



Projeta suas informações de negócios importantes com soluções de segurança de informações da IBM

As organizações sempre se esforçaram para gerenciar o crescimento exponencial de informações criadas e armazenadas e recentemente voltaram sua atenção para a crescente exposição e vulnerabilidade para ataques de todas essas informações. E mais: novas leis exigindo mais responsabilidade das organizações que perdem dados pessoais importantes intensificaram a necessidade de proteger adequadamente informações corporativas importantes.

À medida que as oportunidades de negócios se expandem na economia global, as organizações estão mais distribuídas e os modelos de negócios estão mais colaborativos. Não é mais suficiente proteger as informações internamente; elas também devem ser protegidas no contexto de um ambiente de negócios com um número cada vez maior de colaboradores e um universo de usuários em constantes mudanças. Colaboração também significa que não é suficiente para uma organização proteger suas próprias informações - ela também deve trabalhar para garantir a segurança das informações de seus parceiros.

Os ativos de informações estão crescendo em complexidade e em volume. Eles devem ser protegidos em vários níveis, desde informações armazenadas até informações em aplicativos, até dispositivos físicos na infra-estrutura de informações. Para que a segurança de informações seja eficaz, todas as áreas de risco na infra-estrutura devem ser tratadas.

Antes o principal transtorno para a segurança de uma organização eram os hackers que buscavam emoções, porém hoje os especialistas em segurança reconhecem que

criminosos profissionais e o crime organizado são as principais ameaças. Essas organizações criminosas são tão bem montadas que possuem a tecnologia mais sofisticada e podem contratar cientistas de computador para invadir sistemas considerados altamente seguros. Hoje em dia, muitas dessas organizações violam com sucesso sistemas de segurança de TI corporativos para acessar informações pessoais de grande valor, como números de segurança social e informações de cartão de crédito, que podem ser usadas para roubar a identidade de indivíduos e limpar suas contas bancárias. Com amplos recursos, as organizações criminosas geralmente violam sistemas de segurança implantados envolvendo funcionários da empresa para roubar informações importantes ou fornecer acesso a sistemas seguros. É um problema que continuará frustrando empresas que persistem em gastar recursos de TI para proteger suas infra-estruturas.

O custo de não proteger informações nesse ambiente de alto risco pode ser enorme, especialmente quando os custos financeiros diretos e os custos em áreas como perda de sigilo do cliente e risco de exposição normativa são levados em consideração. Por outro lado, os benefícios do êxito na proteção de informações podem ser inestimáveis. A segurança de informações permite o sucesso de negócios, construindo a base para confiança que é essencial para colaboração e inovação. Quando as informações estão seguras e protegidas, a empresa fica livre para buscar novas oportunidades de negócios em mercados emergentes ou com modelos de negócios inovadores sem medo de risco indevido.

Estrutura da IBM para segurança de informações completa

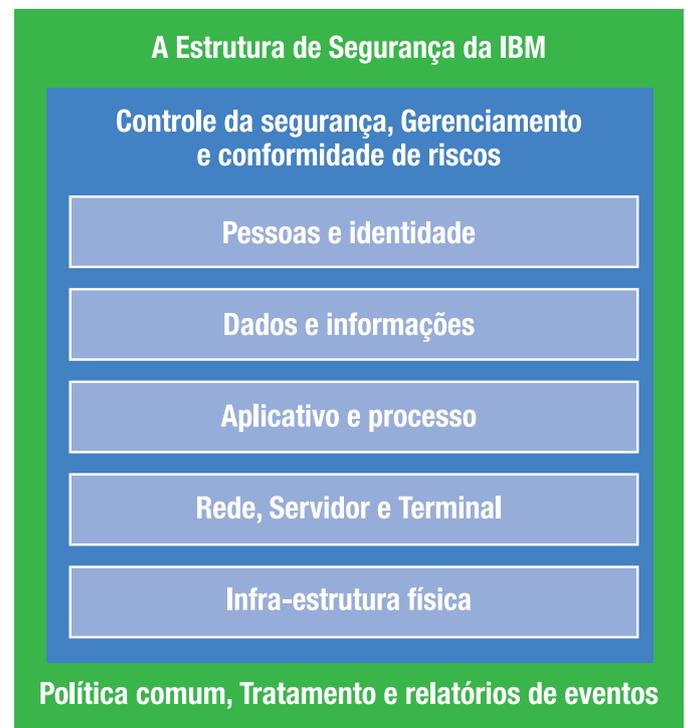
A abordagem da IBM para proteção de informações nas empresas de hoje é gerenciar estrategicamente a segurança de informações em toda a organização, como um Dynamic Infrastructure®, e não apenas no nível de sistemas ou de dados. Essa abordagem significa a instituição de controles que podem gerenciar o risco em todos os domínios de segurança de TI:

- *Identidade: Garantindo que as pessoas certas tenham acesso aos ativos certos no momento certo*
- *Informações: Proteger dados fundamentais onde quer que estejam armazenados na empresa e quando são transmitidos em redes particulares e públicas*
- *Aplicativos: Protegendo aplicativos e serviços de negócios*
- *Infra-estrutura de sistemas: Manter-se à frente de ameaças emergentes em todo o ambiente de TI*
- *Segurança física: Usando os crescentes recursos de controles digitais e monitoramento de vídeo para proteger os espaços físicos*

Em vez de focalizar apenas um domínio ou de gerenciar apenas uma parte do risco total, a IBM pode aplicar as tecnologias e experiência adequadas para oferecer segurança líder em quase todos os domínios. A IBM é exclusiva em sua capacidade de tratar praticamente qualquer dimensão de uma infra-estrutura segura e oferecer a tecnologia e serviços para

ajudar as organizações a desenvolverem uma abordagem estratégica para seus desafios de segurança. Para isso, a IBM oferece soluções de segurança de informações em cinco áreas estratégicas:

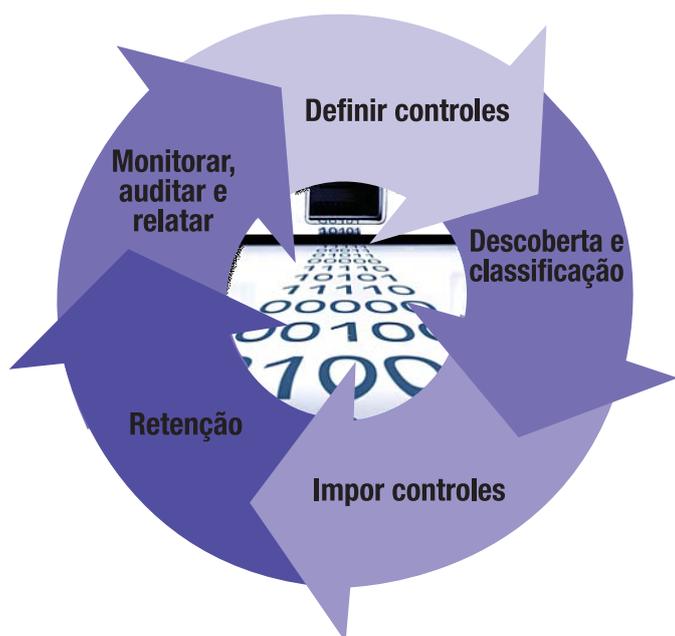
- *Conformidade da segurança*
- *Identidade e acesso*
- *Segurança de informações*
- *Segurança de aplicativos*
- *Segurança da infra-estrutura*



As soluções de armazenamento de informações do IBM System Storage™ têm um papel importante na estratégia de segurança de informações da IBM, ajudando as organizações a assegurarem e protegerem melhor os ativos de informações que residem na empresa.

Impondo controles de segurança com soluções de segurança de informações do IBM System Storage

As soluções do IBM System Storage para proteger informações são uma parte de uma abordagem maior e orientada pelo ciclo de vida que ajuda a oferecer proteção de rede completa para proteger todos os pontos de acesso a informações na rede, em todos os estágios do ciclo de vida da segurança de informações.



