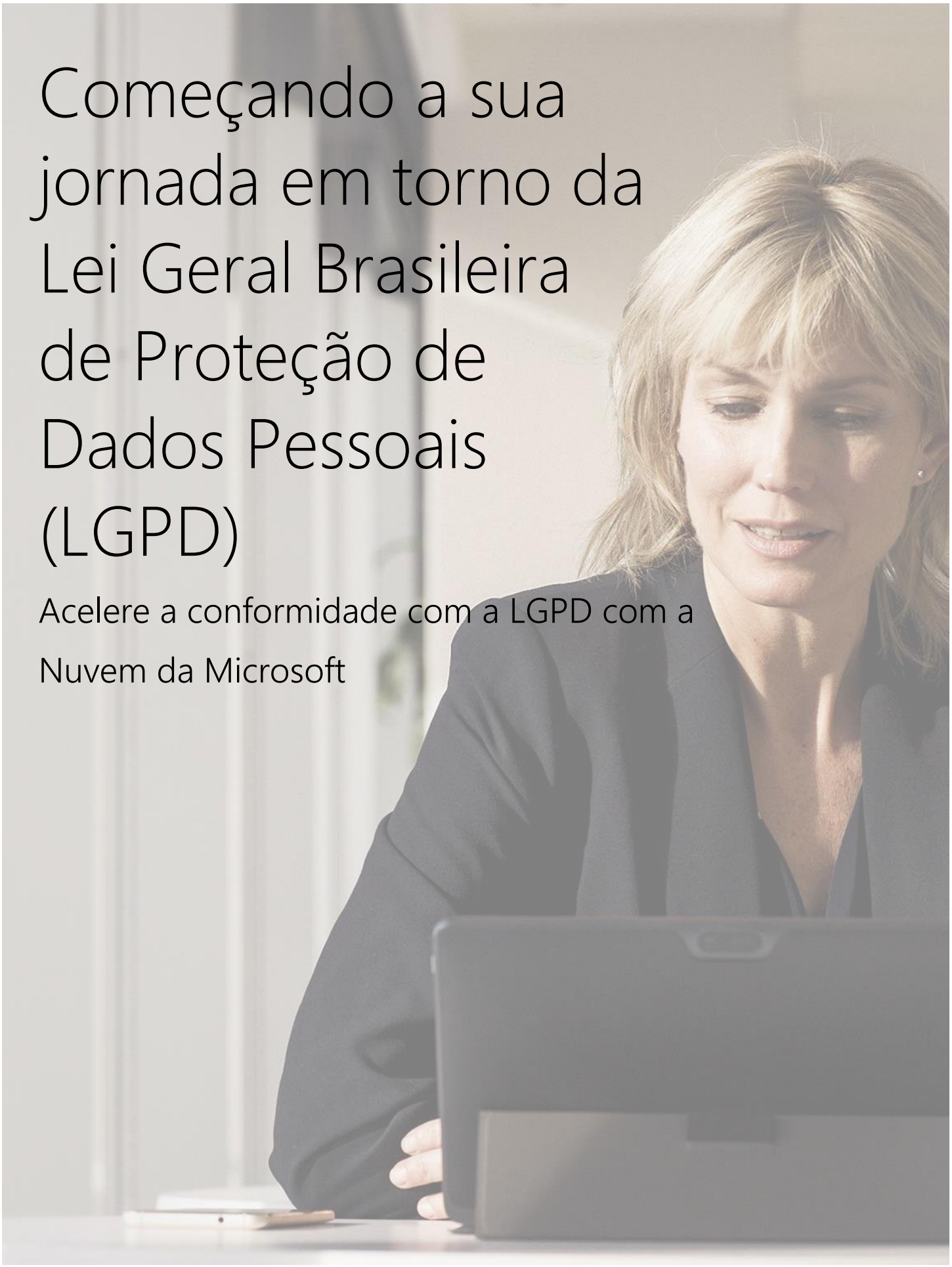
Começando a sua jornada em torno da Lei Geral Brasileira de Proteção de Dados Pessoais (LGPD)

Acelere a conformidade com a LGPD com a Nuvem da Microsoft



Conteúdo

Aviso legal

Este documento é um comentário sobre a LGPD, como a Microsoft a interpreta, desde sua publicação.[1] Embora a LGPD tenha sido criada recentemente, nós dedicamos muito tempo a ela e acreditamos compreender seu objetivo e significado. Mas a aplicação da LGPD será fortemente baseada na especificidade dos fatos, e nem todos os aspectos da LGPD estão bem definidos, especialmente devido ao fato de que a LGPD só entrará em vigor em agosto de 2020.[2]

Além disso, considerando a recente criação da Autoridade Nacional de Proteção de Dados por meio da Lei Federal nº 13.853/2019, provavelmente surgirão dificuldades em termos de interpretação, supervisão, implementação e monitoramento da lei.

Como resultado, este documento é fornecido apenas para fins informativos e não deve ser utilizado como um conselho legal ou para determinar como a LGPD pode se aplicar a você e sua empresa. Nós o encorajamos a trabalhar com um profissional com qualificação jurídica para discutir a LGPD, como ela se aplica especificamente a sua empresa e como melhor assegurar a conformidade.

A MICROSOFT NÃO OFERECE GARANTIAS EXPRESSAS, IMPLÍCITAS OU ESTATUTÁRIAS QUANTO ÀS INFORMAÇÕES DESTE DOCUMENTO. Este documento é oferecido em sua forma original.
As informações e opiniões expressas neste documento, incluindo URLs e outras referências da Página da internet podem ser alteradas sem notificação prévia. Você pode ver a data da última atualização deste documento verificando a data de publicação no final desta seção.

Publicado em dezembro de 2018 e atualizado em setembro de 2019.

Versão 1.2

[1] A LGPD foi oficialmente publicada em 15 de agosto de 2018.

[2] Conforme o art. 65, incisos I e II, da LGPD, a lei deve entrar em vigor em vinte e quatro meses após sua publicação oficial, com exceção dos dispositivos 55-A, 55-B, 55-C, 55-D, 55-E, 55-F, 55-G, 55-H, 55-I, 55-J, 55-K, 55-L, 58-A e 58-B, que já estão em vigor desde 28 de dezembro de 2018.

Introdução

Em 15 de agosto de 2018, a lei brasileira de proteção de dados pessoais foi publicada para definir uma comissão geral de direitos à privacidade, segurança e conformidade no Brasil.

A Lei Geral Brasileira de Proteção aos Dados, ou LGPD, fundamentalmente protege e viabiliza os direitos individuais de privacidade e proteção aos dados pessoais. A LGPD estabelece requisitos rígidos de privacidade governando como você gerencia e protege dados pessoais respeitando as escolhas individuais—sem importar para onde os dados são enviados, onde são processados ou armazenados.

A Microsoft e seus clientes estão agora em uma jornada para alcançar os objetivos de privacidade da LGPD. Na Microsoft acreditamos que a privacidade é um direito fundamental, e acreditamos que a LGPD é um passo importante em direção à clareza e viabilização dos direitos à privacidade individual. Mas também reconhecemos que a LGPD vai exigir mudanças significativas em empresas de todo o mundo.

Embora a nossa jornada em torno da LGPD possa parecer desafiadora, estamos aqui para ajudá-lo.

O compromisso da Microsoft com a LGPD

A confiabilidade é uma característica primordial da nossa missão de capacitar todas as pessoas e todas as organizações do planeta a alcançar mais. Adotamos uma abordagem baseada nos princípios de confiança, segurança, conformidade e transparência. Estamos aplicando estes princípios e estamos preparados para a LGPD.

Entendemos que a conformidade com a LGPD é uma responsabilidade compartilhada. Por isso, nos comprometemos com a mesma em todos os nossos serviços em nuvem quando a obrigatoriedade começar em agosto de 2020.

Também estamos comprometidos a dividir nossa experiência em torno da conformidade com regulamentos complexos para ajudá-lo a desenhar o melhor caminho para sua empresa obter sucesso em satisfazer os requisitos de privacidade da LGPD. Com o mais abrangente conjunto de ofertas de conformidade e segurança entre todos os provedores de nuvem e um ecossistema vasto de parcerias, estamos prontos para suportar suas iniciativas de privacidade e segurança agora e no futuro.

Como parte do nosso compromisso de parceria com você durante a sua jornada em torno da LGPD, desenvolvemos este documento para ajudá-lo com as preparações. Ele oferece uma visão geral da LGPD, descreve o que estamos fazendo para nos prepararmos para a LGPD e compartilha exemplos de medidas que você pode adotar hoje, juntamente com a Microsoft, para começar a sua jornada rumo à conformidade com a LGPD.

Estamos felizes em compartilhar atualizações adicionais sobre como podemos ajudá-lo a adequar-se a esta nova lei e, durante o processo, aprimorar as proteções de dados pessoais. Visite nossa seção do Regulamento Geral da Proteção de Dados da Central de Confiabilidade da Microsoft para encontrar recursos adicionais e para aprender mais sobre como a Microsoft pode ajudá-lo a atender as exigências específicas da LGPD.

Entendendo a LGPD—uma visão geral

Antes de descrever como exatamente a Microsoft pode ajudá-lo a se preparar para a LGPD, gostaríamos de abordar algumas das questões mais fundamentais e críticas sobre a regulamentação e o que ela pode significar para você. Maiores detalhes podem ser encontrados aqui.

O que é a LGPD?

