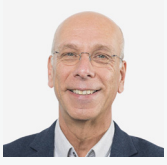
Esse desafio é particularmente agudo em áreas como IA e computação quântica, onde a interseção de tecnologia de ponta e segurança cria complexidades que poucos profissionais entendem completamente. As organizações estão cada vez mais recorrendo a consultores e conselheiros de confiança para preencher essa lacuna de conhecimento, ajudando a orientar a estratégia e a implementação juntamente com as equipes internas.

Construindo equipes cibernéticas sustentáveis

A abordagem tradicional de contratar especialistas individuais em segurança cibernética está se tornando cada vez mais insustentável para muitas organizações. A competição pelos melhores talentos está levando a remuneração a níveis que muitos não conseguem sustentar, enquanto o ritmo acelerado das mudanças dificulta que as equipes internas se mantenham atualizadas com ameaças e tecnologias emergentes.

A automação e a IA estão, é claro, permitindo que as equipes cibernéticas dimensionem suas operações, mas os modelos de serviços compartilhados são cada vez mais comuns, particularmente em cenários que envolvem fusões e aquisições, onde empresas controladoras ou empresas de investimento fornecem recursos cibernéticos e suporte para empresas de portfólio/filhos. As parcerias externas também são cada vez mais valiosas, trazendo abordagens de implementação comprovadas e ajudando as organizações a preencher as lacunas de conhecimento de forma econômica.

> “Os CISOs devem agora ser capazes de quantificar o valor comercial da segurança cibernética, comunicar-se efetivamente com executivos não técnicos e alinhar a estratégia de segurança com os objetivos de negócios. Isso exige muitas habilidades técnicas e interpessoais – para não mencionar a experiência – que muitas organizações não podem pagar até muito depois de precisarem.”



Jan Matto
Consultor Sênior de Confiança Digital, Ex-Sócio, Forvis Mazars nos Países Baixos

Quantificando o valor da segurança cibernética

As organizações estão indo além de meras métricas técnicas para avaliar a eficácia da segurança cibernética por meio do impacto nos negócios, analisando conquistas como interrupções evitadas e receita possibilitada por uma segurança forte. Essa mudança é fundamental para garantir o financiamento e demonstrar o retorno sobre o investimento (ROI).

A preocupação de custo: segurança cibernética como investimento, não despesa

A proliferação de ameaças e a complexidade dos ambientes tecnológicos modernos podem fazer com que a segurança cibernética pareça um centro de custos em constante expansão. No entanto, as principais organizações estão reformulando os gastos com segurança cibernética como um investimento estratégico.

