DELL Technologies

Dell Corporate Security & Resiliency

Visão geral

Na Dell Technologies, nosso foco principal é conquistar a confiança e proteger o mundo conectado. Com o surgimento do mundo conectado e inteligente, da rede 5G e das tecnologias avançadas, como IA e aprendizado de máquina, podemos fazer mais do que havíamos imaginado. Estaremos em segurança, seremos resilientes e nos adaptaremos ao mundo em constante mudança. Além disso, continuaremos cumprindo nossa grande missão: proteger a Dell Technologies e conquistar a confiança de nossos clientes ao incorporar segurança e resiliência em tudo o que a Dell faz.

John Scimone, diretor de segurança

Security & Resiliency Organization

Proteja a Dell Technologies e conquiste a confiança de nossos clientes incorporando segurança e resiliência em tudo o que a Dell Technologies faz

Segurança cibernética

- Proteção dos dados dos clientes e da empresa
- Inteligência de detecção de ameaças avançadas com visibilidade das ameaças emergentes
- Gerenciamento de identidades e acesso
- Gerenciamento dos riscos cibernéticos, manutenção da conformidade e proteção adequada do nosso ambiente

Resiliência corporativa, investigações globais e segurança corporativa

Segurança da resiliência corporativa

- Segurança corporativa: gerenciamento da proteção dos funcionários, das informações, dos ativos e da nossa reputação contra ataques e eventos físicos e ambientais
- Gerenciamento de crises: gerenciamento de eventos inesperados que podem prejudicar a Dell Technologies
- Continuidade dos negócios: garantia da capacidade de recuperação oportuna de processos e operações essenciais aos negócios
- Governança de recuperação de desastres: garantia da capacidade de recuperação oportuna de sistemas e dados essenciais aos negócios.
- Investigações globais: gerenciamento de incidentes físicos, como roubos, fraudes e violência no local de trabalho

Segurança de produtos e aplicativos

- Resposta a vulnerabilidades: resposta imediata às vulnerabilidades relatadas para manter os produtos e aplicativos implementados em segurança
- Ciclo de vida de desenvolvimento seguro: desenvolvimento de produtos e aplicativos mais seguros ao incorporar a segurança no ciclo de vida de desenvolvimento

Governança, riscos e conformidade

Criação, manutenção e garantia da conformidade de processos, padrões e políticas de resiliência e segurança da Dell Technologies

Garantia da conformidade com normas externas, como a Lei Sarbanes-Oxley (SOX) e o Padrão de segurança de dados do setor de cartões de pagamento (PCI DSS)

Realização de auditorias, renovação de contratos (em que a Dell Techonologies é fornecedora do cliente) e fornecimento de informações sobre regras e protocolos de segurança para produtos e serviços da Dell aos clientes.

Dell Federal | Dell Technologies Services | Dell Financial Services

Segurança cibernética

Além de implementar e manter programas e tecnologias de segurança, a segurança cibernética define padrões para esses recursos, que ajudam a Dell Technologies a gerenciar e mitigar riscos e proteger nossas informações, negócios, clientes e marca contra ameaças avançadas.

A segurança cibernética na Dell Technologies é responsável pelo(a):

- Proteção dos dados dos clientes e da empresa
- Inteligência de detecção de ameaças avançadas com visibilidade das ameaças emergentes
- Gerenciamento de identidades e acesso
- Gerenciamento dos riscos cibernéticos, manutenção da conformidade e proteção adequada do nosso ambiente

Por que o foco em segurança cibernética?

4,5 horas

Tempo médio de interrupção para que os agentes de ameaças se movimentem na rede de uma empresa após o comprometimento inicial

US$ 6 trilhões

Custo projetado de violações em todo o mundo até 2021

78 dias

Tempo médio necessário para detectar uma invasão sofisticada

Segurança de produtos e aplicativos

A segurança de produtos e aplicativos garante que os produtos oferecidos aos clientes estejam protegidos contra ameaças cibernéticas e livres de vulnerabilidades.

A segurança de produtos e aplicativos na Dell Technologies é responsável pelo (a):

- Ciclo de vida de desenvolvimento seguro — desenvolvimento de produtos e aplicativos corporativos mais seguros ao incorporar a segurança no ciclo de vida de desenvolvimento
- Resposta a vulnerabilidades — resposta imediata às vulnerabilidades relatadas para manter os produtos e aplicativos implementados em segurança

Por que o foco em segurança de produtos e aplicativos?

90%

dos incidentes de segurança são provenientes de exploits contra defeitos em produtos

100 vezes

mais caro corrigir defeitos de software na fase de manutenção em comparação à fase de criação

cerca de 60%

das violações normalmente envolvem uma vulnerabilidade para a qual já existia um patch disponível

Operações globais de segurança

As operações globais de segurança protegem os funcionários, as informações, os ativos e a nossa reputação contra ataques e eventos físicos e ambientais. As operações globais de segurança na Dell Technologies são responsáveis pelo(a):

- Proteção dos funcionários, dos processos, dos ativos e da marca Dell Technologies em todo o mundo
- Gerenciamento de guardas e câmeras de segurança e investigação de crimes e incidentes não relacionados a segurança cibernética cometidos contra a empresa por funcionários e criminosos

Exemplos e ações das operações globais de segurança:

- Gerenciamento de crises
- Continuidade dos negócios
- Recuperação de desastres
- Gerenciamento de riscos de detentores de informações privilegiadas
- Investigação de crimes e violações do Código de conduta
- Serviços de guardas de segurança uniformizados
- Sistemas de segurança de instalações
- Segurança de eventos
- Proteção avançada para funcionários de alto risco
- Transporte seguro de ativos e funcionários-chave
- Gerenciamento de todos os assuntos relacionados à segurança por meio do site Security@Dell.com

Por que o foco em operações globais de segurança?