A Lei Geral de Proteção de Dados Pessoais é a regulamentação de proteção aos dados pessoais no Brasil. Ela oferece aos indivíduos maior controle sobre seus dados pessoais, garante transparência sobre a utilização dos dados e exige maior segurança e controles de proteção de dados.

A LGPD se aplica à minha organização?

A LGPD aplica-se a muito mais do que você pode perceber. Esta lei impõe novas regras às empresas, ao poder público, às organizações sem fins lucrativos e outras organizações que (i) executam operações de processamento de dados em território brasileiro; (ii) oferecem bens e serviços às pessoas em território brasileiro ou que coletam e analisam dados relacionados às pessoas em território brasileiro; ou (iii) processam dados pessoais coletados em território brasileiro. Diferentemente das leis de privacidade em algumas jurisdições, a LGPD é aplicável às organizações de todos os tamanhos e em todos os setores.[3]A LGPD foi inspirada no GDPR - Regulamento Geral de Proteção de Dados europeu, que é geralmente visto internacionalmente como um modelo em questões de privacidade, portanto esperamos ver as interpretações e desenvolvimentos no GDPR influenciar diretamente a obrigatoriedade da LGPD no decorrer do tempo.

Quando a LGPD se torna efetiva?

A LGPD entra em vigor em agosto de 2020. Ela representa o primeiro regulamento geral sobre proteção de dados pessoais no Brasil, onde o tema era tratado apenas por leis específicas, como o Código Brasileiro de Defesa do Consumidor (Lei No. 8.078 de 11 de setembro de 1990) e a Lei Brasileira da Internet (Lei No. 12.965 de 23 de abril de 2014). A LGPD realmente tornou-se lei no Brasil em agosto de 2018, mas devido a mudanças importantes que algumas organizações terão que fazer para se alinharem ao novo regulamento, um período de transição de 24 meses foi incluído.

Quais são os princípios da LGPD?

A LGPD estrutura-se através de dez princípios:

- Propósito: Limita o processamento de dados pessoais a propósitos especificados, legítimos e explícitos.
- Adequação: Compatibilidade das atividades de processamento com os motivos pretendidos.

- Necessidade: Limita o processamento de dados pessoais ao mínimo necessário para atingir seus objetivos, abrangendo dados que sejam relevantes, proporcionais e não excessivos relacionados aos propósitos do processamento de dados.
- Acesso livre: Proporciona aos indivíduos consultas facilitadas e gratuitas sobre a forma e duração do processamento de dados pessoais.
- Qualidade dos dados: Proporciona aos indivíduos precisão, clareza, relevância e atualização dos dados.
- Transparência: Exige transparência na manipulação e utilização de dados pessoais.
- Segurança: Assegura que os dados pessoais estejam protegidos através de práticas de segurança apropriadas.
- Prevenção: Adota medidas para prevenir-se contra a ocorrência de danos devido ao processamento de dados pessoais.
- Não discriminação: Evita executar o processamento para propósitos abusivos ilegais ou discriminatórios; e
- Prestação de contas: Demonstrar a adoção de medidas que sejam eficientes e capazes de proporcionar a conformidade com as regras de proteção de dados pessoais, incluindo a eficácia de tais medidas.

Quais são alguns exemplos de requisitos da LGPD relacionados a estes princípios?

- Sob a LGPD, os indivíduos têm o direito de saber se uma organização está processando seus dados pessoais e de compreender o motivo deste processamento. Um indivíduo tem o direito de ter seus dados excluídos ou corrigidos, de pedir que não sejam mais processados, de recusar mala direta, e de revogar o consentimento de determinados usos dos seus dados. O direito à portabilidade de dados fornece aos indivíduos o direito de mover seus dados para outro lugar e de receber ajuda para fazê-lo.
- A LGPD exige que as organizações protejam dados pessoais de acordo com sua sensibilidade. No caso de violação de dados, controladores de dados geralmente devem notificar a autoridade correta dentro de um prazo razoável. Além disso, se a violação puder resultar em grandes riscos aos direitos e liberdade de indivíduos, as organizações também deverão notificar os indivíduos assim que possível.
- É preciso que haja uma base legal para o processamento de dados pessoais. Nos casos em que o consentimento seja a base legal para o processamento de dados pessoais, ele deve ser "fornecido de forma voluntária, consciente e não ambígua para propósitos específicos". Há exigências específicas da LGPD para o consentimento com a finalidade de proteger crianças.
- As organizações devem executar avaliações sobre o impacto da proteção de dados, por exigência da autoridade nacional, para prever os impactos de privacidade dos projetos e aplicar medidas corretivas quando preciso. Registros de atividades de processamento, consentimentos para processar dados e conformidade com a LGPD devem ser mantidos.
- A conformidade com a LGPD não é uma atividade pontual, mas sim um processo contínuo. A não conformidade com a LGPD pode resultar em altas multas. Para garantir a conformidade com a LGPD, as organizações são encorajadas a abraçar a cultura da privacidade para proteger os interesses dos indivíduos em seus dados pessoais.

Para uma visão mais detalhada da LGPD e para entender melhor alguns termos como pseudonimização, processamento, controladores, processadores e sujeitos de dados visite Microsoft.com/GDPR. Estamos comprometidos em ajudá-lo a atender às exigências da LGPD para garantir ainda mais os direitos de privacidade dos indivíduos.

Estabelecendo uma parceria com a Microsoft em sua jornada em torno da LGPD

Adequar-se à LGPD é um desafio que atinge os negócios que precisará de tempo????, ferramentas, processos e conhecimento, e poderá exigir mudanças significativas das suas práticas de gerenciamento de privacidade e dados. A sua jornada para adequar-se à LGPD será mais agradável se você estiver operando em um modelo em nuvem bem arquitetado e tiver um programa de governança dos dados vigente. Quando se trata de sucesso na conformidade com a LGPD, você pode contar com a Microsoft e nosso vasto ecossistema de parcerias para ajudá-lo.

A Microsoft tem uma longa história como provedora de serviços em nuvem confiáveis. Adotamos uma abordagem de princípios baseados na privacidade, segurança, conformidade e transparência com um forte compromisso para garantir que você possa confiar na tecnologia digital que você utiliza. Temos o portfólio de conformidade mais extenso do segmento e somos os primeiros a adotar padrões chaves como o padrão de privacidade em nuvem ISO/IEC 27018. Nossos clientes e parceiros se beneficiam da nossa experiente liderança em privacidade, segurança, conformidade e transparência.

Ao se preparar para adequar-se à LGPD, trabalhando em parceria com a Microsoft, sua empresa terá acesso a:

- **Tecnologia que atende às suas necessidades**. Você pode se beneficiar do nosso amplo portfólio de serviços corporativos em nuvem para atender às suas obrigações da LGPD para ações como apagar, retificar, transferir, acessar e recusar o processamento de dados pessoais. Além disso, você pode contar com nosso vasto ecossistema global de parcerias para um suporte especializado ao utilizar as tecnologias da Microsoft.
- **Compromissos contratuais**. Nós o apoiamos através de compromissos contratuais relacionados aos nossos serviços em nuvem, incluindo suporte em segurança e notificações em tempo hábil de acordo com as novas exigências da LGPD. Em agosto de 2020, nossos acordos de licenciamento de clientes para serviços em nuvem da Microsoft incluirão compromissos em conformidade com a LGPD em concomitância com sua entrada em vigor.
- **Compartilhamento de nossas experiências**. Nós compartilharemos a nossa jornada de conformidade com a LGPD para que você possa adaptar aquilo que aprendemos para ajudá-lo a desenhar o melhor caminho a seguir para a sua organização.

