

# Preparando para Proteger o Futuro

---

FIQUE À FRENTE DO JOGO





## A proteção e recuperação de dados não é uma corrida, mas uma jornada ao longo de um caminho muitas vezes sinuoso.

As ameaças aos seus dados estão aumentando e evoluindo, com agentes mal-intencionados desenvolvendo novas formas de atacar e obter acesso à força vital de suas operações.

A proteção de dados evoluiu de um item de linha para um aspecto em evolução da cultura empresarial com várias peças em movimento. A variedade e a localização das cargas de trabalho e a criticidade de cada aplicativo e seus dados são componentes vitais para avaliar os níveis de proteção de que você precisa e como lidar com a recuperação.

Fatores como alta disponibilidade, governança e conformidade desempenham um papel e afetam o objetivo de tempo de recuperação (RTOs) e o objetivo de ponto de recuperação (RPOs).

A Shadow IT e a dívida de tecnologia explodiram. As equipes criam volumes enormes de dados e, por engano, deixam os dados de missão crítica vulneráveis. As organizações carecem de visibilidade total do que é essencial, dificultando a priorização para mitigar os riscos.

Com visão de futuro e diligência, você pode se manter à frente e preparado para possíveis desafios ao longo do caminho.





## Identifique os dados que você possui

### Como você pode proteger adequadamente o que você não sabe que tem?

Um grande número de aplicativos e plataformas prometem melhorar a eficiência e fornecer dados mais eficazes. Seus funcionários começam a usar essas ferramentas em silos, alimentando informações de clientes e dados da empresa em plataformas que provavelmente estão localizadas na nuvem. O resultado? Um dilema de expansão de dados e um problema de cobertura multinuvel.

Maus atores podem se infiltrar nesses dados porque não são devidamente cobertos pela empresa. O comportamento suspeito pode passar despercebido porque a equipe de TI não sabe que deveria estar observando — ou mesmo que existe. Se ocorrer um desastre, você pode descobrir que informações críticas não foram copiadas corretamente e não podem ser recuperadas.

Além disso, há o problema de que, se ocorrer um desastre, as informações são críticas e podem não ter backup adequado e podem não ser recuperáveis.

A expansão de dados é um desafio de governança que requer mais estrutura e treinamento de funcionários, além de maior visibilidade da infraestrutura da empresa.

Para criar resultados mais bem-sucedidos, contextualize os dados e avalie o risco em torno de procedimentos complexos para decidir como executar as estratégias de backup e recuperação de borda, núcleo e nuvem.

### Perguntas-chave:

- Quais dados você possui e onde eles estão?
- Como isso melhora a visibilidade de nossos dados?

## Soluções da Veritas

As soluções de proteção de dados da Veritas oferecem proteção de dados em escala. O mecanismo de detecção de anomalias alimentado por IA ajuda a extrair grandes quantidades de dados, automatizar o monitoramento e a geração de relatórios, identificar insights acionáveis e estabelecer alertas antecipados de possíveis ataques.

As soluções de análise da Veritas ajudam a cruzar servidores e armazenamento com todos os seus fornecedores de backup para garantir que nada seja esquecido e deixado vulnerável. Ele pode escanear e monitorar todos os sistemas, incluindo produtos de terceiros, para ajudar a eliminar pontos cegos.

O Veritas Data Insight pode ajudá-lo a descobrir o potencial de geração de relatórios enquanto permite a detecção de dados potencialmente nocivos, revoga o acesso a dados delicados e colabora com os proprietários de dados para uma melhor tomada de decisão e adesão aos padrões de conformidade. Destaque riscos, descubra dados obscuros e registre a atividade do usuário para várias atividades para descobrir padrões de atividade para identificar e detectar anomalias.



IDENTIFIQUE QUAIS DADOS VOCÊ POSSUI



IMEÇA QUE AS AMEAÇAS OBTENHAM DADOS



DETERMINE QUAIS DADOS SÃO CRÍTICOS E VULNERÁVEIS



TORNE OS DADOS E BACKUPS DISPONÍVEIS E EFICIENTES



CERTIFIQUE-SE DE QUE OS BACKUPS SEJAM IMUTÁVEIS E COM INTERVALO DE AR



DECIDIR UM PROCESSO DE RECUPERAÇÃO DE DESASTRES



PRATIQUE SUA ESTRATÉGIA DE RECUPERAÇÃO DE DESASTRES



OTIMIZE SEU BACKUP E RECUPERAÇÃO



## Afaste os malfeitores

Os cibercriminosos sabem que as pessoas são os pontos mais fracos da sua rede.