US$ 9 mil
custo de uma interrupção não planejada do data center por minuto

21%
das violações de segurança anuais são atribuídas a roubos físicos e de informações privilegiadas

Mais de 2 milhões
de incidentes violentos ocorrem no local de trabalho nos EUA todos os anos

78%
dos homicídios no local de trabalho são mortes a tiros

Segurança organizacional

Na Dell Technologies, garantimos que os membros de nossa equipe global estejam cientes de que é responsabilidade deles cumprir as práticas e os padrões de segurança e resiliência. Para facilitar a adesão corporativa às nossas práticas e padrões, nossa segurança das informações prevê:

1. Estratégia e conformidade com políticas/padrões e normas, conscientização e treinamento, avaliações e gerenciamento de riscos, gerenciamento de requisitos de segurança contratual, consultoria de aplicativos e infraestrutura, testes de qualidade e direcionamento de segurança da empresa.
2. Testes de segurança e design e implementação de soluções de segurança para permitir a adoção de controles de segurança em todo o ambiente.
3. Operações de segurança das soluções de segurança implementadas, do ambiente e dos ativos, bem como gerenciamento de resposta a incidentes.
4. Investigações forenses com operações de segurança e recursos humanos, jurídicos e de proteção de dados para inspeções, incluindo eDiscovery e eForensics.

Sua confiança, nossa transparência

A jornada de transformação digital da Dell Technologies baseia-se nos mesmos pilares que adotamos para capacitar nossos clientes: Transformação dos negócios, Transformação da TI, Transformação da força de trabalho e Transformação da segurança. Adotamos e seguimos o princípio da “segurança intrínseca” em todos os sistemas e soluções que respaldam nossos processos de negócios e personalizamos o uso de estruturas e metodologias comprovadas que garantem o alinhamento à nossa estratégia corporativa. Além de garantirmos a priorização dos controles de segurança, como os recomendados pelo Center for Internet Security (CIS) e pelo SANS Institute, também estamos atentos ao que mais interessa a nossos clientes. Veja a seguir os 20 principais controles sobre os quais nossos clientes solicitam informações com mais frequência. Agrupamos esses controles com base nas cinco principais funções estabelecidas pelo NIST CyberSecurity Framework (CSF).

Identificação

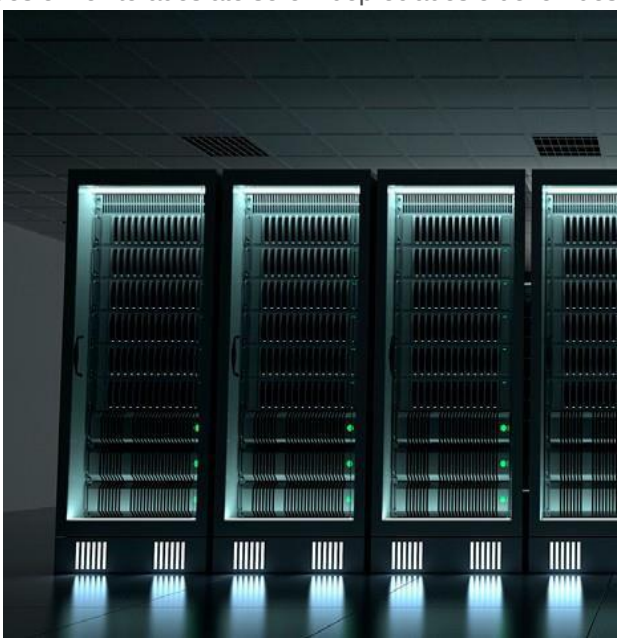
Gerenciamento de ativos

A prática da Dell é controlar e gerenciar ativos físicos e lógicos. Veja a seguir exemplos de ativos que a TI da Dell Technologies pode controlar:

- Ativos de informações: bancos de dados, planos de recuperação de desastres, planos de continuidade dos negócios, classificação de dados e informações arquivadas.
- Ativos de software: software de sistema e aplicativos identificados.
- Ativos físicos: servidores, desktops/notebooks, fitas de backup/arquivamento, impressoras e equipamentos de comunicação identificados.

A identificação, o controle e o gerenciamento de informações, software e ativos físicos são muito importantes na Dell Technologies.

A Dell Technologies possui um programa robusto de gerenciamento de ativos com regras e atividades que são comunicadas a todos os funcionários. Todos os ativos são contabilizados, têm um proprietário designado e são provisionados e monitorados até serem depreciados e devolvidos.



Os ativos são classificados com base na sua importância para os negócios, a fim de determinar os requisitos de confidencialidade, integridade e disponibilidade. As diretrizes do setor para manuseio de dados pessoais estabelecem a estrutura das salvaguardas técnicas, organizacionais e físicas. Essas salvaguardas podem incluir controles como gerenciamento de acesso, criptografia, logs e monitoramento, e destruição de dados.

A política de uso de recursos da empresa se aplica a todos os recursos corporativos de tecnologia da informação, independentemente da localização, e descreve vários requisitos para garantir que os funcionários da Dell Technologies entendam claramente o que é considerado uso aceitável de tais ativos.