Começando com a LGPD

Uma abordagem de plataforma para a LGPD

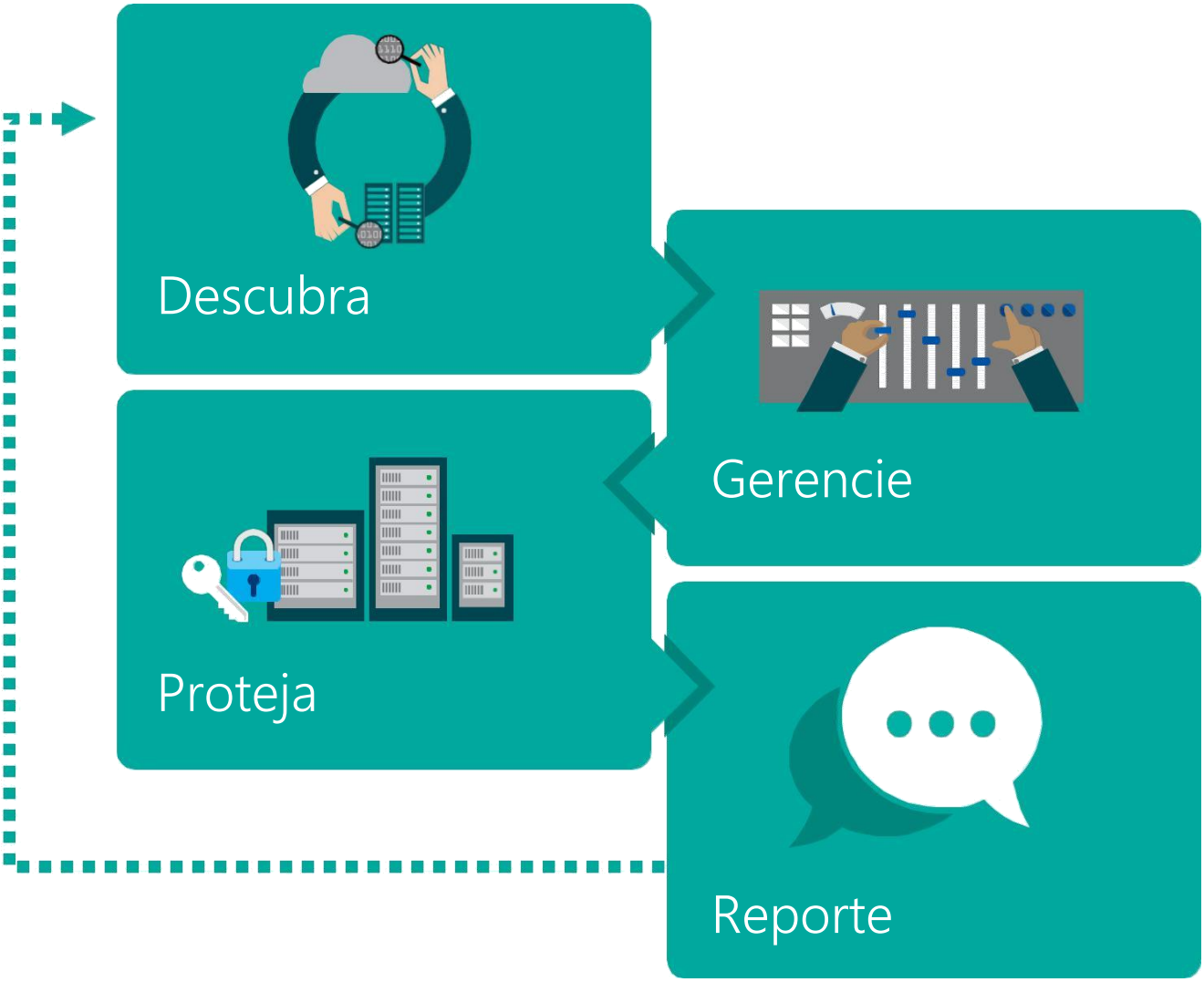
Os sistemas que você utiliza para criar, armazenar, analisar e gerenciar dados podem estar espalhados em diversos ambientes de TI — dispositivos pessoais, servidores locais, serviços em nuvem e até na Internet das Coisas. Isto significa que a maior parte da sua estrutura de TI pode estar sujeita aos requisitos da LGPD.

Os seus esforços para atender às exigências da LGPD serão mais eficazes se você olhar para os requisitos de forma holística e dentro do contexto de todas as suas obrigações de privacidade legais e regulamentares. Por exemplo, muitos dos controles de segurança para prevenir, detectar e responder às vulnerabilidades e violações de dados exigidos pela LGPD são semelhantes aos controles esperados por outros padrões de proteção, tais como o GDPR e o padrão de privacidade em nuvem ISO 27018.

Ao invés de monitorar os controles exigidos por padrões individuais ou regulamentos caso a caso, uma prática melhor é identificar um conjunto de controles e capacidades para atender a estas exigências. Da mesma forma, ao invés de avaliar tecnologias individuais e soluções através de um regulamento abrangente como a LGPD, adotando-se uma visão de plataforma — por exemplo uma que abranja o Windows, o Microsoft SQL Server, o Sharepoint, Exchange, Office 365, Azure e Dynamics 365 — pode proporcionar um caminho mais claro para assegurar não somente a conformidade com a LGPD, mas também com outras exigências importantes para você.

Recomendamos que você comece sua jornada rumo à conformidade com a LGPD focando em quatro passos chaves:

- **Descubra:** identifique quais dados pessoais você tem e onde eles estão.
- **Gerencie:** gerencie como os dados pessoais são usados e acessados.
- **Proteja:** estabeleça controles de segurança para prevenir, detectar e responder às vulnerabilidades e violações de dados.
- **Reporte:** responda às solicitações de dados, reporte as violações de dados e mantenha a documentação necessária.



Para cada uma dessas etapas, definimos exemplos de ferramentas, recursos e características em várias soluções da Microsoft que podem ser usadas para ajudá-lo a abordar os requisitos relacionados. Já que este documento não é um guia abrangente, incluímos links para você encontrar mais detalhes e mais informações em Microsoft.com/GDPR.

Devido ao grande conteúdo envolvido, você não deve esperar para se preparar quando a obrigatoriedade da LGPD começar.

Você deve rever suas práticas gerenciais de dados e de privacidade agora.

As próximas seções deste documento definem os elementos específicos de cada componente da LGPD e descrevem como você pode usar os produtos e serviços da Microsoft disponíveis para começar hoje.

Agindo hoje

Descubra: identifique quais dados pessoais você tem e onde eles estão.

O primeiro passo para a conformidade com a LGPD é avaliar se a LGPD se aplica à sua organização e, em caso afirmativo, até que ponto. Esta análise começa compreendendo-se quais dados você tem e onde estão.

A LGPD se aplica aos meus dados?

A LGPD regulamenta qualquer operação executada com "dados pessoais", como aquisição, armazenamento, uso e compartilhamento de dados pessoais. Dados pessoais têm uma definição muito ampla: de acordo com a LGPD *qualquer* dado que se refira a uma pessoa física identificada ou identificável.

Se a sua organização possui tais dados — em bancos de dados, em formulários de feedback preenchidos por seus clientes, em conteúdo de e-mails, em fotos, em gravações de circuito fechado de TV, em registros de programas de fidelidade ou em qualquer outro lugar — ou pretende obtê-los, e se os dados forem processados em território brasileiro, então você precisa da conformidade com a LGPD. Lembre-se que os dados pessoais não precisam estar armazenados no Brasil para estarem sujeitos a LGPD — a LGPD também se aplica se o propósito da atividade de processamento for oferecer bens ou serviços ou processar dados de indivíduos localizados no território nacional, ou se os dados pessoais processados forem coletados no território nacional.

Construindo o seu inventário

Para entender se a LGPD *realmente* se aplica à sua organização e, em caso afirmativo, quais obrigações ela impõe, é importante inventariar os dados da sua organização. Isto o ajudará a entender qual dado é pessoal e a identificar os sistemas em que os dados são coletados e armazenados, a entender por que eles são coletados, como são coletados e armazenados, processados e compartilhados, e por quanto tempo são mantidos.

Aqui estão alguns exemplos de maneiras específicas com que nossa nuvem e soluções locais podem ajudá-lo com o primeiro passo da LGPD.

Azure

Uma vez que o Azure é uma plataforma de nuvem aberta e flexível, ele inclui um serviço para ajudar a tornar as fontes de dados facilmente identificáveis e fáceis de descobrir. O Catálogo de Dados do Azure é um serviço de nuvem totalmente gerenciado que funciona como um sistema de registros e um sistema de descoberta para as fontes de dados da sua organização. Em outras palavras, o Catálogo de Dados do Azure tem tudo para ajudá-lo a descobrir, compreender e usar fontes de dados para obter mais valor dos dados existentes. Uma vez que uma fonte de dados é registrada com o Catálogo de Dados, o seu metadado é indexado pelo serviço de modo que você possa facilmente buscar para descobrir os dados que precisa.

Dynamics 365

O Dynamics 365 oferece diversas capacidades de visibilidade e auditoria que podem ser utilizadas através dos painéis de análise e relatórios do Dynamics 365 para identificar dados pessoais:

- O Dynamics 365 inclui o Assistente de Relatório que você pode usar com facilidade para criar relatórios sem usar buscas baseadas em XML ou SQL.
- Os painéis do Dynamics 365 proporcionam uma visão geral dos dados—informação que gera ações visíveis em toda a organização.
- O Microsoft Power BI é uma plataforma de autoatendimento de business intelligence (BI) que você pode utilizar para descobrir, analisar e visualizar dados, além de compartilhar ou colaborar insights com seus colegas.

Enterprise Mobility + Security (EMS) Suite

O Enterprise Mobility + Security oferece tecnologias de segurança voltadas para a identidade que podem ajudá-lo a descobrir, controlar e proteger dados pessoais mantidos por sua organização, bem como revelar potenciais pontos cegos e detectar quando violações de dados ocorrerem.

O Microsoft Cloud App Security é um serviço abrangente que oferece maior visibilidade, controles abrangentes e proteção aprimorada para os seus dados nos seus aplicativos em nuvem. Você pode ver até mesmo quais aplicativos em nuvem estão em uso em sua rede — identificando mais de 13.000 aplicativos de todos os dispositivos — e ainda obter a análise de riscos e análise contínua.

A Proteção de Informações do Azure pode ajudar a identificar quais são os seus dados mais sensíveis e onde estão. Você pode buscar por dados marcados com uma sensibilidade específica ou facilmente identificar dados sensíveis quando um arquivo ou e-mail for criado. Uma vez identificado, você pode automaticamente classificar e marcar o dado — tudo de acordo com as diretivas desejadas da empresa.

Office 365

Há várias soluções específicas do Office 365 que podem ajudá-lo a identificar ou gerenciar o acesso a dados pessoais:

- A Prevenção contra Perda de Dados (DLP) no Office e no Office 365 pode identificar mais de 80 tipos comuns de dados sensíveis incluindo informações financeiras, médicas e pessoalmente identificáveis.
- A busca de conteúdos na Central de Segurança e Conformidade do Office 365 pode fazer buscas em caixas postais, arquivos públicos, no Office 365 Groups, no Microsoft Teams, em páginas do SharePoint Online, locais do OneDrive for Business e conversas no Skype for Business e Microsoft Teams.