A maioria dos ataques cibernéticos e violações de dados são resultado da interação humana e da falta de atenção. É por isso que o phishing é tão eficaz.

Como você evita um ataque? Elementos como gerenciamento de identidade e acesso e criptografia são medidas de proteção vitais. Você pode reduzir as chances de um ataque bem-sucedido implementando autenticação multifator e controle de acesso baseado em função. A criptografia de dados em repouso e em movimento reduz a usabilidade de seus dados e ajuda a proteger contra a exfiltração de dados. Coisas como autenticação de cartão inteligente, logon único e gerenciamento de acesso privilegiado ajudam a reforçar o princípio de "menor privilégio" de Zero Trust.

As estratégias de prevenção e proteção em camadas usam várias soluções implementadas em vários níveis. Você pode (e deve) emitir certificados digitais para dispositivos para posterior autenticação. Use a autorização dupla para acessar os backups como mais uma camada.

Gerenciar o acesso seguro e proteger seus dados contra configuração incorreta é de extrema importância. Identificar e entender os recursos, ações e identidades em seu ambiente é crucial para gerenciar privilégios e impor permissões apropriadas, esteja você no local ou na nuvem. Rastrear e monitorar as tentativas e a progressão das alterações ajudam você a aprimorar sua postura de segurança e a fazer melhorias em tempo real.

### Perguntas-chave

- O que estamos fazendo atualmente para evitar violações de phishing e malware?
- Existem maneiras de melhorar nossas medidas de proteção atuais?

## Soluções da Veritas

As soluções de proteção de dados da Veritas são independentes de fornecedores e construídas com base no Zero Trust. Ele ajuda a proteger sua rede, proteger os dados em trânsito e em repouso com criptografia AES de 256 bits, atender à certificação FIPS 140-2, limitar o acesso do usuário e habilitar o controle de acesso baseado em função e a autenticação multifator.

O Veritas Data Insight oferece visibilidade quase em tempo real dos dados de produção para ajudar a identificar o ransomware com base no comportamento anômalo do usuário e nas extensões de ransomware conhecidas. Ele também pode descobrir dados superexpostos para limitar e reduzir as superfícies de ataque.

As Veritas Analytics Solutions oferecem um painel único e unificado com insights e inteligência operacional para ajudar a identificar ransomware, sistemas desprotegidos e anomalias de backup. Use-os para otimizar o armazenamento, diminuir os custos e manter-se atualizado com os requisitos regulamentares e de conformidade.

A classificação Veritas Alta™ remove os obstáculos que impedem que você alcance a segurança e a conformidade dos dados. Reúna atributos de metadados e análises forenses de comportamento do usuário para inteligência acionável; identificar propriedade de dados, uso e controles de acesso; e mitigar a privacidade de dados e os riscos de segurança.



IDENTIFIQUE QUAIS DADOS VOCÊ POSSUI



AFASTE OS MALFEITORES



DETERMINE QUAIS DADOS SÃO CRÍTICOS E VULNERÁVEIS



TORNE OS DADOS E BACKUPS DISPONÍVEIS E EFICIENTES



CERTIFIQUE-SE DE QUE OS BACKUPS SEJAM IMUTÁVEIS E COM INTERVALO DE AR



DECIDIR UM PROCESSO DE RECUPERAÇÃO DE DESASTRES



PRATIQUE SUA ESTRATÉGIA DE RECUPERAÇÃO DE DESASTRES



OTIMIZE SEU BACKUP E RECUPERAÇÃO



## Identifique seus dados críticos e vulneráveis

Seus dados não são estáticos, sua estratégia e soluções também não deveriam ser.

Certifique-se de implementar produtos e serviços escaláveis e prontos para se adaptar. A flexibilidade é crucial para fornecer desempenho sob pressão com várias integrações em várias nuvens.

Não faz sentido presumir que uma empresa comprará todas as soluções de um único fornecedor em uma única fatura. O desenvolvimento de negócios não funciona dessa maneira: é confuso e envolve combinações de software e tecnologia antigos e legados com soluções mais novas e sofisticadas.