Conformidade

O portfólio de políticas, padrões e controles da nossa Security & Resiliency Organization está alinhado às estruturas do NIST e da ISO. Essas regras fundamentais abrangem todo o ciclo de vida dos dados, dos nossos ambientes físicos e cibernéticos, bem como a responsabilidade de cada membro da equipe de contribuir com nossa cultura de segurança. Os departamentos jurídico, de segurança das informações, de privacidade e de conformidade trabalham para identificar todas as leis e normas regionais aplicáveis. Esses requisitos abrangem áreas como propriedade intelectual da empresa e de seus clientes, licenças de software, proteção de informações pessoais de funcionários e clientes, procedimentos de proteção e manuseio de dados, transmissão de dados além-fronteiras, procedimentos financeiros e operacionais, controles regulatórios de exportação de tecnologias e requisitos jurídicos.

Temos vários mecanismos em vigor para garantir que esses requisitos sejam cumpridos: o programa de segurança das informações, o conselho executivo de privacidade, o comitê diretor executivo de riscos, o conselho global de riscos e conformidade, auditorias/avaliações internas e externas, consultoria jurídica interna e externa, avaliações de controles internos, testes internos de penetração e avaliações de vulnerabilidades, gerenciamento de contratos, conscientização de segurança, consultoria de segurança, análises de exceção de política e gerenciamento de riscos. Além disso, diversas certificações e auditorias de segurança independentes estão em vigor, com base na necessidade geográfica e dos negócios, incluindo SOX, ISO 27001, SOC1, SOC2 e PCI DSS.

Nosso Código de conduta nos ajuda a realizar nossas atividades diárias na Dell Technologies de acordo com nossa cultura e valores, em conformidade com a força e o espírito de todas as leis aplicáveis nos países em que trabalhamos.

Gerenciamento de riscos

Temos um programa de gerenciamento de riscos estabelecido que fornece processos adequados para identificarmos, avaliarmos e tratarmos os riscos relacionados às valiosas informações da organização. Ele aborda as incertezas em torno desses ativos para garantir que os resultados de negócios desejados sejam alcançados.

Nosso programa de gerenciamento de riscos utiliza uma estrutura integrada de controle e risco que se concentra nas principais necessidades de disponibilidade, acesso, precisão e agilidade dos negócios em relação à tecnologia da informação e à segurança das informações. Ele fornece a estrutura e a disciplina para garantir que os riscos relacionados à tecnologia da informação e à segurança das informações a que estaremos expostos sejam continuamente avaliados e tratados de maneira proativa e econômica, incluindo funcionários, processos, dados e tecnologias. Os riscos são documentados e gerenciados por meio do plano de ação de gerenciamento/processo de correção (MAP); cada um deles tem um proprietário de risco designado, que é responsável pela correção.

Cadeia de suprimentos

Adotamos uma abordagem holística e abrangente para proteger a cadeia de suprimentos e entregar soluções em que os clientes possam confiar. Nossa estratégia de defesa aprofundada e defesa ampla envolve várias camadas de controles para reduzir os riscos que podem ser introduzidos na cadeia de suprimentos. Esses controles ajudam a estabelecer a garantia da cadeia de suprimentos, que representa a confiança de que o conjunto agregado de processos e controles em toda a cadeia de suprimentos e ciclo de vida dos produtos produzirá e fornecerá produtos, processos e informações sem elementos indesejados e que funcionem da forma projetada e esperada.

Nossa estrutura de gerenciamento de riscos da cadeia de suprimentos está em conformidade com a abrangente estrutura de gerenciamento de riscos do plano nacional de proteção de infraestrutura (NIPP), que descreve como o governo e o setor privado podem trabalhar juntos para reduzir riscos e cumprir os objetivos de segurança. Nossa estrutura incorpora um circuito de feedback aberto que permite fazer melhorias contínuas. Os planos de diminuição de riscos são priorizados e implementados conforme apropriado durante todo o ciclo de vida das soluções.

A governança de fornecedores é fundamental para salvaguardar o desempenho e a integridade da cadeia de suprimentos. Por isso, ela começa com uma análise completa de potenciais fornecedores e parceiros antes da integração. A análise antes do fornecimento de trabalho pode incluir pesquisas iniciais no local e compilações de qualificação de produção com a conclusão da solicitação de informações (RFI) ou de cotação (RFQ) específica de cada produto. Estamos posicionados de maneira única para aproveitar insights, práticas recomendadas, tecnologia e conhecimento especializado de marcas líderes do setor, confiáveis e respeitadas no portfólio da Dell Technologies. Acreditamos que é fundamental ouvir e trabalhar com clientes, fornecedores e parceiros para continuar melhorando a forma como a Dell Technologies controla a cadeia de suprimentos.

Proteção

Gerenciamento de acesso

Imaginar o ciclo de vida das identidades digitais e o acesso delas aos recursos da Dell é um fator crucial para proteger a rede e os sistemas da Dell. A transformação digital abandonou rapidamente o data center tradicional e aderiu à nuvem, criando um risco significativo sob a forma de ransomware e perda de dados. Nossas políticas de gerenciamento de identidades e acesso garantem maior postura de segurança, conformidade com normas e excelência operacional por meio da automação e da priorização baseada em risco.

O gerenciamento rígido de identidade, o acesso de usuário so o princípio de “menor privilégio” e a autenticação baseada em vários fatores ajudam a enfrentar os riscos associados a ambientes híbridos, multicloud e de borda. A abordagem da Dell inclui governança adequada para integração, transferência e rescisão de funcionários e contratados. Análises e relatórios robustos em tempo real permitem que as equipes de operações e garantia ofereçam uma experiência de usuário contemporânea, garantindo que as identidades digitais (pessoas, dispositivos e aplicativos) tenham o “acesso certo aos recursos certos no momento certo”.

