

Resiliência cibernética empresarial

Um guia para acelerar a recuperação
diante dos piores cenários





Conteúdos

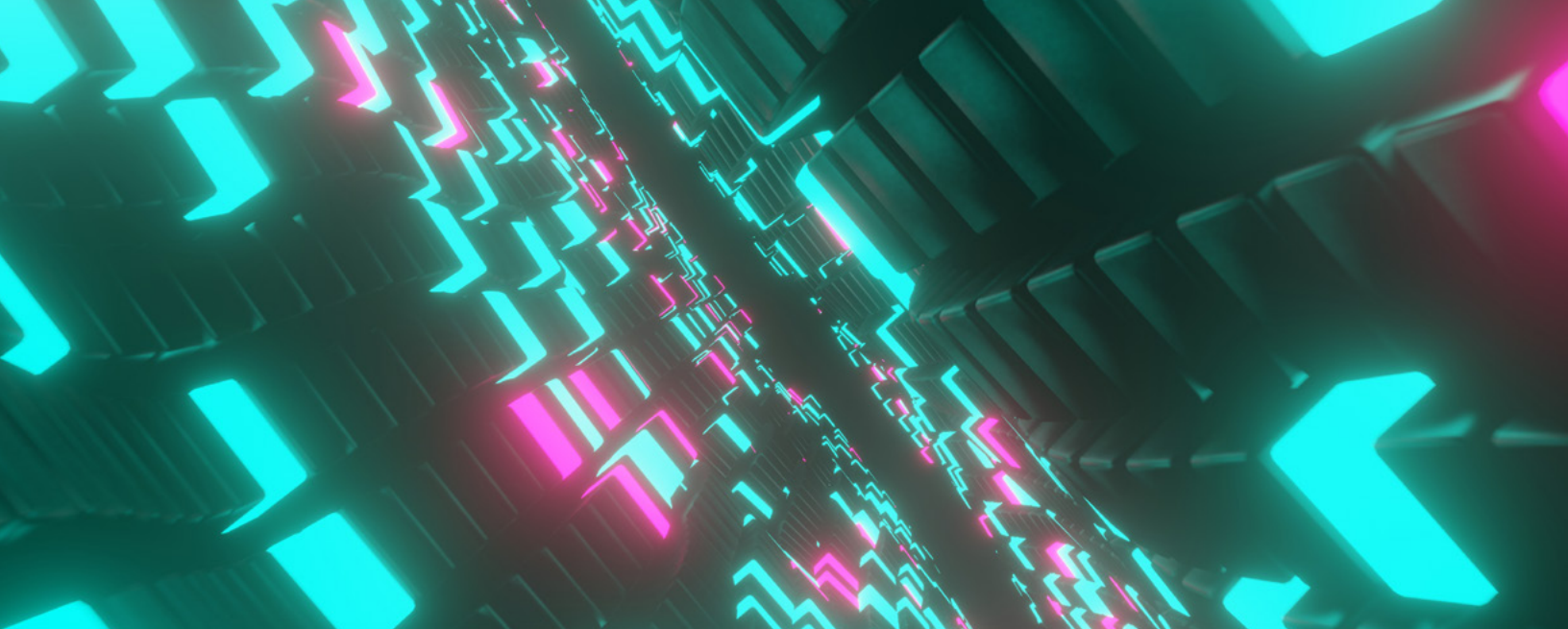
O valor da resiliência cibernética empresarial	3
Etapas para uma maior resiliência	4
01 Avalie seu ambiente cibernético	4
02 Desenvolva uma estratégia de resiliência	5
03 Estabeleça fundamentos de segurança cibernética	6
Benefícios da resiliência cibernética empresarial	7
Como a Unisys pode ajudar	8



O valor da resiliência cibernética empresarial

No metrô de Londres, os sinais com a frase “Cuidado com o vão” recomendam aos passageiros serem cuidadosos ao se moverem de uma plataforma e a porta do trem ou vice-versa. Essa frase pode ser igualmente útil ao considerar lacunas de segurança cibernética e potenciais vulnerabilidades em suas estratégias de resiliência cibernética. A longevidade da empresa pode ser medida pela capacidade da sua organização de resistir a tempestades não planejadas. A resiliência cibernética é crucial para se adaptar e responder de forma eficaz a interrupções, riscos e eventos inesperados que possam afetar as operações.