Priorize os dados e identifique qual nível de conformidade e regulamentações você precisa atender. Decida como gerenciar backups e, por fim, como lidar com o dimensionamento e o tamanho dos backups que influenciam o tempo de recuperação. Entenda como sua capacidade de largura de banda afeta seu backup e recuperação para que você possa moldar como fazer backup e recuperar fluxos de trabalho críticos com mais eficiência.

### Perguntas-chave

- Quais dados são mais importantes para "manter as luzes acesas"?
- Como priorizamos nossos backups de dados?

## Soluções da Veritas

As soluções de proteção de dados da Veritas são independentes de fornecedor e oferecem um sólido fluxo de trabalho de proteção e retenção que é econômico e fácil de implantar e gerenciar. Simplifique e organize em uma única plataforma em ambientes multinuvem e nuvem híbrida.

O Veritas Alta™ Shared Storage foi projetado para capacitar seus aplicativos essenciais aos negócios e fornecer armazenamento compartilhado de nível empresarial com desempenho e resiliência superiores, mantendo os custos baixos. Ele permite que os administradores de aplicativos e infraestrutura protejam dados confidenciais. E oferece criptografia; capacidades de escrever uma vez, ler qualquer coisa (WORM); instantâneos consistentes; e aceleração de banco de dados.

O Veritas Alta™ SaaS Protection permite que você mantenha o acesso aos dados armazenados nas contas do Microsoft 365 após a saída do funcionário sem ter que manter e pagar pela licença extra. Restaure pastas, caixas de correio ou sites com recuperação granular de vários níveis para um local preferido, seja na nuvem ou no local. Maximize o desempenho e a flexibilidade dimensionando o armazenamento de backup para petabytes e bilhões de objetos. Execute backups incrementais com mais regularidade para minimizar RPO e RTO enquanto implementa proteção de dados contínua para conjuntos de sites.



IDENTIFIQUE QUAIS DADOS VOCÊ POSSUI



IMEÇA QUE AS AMEAÇAS OBTENHAM DADOS



DETERMINE QUAIS DADOS SÃO CRÍTICOS E VULNERÁVEIS



TORNE OS DADOS E BACKUPS DISPONÍVEIS E EFICIENTES



CERTIFIQUE-SE DE QUE OS BACKUPS SEJAM IMUTÁVEIS E COM INTERVALO DE AR



DECIDIR UM PROCESSO DE RECUPERAÇÃO DE DESASTRES



PRATIQUE SUA ESTRATÉGIA DE RECUPERAÇÃO DE DESASTRES



OTIMIZE SEU BACKUP E RECUPERAÇÃO



## Torne os dados e backups disponíveis e eficientes

**Você fez backup de seus dados. Por que é tão difícil restaurá-lo quando ocorre um desastre?**

Migrar grandes quantidades de dados (como movê-los para armazenamento secundário) consome uma quantidade significativa de tempo e recursos de computação. E você não está fazendo isso apenas uma vez, mas se estiver usando a regra de backup 3-2-1, estará fazendo três vezes para dois tipos diferentes de armazenamento com pelo menos um externo para proteção extra.

Muitas coisas podem inviabilizar um backup completo durante a migração, e é por isso que a alta disponibilidade e o failover são importantes. É como despejar água de uma jarra em um copo; quando um copo transborda, um copo secundário pode pegar o excesso. O balanceamento de carga distribui uma carga de trabalho avaliando qual sistema pode lidar com sua solicitação. Você pode agrupar vários servidores para garantir alta disponibilidade e habilitar o failover. Se um servidor falhar, outro pode ocupar seu lugar - e nada pula uma batida.

### Perguntas-chave

- Onde temos oportunidades de melhorar nossa eficiência de backup?
- Como sabemos se nossos backups estão limpos, livres de malware e não corrompidos?

### Soluções da Veritas

**As soluções de proteção de dados da Veritas** cobrem facilmente a estratégia de backup 3-2-1+1 e adicionam uma camada adicional de segurança com um sistema integrado de prevenção contra invasões e um ambiente de recuperação isolado e isolado para armazenamento indelével e um sistema integrado imutável e isolado cofre de dados.