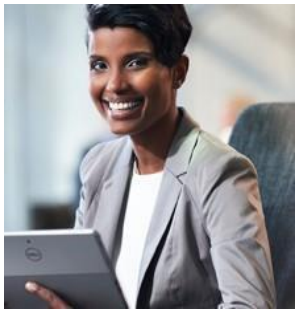
Governança de dados

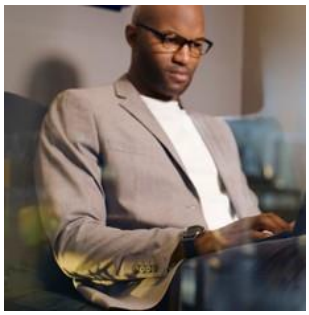
Nossa estrutura corporativa consolidada de governança de informações inclui requisitos para o ciclo de vida de dados e informações impressos e eletrônicos. Ela abrange a criação, o recebimento, o gerenciamento, o processamento, o armazenamento e o descarte de todas as informações utilizadas no curso normal dos negócios, independentemente do formato ou mídia. As diretrizes de segurança e privacidade das informações abrangem a identificação, a proteção de classificação, a retenção e o descarte de todos os aplicativos/bancos de dados e documentos em repositórios/locais de armazenamento aprovados.

- Os ativos de informação são identificados e inventariados de acordo com sua localização e movimentação durante todo o seu ciclo de vida.
- Dados estruturados e não estruturados são classificados de acordo com as categorias de classificação de dados adotadas (Público, Uso interno, Restrito e Altamente restrito). Quando as informações se enquadram em mais de uma classificação, o rótulo de classificação mais restritivo é aplicado. Os ativos são classificados com base na sua importância para os negócios, a fim de determinar os requisitos de confidencialidade.
- Com base no valor, no uso e na finalidade dos dados, os requisitos de proteção são definidos para cada categoria de classificação de dados desde o ponto de sua criação até o final de seu ciclo de vida. As diretrizes do setor para manuseio de dados pessoais estabelecem a estrutura das salvaguardas técnicas, organizacionais e físicas.
- As informações são retidas de acordo com a exigência de período de retenção, com base nos requisitos legais ou regulamentares, incluindo retenção legal e necessidades operacionais dos negócios.
- O descarte seguro das informações ocorre quando o prazo de exigência do período de retenção expira.

Contratação pela Dell

Os controles que implementamos abrangem a verificação de antecedentes e de competência de todos os candidatos a vagas de emprego, para garantir que nossos funcionários e contratados entendam suas responsabilidades e desempenhem adequadamente as funções às quais concorreram. Essas verificações são realizadas de acordo com as leis, as normas e a ética relevantes e são proporcionais às necessidades de negócios, à classificação das informações que serão acessadas e aos riscos percebidos associados.

Como parte do processo de contratação, todos os nossos funcionários e subcontratados devem assinar um contrato de confidencialidade e ser submetido a um processo de triagem aplicável de acordo com a lei regional.

Criptografia

Nossa política de criptografia está alinhada às práticas recomendadas do setor. Além disso, os padrões e controles que dão suporte às nossas políticas são alinhados dinamicamente aos requisitos comerciais e legais exigidos pelas partes interessadas.

Estabelecemos e gerenciamos chaves criptográficas para a criptografia necessária empregada no sistema de informações de acordo com os requisitos definidos pela organização para geração, distribuição, armazenamento, acesso e destruição de chaves. A criptografia é implementada para dados com uma classificação específica conforme definido pelas políticas ou padrões relevantes adotados. Nossa rede sem fio é segura, pois utiliza os melhores métodos criptográficos padrão do setor.

Nossos processos e sistemas criptográficos fornecem serviços para dados em repouso, em uso e em movimento, que incluem suporte a infraestrutura, bancos de dados e aplicativos. Além disso, nosso forte processo de gerenciamento de chaves criptográficas garante que chaves, certificados e assinaturas digitais sejam protegidos durante todo o seu ciclo de vida. Isso inclui geração, distribuição, armazenamento, backup, rodízio, expiração, arquivamento e destruição.

Gerenciamento de rede

A Dell Technologies implementa as medidas protetivas de rede necessárias, como o uso de controles técnicos e administrativos para gerenciar a segurança da rede e o suporte à infraestrutura.

Nossos controles estão alinhados ao NIST e ao Center for Internet Security para proteger e fortalecer os dispositivos de rede. O gerenciamento de rede fornece conectividade com a Internet, rede local e acesso remoto aos nossos recursos, juntamente com padrões de projeto de rede que fornecem a base a partir da qual protegemos os serviços de rede fornecidos aos usuários. Por meio de controles administrativos, físicos e tecnológicos, implementados de acordo com as práticas recomendadas do setor, garantimos um ambiente seguro baseado em camadas de componentes de proteção que se apoiam e se complementam para aumentar a segurança geral.

Gerenciamento de senhas

A Dell Technologies reconhece que é imperativo que nossos usuários pratiquem a devida diligência para obter acesso aos nossos sistemas, o que protegerá suas contas de usuário com senhas que não são facilmente adivinhadas ou deduzidas. As senhas são um aspecto importante da segurança do computador e são a primeira linha de proteção para as contas de usuário. Uma senha inapropriada pode comprometer toda a rede corporativa. Portanto, todos os funcionários, contratados e terceiros com acesso aos sistemas são responsáveis por tomar as medidas apropriadas para selecionar e proteger suas senhas, bem como aderir à autenticação baseada em dois fatores para acessar nossa rede interna.