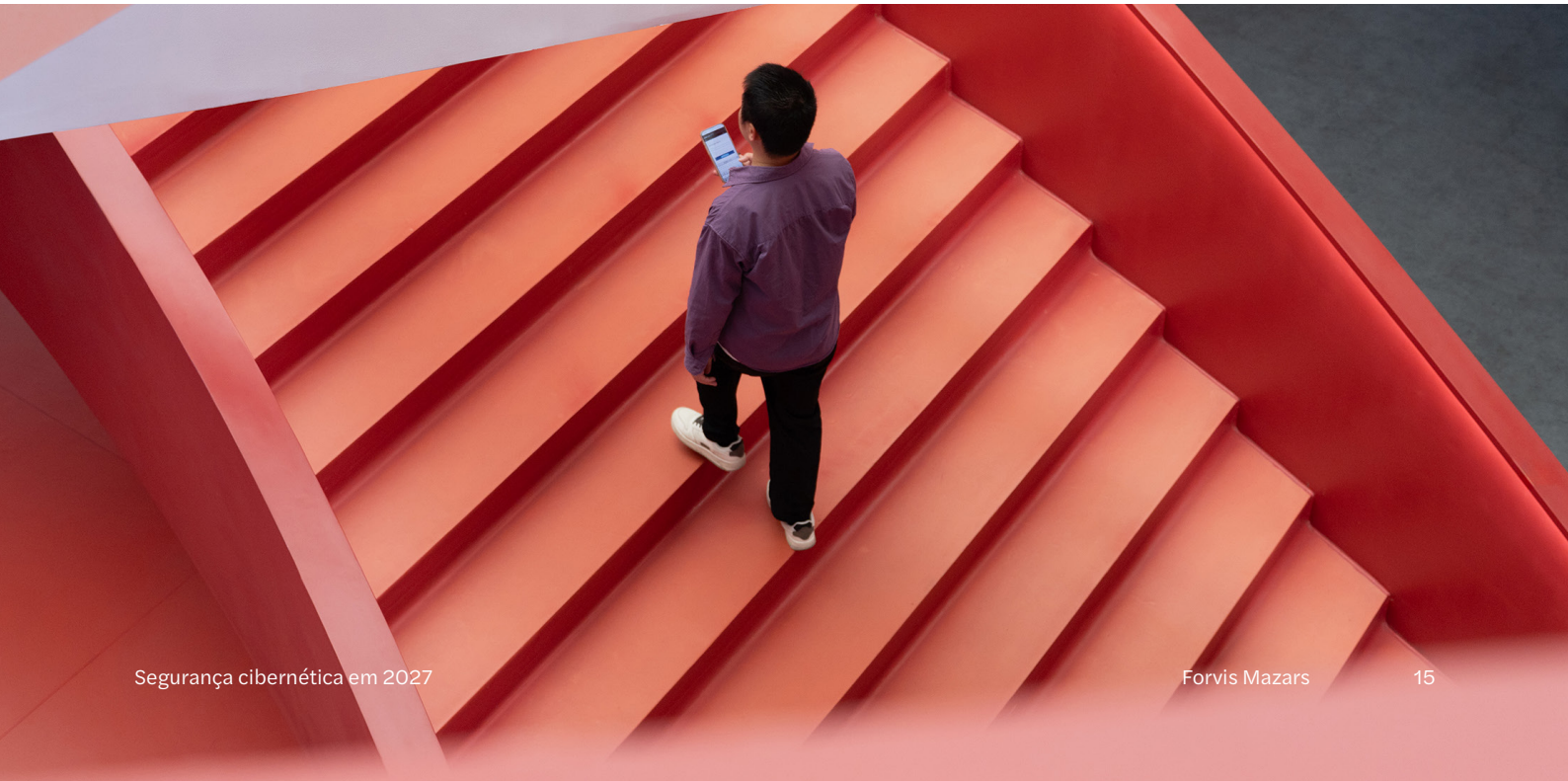
Muitas organizações estão percebendo a vantagem competitiva de práticas cibernéticas sólidas. As fortes posturas de segurança cibernética são um diferencial cada vez mais valioso no mercado, particularmente nos setores B2B, onde os clientes avaliam a segurança do fornecedor como parte de sua própria gestão de riscos. Há um elemento de conformidade para esse foco maior – os clientes precisam pensar em suas cadeias de suprimentos para fins de sua própria conformidade – mas os clientes também citam frequentemente incidentes de alto perfil ao ao apresentar requisitos cibernéticos, mostrando uma maior conscientização do mercado sobre o impacto potencial de uma interrupção. Equipes cibernéticas que podem quantificar e comunicar o valor dessa vantagem podem desbloquear níveis sem precedentes de adesão.

> "A era da segurança cibernética como um custo necessário está terminando, e a era da segurança cibernética como um diferencial estratégico começou."

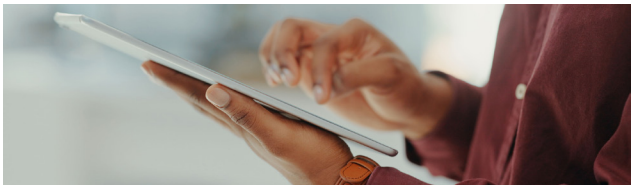


Jeffrey de Bruijn
Diretor,
Forvis Mazars nos Países Baixos

Claro, a segurança cibernética é importante para mais do que apenas clientes. As seguradoras cibernéticas estão naturalmente mais preocupadas do que nunca com as medidas que estão em vigor, e as instituições financeiras estão cada vez mais considerando a prontidão para a segurança cibernética em suas avaliações de risco. Tanto o seguro quanto o financiamento oferecem incentivos quantificáveis para programas de segurança fortes.



Quantificando o valor da segurança cibernética





Medir o que importa

As organizações líderes estão indo além das métricas tradicionais de segurança para se concentrar em medir o sucesso de maneiras que se relacionam diretamente com os resultados de negócios e o valor para as partes interessadas. Isso inclui:

- **Objetivos de tempo de recuperação:** com que rapidez as operações normais podem ser restauradas após um incidente?
- **Métricas de impacto nos negócios:** qual é o custo real dos incidentes de segurança em termos de receita, relacionamento com o cliente e posição competitiva?
- **Medidas de confiança dos stakeholders**: como as capacidades de segurança afetam a confiança do cliente, investidor e parceiro?
- **Capacitação de inovação:** com que eficácia o programa de segurança apoia a inovação empresarial?