**O Veritas InfoScale** ajuda a reduzir a superfície de ataque para dados de produção e isola os dados de produção de E/S com instantâneos e espelhamento de dados. Ele também otimiza a recuperação para baixo RTO e RPO. Usando scripts automatizados, você pode executar varreduras de malware no volume isolado para garantir que esteja livre de malware.

**O Veritas NetBackup Flex e o Flex Scale** aplicam uma camada adicional de segurança, eliminando vários pontos de falha no hardware. Eles usam componentes de agrupamento para permanecer continuamente disponíveis.

**As soluções de análise da Veritas** criam uma linha de base de backups bem-sucedidos conhecidos, usando-a para comparar backups futuros e ajudá-lo a detectar anomalias. Você também pode classificar os backups por aplicativo para visualizar a capacidade de restauração de todos os seus aplicativos em um único painel.



IDENTIFIQUE QUAIS DADOS VOCÊ POSSUI



IMEÇA QUE AS AMEAÇAS OBTENHAM DADOS



DETERMINE QUAIS DADOS SÃO CRÍTICOS E VULNERÁVEIS



TORNE OS DADOS E BACKUPS DISPONÍVEIS E EFICIENTES



CERTIFIQUE-SE DE QUE OS BACKUPS SEJAM IMUTÁVEIS E COM INTERVALO DE AR



DECIDIR UM PROCESSO DE RECUPERAÇÃO DE DESASTRES



PRATIQUE SUA ESTRATÉGIA DE RECUPERAÇÃO DE DESASTRES



OTIMIZE SEU BACKUP E RECUPERAÇÃO



# Proteja os dados com air gap e um cofre de dados imutável

## Como você garante que os dados de backup sejam invulneráveis à criptografia?

Mesmo que sua empresa seja cuidadosa com o backup de dados, ainda existe o risco de erro humano e falha do equipamento. O risco de exclusão ou modificação acidental é alto.

Os backups devem ser feitos de forma a garantir que os dados não possam ser alterados. Os arquivos armazenados em armazenamento imutável podem ajudá-lo a evitar o estresse da corrupção e dos ataques cibernéticos.

Os backups imutáveis oferecem o mais alto nível de proteção de dados para sua empresa. A permanência dos dados é parte integrante do armazenamento imutável, garantindo que os arquivos não sejam alterados por acidente ou propositalmente. Isso cria um processo mais eficiente e eficaz em sua estratégia de segurança cibernética e recuperação de desastres e pode ajudá-lo a evitar perdas financeiras e tempo de inatividade.

A camada adicional de uma solução de air gap garante que seus dados de backup imutáveis sejam isolados e não corrompidos para que você possa prosseguir com uma restauração limpa dos dados.

### Perguntas-chave

- Como atualmente protegemos os backups contra corrupção?
- Existem padrões de conformidade que exigem que você tenha um espaço de ar e isolamento para seus dados?

## Soluções da Veritas

A Veritas se alinha aos princípios do NIST para oferecer imutabilidade, visibilidade, recuperação rápida e indelebilidade inigualáveis. Ele oferece suporte a vários métodos para soluções locais e externas, incluindo backups baseados em fita, armazenamento de objetos bloqueados baseados em nuvem e armazenamento eficiente de dados no AWS S3 Object Lock.

As soluções de proteção de dados da Veritas bloqueiam proativamente comportamentos indesejados de acesso a recursos antes que o sistema operacional possa agir sobre eles.

O Veritas Flex permite implementar um ambiente de recuperação isolado (IRE) com um cofre de dados imutável e fornecer uma cópia segura de dados de backup críticos de um ambiente isolado e imutável. A arquitetura IRE protege seus backups importantes e fornece um espaço seguro que você pode usar para orquestrar uma recuperação limpa ou ensaiar seu plano de recuperação de resiliência cibernética. O espaço de ar virtual independente de infraestrutura da Veritas oferece uma camada adicional de proteção e isolamento para ajudar a impedir ataques invasores.