A política e os padrões de senha, em conformidade com os padrões do setor, estão em vigor para garantir que todos os usuários mantenham práticas seguras e respaldem a estratégia de proteção da infraestrutura de informações. Isso inclui, entre outras medidas, a criação de senhas fortes, a proteção dessas senhas e a mudança frequente de senhas. Além disso, utilizamos sistemas de logs, monitoramento, automação e alertas que aplicam políticas de senha e fornecem uma camada de segurança adicional.

Gerenciamento de patches

Mantemos um programa global de gerenciamento de patches que segue os padrões do setor e atende aos requisitos regulamentares e de conformidade. Nosso processo de gerenciamento de patches está de acordo com as práticas recomendadas de segurança e inclui:

- Conhecimento dos patches atualmente disponíveis.
- Lista de inventário de todos os nossos ativos que exigirão aplicação de patches por meio de ferramentas de monitoramento automatizadas.
- Determinação de quais patches são apropriados para sistemas específicos, garantindo testes adequados.
- Instalação de acordo com um programa de gerenciamento de controle de mudanças.
- Análise do processo e dos resultados de aplicação de patches, bem como documentação de todos os procedimentos associados, como configurações necessárias e procedimentos padrão e emergenciais de aplicação de patches.

Nossos aplicativos e sistemas novos e existentes são mantidos de acordo com os níveis mais recentes de patches de segurança.

Segurança física

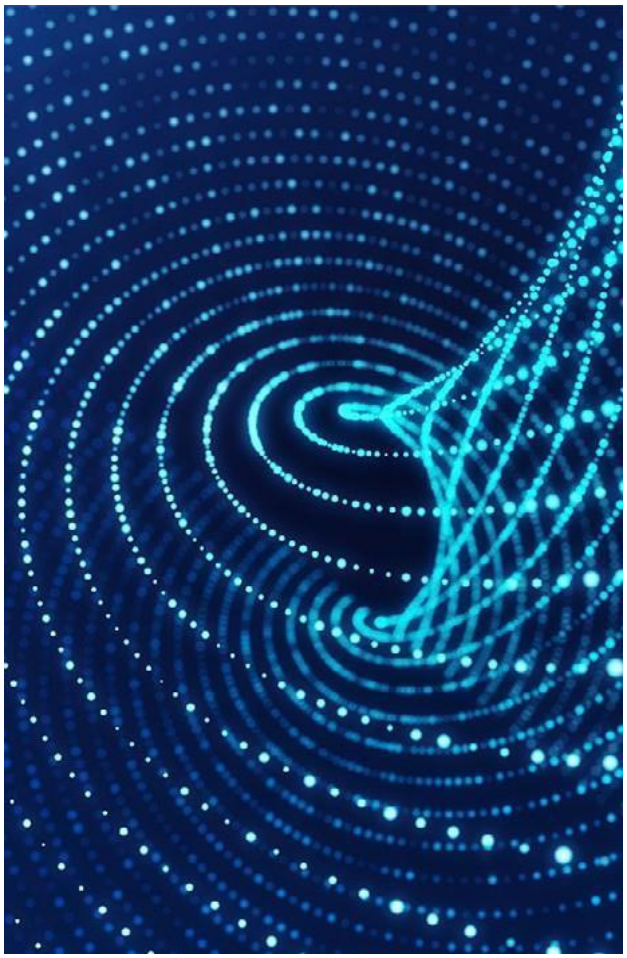
Os ambientes computacionais são um dos nossos ativos mais valiosos e devem ser protegidos. A restrição de acesso físico ao pessoal autorizado, bem como controles ambientais robustos, protege a confidencialidade, a integridade e a disponibilidade de nossos dados e ambientes computacionais contra uma ampla variedade de ameaças, a fim de garantir a continuidade dos negócios, minimizar os impactos nos negócios e maximizar o retorno sobre o investimento e as oportunidades de negócios.

O programa de segurança física segue os requisitos regulamentares e as práticas recomendadas de segurança do setor para garantir que o acesso físico às nossas instalações operacionais seja controlado com pontos de entrada físicos seguros, a fim de evitar acesso não autorizado, danos e interferência nas instações e informações. O acesso às instalações que contêm informações essenciais ou confidenciais é controlado e analisado regularmente para que seja restrito aos funcionários que precisam de acesso válido e autorizado, garantindo que apenas os funcionários apropriados o recebam.

Ciclo de vida de desenvolvimento seguro

Utilizamos um ciclo de vida de desenvolvimento de sistema robusto para controlar as etapas que devem ser realizadas, garantindo que todo o hardware, software e firmware distribuído aos clientes (internos e externos) sejam projetados, desenvolvidos e empacotados adequadamente de acordo com a estrutura de um programa de governança formal.

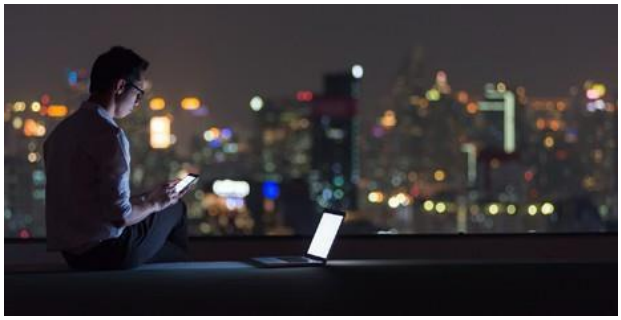
Nós nos esforçamos para incorporar a segurança ao longo do ciclo de vida do produto ou aplicativo, para que cada produto e aplicativo seja criado com segurança e permaneça protegido. O programa de segurança da Dell inclui atividades de análise, como modelagem de ameaças, análise de código estático e testes de segurança para descobrir e solucionar defeitos de segurança ao longo do ciclo de vida do desenvolvimento.