- A busca do Office 365 eDiscovery pode ser usada para encontrar texto e metadados em conteúdo de todo o seu Office 365 — SharePoint Online, OneDrive for Business, Skype for Business Online e Exchange Online.
- O Office 365 Advanced eDiscovery, equipado com tecnologias de aprendizado de máquina, pode ajudá-lo a identificar documentos que são relevantes para um determinado assunto (por exemplo, uma investigação de conformidade) rapidamente e com mais precisão do que buscas tradicionais por palavras chaves ou a revisão manual de uma enorme quantidade de documentos. O Advanced eDiscovery pode reduzir significativamente custos e esforços para identificar documentos e relações de dados usando o aprendizado de máquina para treinar o sistema para, de maneira inteligente, explorar grandes conjuntos de dados e rapidamente identificar o que é relevante — reduzindo a quantidade de dados antes de uma revisão.
- A Governança de Dados Avançada utiliza inteligência e insights auxiliados por máquina para ajudá-lo a encontrar, classificar, definir diretivas e agir para gerenciar o ciclo de vida dos dados mais importantes para a sua organização.

SharePoint

Você pode utilizar o Serviço de Busca do SharePoint e a funcionalidade de busca dentro do aplicativo para rastrear dados pessoais. Para identificar e buscar conteúdos sensíveis, o SharePoint Server 2016 oferece a mesma capacidade de prevenção contra perda de dados que o Office 365.

Server SQL e Azure SQL Database

A linguagem SQL pode ser utilizada para pesquisar bancos de dados e para personalizar ferramentas ou serviços que possam permitir este requisito. A busca é totalmente suportada por pesquisas, embora o registro total do rastreamento deva ser feito em nível de aplicativo. A tarefa de Script oferece um código para realizar funções personalizadas, como pesquisas complexas de dados que não estão disponíveis nas tarefas integradas e transformações que os serviços de integração do SQL Server proporcionam. A tarefa de Script também pode combinar funções em um script ao invés de tarefas e transformações múltiplas. Este pacote de produtos também inclui uma funcionalidade de Business Intelligence poderosa, dando ao usuário final acesso a insights de dados.

Windows e Windows Server

Para encontrar dados no Windows, você pode utilizar a Busca do Windows para rastrear e localizar dados pessoais em sua máquina local e em qualquer dispositivo conectado para os quais você tiver permissão de acesso adequado. Para aumentar as capacidades da Busca do Windows para localizar os dados pretendidos, você pode configurar as Opções de Indexação no Painel de Controle para personalizar as capacidades da Busca do Windows (por exemplo, indexando conteúdos de arquivos).

Gerencie: gerencie como os dados pessoais são usados e acessados.

A LGPD proporciona ao sujeito dos dados — indivíduos a quem os dados se referem — muito mais controle sobre como seus dados pessoais são obtidos e usados. Os sujeitos dos dados podem, por exemplo, solicitar que a sua organização compartilhe os dados que se referem a eles, transfira seus dados para outros serviços, corrija erros em seus dados ou restrinja o futuro processamento deles em determinados casos. Em alguns casos, estas solicitações devem ser resolvidas dentro de prazos determinados.

Governança dos dados

A fim de atender às suas obrigações com os sujeitos de dados, você terá que entender que tipo de dados pessoais a sua organização processa, como e para que fim. O inventário de dados mencionado anteriormente é o primeiro passo para chegar a esta compreensão. Assim que o inventário estiver completo, também é importante desenvolver e implementar um plano de governança de dados. Um plano de governança de dados pode ajudá-lo a definir as diretivas, perfis ou responsabilidades para o gerenciamento de acesso, o gerenciamento e uso de dados pessoais, e podem também ajudá-lo a garantir que suas práticas de utilização de dados estejam em conformidade com a LGPD. Por exemplo, o plano de governança de dados pode proporcionar para a sua organização a confiança de que ela efetivamente respeita as exigências dos sujeitos de dados de apagar ou transferir dados.

Serviços em nuvem da Microsoft

Para suportar sua estratégia de governança dos dados, os serviços em nuvem da Microsoft são desenvolvidos usando as metodologias Microsoft de Privacidade por Design e Privacidade por Padrão. Quando você confia seus dados ao Azure, ao Office 365 ou ao Dynamics 365, você permanece o dono exclusivo: você mantém os direitos, o título e o interesse nos dados armazenados nesses serviços.

Os serviços em nuvem da Microsoft adotam medidas eficazes para ajudar a proteger os dados dos seus clientes de acessos indevidos ou uso por pessoas não autorizadas, como explicado na Central de Confiabilidade da Microsoft. Estas medidas incluem a restrição de acesso aos funcionários da Microsoft e terceiros, e cuidadosamente define requisitos para responder às solicitações governamentais de dados de clientes. Contudo, você pode acessar os seus próprios dados de clientes a qualquer momento e por qualquer motivo.

Além disso, nós redirecionamos as solicitações de órgãos públicos dos seus dados diretamente para você, exceto quando legalmente proibido, e já desafiamos tentativas oficiais de proibir a exibição destas solicitações em tribunal.

Para garantir que os serviços em nuvem da Microsoft sejam gerenciados corretamente e para oferecer garantias aos nossos clientes, os serviços em nuvem são auditados ao menos uma vez por ano contra vários padrões mundiais de privacidade de dados, incluindo o GDPR, o HIPAA e HITECH, o CSA Star Registry e vários outros padrões ISO. Estes relatórios podem ser acessados em https://servicetrust.microsoft.com/Documents/ComplianceReports.

Além destes compromissos, nós proporcionamos a você o controle necessário para assegurar como os dados são gerenciados e quem tem acesso a qual dado dentro da sua organização.

Azure

O Azure Active Directory é uma solução em nuvem de gerenciamento de identidade e acesso. Ela gerencia identidades e controla o acesso ao Azure, no ambiente local e em outros recursos em nuvem, dados e aplicativos. Com o Azure Active Directory Privileged Identity Management, você pode atribuir direitos administrativos Just In Time temporariamente a usuários elegíveis para gerenciar os recursos do Azure.

O Azure Role-Based Access Control (RBAC) ajuda você a gerenciar o acesso aos seus recursos do Azure. Isto permite que você atribua o acesso baseado no perfil designado do usuário, tornando mais fácil dar apenas as permissões necessárias que os usuários precisam para desempenhar suas funções. Você pode personalizar o RBAC de acordo com o modelo de negócios e tolerância a riscos da sua organização.

Office 365

As soluções do Office 365 tem diversas características que podem ajudá-lo a gerenciar dados pessoais:

- Recursos de governança de dados na Central de Segurança e Conformidade do Office 365 ajudam você a arquivar e preservar conteúdo das caixas postais do Exchange Online, páginas do SharePoint Online, e locais do OneDrive for Business, importando dados para o Office 365 da sua organização.
- A Retenção no Office 365 pode ajudá-lo a gerenciar o ciclo de vida de e-mails e documentos, mantendo o conteúdo que você precisa e removendo conteúdo desnecessário.
- A Governança de Dados Avançada utiliza inteligência e insights auxiliados por máquina para ajudá-lo a encontrar, classificar, definir diretivas e agir para gerenciar o ciclo de vida dos dados mais importantes para a sua organização.
- As diretivas para gerenciamento de informações no SharePoint Online permite que você controle por quanto tempo quer reter o conteúdo, que você audite o que as pessoas fazem com o conteúdo, e que você adicione códigos de barra ou etiquetas aos documentos.
- O Journaling no Exchange Online pode ajudá-lo a adequar-se aos requisitos de conformidade legais, regulatórios e organizacionais, registrando as comunicações por e-mails recebidos e enviados.

Classificação de dados

A classificação de dados é uma parte importante de qualquer plano de governança dos dados. Adotando um esquema de classificação aplicável em toda a sua organização pode ser particularmente útil para responder às solicitações de sujeitos de dados, já que ele pode capacitá-lo a identificar e processar mais prontamente as solicitações de dados pessoais. A classificação de dados também é relevante devido ao fato de que a LGPD impõe condições específicas para o processamento de certos tipos de dados, tais como dados pessoais sensíveis (art. 11) ou dados pessoais de crianças e adolescentes (art. 14).

Hoje, oferecemos acompanhamento e ferramentas para ajudá-lo a trabalhar com todas as complexidades da classificação de dados.

Azure

Este documento sobre Classificação de Dados proporciona um direcionamento específico para a classificação de dados no Azure e o acompanha pelos princípios que permeiam as técnicas para a classificação de dados, o processo, a terminologia e a implementação. O documento contém muitas outras informações e links.

Dynamics 365

O Guia de planejamento de segurança e conformidade do Dynamics 365 (online) oferece um direcionamento abrangente para a compreensão de considerações importantes sobre conformidade e segurança associadas ao planejamento para o emprego do Dynamics 365 (online) em ambientes que incluam serviços de integração de diretório empresarial, tais como sincronização de diretório e login único (SSO). Ele traz informações sobre a privacidade de dados e diretivas de confidencialidade, classificação de dados e impactos.

Enterprise Mobility + Security (EMS)

A Proteção de Informações do Azure pode ajudá-lo a classificar e identificar seus dados no momento da criação ou modificação. Proteção (criptografia mais autenticação mais direitos de uso) ou marcações visuais podem então ser aplicadas aos dados sensíveis. Etiquetas de classificação e proteção são persistentes, viajando com o dado para que ele seja identificável e protegido o tempo todo — independentemente de onde é armazenado ou com quem é compartilhado.