## Definir um processo de recuperação de desastres

**A solução de recuperação ideal suporta todas as cargas de trabalho.**

Crie um processo que incorpore fácil integração, atenda ao seu RPO e RTO desejado, suporte todo o armazenamento e ofereça um painel consolidado de tudo sob proteção. Ao definir seu processo, considere fatores, incluindo o seguinte:

- Recuperação orquestrada (decidindo em que ordem recuperar)
- Eliminação de duplicações inteligente
- Integração de instantâneo
- Camadas de armazenamento
- Replicação automatizada de imagens, catálogos e instantâneos para armazenamento local e na nuvem
- Suporte de contêiner
- Percepção e análise de dados
- Segurança e conformidade para local e flexibilidade na nuvem
- Certifique-se de que seus dados e sistemas de backup estejam protegidos com criptografia

Aproveite o poder do Zero Trust, segurança de dados em várias camadas e automação inteligente para garantir que as operações de negócios permaneçam resilientes. Desbloqueie a inteligência multinuvem e atualize as defesas cibernéticas enquanto corta custos e utiliza soluções integradas. Minimizar seus custos e manter a conformidade com as regulamentações em evolução, consolidando o backup e a recuperação de cargas de trabalho baseadas em nuvem, automatizando a migração de carga de trabalho e implementando a recuperação de desastres sem complicações com recuperação com um único clique, scripts personalizados e ensaios.

### Perguntas-chave

- Quanto tempo vou demorar para me recuperar?
- Qual é a prioridade da recuperação?

### Soluções da Veritas

Você pode escolher entre recuperação bare metal ou recuperação de arquivo granular se apenas uma parte de seus arquivos tiver sido comprometida. Também oferecemos reversão instantânea para VMs para recuperar e reverter simultaneamente centenas de VMs em minutos.

**A resiliência de dados aprimorada e a Veritas Resiliency Platform** permitem que você atribua diferentes prioridades de recuperação entre aplicativos e recupere aplicativos multicamada em uma sequência de acordo com a criticidade dos negócios. Pontos de verificação contínuos de proteção de dados permitem recuperação de baixo RPO.

**Veritas NetBackup Flex e Flex Scale** têm um sistema operacional reforçado, arquitetura Zero Trust e armazenamento imutável e indelével. O IRE e o cofre de dados imutável oferecem uma solução isolada e isolada que não pode ser descoberta de fora. A varredura de malware e anomalias fornece confiança de que seus dados de backup estão limpos para que você possa se recuperar instantaneamente, independentemente do ambiente, no local ou na nuvem.





## Ensaie sua resiliência

**Ensaiar não é sobre restauração; trata-se de evitar o tempo de inatividade.**

Os cibercriminosos esperam que sua organização, como a maioria, não esteja otimizada para recuperação. Eles querem danos máximos e tempo de inatividade para garantir o pagamento dos resgates. Se você está pronto e ensaiado para a recuperação, já está um grande passo à frente. Para obter uma recuperação rápida, você deve ter um plano de resposta de segurança cibernética para todo o seu ambiente que inclua testes antecipados e frequentes. O ensaio regular e o exercício de sua recuperação ajudam a limitar o tempo de inatividade e as interrupções e a reduzir o impacto de um ataque.

À medida que a demanda por sistemas híbridos e multinuvem aumenta, você precisa da capacidade de gerenciar várias estruturas, bem como coordenar várias nuvens e sistemas de armazenamento. As equipes têm a tarefa de gerenciar e dimensionar vários servidores e aplicativos.

Aproveite a automação para gerenciar a complexidade de seus ambientes, identificar possíveis ameaças e gerenciar ensaios de forma proativa para garantir prontidão contínua e minimizar o tempo de inatividade.

### Perguntas-chave

- Como reduzo o tempo de inatividade?
- Como faço para acelerar a correção?

## Soluções da Veritas

**Veritas NetBackup Flex e Flex Scale** maximizam o potencial de proteção de dados com arquitetura facilmente expansível. Com várias camadas de imutabilidade, provisionamento automatizado e balanceamento de carga, você pode implantar uma solução completa de proteção de dados pronta para uso.