O programa de ciclo de vida de desenvolvimento seguro da Dell está alinhado aos princípios descritos na ISO/IEC 27034 – “Tecnologia da informação, técnicas de segurança e segurança dos aplicativos”. A Dell Technologies também colabora por meio de muitas iniciativas padrão do setor, como SAFECode, BSIMM e IEEE Center for Secure Design, para garantir que sigamos as práticas do setor.

Além disso, muitos funcionários da Dell Technologies estão envolvidos ativamente em organizações focadas no desenvolvimento de normas de segurança e na definição de práticas de segurança em todo o setor, que incluem:

- Cloud Security Alliance (CSA)
- Distributed Management Task Force (DMTF)
- The Forum for Incident Response (FIRST)
- International Committee for Information Technology Standards (INCITS)
- Organização Internacional para Padronização (ISO)
- Internet Engineering Task Force (IETF)
- The Open Group
- Organization for the Advancement of Structured Information Standards (OASIS)
- Software Assurance Forum for Excellence in Code (SAFECode)
- Storage Networking Industry Association (SNIA)



Vulnerabilidades de terceiros divulgadas publicamente são analisadas regularmente para determinar o impacto e a aplicabilidade que elas causariam em nosso ambiente. Com base nos riscos que elas representam para nossos negócios e clientes, existem prazos predeterminados para a correção. Além disso, com uma abordagem proativa e baseada em riscos, realizamos verificações periódicas de vulnerabilidades e avaliações de nossos aplicativos e infraestrutura. Análises seguras de códigos e scanners de vulnerabilidades são usados ao longo do processo de desenvolvimento e antes que os aplicativos sejam liberados para produção, a fim de detectar proativamente vulnerabilidades ou riscos de codificação.

Detecção

Antimalware

Implementamos vários controles para detecção, prevenção e recuperação, combinados com um programa de conscientização adequado para proteger o ambiente contra qualquer software mal-intencionado e vírus.

Utilizamos um modelo de proteção antivírus e de detecção e resposta de endpoints (EDR) gerenciado centralmente em vários níveis, incluindo três níveis de proteção de gateway de três fornecedores líderes do setor. Temos um conjunto definido e padrão de soluções que é instalado em todos os dispositivos em escopo. Esses dispositivos devem permanecer operacionais e estar de acordo com as configurações fornecidas pelo processo e servidor de política de gerenciamento, conforme apropriado para o sistema operacional. Além disso, nosso programa antimalware exige que todas as mensagens recebidas e enviadas sejam verificadas quanto a spam, vírus, políticas DLP, proteção de anexos, phishing e e-mails em massa.

Gerenciamento de mudanças

Implementamos um processo de gerenciamento de mudanças com práticas recomendadas do setor para garantir que seus ativos em linha de produção sejam estáveis, controlados e protegidos.

Nosso processo de gerenciamento de mudanças garante que as mudanças nos recursos de TI sejam gerenciadas de maneira controlada, para que causem o mínimo de disrupção nos negócios. O gerenciamento de mudanças oferece as ferramentas, as orientações e os requisitos necessários para controlar essas mudanças, a fim de garantir que elas sejam submetidas a análises e aprovações apropriadas e sejam comunicadas de maneira eficaz aos usuários.

Veja a seguir a lista de alguns benefícios:

- Minimiza os riscos operacionais das mudanças necessárias
- Maximiza a eficácia das mudanças implementadas
- Viabiliza a priorização e a programação centralizadas de todas as mudanças no ambiente
- Simplifica mudanças futuras por meio de documentação clara e processos bem definidos
- Oferece níveis de serviço consistentes e previsíveis para todos os tipos de mudanças no ambiente
- Aumenta a capacidade de processar grandes volumes de mudanças
- Evita conflitos de mudanças por meio de um agendador central

Logs e alertas

Estabelecemos e mantemos um programa de gerenciamento de logs e alertas que segue os padrões do setor e os requisitos regulamentares e de conformidade para registrar eventos e rastrear atividades autorizadas/não autorizadas e acesso a sistemas, aplicativos e dados.

Nosso programa de logs e alertas garante a captura, a notificação, o rastreamento e o gerenciamento de eventos de segurança para sistemas, aplicativos, plataformas e dispositivos de rede, de acordo com sua classificação e importância para os negócios. Como parte do programa, implementamos controles de padronização e retenção de logs e de proteção desses logs contra alterações não autorizadas. Além disso, o formato normalizado dos detalhes capturados nos logs facilita o gerenciamento de eventos e sua identificação por tipo, local, assunto, usuário, carimbo de data/hora e até mesmo quais dados foram acessados.

Por fim, usamos métodos de monitoramento em tempo real para monitorar e gerar alertas sobre atividades suspeitas ou quando ocorre uma falha no log de auditoria e até mesmo para acionar a correção automatizada para eventos conhecidos.