Office e Office 365

- A Proteção contra Perda de Dados (DLP) no Office e no Office 365 pode identificar mais de 80 tipos comuns de dados sensíveis incluindo informações financeiras, médicas e pessoalmente identificáveis. Além disso, a DLP permite às organizações configurar ações a serem tomadas na identificação para proteger informações sensíveis e evitar exposições acidentais.
- A Governança de Dados Avançada utiliza inteligência e insights auxiliados por máquina para ajudá-lo a encontrar, classificar, definir diretivas e agir para gerenciar o ciclo de vida dos dados mais importantes para a sua organização. Ela classifica dados baseados em análise automática e recomendações de diretivas, e então aplica medidas para preservar os dados existentes ou eliminar o que for necessário. Os dados locais existentes, bem como as fontes de dados de terceiros, podem ser incluídos no Office 365 e classificados por tipo de mensagem. A classificação por tipo de mensagem permite a busca, separação e exportação das diversas fontes de dados, o que facilita o processo de execução de revisões de e-discovery.

Windows e Windows Server

O Microsoft Data Classification Toolkit para Windows Server 2012 R2 proporciona uma amostragem de busca de expressões e regras que você pode usar para auxiliar nas atividades de conformidade conduzidas por profissionais de TI, auditores, contabilistas, advogados e outros profissionais de conformidade da sua organização.

Proteja: estabeleça controles de segurança para prevenir, detectar e responder a vulnerabilidades e a violações de dados.

As organizações compreendem melhor a importância da segurança da informação — mas a LGPD eleva o nível de exigências. Ela requer que as organizações tomem medidas técnicas e organizacionais adequadas para proteger dados pessoais contra perda, acesso não autorizado ou exposição.

Protegendo seus dados

A segurança de dados é uma área complexa. Há muitos tipos de riscos a identificar e considerar — desde a invasão física por funcionários desonestos até a perda acidental e ataques por hackers. Construir planos de gerenciamento de riscos e tomar medidas para mitigar os riscos, tais como proteção de senhas, registros de auditoria e criptografia podem ajudar a garantir a conformidade.

A nuvem da Microsoft foi construída especificamente para ajudá-lo a compreender os riscos e defender-se contra eles, sendo mais segura do que ambientes de computação internos de muitas maneiras. Por exemplo, nossos datacenters são certificados por normas de segurança internacionalmente reconhecidas; são protegidos por monitoramento físico 24 horas por dia e possuem controles de acesso restritos.

A forma como protegemos a nossa infraestrutura de nuvem é apenas parte de uma solução de segurança abrangente e cada um dos nossos produtos, tanto na nuvem quanto instalados localmente, possui recursos de segurança que o ajudam a proteger seus dados.

Azure

Os seguintes serviços e ferramentas do Azure o ajudarão a proteger dados pessoais no seu ambiente em nuvem:

- A Central de Segurança do Azure oferece visibilidade e controle da segurança dos seus recursos do Azure. Ela monitora permanentemente os seus recursos e proporciona recomendações úteis de segurança. Ela possibilita a você definir diretivas para suas assinaturas do Azure e grupos de recursos baseadas nos requisitos de segurança da sua empresa, nos tipos de aplicativos que você utiliza e na sensibilidade dos seus dados. Também utiliza recomendações de segurança direcionadas às diretivas para guiar os donos de serviços em todo o processo de implementação do controle necessário — por exemplo, ativando o antimalware ou a criptografia de discos para os seus recursos. A Central de Segurança também o ajuda a empregar rapidamente serviços de segurança e appliances da Microsoft e de parceiros para fortalecer a proteção do seu ambiente de nuvem.
- A criptografia de dados no Azure garante a segurança dos seus dados em repouso ou em trânsito. Você pode, por exemplo, automaticamente criptografar seus dados quando destinados ao Armazenamento do Azure usando a Criptografia do Serviço de Armazenamento. Além disso, você pode usar a Criptografia de Discos do Azure para criptografar sistemas operacionais e discos de dados usados pelas máquinas virtuais do Windows e do Linux. Os dados estão protegidos em trânsito entre um aplicativo e o Azure de forma que eles permanecem sempre altamente seguros.

- O Azure Key Vault permite a você proteger suas chaves de criptografia, certificados e senhas que protegem os seus dados. O Key Vault usa módulos de segurança de hardware (HSMs) e foi projetado para que você tenha controle das suas chaves e assim dos seus dados, e assegurando que nem mesmo a Microsoft possa ver ou remover suas chaves. Você pode monitorar e auditar o uso das suas chaves armazenadas com os registros do Azure, e importar os seus registros para o Azure HDInsight ou o seu Gerenciamento de Informações de Segurança e Eventos (SIEM).
- O Microsoft Antimalware for Azure com serviços em nuvem e máquinas virtuais é uma capacidade de proteção gratuita em tempo real que o ajuda a identificar e remover vírus, spyware e outros software maliciosos que visam o roubo de dados, com alertas configuráveis que o avisam quando algum software malicioso ou indesejável tenta se instalar ou rodar em seus sistemas Azure.

Dynamics 365

Você pode usar os conceitos de segurança do Dynamics 365 para proteger a integridade dos dados em uma organização do Dynamics 365. Você pode combinar unidades de negócios, segurança baseada no perfil, segurança baseada em registros e segurança em nível de campo para definir o acesso geral à informação que os usuários têm na sua organização em Dynamics 365.

- A segurança baseada em função do Dynamics 365 permite agrupar um conjunto de privilégios que limitam as tarefas que podem ser executadas por um determinado usuário. Este é um recurso importante, especialmente quando as pessoas mudam de perfil dentro de uma organização.
- A segurança baseada em registros do Dynamics 365 permite restringir o acesso a registros específicos.
- A segurança em nível de campo do Dynamics 365 permite restringir o acesso a áreas específicas de alto impacto, tais como informações pessoalmente identificáveis.

Enterprise Mobility + Security (EMS)

Na maioria dos casos de violação de dados, os invasores ganham acesso à rede corporativa através de credenciais de usuários frágeis, padronizadas ou roubadas. Nossa abordagem de segurança começa com a proteção da identidade na porta da frente com acesso condicional baseado em risco.

- O Azure Active Directory (Azure AD) O Enterprise Mobility + Security pode ajudá-lo a proteger a sua organização no nível de acesso, gerenciando e protegendo suas identidades — incluindo identidades privilegiadas e não privilegiadas. O Azure AD oferece uma identidade comum protegida para acessar milhares de aplicativos. O Azure AD Premium traz a autenticação multifatorial (MFA), um controle de acesso baseado na integridade do dispositivo, localização do usuário, risco de identidade e sign-in e relatórios, auditorias e alertas de segurança holísticos.

O AD Privileged Identity Management (PIM) do Azure ajuda a descobrir, restringir e monitorar identidades privilegiadas e seu acesso a recursos através de um assistente de segurança, revisões e alertas. Isto possibilita cenários tais como acessos de administração "Just in Time" e de administração "Just Enough".

O Enterprise Mobility + Security permite a visibilidade detalhada do usuário, do dispositivo e atividade de dados no local e na nuvem e o ajuda a proteger seus dados com fortes controles e imposição de diretivas.

- A Proteção de Informações do Azure ajuda a aumentar o controle dos seus dados em todo o ciclo de vida dos dados — desde a criação até o armazenamento, no local e na nuvem, no compartilhamento interno ou externo, no monitoramento da distribuição de arquivos e finalmente nas respostas a atividades inesperadas.
- O Cloud App Security proporciona ampla visibilidade e fortes controles de dados para o software como um Serviço (SaaS) e aplicativos em nuvem que os seus funcionários estão usando, assim você pode obter o contexto completo e começar a controlar dados com diretivas detalhadas.
- O Microsoft Intune possibilita o gerenciamento de dispositivos móveis, de aplicativos móveis e das capacidades do PC a partir da nuvem. Usando o Intune, você pode fornecer aos seus funcionários acesso a aplicativos corporativos, dados e recursos de qualquer local e a partir de qualquer dispositivo, e ainda mantendo as informações corporativas altamente seguras.

Office e Office 365

A plataforma Office 365 incorpora segurança em todos os níveis, desde o desenvolvimento de aplicativos e datacenters físicos até o acesso do usuário final. Os aplicativos do Office 365 incluem tantos recursos de segurança interna que simplificam o processo de proteção de dados quanto a flexibilidade para você configurar, gerenciar e integrar a segurança de modo que faça sentido para as suas necessidades de negócios específicas. A estrutura de conformidade do Office 365 possui mais de 1.000 controles que possibilitam manter o Office 365 atualizado com os padrões industriais sempre em evolução, incluindo mais de 50 certificações e atestados.

Muitos controles de segurança padronizados estão disponíveis. O SharePoint e o OneDrive, por exemplo, usam criptografia para dados em repouso e em trânsito. Além disso, você pode configurar e empregar certificados digitais para ofuscar dados pessoais, e você pode usar controles do Office Access para liberar ou restringir acesso a dados pessoais.

O Office 365 oferece outros recursos que o ajudam a proteger dados e identificar quando uma violação ocorre:

- O Secure Score fornece insights sobre sua posição de segurança e quais recursos estão disponíveis para reduzir riscos, enquanto equilibra a produtividade e a segurança.