A resiliência permite manter a continuidade, minimizar o tempo de inatividade, se recuperar rapidamente de ataques cibernéticos e desastres e manter processos de negócios críticos funcionando sem problemas. Investir em medidas de resiliência pode ajudá-lo a salvaguardar sua reputação, construir confiança com funcionários, clientes e parceiros e demonstrar seu compromisso com a sustentabilidade e o crescimento a longo prazo. Seguir estes três passos pode colocar você no caminho rumo à resiliência.



Etapas para uma maior resiliência

01 Avalie seu ambiente cibernético

O caminho para a resiliência cibernética começa com a avaliação do seu ambiente de operações. Uma avaliação oferece uma compreensão completa dos riscos de segurança e informações para desenvolver uma estratégia abrangente, fortalecendo sua organização contra ameaças cibernéticas.

- Mapeie seus ativos críticos, sistemas, dependências e todos os outros componentes de seu ambiente cibernético.
- Identifique ameaças à segurança, riscos-chave e potenciais vulnerabilidades de segurança em sua infraestrutura digital.
- Avalie a eficácia das medidas de segurança da sua organização, identificando lacunas ou fraquezas nas suas defesas, incluindo aquelas que já resultaram em um comprometimento não detectado ou que foram potencialmente exploradas.
- Use essa inteligência para priorizar áreas de melhoria para abordar mais tarde como parte de seu plano estratégico.
- Integre avaliações contínuas à sua estratégia de segurança cibernética para identificar falhas antes que se tornem problemas.



Descoberta da superfície de ataque

A descoberta da superfície de ataque envolve explorar todos os caminhos que um invasor poderia usar para se infiltrar em seus sistemas e rede. Isso inclui identificar riscos de segurança e casos de *shadow IT*, quando colaboradores adotam tecnologias sem antes obter a aprovação da TI. Identificar o *shadow IT* pode reduzir a exposição da sua organização a novos riscos de segurança, além de reduzir desperdícios.

02 Desenvolva uma estratégia de resiliência

Use os conhecimentos obtidos na avaliação para construir uma base para a resiliência. Uma estratégia eficaz envolve políticas, controles e procedimentos robustos em linha com a tolerância ao risco e os objetivos de negócios da sua organização. A solidificação de sua estratégia facilita a implementação de medidas de mitigação de riscos, fortalece sua postura de resiliência, prepara sua empresa para um cenário de segurança de pior caso e estabiliza as operações do negócio caso esse cenário se concretize.



Ingredientes para o sucesso da estratégia

Ao desenvolver um plano abrangente de resiliência cibernética para proteger sua organização contra ameaças cibernéticas, priorize a incorporação de vários componentes vitais.

- **Preparação e prevenção** que reconhece que a resiliência começa muito antes de um ataque ocorrer
- **Monitoramento e resposta a incidentes** que fornecem visibilidade sobre possíveis ataques e minimizam o impacto nas operações
- **Backup e recuperação** que restauram os dados e a funcionalidade do sistema após um incidente
- **Continuidade de negócios** após um ataque cibernético ou interrupção
- **Treinamento dos colaboradores** para educá-los sobre as melhores práticas de segurança cibernética e incentivar uma cultura consciente de segurança
- **Conformidade regulatória** para alinhar sua estratégia de resiliência cibernética com os requisitos legais e regulatórios relevantes
- **Melhoria contínua** das capacidades de resiliência através do monitoramento contínuo

03 Estabeleça fundamentos de segurança cibernética

Depois de traçar sua estratégia, é hora de transformar suas medidas de segurança existentes reavaliando os protocolos, tecnologias e práticas de segurança atuais para lidar com ameaças e vulnerabilidades emergentes. Isso permite que você proteja melhor seus ativos, dados e operações contra interrupções e riscos cibernéticos. Outro imperativo da segurança cibernética é fortalecer a preparação e as capacidades de resposta da sua organização com protocolos de resposta a incidentes, planos de continuidade de negócios e estratégias de recuperação de desastres.