Gerenciamento de vulnerabilidades

Para atender aos objetivos de negócios da empresa e garantir a proteção eficaz de nosso ambiente e operações, estabelecemos uma estratégia global de aplicação de patches de segurança e gerenciamento de vulnerabilidades. Vários controles estão em vigor para garantir que nosso ambiente seja cuidadosamente gerenciado para manter uma proteção eficaz contra ameaças internas e externas. Protegemos a integridade, a disponibilidade e a confidencialidade dos dados, aplicativos, infraestrutura e dados do cliente em conformidade com os padrões do setor.

Como parte da nossa estratégia de gerenciamento de vulnerabilidades, as informações sobre ameaças cibernéticas são compiladas a partir de recursos confiáveis e são formadas alianças com os principais fornecedores. Nossos ativos e sistemas são verificados em busca de vulnerabilidades. A aplicação de patches e a correção são executadas com base em nossas políticas, prioridades e impacto de risco potencial.

Reação

Continuidade dos negócios

Os negócios globais e dinâmicos da Dell Technologies exigem uma abordagem flexível de resiliência operacional, para que possamos responder aos riscos com o mínimo de tempo de inatividade e fornecer uma infraestrutura adaptável que permita o crescimento e, ao mesmo tempo, proteja os interesses de nossos clientes, funcionários, parceiros de negócios e partes interessadas. Integramos um programa global de continuidade de negócios que define a estrutura de nossos padrões de resiliência operacional e auxilia as unidades de negócios da Dell Technologies no planejamento e mitigação de riscos, para garantir que estamos atendendo às necessidades de nossos clientes em um mundo em constante mudança.

O programa de resiliência corporativa é voltado para os riscos desde o início e está em conformidade com padrões internacionais reconhecidos do setor, como a ISO 22301. Ele orienta as unidades de negócios a especificar procedimentos alternativos e de recuperação em caso de perda de dependências funcionais importantes, de forma a permitir que a empresa mantenha o provisionamento de serviços sem afetar os níveis de serviço, os Recovery Point Objectives (RPO) e/ou os Recovery Time Objectives (RTO) conforme acordado com os clientes. Uma análise de impacto nos negócios (BIA) é usada para definir as funções mais essenciais.

Práticas de segurança

A orientação geral do programa da Dell é fornecida pelo Global Business Continuity Office (GBCO) e é liderada por uma equipe especializada e certificada em práticas de continuidade dos negócios. O GBCO fornece à empresa orientações sobre como evitar, se preparar e se recuperar de uma interrupção de negócios, com o melhor programa de continuidade de negócios da categoria, à altura de um fornecedor de primeiro nível. O programa orienta as unidades de negócios a especificar procedimentos alternativos e de recuperação em caso de perda de dependências funcionais importantes, de forma a permitir que a empresa mantenha o provisionamento de serviços sem afetar os níveis de serviço, os Recovery Point Objectives (RPO) e/ou os Recovery Time Objectives (RTO) conforme acordado com os clientes. Uma análise de impacto nos negócios é usada para definir as funções mais essenciais.

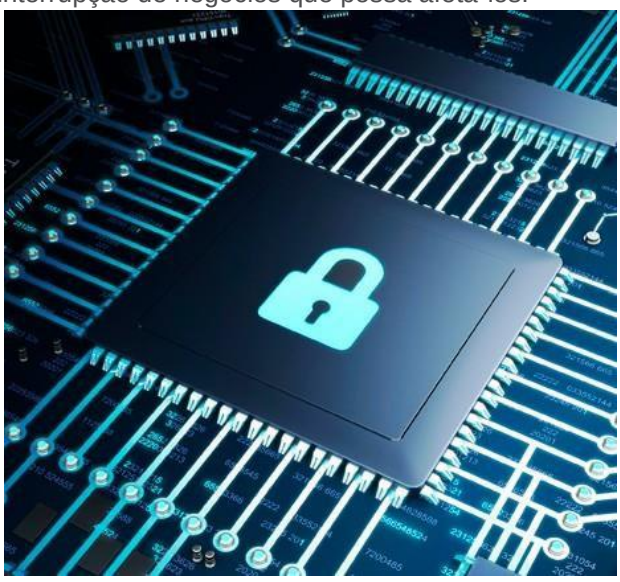
O processo de planejamento de continuidade dos negócios da Dell inclui uma política corporativa, que demonstra comprometimento com uma abordagem global de negócios e é apoiada pela gerenciamento sênior. Os planos de continuidade de negócios abordam o planejamento de cenários críticos para incluir continuidade e recuperação da perda de:

- Capital humano e conhecimento especializado
- Infraestrutura essencial
- Instalações
- Ativos, incluindo documentos vitais, IP e dados essenciais
- Aplicativos e infraestrutura de TI
- Dependências internas e externas essenciais
- Serviços gerenciados pelo fornecedor e de terceiros

A Dell Technologies exige que todas as funções essenciais aos negócios atualizem e testem seus planos de continuidade de negócios anualmente.

Comunicação

Um plano de comunicação foi desenvolvido para garantir que os principais tomadores de decisão e especialistas possam colaborar durante a ameaça de uma interrupção dos negócios. O plano de comunicação inclui entrar em contato com os clientes quando a empresa estiver sob ameaça de uma interrupção de negócios que possa afetá-los.




Avaliação de riscos

Uma avaliação de riscos é realizada anualmente para identificar e se preparar para os eventos naturais e causados pelo homem que têm maior probabilidade de impactar as operações de negócios.

