A gestão da proteção de dados pessoais (DP) em nuvens públicas

Redação - Publicado em 04 May 2021

A nuvem pública é definida como uma série de serviços de computação oferecidos por terceiros à internet pública, os quais são disponibilizados a qualquer pessoa que queira utilizá-los ou comprá-los. Eles podem ser gratuitos ou vendidos sob demanda, permitindo que os clientes paguem apenas pelo seu consumo de ciclos de CPU, armazenamento ou largura de banda. Ao contrário das nuvens privadas, as públicas podem poupar as empresas dos enormes gastos de compra, gerenciamento e manutenção e hardware local e infraestrutura de aplicativo. No caso da nuvem pública, o provedor de serviços de nuvem é responsável por todo o gerenciamento e manutenção do sistema. Elas também podem ser implantadas mais rápido do que infraestruturas locais e com uma plataforma quase infinitamente escalonável. Todos os funcionários de uma empresa podem utilizar o mesmo aplicativo de um escritório ou filial usando o dispositivo de sua escolha, contanto que tenham acesso à internet. Embora algumas questões sobre segurança tenham sido levantadas em relação aos ambientes de nuvem pública, quando implantada corretamente, ela pode ser tão segura quanto a implantação de uma nuvem privada com gerenciamento altamente eficaz caso o provedor utilize métodos adequados de segurança, como sistemas de prevenção e detecção de invasão. Com relação ao uso atual de cloud computing no ambiente corporativo, existem três modelos de entrega mais utilizados: nuvem pública, privada e híbrida. Nesse tipo de contrato, a empresa provedora mantém a infraestrutura de TI e aloca seus recursos de computação e armazenamento para vários clientes simultâneos. Um exemplo desse método é o icloud ou o google drive — embora esses sejam primariamente feitos para o uso pessoal. Quando a empresa contrata a nuvem pública, a provedora virtualiza diversos itens, softwares, plataformas e infraestrutura dentro do próprio sistema para uso remoto, de forma totalmente independente e isolada de outros clientes. Recebe-se exatamente o que contratou e pode, quando necessário, diminuir ou aumentar essa oferta. Com a Lei Geral de Proteção de Dados Pessoais (LGPD), mais um desafio se apresentou aos líderes de TI com uma nova etapa na transformação digital – a jornada para a conformidade. Além de recursos desenvolvidos especialmente para atender a normas de proteção de dados, um serviço de nuvem inteligente também deve contar com soluções de identidade e acesso, criptografia, monitoramento, detecção de ameaças, etc. Deve-se entender o os controles e as diretrizes comumente aceitos para implementação de medidas para proteção de dados pessoais (DP), de acordo com os princípios de privacidade, para o ambiente de computação em nuvem pública.

Hayrton Rodrigues do Prado Filho –

Pode-se dizer que os sistemas de tratamento de informações com base no modelo de computação em nuvem introduzem mecanismos adicionais ou alternativos para cópias de segurança em local remoto para proteção contra perda de dados, assegurando a continuidade das operações de tratamento de dados e fornecendo a capacidade de restaurar as operações de tratamento de dados após um evento desastroso. Assim, múltiplas cópias de dados devem ficar em locais fisicamente e/ou logicamente diversos (que podem estar dentro do próprio sistema de tratamento de informações) sejam criadas ou mantidas para fins de cópia de segurança e/ou recuperação.

As responsabilidades específicas de DP a este respeito podem recair sobre o cliente que utiliza os serviços em nuvem. Quando o operador de DP em nuvem pública fornece explicitamente os serviços de cópia de segurança e restauração ao cliente que utiliza serviços em nuvem, o operador de DP em nuvem pública deve fornecer as informações claras ao cliente que utiliza serviços em nuvem sobre as capacidades do serviço em nuvem referentes à cópia de segurança e restauração dos dados do cliente que utiliza serviços em nuvem.

Em consequência, deve-se ter um processo seja implementado para analisar criticamente os registros de eventos com uma periodicidade especificada e documentada, a fim de identificar irregularidades e propor esforços de medidas corretivas.

Quando possível, os registros de eventos devem ser registrados se os DP foram alterados ou não (adicionados, modificados ou excluídos) como resultado de um evento e por quem. Quando vários provedores de serviços forem envolvidos em fornecer serviços das diferentes categorias de serviço da arquitetura de referência de computação em nuvem, pode haver funções variadas ou compartilhadas na implementação destas diretrizes.

O operador de DP em nuvem pública deve dispor de critérios sobre se, quando e como as informações de registros podem ser disponibilizadas ou utilizadas pelo cliente que utiliza serviços em nuvem. Esses procedimentos devem ser disponibilizados ao cliente que utiliza serviços em nuvem.

Quando for permitido que um cliente que utiliza serviços em nuvem acesse os registros controlados pelo operador de DP em nuvem pública, o operador de DP em nuvem pública deve assegurar que o cliente que utiliza serviços em nuvem somente possa acessar os registros que se relacionem às atividades do cliente que utiliza serviços em nuvem e que possa não acessar quaisquer registros que se relacionem às atividades de outros clientes que utilizam serviços em nuvem. Além disso, sempre que mídias físicas forem utilizadas para transferência de informações, convém que um sistema seja implementado para registrar a entrada e a saída de mídia física que contém DP, incluindo o tipo de mídia física, o remetente/destinatários autorizados, a data e hora e a quantidade de mídia física.