As soluções de armazenamento são especificamente relevantes até o ponto no ciclo de vida em que os controles de segurança são impostos, permitindo que as informações sejam compartilhadas com segurança dentro e fora da empresa.

Protegendo informações com soluções de armazenamento de autocriptografia da IBM

As soluções do IBM System Storage podem ajudar as organizações a imporem controles de segurança criptografando os dados armazenados. A criptografia é crítica porque o armazenamento do data center é basicamente móvel: As fitas são arquivadas, as unidades de disco são substituídas rotineiramente e as empresas se interessam cada vez mais com os dados importantes que residem em seus sistemas de armazenamento. A ideia da criptografia de armazenamento é proteger os dados armazenados nesses sistemas para que, se um cartucho de fita ou disco for perdido ou roubado, as informações armazenadas ali sejam inúteis para qualquer pessoa que as acesse, ilegíveis devido à criptografia.

A IBM oferece um portfólio de soluções de segurança de informações com base em suas inovadoras unidades de disco e fita de autocriptografia. Essas unidades são projetadas para criptografar automaticamente os dados à medida que são inseridos na unidade a ser armazenada e depois decifrados automaticamente quando são transferidos da unidade. O mecanismo de criptografia integrado ajuda a garantir que praticamente não haja diminuição do desempenho, em comparação com as unidades sem criptografia. Essa abordagem de criptografia no nível da unidade reduz o risco de comprometimento das informações quando a mídia de armazenamento é removida fisicamente dos sistemas de armazenamento para arquivamento.

Em 2006, a IBM apresentou a primeira unidade de fita corporativa de autcriptografia do mercado, o IBM System Storage TS1120, seguida pelas unidades de autcriptografia de próxima geração IBM System Storage TS1130 e Linear Tape Open (LTO), que podem tratar diversos ambientes corporativos e de fita acessível. Em fevereiro de 2009, a IBM introduziu unidades de criptografia de disco completo em seu importante IBM System Storage DS8000® e em seguida anunciou as unidades de criptografia de disco completo em sua plataforma de disco de mid-range: o IBM System Storage DS5000. A inclusão de soluções de disco de autcriptografia nas soluções de fita de autcriptografia de alto sucesso oferece aos clientes uma abordagem consistente para proteger os dados fixos, permitindo que as organizações tratem adequadamente suas questões de segurança de dados.

O uso dessas unidades de autcriptografia da IBM para criptografar dados no terminal de armazenamento permite armazenar dados em um formato criptografado com complexidade operacional mínima e impacto mínimo no desempenho. A criptografia no terminal de armazenamento pode ajudar as organizações a:

- *Minimizar a necessidade de criptografia baseada em host, o que pode diminuir o desempenho do host.*
- *Minimizar a necessidade de usar dispositivos de criptografia especializados que possam aumentar a complexidade da infra-estrutura.*
- *Acomodar a compactação de dados do armazenamento de fita, para que sejam necessários menos cartuchos de fita.*
- *Reduzir o risco de que as janelas de processamento do lote sejam afetadas dando nenhum impacto significativo para o desempenho nativo da unidade de fita.*

As unidades de autcriptografia estão se tornando rapidamente o modelo preferencial para proteger cartuchos de fita armazenados e unidades de disco de dados. Por exemplo, a Agência Nacional de Segurança recentemente qualificou as unidades de disco de autcriptografia para proteção de informações em computadores empregados por agências e contratados governamentais dos Estados Unidos para segurança nacional.

Quando falamos sobre proteger sua infra-estrutura de informações, é difícil não mencionar o mainframe. Durante anos, o mainframe da IBM tem satisfeito aos clientes mais exigentes com os níveis mais elevados de desempenho, disponibilidade e segurança. Originalmente projetado para ser compartilhado por milhares de usuários, o mainframe tem segurança integrada em quase todos os níveis do sistema, desde o nível do processador até o nível do sistema operacional e aplicativo. O design ajuda a proteger contra malwares, vírus e ameaças tanto dentro quanto fora da organização.