**O Veritas InfoScale e o Veritas Alta™ Application Resiliency** abordam não apenas se sua configuração está funcionando, mas também se está funcionando bem o suficiente. É uma solução de infraestrutura abrangente projetada para maximizar a disponibilidade e a recuperação de desastres por meio de uma forte integração com aplicativos de negócios críticos para garantir o máximo de tempo de atividade e failover. Uma plataforma abrangente que oferece flexibilidade para personalizar os níveis de proteção, dependendo da demanda do setor, com recursos que incluem:

- Conformidade de integridade de dados
- Runbooks automatizados para aplicativos de várias camadas para reduzir esforços manuais
- Mobilidade que permite que cargas de trabalho se movam entre plataformas sem esforço
- Integração perfeita com sistemas e ambientes tradicionais





# Otimize seu backup e recuperação

**Facilite o desafio de gerenciar a proteção de dados em toda a organização.**

A orquestração de dados é a resposta para identificar gargalos e entender onde estão seus processos mais demorados. A orquestração pode ajudar a economizar tempo automatizando processos, incluindo provisionamento de servidor, gerenciamento de banco de dados e aplicativos. Use-o para lidar com tarefas, incluindo verificação de vulnerabilidades, pesquisa de logs e até mesmo para ajudar a conectar ferramentas de segurança e integrar sistemas para que as equipes evitem ficar sobrecarregadas com tarefas.

Escolher a solução certa pode facilitar o gerenciamento de dados, mas é um desafio contínuo.

O acesso à análise correta fornece visibilidade dos elementos essenciais do seu ambiente. Aprofunde-se e você também pode identificar o que é subutilizado, mal configurado ou não indexado, ajudando a TI a resolver problemas e identificar recursos a serem redirecionados para obter economia de custos.

Descubra insights acionáveis para melhorar sua utilização, desempenho e resiliência enquanto prevê falhas e identifica recomendações proativas para mitigar riscos aos acordos de nível de serviço (SLAs).

A automação inteligente pode ajudá-lo a eliminar as ineficiências dos processos manuais e desbloquear infinitas possibilidades.

Implemente e implante backup e recuperação ágeis e seguros para proteção e otimização completas de dados.

Simplifique os recursos, reduza os custos e monitore toda sua rede, da borda ao núcleo e à nuvem por meio de uma exibição de console abrangente.

## Soluções da Veritas

O **Veritas Data Insight** permite que você analise a atividade e forneça uma análise aprofundada do uso e da atividade colaborativa. Ele pode ajudar a classificar os usuários e entender melhor os padrões de atividade; identificar dados duplicados, obsoletos ou órfãos; e alavancar pontuações de risco para avaliar ameaças potenciais e priorizar dados de alto risco. Crie trilhas de auditoria detalhadas e aproveite a análise integrada de arquivos, prevenção contra perda de dados e arquivamento com as soluções de conformidade da Veritas.

As soluções **Veritas Analytics** ajudam a identificar rapidamente aplicativos e serviços em risco. Recupere-se mais rapidamente obtendo a capacidade de monitorar e otimizar backups em todos os ambientes e localizar com eficiência os hosts afetados por local, ambiente ou aplicativo.

### Perguntas-chave

- Seus dados estão otimizados para recuperação rápida?
- Você entende seus SLAs?





Elimine as lacunas em sua estratégia de segurança cibernética. Saiba mais >

### Sobre a Veritas

A Veritas Technologies é líder em gerenciamento de dados em várias nuvens. Mais de 80 mil clientes, incluindo 95% das empresas da Fortune 100, confiam na Veritas para ajudar a garantir a proteção, capacidade de recuperação e conformidade de seus dados. A Veritas tem uma reputação de confiabilidade em escala, o que oferece a resiliência de que seus clientes precisam contra as interrupções ameaçadas por ataques cibernéticos, como ransomware. Nenhum outro fornecedor é capaz de igualar a capacidade de execução da Veritas, com suporte para mais de 800 fontes de dados, mais de 100 sistemas operacionais, mais de 1.400 destinos de armazenamento e mais de 60 nuvens por meio de uma abordagem única e unificada. Com tecnologia de escala de nuvem, a Veritas está entregando hoje sua estratégia de gerenciamento autônomo de dados, que reduz a sobrecarga operacional e, ao mesmo tempo, oferece maior valor. Saiba mais em [veritas.com/pt/br](https://www.veritas.com/pt/br). Siga-nos no Twitter em [@veritastechllc](https://twitter.com/veritastechllc).

**VERITAS™**

[www.veritas.com/pt/br](https://www.veritas.com/pt/br)

Para obter informações de contato globais, visite: [veritas.com/pt/br/company/contact](https://www.veritas.com/pt/br/company/contact)