Soluções centrais para resiliência

- **Deteção e resposta gerenciadas:**

identifique incidentes de segurança cibernética prontamente e minimize seus impactos nas operações e na postura de segurança. O monitoramento contínuo e as capacidades de resposta imediata ajudam a proteger sua organização contra ameaças e ataques cibernéticos de forma proativa.

- **Descoberta da superfície de ataque:**

obtenha visibilidade contínua dos ativos expostos, permitindo a mitigação proativa de riscos, resposta mais rápida a incidentes e defesas ágeis à medida que o ambiente e as ameaças evoluem.

- **Resiliência cibernética, integração e inovação contínua:**

integre práticas de segurança cibernética perfeitamente às operações, ao gerenciamento de riscos e às estratégias de negócios da sua organização. As ameaças cibernéticas são dinâmicas, por isso é crucial avançar nas medidas de segurança cibernética para permanecer à frente em um panorama de ameaças em constante evolução.

- **Recuperação cibernética:**

mantenha a continuidade dos negócios e reduza o tempo em que sua organização fica sem acesso a ativos críticos, como dados e sistemas de comunicação, após um ataque cibernético. Os princípios e práticas de recuperação de desastres (disaster recovery), como protocolos de backup, servem como base para esforços de recuperação cibernética, exigindo ainda medidas adicionais de resiliência e proteção, como o isolamento dos sistemas afetados.

- **Disaster Recovery:**

recupere-se rapidamente de desastres nacionais, como inundações e terremotos, assim como de eventos tecnológicos, como falhas de servidores, para minimizar o tempo de inatividade e manter os sistemas operacionais. Planos robustos de recuperação de desastres mantêm seu negócio funcionando sem problemas após eventos inesperados.

- **Resposta a incidentes de segurança cibernética:**

contenha ataques cibernéticos para evitar que se espalhem e causem danos adicionais aos sistemas e dados da sua organização. A resposta a incidentes protege seus dados e restaura os sistemas afetados para produção.

Benefícios da resiliência cibernética empresarial

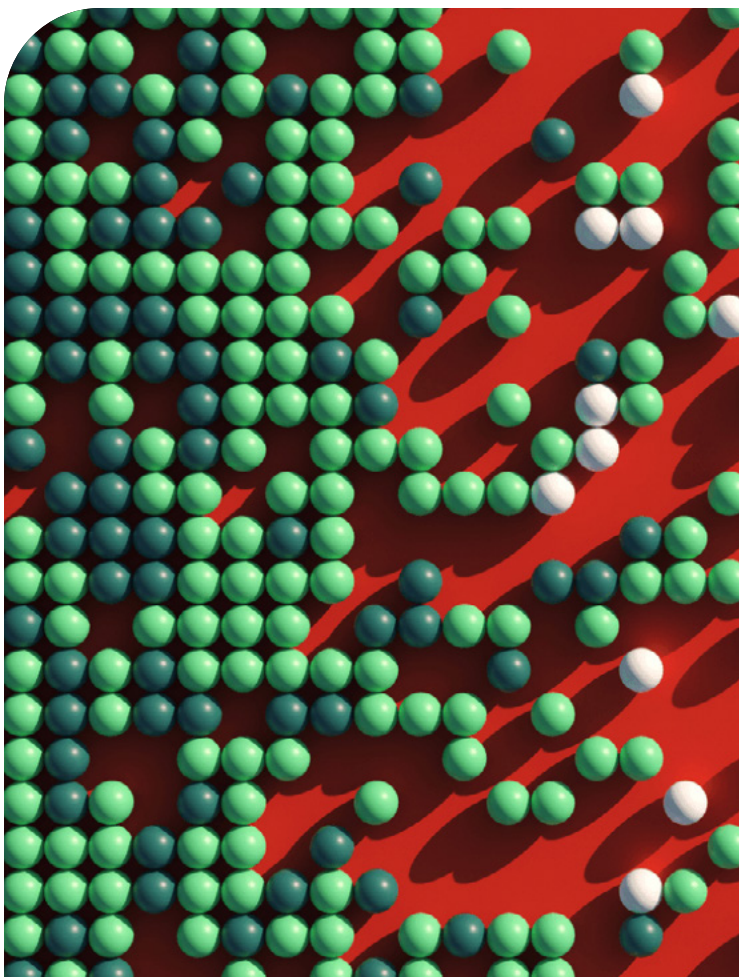
Adotar uma abordagem resiliente — especialmente quando você prioriza a prevenção de riscos — oferece várias vantagens que reforçam a segurança cibernética da sua organização. Esses benefícios contribuem para construir uma estrutura robusta de resiliência que facilita a superação de potenciais desafios.