Fornecedores/terceiros

A política da Dell Technologies exige dos fornecedores a aplicação de padrões de resiliência corporativa ao avaliar a capacidade do fornecedor, monitorar a conformidade em intervalos regulares, estabelecer fontes alternativas e usar um plano para lidar com itens falsificados, roubados ou ilegais.

Conformidade com normas e programas relacionados

A Dell Technologies estabeleceu procedimentos e políticas necessários para manter a conformidade com as leis e regulamentos operacionais e de produto aplicáveis, como segurança no local de trabalho, segurança do produto, proteção ambiental, normas de trabalho, códigos de construção e conformidade de importação/exportação. Além disso, os principais locais e/ou processos de negócios são certificados de acordo com padrões voluntários relevantes, como ISO 9001, ISO 14001, OHSAS 18001, ISO 20000, entre outros. Os procedimentos e processos da Dell são ajustados conforme necessário para refletir mudanças nas operações internas e nos fatores externos (por exemplo, mudança climática, crescimento populacional e acesso a energia e água).

Problemas

Controles e procedimentos de segurança física foram estabelecidos para monitorar, deter, detectar e proteger ativos essenciais que respaldam o provisionamento de serviços da Dell Technologies contra ameaças físicas. Esses procedimentos são proporcionais aos riscos avaliados e ao valor dos ativos e sua eficácia é verificada regularmente. Controles de segurança de dados relevantes, incluindo controle de acesso, criptografia e classificação de informações, foram estabelecidos para proteger a Dell Technologies e os dados dos clientes. Há também um plano para garantir a segurança de nossos funcionários e mitigar o impacto de possíveis paralisações devido a reduções imprevistas da força de trabalho.

Sustentabilidade e melhoria contínua

A Dell Technologies exige que a gerência analise e aprove as estratégias de continuidade e recuperação pelo menos uma vez por ano. A política de negócios da Dell Technologies exige a análise dos processos operacionais em busca de riscos e pontos únicos de falha e a implementação de estratégias para fechar quaisquer lacunas inaceitáveis.

Se você tiver mais dúvidas sobre o programa de continuidade de negócios da Dell Technologies, entre em contato com seu representante de conta da Dell Technologies.

Gerenciamento de incidentes

O principal objetivo do programa de resposta a incidentes de segurança cibernética é mitigar e conter os riscos associados a incidentes de segurança de computadores.

A proteção de nossa reputação e relacionamentos é de extrema importância para a empresa. Um programa eficaz e abrangente de segurança cibernética desempenha um papel fundamental no estabelecimento dessa proteção, ajudando a proteger as informações e os ativos da empresa. Nosso plano de resposta a incidentes de segurança cibernética é um componente essencial desse programa e foi projetado para descrever como identificamos, avaliamos, respondemos e corrigimos incidentes de segurança cibernética. O plano também define funções e responsabilidades entre as várias partes interessadas que participam de nossa resposta a um incidente de segurança cibernética.

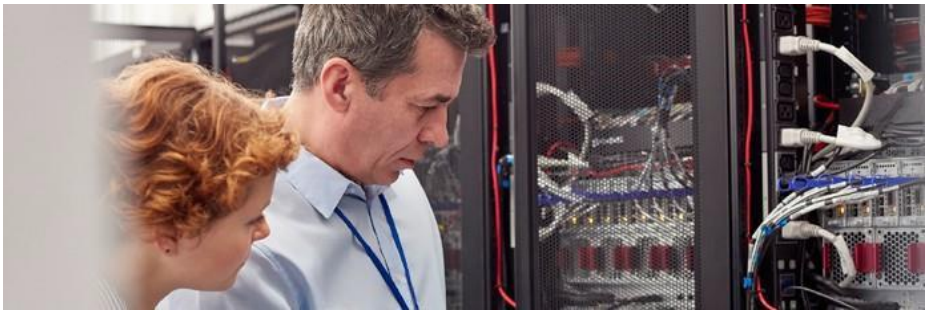
Um plano de resposta corporativa para incidentes de segurança cibernética está em vigor e descreve a finalidade, o escopo, a identificação, a avaliação, a resposta e a correção de incidentes de segurança, incluindo notificações a reguladores, controladores e/ou titulares de dados, conforme necessário.

Recuperação

Recuperação de desastres

Reconhecemos a importância de uma abordagem consistente, escalável, flexível e coordenada de resiliência no ambiente global em que operamos, pois ele está cada vez mais incerto e desafiador.

Se um incidente afetar gravemente nossa capacidade de conduzir os negócios normalmente, nosso programa de recuperação de desastres permite restaurar oportunamente processos, aplicativos, dados e sistemas essenciais aos negócios que dão suporte às nossas operações essenciais.



O programa de recuperação de desastres estabelece padrões, processos e controles para a recuperação oportuna de dados, aplicativos, sistemas e infraestrutura essenciais usados para gerenciar e respaldar nossas funções de negócios. Esses requisitos garantem a continuidade dos recursos que respaldam nossas funções essenciais.

Nosso programa e metodologia garantem que os aplicativos e a infraestrutura que atendem aos nossos clientes tenham recursos de resiliência alinhados aos acordos de nível de serviço, RTO e RPO obrigatórios. Um local de recuperação designado, bem como a disponibilidade da equipe de recuperação de desastres de TI, foi previamente estabelecido para ser mobilizado rapidamente em caso de interrupção dos negócios. Além disso, os planos de recuperação de desastres são analisados e testados pelo menos uma vez por ano, quando novos aplicativos são colocados on-line ou quando ocorrem mudanças no ambiente de TI. Os métodos de teste são proporcionais à importância do aplicativo/sistema.