Otimizar o ROI dos gastos com segurança cibernética

As organizações que investem em medidas proativas de segurança cibernética demonstram consistentemente melhores resultados do que aquelas que adotam abordagens reativas. No entanto, com recursos limitados mesmo nas maiores organizações, os seguintes focos de investimento podem ajudar a otimizar o ROI e reduzir o risco:

- **Priorização baseada em risco:** concentre os recursos humanos e o capital na proteção dos ativos mais críticos, em vez de tentar proteger tudo de forma igual.
- **Segurança desde a Concepção:** crie requisitos de segurança em sistemas e processos desde o início, em vez de tentar adicioná-los mais tarde.
- **Abordagens integradass:** procure soluções de segurança que atendam a vários requisitos simultaneamente, reduzindo a necessidade de soluções pontuais.
- **Automação e eficiência:** invista em ferramentas e processos que amplifiquem as capacidades humanas em vez de simplesmente adicionar mais pessoal, especialmente no que diz respeito ao monitoramento contínuo de visibilidade contínua.
- **Educação dos funcionários:** implementar programas regulares de treinamento e conscientização que reduzam a probabilidade de incidentes relacionados a erros humanos e a vulnerabilidade da engenharia social.
- **Preparação de resposta a incidentes:** desenvolva e teste regularmente as capacidades de resposta a incidentes na íntegra antes que elas sejam necessárias.
- **Serviços compartilhados:** cconsidere serviços de segurança cibernética compartilhados ou virtuais, quando apropriado, especialmente para conhecimentos especializados que não exigem recursos internos em tempo integral.

Como as empresas podem melhorar sua resiliência cibernética em 2027?

Olhando para 2027 e além, a resiliência cibernética significará mais do que prevenir ataques. As organizações precisarão mostrar que podem antecipar interrupções, manter operações críticas em execução e se adaptar à medida que as ameaças mudam.

Por um lado, a Segurança desde a Concepção continuará a fazer a transição de uma prática recomendada para uma necessidade comercial. De forma mais consistente, espera-se que as organizações demonstrem aos clientes, órgãos reguladores e seguradoras que as considerações de segurança são parte integrante do design do sistema e dos processos de negócios.

Essa abordagem será particularmente crítica quando a IA estiver envolvida, e as implicações de segurança das decisões de design podem não se tornar aparentes até que os sistemas já estejam em produção. As organizações que não implementam os princípios de Segurança desde a Concepção podem encontrar-se em desvantagens significativas na eficácia da segurança, na recepção do mercado e na conformidade regulamentar.

O ritmo da mudança tecnológica também exigirá estruturas de governança que possam se adaptar rapidamente a novos desafios, mantendo princípios fundamentais consistentes. Organizações resilientes desenvolverão estruturas de governança que possam funcionar perfeitamente através das fronteiras organizacionais e sistemas técnicos, aprender continuamente e antecipar ameaças e oportunidades emergentes.

À medida que o cenário tecnológico é moldado por mudanças sísmicas imparáveis, as organizações resilientes estão construindo capacidades que podem resistir às mudanças, independentemente de quaisquer modelos, plataformas ou ferramentas de tecnologia específicas. Isso significa adotar uma abordagem contínua baseada em riscos para a avaliação de ameaças, criando arquiteturas independentes de ferramentas e fornecedores sempre que possível e com foco no desenvolvimento da força de trabalho baseada em habilidades.

Gestão de riscos em todo o ecossistema

A resiliência em 2027 exigirá que as empresas pensem além de seus próprios limites para considerar a segurança de todo o ecossistema de negócios. Isso inclui não apenas os parceiros tradicionais da cadeia de suprimentos, mas também fornecedores de tecnologia, prestadores de serviços e até mesmo concorrentes em acordos de infraestrutura compartilhada.

Os principais componentes da gestão de riscos em todo o ecossistema incluem:

- **Inteligência compartilhada de ameaças:** colaborar com parceiros para identificar e responder a ameaças que afetam várias organizações ou entidades.
- **Resposta coordenada a incidentes:** desenvolver capacidades de resposta que possam funcionar além das fronteiras organizacionais.
- **Avaliação de risco padronizada:** usando estruturas, métricas e taxonomia comuns para avaliar e comunicar o risco em todo o ecossistema.
- **Capacidades de defesa coletiva:** participar de iniciativas em toda a indústria para desenvolver capacidades defensivas compartilhadas.