- O Advanced Threat Protection (ATP) for Exchange Online ajuda a proteger seus e-mails contra novos e sofisticados ataques de malware em tempo real. Ele também permite criar diretivas para ajudá-lo a prevenir que seus usuários acessem anexos ou websites maliciosos conectados por e-mail. O ATP for Exchange Online inclui proteção contra malware e vírus desconhecidos, proteção *time-of-click* contra URLs maliciosos, e excelentes recursos de relatórios e rastreamento de URL.
- O Information Rights Management (IRM) pode ajudar você e seus usuários prevenindo que informações sensíveis sejam impressas, encaminhadas, salvas, editadas ou copiadas por pessoas não autorizadas. Com o IRM no SharePoint Online, você pode limitar as ações que os usuários podem tomar em arquivos que tenham sido descarregados de listas ou bibliotecas, como imprimir cópias dos arquivos ou copiar textos deles. Com o IRM no Exchange Online, você pode prevenir que informações sensíveis em e-mails e anexos vazem via e-mail, online e off-line.
- O Mobile Device Management (MDM), ou Gerenciamento de Dispositivos Móveis no Office 365 permite que você defina diretivas e regras para ajudar a assegurar e gerenciar dispositivos como iPhones, iPads, Androids e Windows Phones registrados dos seus usuários. Por exemplo, você pode fazer a formatação remota de um dispositivo e ver relatórios detalhados sobre eles. O Office 365 também usa a autenticação multifatorial para oferecer segurança extra.

Server SQL e Azure SQL Database

O SQL Server e Azure SQL Database oferecem controles para gerenciar a autorização e o acesso aos bancos de dados em vários níveis:

- O Firewall do Azure SQL Database limita o acesso a bancos de dados individuais no servidor do Azure SQL Database restringindo o acesso apenas para conexões autorizadas. Você pode criar regras de firewall no servidor e no nível de banco de dados, especificando faixas de endereços IP aprovados para a conexão.
- A Autenticação do SQL Server garante que apenas usuários autorizados com credenciais válidas possam acessar seu servidor de banco de dados. O SQL Server suporta tanto a autenticação do Windows quanto os logins do SQL Server. A autenticação do Windows oferece segurança integrada e é recomendada como a opção mais segura, onde o processo de autenticação é totalmente criptografado. O Azure SQL Database suporta a autenticação via Azure Active Directory, que oferece o recurso de login único (Single Sign-On), sendo suportado por domínios gerenciados e integrados.
- A autorização do SQL Server permite gerenciar permissões de acordo com o princípio do privilégio mínimo. O SQL Server e o SQL Database usam a segurança baseada em perfil, que suporta o controle detalhado de permissões de dados através do gerenciamento dos participantes do perfil e de permissões em nível de objeto.

- O Mascaramento de Dados Dinâmico (DDM) é um recurso integrado que pode ser usado para limitar a exposição de dados sensíveis mascarando o dado quando ele é acessado por usuários ou aplicativos não privilegiados. Campos de dados designados são mascarados em resultados de pesquisa durante o processo, enquanto os dados no banco de dados permanecem inalterados. O DDM é simples para configurar e não requer alterações no aplicativo. Para os usuários do Azure SQL Database, o Mascaramento de Dados Dinâmicos pode descobrir automaticamente dados potencialmente sensíveis e sugerir o mascaramento apropriado a ser aplicado.
- A segurança em nível de linha é um recurso integrado adicional que permite aos clientes do SQL Server e Azure SQL Database implementar restrições ao acesso em nível de cada linha de dados. A RLS pode ser usada para permitir um acesso altamente controlado de linhas em um banco de dados, para maior controle sobre quais usuários podem acessar quais dados. Uma vez que a lógica de restrição de acesso é localizada na camada de banco de dados, esta capacidade simplifica muito o projeto e implementação da segurança do aplicativo.

O SQL Server e o Azure SQL Database oferecem um forte conjunto de recursos integrados que protegem dados e identificam quando uma violação de dados ocorre:

- A criptografia de dados transparente protege os dados em repouso criptografando o banco de dados, backups associados e arquivos de log de transações em uma camada de armazenamento física. Esta criptografia é transparente ao aplicativo e usa a aceleração do hardware para melhorar o desempenho.
- O Transport Layer Security (TLS) oferece segurança aos dados em trânsito em conexões do SQL Database.
- O Always Encrypted é o primeiro recurso da indústria projetado para proteger dados altamente sensíveis no SQL Server e Azure SQL Database. O Always Encrypted permite aos clientes criptografar dados sensíveis no aplicativo cliente e nunca revelar as chaves de criptografia ao mecanismo de banco de dados. O mecanismo é transparente aos aplicativos, já que a criptografia e descriptografia de dados são feitas de forma transparente no driver do lado cliente que utiliza o Always Encrypted.
- A Auditoria para SQL Database e a Auditoria do SQL Server rastreiam os eventos de bancos de dados e os transcrevem em um registro de auditoria. A Auditoria permite que você compreenda as atividades de bancos de dados em andamento, análise e investigue o histórico de atividades para identificar ameaças potenciais ou suspeitas de violações de segurança ou abuso.
- O SQL Database Threat Detection detecta atividades anômalas em bancos de dados indicando ameaças de segurança potenciais ao banco de dados. O Threat Detection usa um conjunto avançado de algoritmos para continuamente aprender e definir o perfil do comportamento do aplicativo, e notifica imediatamente quando detecta atividades incomuns ou suspeitas. O Threat Detection pode ajudá-lo a adequar-se aos requisitos de notificação de violação de dados da LGPD.

Windows e Windows Server

O Windows 10 e o Windows Server 2016 incluem criptografia líder no setor, tecnologias antimalware e soluções de identidade e acesso que permitem mudar a autenticação de senhas para formas mais seguras:

- O Windows Hello é uma alternativa conveniente de nível corporativo às senhas, que utiliza um método natural (biometria) ou familiar (PIN) para validar a identidade, proporcionando os benefícios de segurança dos smartcards sem a necessidade de periféricos adicionais.
- O Windows Defender Antivirus é uma solução antimalware robusta e pronta para uso que o ajuda a manter-se protegido. O Windows Defender Antivirus é ágil ao detectar e proteger contra novos malwares, e pode imediatamente proteger os seus dispositivos quando uma ameaça é primeiramente observada em qualquer parte do seu ambiente.
- O Device Guard permite a você bloquear seus dispositivos e servidores para protegê-los contra novas e desconhecidas variantes de malwares e ameaças persistentes. Diferentemente das soluções baseadas em detecção, como programas antivírus que precisam de constantes atualizações para detectar as mais novas ameaças, o Device Guard bloqueia os dispositivos de modo que rodem apenas os aplicativos autorizados que você escolher, o que significa uma maneira mais eficaz de combater malwares.
- O Credential Guard é um recurso que isola os seus segredos em um dispositivo, como os seus tokens de login único, do acesso mesmo no evento de um comprometimento geral do sistema operacional Windows. Esta solução fundamentalmente previne ataques de difícil defesa, como o "Pass the Hash".
- A Criptografia de Unidade BitLocker no Windows 10 e no Windows Server 2016 proporciona criptografia de nível corporativo para ajudar a proteger seus dados quando um dispositivo é perdido ou roubado. O BitLocker criptografa completamente o disco e unidades flash do seu computador para prevenir que usuários não autorizados acessem seus dados.
- A Proteção de Informações do Windows assume quando o BitLocker para de atuar. Enquanto o BitLocker protege todo o disco de um dispositivo, a Proteção de Informações do Windows protege os seus dados contra usuários não autorizados e aplicativos operando em uma máquina. Ela também ajuda a prevenir contra vazamentos de dados de documentos profissionais para não profissionais ou outros locais na web.
- As Máquinas Virtuais Blindadas permitem que você use o BitLocker para criptografar discos e máquinas virtuais (VMs) operando em Hyper-V, para prevenir que administradores comprometidos ou maliciosos ataquem o conteúdo de VMs protegidas.
- A Administração Just Enough e a Administração Just in Time permitem que administradores desempenhem suas funções e ações, enquanto possibilitam a você limitar o escopo de recursos e tempo que um administrador pode funcionar. Se uma credencial privilegiada é comprometida, o escopo dos danos é severamente limitado.

Esta técnica oferece aos administradores apenas o nível de acesso necessário enquanto estão trabalhando em um projeto.

Detectando e respondendo a violações de dados

Em certos cenários, a LGPD exige que no caso de violação de dados, as organizações têm que rapidamente notificar os reguladores. Em alguns casos, as organizações também precisarão notificar os sujeitos de dados afetados. Para atender a esta exigência, as organizações se beneficiarão tendo condições de monitorar e detectar invasões do sistema.

Para incidentes nos quais nós temos alguma ou toda a responsabilidade de responder, estabelecemos processos de Gestão de Respostas a Incidentes de Segurança, como explicados para o Azure e o Office 365.

Além disso, explicamos como trabalhamos colaborativamente com os nossos clientes sob um Modelo de Responsabilidade Compartilhada detalhado no documento Responsabilidades Compartilhadas na Computação em Nuvem.