- **Identificação de riscos:** compreenda os riscos da sua organização para adaptar suas estratégias de resiliência e mitigar potenciais vulnerabilidades de forma eficaz.
- **Gerenciamento de riscos:** trate e mitigue riscos de forma estratégica para garantir resiliência e continuidade durante interrupções.
- **Prevenção de riscos:** reduza a probabilidade de ataques bem-sucedidos que possam afetar as operações do negócio.
- **Maior flexibilidade:** ganhe agilidade para evoluir conforme as circunstâncias mudam, adaptando sua abordagem para lidar com riscos emergentes e mitigar ameaças, com impacto mínimo nas operações.
- **Preparo aprimorado:** prepare sua organização para diversos cenários, incluindo ameaças cibernéticas e falhas do sistema, com ferramentas e estratégias para responder eficazmente a interrupções.



Como a Unisys pode ajudar

Os especialistas em segurança cibernética da Unisys podem orientar seus esforços para melhorar a resiliência empresarial em todas as etapas de sua jornada de segurança, desde a avaliação inicial até o gerenciamento contínuo. Nossos serviços abrangentes permitem que você crie e mantenha suas capacidades de resiliência.



Suporte de ponta a ponta:

conte com nossa expertise na identificação de riscos, na definição de ferramentas para mitigá-los, na criação de uma infraestrutura resiliente e gestão eficaz das operações.

Soluções personalizadas:

obtenha soluções adaptadas às necessidades específicas de sua organização, à infraestrutura de TI atual e futura, além dos desafios únicos e requisitos de negócios.

Monitoramento contínuo:

tenha visibilidade sobre potenciais ameaças ou interrupções nas operações do negócio por meio de monitoramento contínuo dos sistemas.

Sua resiliência cibernética poderia ser mais forte?

Visite nosso site unisys.com ou **entre em contato conosco** para agendar uma consulta com nossos especialistas hoje mesmo.



unisys.com

© 2026 Unisys Corporation. Todos os direitos reservados.

A Unisys e outros produtos e serviços da Unisys aqui mencionados, bem como seus respectivos logotipos, são marcas comerciais ou marcas registradas da Unisys Corporation. O material contido neste documento reflete informações disponíveis no momento em que este documento foi elaborado, conforme indicado pela data nas propriedades do documento. Este conteúdo descreve as melhores práticas gerais e é fornecido apenas para fins informativos; não leva em consideração as circunstâncias específicas do leitor e não se destina a substituir a consulta aos nossos consultores profissionais. Para orientações específicas e adequadas à sua situação particular, são necessários um contrato formal e a consulta aos nossos profissionais qualificados. A Unisys isenta-se, na máxima extensão permitida pela legislação aplicável, de toda e qualquer responsabilidade pela precisão e integridade das informações contidas neste documento e por quaisquer atos ou omissões realizados com base nessas informações.