> “As organizações mais resilientes se concentram em estratégias de governança que lhes permitem escalar rapidamente. Elas precisam ser capazes de acomodar novas tecnologias e modelos de negócios sem exigir revisões completas da estrutura.”



Paul Truitt
Diretor, Líder de Práticas de Segurança Cibernética, Forvis Mazars US

Inovação baseada em segurança

À medida que olhamos para 2027 e além, as organizações que terão sucesso são aquelas que começam a se preparar hoje, construindo as capacidades, parcerias e estruturas de governança para navegar em um cenário de ameaças cada vez mais complexo e em rápida evolução, enquanto capitalizam as enormes oportunidades que as tecnologias emergentes apresentam.

"O futuro da segurança cibernética não é sobre escolher entre segurança e inovação, é sobre alcançar as duas simultaneamente. Isso significa planejamento cuidadoso, investimento estratégico e abordagens colaborativas que reconhecem a segurança cibernética como uma responsabilidade compartilhada."



Jan Matto
Consultor Sênior de Confiança Digital, Ex-Sócio, Forvis Mazars nos Países Baixos

O caminho a seguir requer vários compromissos importantes:

Abrace a mudança mantendo os princípios: a tecnologia continuará a evoluir, mas os princípios fundamentais de segurança devem permanecer constantes. As organizações devem se esforçar para ser ágeis o suficiente para se adaptar às novas tecnologias e, ao mesmo tempo, permanecer consistentes o suficiente para manter fortes posturas de segurança.

Investir em pessoas e parcerias: os desafios de segurança cibernética de 2027 e além ampliarão as capacidades internas de muitas organizações, tornando as parcerias estratégicas e o desenvolvimento contínuo da força de trabalho cada vez mais importantes.

Medir o impacto nos negócios: os programas de segurança devem demonstrar seu valor em termos de negócios, não apenas em métricas técnicas. Isso requer que os profissionais de segurança cibernética desenvolvam visão de negócios juntamente com conhecimentos técnicos.

Pense em todo o ecossistema: as organizações individuais não podem alcançar a verdadeira resiliência isoladamente. A segurança cibernética precisa ser abordada como um desafio compartilhado que requer respostas coordenadas.

Contatos

George Lagarias
Economista-Chefe,
Forvis Mazars
george.lagarias@mazars.co.uk

Wadi Mseddi
Líder do Grupo de Consultoria em Segurança Cibernética, Forvis Mazars
wadi.mseddi@forvismazars.com

Ali-Sultan Kirgizbaev
Sócio, Líder do Centro de Excelência em Dados e IA, Forvis Mazars
ali-sultan.kirgizbaev@forvismazars.com

Anton Yunussov
Líder de Prática de Segurança Cibernética, Forvis Mazars no Reino Unido
anton.yunussov@mazars.co.uk

Christopher Hock
Diretor,
Forvis Mazars na Alemanha
christopher.hock@forvismazars.com

Jakob Haesler
LíderGlobal de Consultoria,
Forvis Mazars
jakob.haesler@forvismazars.com

Jan Matto
Consultor Sênior de Confiança Digital, Ex-Sócio,
Forvis Mazars nos Países Baixos
jan.matto@forvismazars.com

Jeffrey de Bruijn
Diretor,
Forvis Mazars na Holandas
jeffrey.debruijn@forvismazars.com

Paul Truitt
Diretor, Líder de Práticas de Segurança Cibernética,
Forvis Mazars US
paul.truitt@us.forvismazars.com

Sean Andrews
Gerente de Risco de TI e Conformidade,
Forvis Mazars US
sean.andrews@us.forvismazars.com

Tom Tollerton
Diretor, CMMC Practice Lead,
Forvis Mazars US
tom.tollerton@us.forvismazars.com

A Forvis Mazars Group SC é um membro independente da Forvis Mazars Global Limited, uma rede líder em serviços profissionais. Atuando como uma parceria internacionalmente integrada em mais de 100 países e territórios, o Forvis Mazars Group é especializado em serviços de auditoria, consultoria tributária e consultoria empresarial. A parceria conta com a expertise e a compreensão cultural de mais de 40.000 profissionais em todo o mundo para auxiliar clientes de todos os portes em todas as etapas de seu desenvolvimento.

© Outubro 2026

forvismazars.com/br