Oferecendo a capacidade de impor, monitorar e gerenciar a segurança, o IBM System z® é o ponto lógico de gerenciamento central para a segurança na empresa. Desde identificação e autenticação do usuário, controle e auditoria de acesso, serviços distribuídos de diretório, segurança de rede e administração de segurança, o mainframe foi desenvolvido para oferecer recursos de integridade, isolamento do processo e de criptografia para ajudar a manter as informações seguras. Sobre esta sólida base de hardware, os sistemas operacionais System z oferecem diversos elementos de segurança personalizáveis nos componentes Servidor de Segurança e Servidor de Comunicação.

E, obviamente, junto com a segurança herdada integrada no mainframe, há ofertas de gerenciamento de segurança adicionais do software IBM Tivoli®, como soluções de gerenciamento de identificação e de acesso e o conjunto IBM Tivoli zSecure, que podem oferecer segurança avançada para ajudar a proteger a infra-estrutura de informações.

Principais estratégias de sucesso no gerenciamento

Da mesma forma como cada unidade de fita possui um mecanismo de criptografia integrado, cada unidade de disco terá um mecanismo de criptografia integrado, que também usará o software de gerenciamento de chaves de criptografia da IBM para gerenciar as chaves associadas à solução. Esse sistema de gerenciamento de chaves simplificado e comprovado está sendo usado em alguns dos maiores bancos do mundo. Semelhante à solução de fita de criptografia, a solução de disco de criptografia foi projetada para ser transparente ao sistema operacional, aplicativos, bancos de dados, administradores do sistema e usuários, tornando a implementação muito mais simples que com dispositivos de criptografia especializados.

A IBM atualmente trata o gerenciamento de chaves em suas soluções de armazenamento em fita de autcriptografia com o IBM Tivoli Key Lifecycle Manager (TKLM) baseado em padrões e seu antecessor, o Encryption Key Manager (EKM). O TKLM foi projetado para ajudar a gerenciar o volume crescente de chaves de criptografia na empresa com implementação, configuração e administração simplificadas durante seus ciclos de vida.

Parte da abordagem holística da IBM com desafios de armazenamento e segurança

O sucesso da implementação de uma abordagem de ponta a ponta com a segurança de informações requer mais que tecnologia; requer serviços especializados de planejamento, design, implementação e suporte. A IBM oferece um amplo portfólio de serviços que podem ajudar os clientes a tratarem suas questões de segurança de curto prazo, além de projetar e implementar um ambiente de segurança de informações holísticas. Assim, em combinação com nosso portfólio integrado e igualável de ofertas e recursos de segurança, a IBM torna-se seu parceiro de escolhas para a segurança de informações de ponta a ponta. Considere o que a IBM oferece:

- *Profissionais qualificados: O negócio de segurança e privacidade da IBM inclui 3500 profissionais em todo o mundo, incluindo 1700 que concluíram o rigoroso treinamento da metodologia de segurança e privacidade da IBM.*
- *Uma presença mundial: A IBM mantém práticas de segurança e privacidade nos Estados Unidos, Canadá, EMEA (Europa, Oriente Médio, África), Ásia, Austrália e América Latina e do Sul.*
- *Liderança em P&D: A IBM possui mais direitos autorais e patentes de segurança e privacidade que qualquer outra empresa no mundo.*
- *Capacidade de oferecer: A IBM demonstra liderança em segurança diariamente ao entregar serviço com sucesso na IBM e para os clientes da IBM no mundo todo.*
- *Reconhecimento do setor: A IBM já foi reconhecida várias vezes por analistas do setor pela nossa liderança em serviços gerenciados de segurança e áreas de segurança relacionadas.*

Caso em questão: implementar a tecnologia de criptografia baseada em unidade na empresa

A organização de TI de uma grande firma de assistência médica baseada nos Estados Unidos para criptografar todos os dados na empresa a fim de ajudar a cumprir o compromisso da empresa de conformidade com os regulamentos da privacidade de dados.

Desafio

Os dados deveriam ser criptografados em vários ambientes de tecnologia: Computação do mainframe do IBM System z, computação distribuída e computação de desktop baseada no Microsoft® Windows®. A solução não poderia aumentar o tempo significativo para os processos de backup de dados atuais da empresa.