Uma vez que você tenha detectado uma violação em potencial, recomendamos o que usamos em nosso próprio programa de respostas a incidentes – um processo de quatro passos:

- Avalie o impacto e severidade do evento. Baseado em evidências, a avaliação pode ou não resultar em escalonamento para a equipe de resposta da cibersegurança / proteção de dados.
- Execute uma investigação técnica ou forense, e identifique contenções, mitigação e estratégias para contornar a situação. Se a equipe de proteção de dados / cibersegurança acredita que dados pessoais podem ter sido expostos a alguém perigoso ou não autorizado, um processo de notificação é iniciado em paralelo, como exigido pela LGPD.
- Crie um plano de recuperação para mitigar a questão. Os passos para a contenção de crises, tais como colocar em quarentena os sistemas afetados, devem ocorrer imediatamente e em paralelo com o diagnóstico. Mitigações de longo prazo podem ser planejadas e devem ocorrer depois que os riscos imediatos tenham terminado.
- Crie um post-mortem que detalhe o incidente, com a intenção de rever diretivas, procedimentos e processos para evitar a recorrência do evento. Esta etapa está alinhada com os artigos 37, 38 e 48 da LGPD para gravar os fatos em torno do evento, seus efeitos e medidas de remediação adotadas.

Azure

Proteger os dados pessoais no seu sistema e reportar e rever a conformidade são requisitos chaves da LGPD. Os seguintes serviços e ferramentas do Azure podem ajudá-lo a atender a estas exigências da LGPD:

- Serviços integrados ao Azure permitem que você entenda a postura geral de segurança facilmente, e detecte e investigue ameaças ao seu ambiente de nuvem. A Central de Segurança do Azure emprega análises avançadas de segurança. Grandes descobertas em tecnologias de big data e aprendizado de máquina são usadas para avaliar eventos em toda a nuvem—detectando ameaças que seriam impossíveis identificar usando abordagens manuais e prevendo a evolução dos ataques. Estas análises de segurança incluem:
    - Threat Intelligence integrada, que procura agentes maléficos conhecidos usando o Global Threat Intelligence dos produtos e serviços da Microsoft Digital Crimes Unit (DCU), da Microsoft Security Response Center (MSRC) e fontes externas.
    - Análise comportamental, que aplica padrões conhecidos para descobrir comportamentos maliciosos.
    - Detecção de anomalias, que utiliza perfis estatísticos para criar uma linha de base histórica.

      Isto alerta sobre desvios da linha de base estabelecida que equivalem a um vetor de ataque potencial.

    Além disso, a Central de Segurança fornece alertas de segurança priorizados com insights sobre a campanha de ataque, incluindo eventos relacionados e recursos impactados.
- O Azure Log Analytics oferece opções de registros e auditoria de segurança configuráveis que podem ajudar a coletar e analisar dados gerados por recursos tanto em ambientes de nuvem quanto em ambientes locais. Permite insights em tempo real usando painéis de busca e personalização para rapidamente analisar milhões de registros em todas as cargas de trabalho e servidores, independentemente da localização física. Ajuda a facilitar uma resposta rápida e a investigação detalhada de qualquer evento de segurança.

Dynamics 365

Mantemos e atualizamos regularmente o Dynamics 365 (online) para garantir segurança, desempenho e disponibilidade, e para oferecer novos recursos e funcionalidade. Regularmente, também respondemos a incidentes de serviço. Para cada uma destas atividades, o administrador do Dynamics 365 da sua organização recebe notificações por e-mail. Durante um incidente de serviço, um representante de atendimento ao cliente do Dynamics 365 (online) também poderá telefonar e acompanhar via e-mail. Veja todos os detalhes das nossas diretivas e comunicações para o Dynamics 365 no TechNet.

Enterprise Mobility + Security (EMS)

Nossa abrangente Threat Intelligence utiliza tecnologias de ponta para análise comportamental e de detecção de anomalias para descobrir atividades suspeitas e localizar ameaças — tanto no local como na nuvem.

Isto inclui conhecidos ataques maliciosos (como Pass the Hash, Pass the Ticket) e vulnerabilidades de segurança no seu sistema. Você pode adotar medidas imediatas contra ataques detectados e agilizar a recuperação com um suporte poderoso. Nossa Threat Intelligence é aprimorada com o Microsoft Intelligent Security Graph, dirigido por um vasto número de conjuntos de dados e aprendizado de máquina na nuvem:

- A Microsoft Advanced Threat Analytics (ATA) é um produto instalado localmente que pode ajudar os profissionais de segurança da área de TI a proteger sua organização contra ataques avançados, automaticamente analisando, aprendendo e identificando o comportamento normal ou anormal da entidade (usuário, dispositivo e recursos). A ATA identifica ameaças persistentes avançadas (APTs) no local detectando o comportamento suspeito de usuário ou entidade (dispositivo e recursos), usando o aprendizado de máquina e informações do Active Directory, sistemas SIEM, e o log de eventos do Windows local. Ela também detecta ataques maliciosos conhecidos (como Pass the Hash). Por fim, oferece uma linha de tempo simples dos ataques, com informações claras e relevantes, permitindo que você dê atenção ao que é importante.
- O Cloud App Security proporciona proteção contra ameaças aos seus aplicativos em nuvem otimizado pela vasta pesquisa e inteligência de ameaças da Microsoft. Você pode identificar usos de alto risco, incidentes de segurança e detectar o comportamento anormal de usuários para prevenir-se contra ameaças. A heurística avançada de aprendizado de máquina do Cloud
  App Security aprende como cada usuário interage com cada aplicativo SaaS e, através de análise comportamental, avalia o risco de cada transação. Isto inclui logins simultâneos de dois países diferentes, o download repentino de terabytes de dados, ou múltiplas tentativas fracassadas de login que podem significar um ataque violento.
- O Azure Active Directory (Azure AD) Premium proporciona a detecção de ameaça em nível de identidade na nuvem. O Azure AD monitora o uso de aplicativos e protege sua organização de ameaças avançadas com relatórios de segurança e monitoramento. Relatórios de acesso e uso dão visibilidade da integridade e segurança do diretório da sua organização. Além disso, o Azure AD oferece proteção de identidade com notificações, análises e remediação recomendada.

Office e Office 365

O Office 365 oferece vários recursos que o ajudam a identificar e agir quando uma violação de dados ocorre:

- O Threat Intelligence pode ajudá-lo a descobrir e proteger-se proativamente contra ameaças avançadas no Office 365. Insights detalhados sobre as ameaças — disponíveis em parte por causa da presença global da Microsoft, o Intelligent Security Graph, e conhecimentos obtidos dos caçadores de ciberameaças — podem ajudá-lo a ativar rapidamente e com eficiência: alertas, diretivas dinâmicas e soluções de segurança.
- O Gerenciamento Avançado de Segurança permite identificar uso de alto risco ou anormal, alertando-o para potenciais violações. Além disso, ele permite que você organize diretivas de atividades para rastrear e responder às ações de alto risco ou atividade suspeita.

Você também pode obter a descoberta dos aplicativos de produtividade, que permitem que você use as informações dos arquivos de registros da sua organização para compreender e atuar na utilização de aplicativos de usuários no Office 365 e em outros aplicativos em nuvem.

- O Advanced Threat Protection para Exchange Online ajuda a proteger seus e-mails contra novos e sofisticados ataques de malware em tempo real. Ele também permite criar diretivas para ajudá-lo a prevenir que seus usuários acessem anexos ou websites maliciosos conectados por e-mail.

Server SQL e Azure SQL Database

O SQL Server e o Azure SQL Database proporcionam um forte conjunto de recursos integrados que protegem dados e identificam quando uma violação de dados ocorre:

- A Auditoria do Azure SQL Database e a auditoria do SQL Server rastreiam os eventos de bancos de dados e os transcrevem em um log de auditoria. A auditoria permite que você compreenda as atividades de bancos de dados em andamento, análise e investigue o histórico de atividades para identificar ameaças potenciais ou suspeitas de violações de segurança ou abuso.
- O SQL Database Threat Detection detecta atividades anômalas em bancos de dados indicando ameaças de segurança potenciais. O Threat Detection usa um conjunto avançado de algoritmos para continuamente aprender e definir o perfil do comportamento de aplicativo, e notifica imediatamente quando detecta atividades incomuns ou suspeitas. O Threat Detection pode ajudá-lo a adequar-se aos requisitos de notificação de violação de dados da LGPD.

Windows e Windows Server

O Windows Defender Advanced Threat Protection (ATP) permite às suas equipes de operações de segurança detectar, investigar, conter e responder às violações de dados em sua rede. Com o Windows Defender ATP, você obtém recursos avançados de detecção de violação, investigação e resposta em todas as pontas com até 6 meses de dados históricos, mesmo quando um endpoint estiver off-line, fora do domínio da rede, sua imagem tenha sido refeita ou não exista mais. O Windows Defender ATP vai ajudá-lo a atender um requisito chave da LGPD - o de ter procedimentos claros para detectar, investigar e reportar violações de dados.

Reporte: responda às solicitações de dados, reporte as violações de dados e mantenha a documentação necessária.

A LGPD define novos padrões de transparência, responsabilidade e manutenção de registros. Você precisará ser mais transparente, não somente sobre como administra dados pessoais, mas também como ativamente mantém documentos que definam os seus processos e utilização de dados pessoais.

Manutenção de registros

As organizações que processam dados pessoais precisarão manter registros sobre o propósito do processamento; as categorias de dados pessoais processados; a identidade de terceiros com quem os dados são compartilhados; se e quais países recebem dados pessoais e as bases legais para tais transferências; medidas de segurança técnicas e organizacionais; e o tempo de retenção de dados aplicável a vários conjuntos de dados. Uma maneira de fazer isto é usar ferramentas de auditoria, que podem ajudá-lo a garantir que qualquer processamento de dados — a obtenção, o uso, o compartilhamento ou outro motivo — seja registrado e rastreado.

Os serviços em nuvem da Microsoft oferecem serviços de auditoria embutidos que podem ajudá-lo a atender a esta exigência.

Azure, Office 365, e Dynamics 365

No Service Trust Portal, você pode encontrar informações detalhadas sobre as diversas ofertas de conformidade, segurança, privacidade e confiabilidade do Azure, do Office 365 e do Dynamics 365, incluindo relatórios e atestados. Os relatórios de avaliação de auditorias independentes, terceirizadas e de GRC (governança, gerenciamento de risco e conformidade) vão ajudá-lo a se manter atualizado sobre a conformidade dos serviços em nuvem da Microsoft com as normas mundiais que importam para a sua organização. Documentos de confiabilidade podem ajudá-lo a compreender como os serviços em nuvem da Microsoft protegem seus dados e como você pode gerenciar a segurança de dados e conformidade para os seus serviços em nuvem.

Azure

Auditorias e registros de eventos relacionados à segurança e alertas relacionados, são importantes componentes para uma estratégia de proteção de dados eficaz.

Os recursos de auditoria e registros do Azure permitem que você:

- Crie uma trilha de auditorias para os aplicativos empregados no Azure e em máquinas virtuais criadas a partir da Galeria de Máquinas Virtuais do Azure.
- Execute análises centralizadas de grandes conjuntos de dados coletando eventos de segurança a partir da Infraestrutura como um Serviço (IaaS) e Plataforma como um Serviço (PaaS) do Azure. Você poderá então usar o Azure HDInsight para agregar e analisar estes eventos, e exportá-los para sistemas SIEM locais para um monitoramento contínuo.

- Monitore os relatórios de acesso e uso com a vantagem dos registros de operações administrativas do Azure, incluindo acesso ao sistema, para criar uma trilha de auditoria para casos de alterações acidentais ou não autorizadas. Você pode recuperar registros de auditoria para o seu inquilino do Azure Active Directory, e ver os relatórios de acesso e uso.
- Exporte os alertas de segurança para os sistemas SIEM locais usando o Azure Diagnostics, que pode ser configurado para registros de eventos de segurança do Windows e outros registros relacionados à segurança.
- Obtenha ferramentas de monitoramento, relatórios e alertas de segurança de terceiros com o Azure Marketplace.

O Microsoft Azure Monitor permite que as organizações vejam e gerenciem com facilidade todas as suas atividades de monitoramento de dados a partir de um painel central. Você obtém dados sobre utilização e desempenho detalhados e atualizados, acesso ao registro de atividades que rastreia todas as chamadas de API e registros de diagnósticos que vão ajudá-lo a rastrear problemas nos seus recursos do Azure. Além disso, você pode definir alertas e tomar ações automatizadas. O Azure Monitor integra-se às suas ferramentas atuais, assim você obtém monitoramento e análises otimizados, de fim a fim, combinando o Azure Monitor com as ferramentas de análise com que você já está familiarizado.

Office e Office 365

- A Garantia do Serviço na Central de Segurança e Conformidade do Office 365 proporciona insights profundos para conduzir a análise de riscos, com detalhes nos relatórios de conformidade da Microsoft e o status transparente de controles auditados, incluindo:
    - Práticas de segurança da Microsoft para dados de clientes armazenados no Office 365.
    - Relatórios de auditoria de terceiros independentes do Office 365.
    - Detalhes de implementação e testes para a segurança, privacidade e controles de conformidade que ajudam o cliente a adequar-se às normas, leis, e regulamentações em todos os segmentos, tais como ISO 27001 e ISO 27018, bem como o Health Insurance Portability and Accountability Act (HIPAA).
- Os logs de auditoria do Office 365 permitem monitorar e rastrear as atividades de usuários e de administradores em todas as cargas de trabalho do Office 365, o que facilita a detecção e investigação precoce de questões relacionadas à segurança e conformidade. Use a página de busca de logs de auditoria do Office 365 para começar a registrar as atividades de usuários e administradores em sua organização. Assim que o Office 365 prepara o relatório de auditoria, você pode consultá-lo para confirmar uma grande variedade de atividades incluindo uploads para o OneDrive ou SharePoint Online e reconfiguração de senhas de usuários. O Exchange Online pode ser organizado para rastrear alterações feitas por administradores, e rastrear sempre que uma caixa postal é acessada por alguém que não seja o seu dono original.

- O Customer Lockbox oferece para você a autoridade para definir como um engenheiro de suporte da Microsoft pode acessar seus dados durante uma consulta. Nos casos em que o engenheiro requisite acesso aos seus dados para estudar e reparar um erro, o Customer Lockbox permite que você aprove ou rejeite a solicitação de acesso. Se você aprovar, o engenheiro estará apto a acessar os dados. Cada solicitação tem um prazo de validade, e uma vez que o problema esteja resolvido, a solicitação é fechada e o acesso é revogado.

Enterprise Mobility + Security (EMS)

A Proteção de Informações do Azure oferece recursos importantes de controle de log e relatórios para analisar a sensibilidade dos dados distribuídos. O rastreamento de documentos permite aos usuários e administradores monitorar atividades em dados compartilhados e revogar acesso em eventos inesperados. A Proteção de Informações do Azure também oferece recursos de análises de dados não estruturados que residem em compartilhamentos de arquivos, repositórios online e em unidades de disco de desktops e laptops. Com acesso aos arquivos, você pode varrer os conteúdos de cada arquivo e determinar se certas classes de dados pessoais existem nos arquivos. Você pode então classificar e identificar cada arquivo baseado no tipo de dado presente. Além disso, você pode gerar relatórios deste processo, com informações sobre os arquivos escaneados, diretivas de classificação que combinaram e a identificação aplicada.

Windows e Windows Server

O Log de Eventos do Windows proporciona recursos de registro de eventos que permitem aos administradores ver as informações registradas sobre sistemas operacionais, aplicativos e atividades do usuário. Este sistema de registros/log pode ser configurado para auditar ações detalhadas de um usuário ou aplicativo incluindo acesso à arquivos, uso do aplicativo e alterações de diretivas, só para mencionar algumas. O Log de Eventos do Windows também permite aos administradores encaminhar eventos de clientes e servidores para uma localização central para fins de relatórios ou auditoria.

Ferramentas de relatórios e documentação dos serviços em nuvem

Como em todo banco de dados ou sistema administrando dados pessoais, o seu uso de serviços em nuvem deve ser bem registrado e compreendido pela sua organização. Por exemplo, sua organização precisará entender os dados pessoais mantidos por provedores de serviços em nome da sua organização; a relação contratual regendo estes provedores; e o que acontece com os dados quando a relação terminar.

Nós o ajudamos a gerenciar esta informação mantendo ferramentas de relatórios simples e claras sobre sua conta na nuvem da Microsoft, juntamente com extensa documentação sobre nossos serviços em nuvem, como funcionam e nossa relação contratual com você.

Notificando sujeitos de dados

A LGPD mudará os requisitos de proteção de dados e empregará obrigações mais severas para processadores e controladores de dados com relação a avisos de violações de dados pessoais que resultem em riscos aos direitos ou liberdade do indivíduo. Sob a nova regulamentação, como definido no art. 48, o controlador de dados deve notificar a autoridade nacional de proteção de dados responsável em um prazo razoável. Se a violação pode resultar em alto risco aos direitos e liberdade dos indivíduos, os controladores também precisarão notificar os indivíduos afetados imediatamente. Isto significa que se você está usando um processador de dados em sua função como controlador de dados, você precisa se certificar de que tem um conjunto claro de expectativas integradas aos seus contratos sobre notificações de violação potencial.

Para incidentes onde a Microsoft tem alguma ou toda a responsabilidade de responder, nós estabelecemos processos detalhados de gerenciamento de resposta a incidentes de segurança como definidos para o Azure, Office 365 e Dynamics 365. Também sustentamos nosso compromisso com a LGPD em nossa linguagem contratual.

Os produtos e serviços da Microsoft — tais como Azure, Dynamics 365, Enterprise Mobility + Security, Office 365 e Windows 10 — têm soluções disponíveis hoje para ajudá-lo a detectar e avaliar ameaças de segurança e violações e atender às exigências de notificação de violação da LGPD.

Trabalhando com os requisitos de sujeitos de dados

Entre os pontos mais importantes da LGPD estão os direitos dos sujeitos de dados estipulados nos artigos do Capítulo III: Direitos do Titular.

Estas obrigações podem ter implicações no seu ambiente de TI e operações como um controlador de dados, e o ambiente de TI e operações de qualquer provedor de serviços que você utiliza como processador de dados.

A governança de dados adequada tem sido um elemento fundamental das leis de privacidade e encontra apoio na maioria das leis e regulamentos sobre privacidade e proteção de dados. Um elemento chave da governança sob a LGPD é a designação de um Data Protection Officer (DPO) em circunstâncias específicas definidas no art. 41. O DPO precisa estar envolvido em todas as questões relacionadas à proteção de dados pessoais.

Um segundo elemento importante da governança da LGPD é a totalidade da Revisão da Conformidade da Proteção de Dados gerando a Avaliação de Impacto da Proteção de Dados (DPIA), art. 38, parágrafo único, é específico sobre os requisitos de tal relatório, bem como o art. 50, inciso I, que discorre sobre a possibilidade de um programa de governança em privacidade para demonstrar o compromisso do controlador em proteger dados pessoais.

A Central de Confiabilidade da Microsoft oferece informações sobre as maneiras em que você pode sustentar a sua jornada, incluindo uma seção especial sobre as visões e compromissos da Microsoft em relação ao GDPR.