Solução

A empresa recorreu ao IBM System Storage para uma solução de criptografia de fita que ajudasse a garantir a segurança e a disponibilidade dos dados em todos os ambientes de TI. Ela implementou a unidade de fita IBM System Storage TS1120, permitindo a criptografia completa entre o mainframe da empresa, ambientes distribuídos e ambientes de computação de desktop.

Benefícios da solução

- *Oferece criptografia completa e gerenciamento simplificado de chaves na empresa*
- *Simplifica e dinamiza a TI permitindo uma solução de criptografia comum em todas as plataformas de computação*
- *Ajuda a garantir a proteção de dados sensíveis e facilita a conformidade com regulamentos, incluindo os componentes de privacidade da Lei de Portabilidade e Responsabilidade de Seguros de Saúde (HIPAA)*



Para obter mais informações

Para saber mais sobre como as soluções IBM de segurança de informações completas podem ajudar a proteger informações de negócios fundamentais em todo o ciclo de vida, entre em contato com o seu representante IBM ou com o Parceiro de Negócios da IBM, ou visite ibm.com/security.

Para obter mais informações sobre como as soluções do IBM System Storage podem proteger os dados armazenados em sua rede, visite ibm.com/storage.

© Copyright IBM Corporation 2009

IBM Systems and Technology Group
Route 100
Somers, NY 10589
U.S.A.

Produzido nos Estados Unidos da América
Março de 2009

Todos os direitos reservados

IBM, o logotipo IBM, ibm.com, DS8000, Dynamic Infrastructure, System Storage, System z e Tivoli são marcas ou marcas registradas da International Business Machines Corporation nos Estados Unidos e/ou em outros países. Se estes e outros termos com marca IBM estiverem marcados em sua primeira ocorrência nestas informações com um símbolo de marca comercial ou registrada (® ou ™), esses símbolos indicarão marcas comerciais comuns ou registradas nos EUA de propriedade da IBM no momento da publicação destas informações. Essas marcas comerciais também podem ser marcas registradas ou de leis comuns em outros países. Uma lista atualizada das marcas registradas IBM encontra-se disponível na Web em "Copyright and trademark information" ("Informações de copyright e marca registrada"), em ibm.com/legal/copytrade.shtml.

Microsoft e Windows são marcas registradas da Microsoft Corporation nos Estados Unidos, em outros países ou ambos.

Outros nomes de empresas, produtos e serviços podem ser marcas comerciais ou marcas de serviço de terceiros.

Este documento pode conter imprecisões técnicas ou erros tipográficos. A IBM pode não oferecer os produtos, serviços ou recursos descritos neste documento em outros países, e as informações de produtos podem estar sujeitas a alteração sem aviso. Consulte seu contato comercial IBM local para obter informações sobre produtos ou serviços disponíveis em sua região. Todas as declarações referentes às futuras direções e intenções da IBM estão sujeitas a alteração ou retratação sem notificação e representam apenas metas e objetivos. As informações contidas neste documento serão consideradas atuais a partir da data inicial de publicação e estarão sujeitas a alteração sem notificação. Todas as informações sobre desempenho foram determinadas em um ambiente controlado. Os resultados práticos podem variar. As informações de desempenho são fornecidas "COMO ESTÃO" e a IBM não expressa nem assume nenhuma garantia.

As informações referentes a produtos não pertencentes à IBM foram obtidas dos fornecedores desses produtos, de suas publicações ou de outras fontes disponíveis publicamente. As dúvidas sobre os recursos dos produtos não pertencentes à IBM devem ser encaminhadas a esses fornecedores. A IBM não garante que as informações oferecidas aqui atendam as suas necessidades ou as dos seus distribuidores ou clientes. A IBM fornece estas informações "COMO ESTÃO", sem qualquer garantia. A IBM nega quaisquer garantias, explícitas ou implícitas, incluindo garantias implícitas de não-infração, de comercialização ou de adequação a uma finalidade específica ou não-infração. Os produtos IBM possuem garantias de acordo com os termos e as condições dos contratos firmados.