Quando possível, convém que os clientes que utilizam serviços em nuvem sejam convidados a implementar medidas adicionais (como criptografia) para assegurar que os dados somente possam ser acessados no ponto de destino e não em transporte. Dessa forma, um incidente de segurança da informação deve provocar uma análise crítica pelo operador de DP em nuvem pública como parte de seu processo de gestão de incidentes de segurança da informação, para determinar se ocorreu uma violação de dados que envolva DP.

Um evento de segurança da informação não deve provocar necessariamente essa análise crítica. Um evento de segurança da informação é aquele que não resulta em probabilidade real ou significativa de acesso não autorizado aos DP ou a quaisquer equipamentos ou instalações do operador de DP em nuvem pública que armazenam DP e que podem incluir, sem limitação, pings e outros ataques de disseminação sobre firewalls ou servidores periféricos, varreduras de portas, tentativas malsucedidas de entrada em sistemas (logon), negação de ataques de serviço e detecção de pacotes.

A **NBR ISO/IEC 27018 de 03/2021 - Tecnologia da informação - Técnicas de segurança - Código de prática para proteção de dados pessoais (DP) em nuvens públicas que atuam como operadores de DP** estabelece objetivos de controle, controles e diretrizes comumente aceitos para implementação de medidas para proteção de dados pessoais (DP), de acordo com os princípios de privacidade descritos na NBR ISO/IEC 29100, para o ambiente de computação em nuvem pública. Em particular, este documento especifica diretrizes com base na NBR ISO/IEC 27002, levando em consideração os requisitos regulatórios para a proteção de DP que podem ser aplicáveis dentro do contexto do (s) ambiente (s) de risco de segurança da informação de um provedor de serviços em nuvem pública.

Este documento é aplicável a todos os tipos e tamanhos de organizações, incluindo empresas públicas e privadas, entidades governamentais e organizações sem fins lucrativos, que fornecem serviços de tratamento de informações, como operadores de DP, por meio da computação em nuvem sob contrato para outras organizações. As diretrizes deste documento também podem ser pertinentes para organizações que atuam como controladores de DP. Os controladores de DP, entretanto, podem estar sujeitos à legislação, regulamentos e obrigações adicionais de proteção de DP, não aplicáveis aos operadores de DP. Este documento não se destina a abranger estas obrigações adicionais.

Os provedores de serviços em nuvem que tratam dados pessoais (DP) sob contrato com seus clientes têm que operar seus serviços de forma a permitir que ambas as partes atendam aos requisitos da legislação e aos regulamentos aplicáveis que abrangem a proteção de DP. Os requisitos e a forma como os requisitos são divididos entre o provedor de serviços em nuvem e seus clientes variam de acordo com a jurisdição legal e de acordo com os termos do contrato entre o provedor de serviços em nuvem e o cliente.

A legislação, que regula como os DP podem ser tratados (ou seja, coletados, utilizados, transferidos e descartados), é algumas vezes referida como legislação de proteção de dados. Os DP são algumas vezes referidos como dados pessoais ou informações pessoais. As obrigações que incidem sobre um operador de DP variam de jurisdição para jurisdição, sendo um desafio para as empresas que fornecem serviços de computação em nuvem os operarem multinacionalmente.

Um provedor de serviços em nuvem pública é um operador de DP quando ele trata DP de acordo com as instruções de um cliente que utiliza serviços em nuvem. O cliente que utiliza serviços em nuvem, que tem o relacionamento contratual com o operador de DP em nuvem pública, pode variar de uma pessoa física, um titular de DP, tratando sua própria DP na nuvem, até uma organização, um controlador de DP, que trata o DP relativo a muitos titulares de DP.

O cliente que utiliza serviços em nuvem pode autorizar um ou mais usuários para serviço em nuvem associados a ele a utilizar os serviços disponibilizados sob seu contrato com o operador de DP em nuvem pública. Observar que o cliente que utiliza serviços em nuvem tem autoridade sobre o tratamento e uso dos dados.

Um cliente que utiliza serviços em nuvem, que também é um controlador de DP, pode estar sujeito a um conjunto mais amplo de obrigações que regulam a proteção de DP do que o operador de DP em nuvem pública. A manutenção da distinção entre o controlador de DP e o operador de DP depende de o operador de DP em nuvem pública não ter objetivos de tratamento de dados diferentes dos estabelecidos pelo cliente que utiliza serviços em nuvem em relação ao DP que ele trata e às operações necessárias para atingir os objetivos do cliente que utiliza serviços em nuvem.

Quando o operador de DP em nuvem pública estiver tratando de dados da conta do cliente que utiliza serviços em nuvem, ele pode estar atuando como um controlador de DP para esta finalidade. Este documento não abrange esta atividade. A intenção deste documento, quando utilizado em conjunto com os objetivos e controles de segurança da informação descritos na NBR ISO/IEC 27002, é criar um conjunto comum de categorias e controles de segurança que possam ser implementados por um provedor de serviços de computação em nuvem pública que atua como um operador de DP.

Este documento tem os seguintes objetivos: auxiliar o provedor de serviços em nuvem pública a atender às obrigações aplicáveis ao atuar como um operador de DP, se estas obrigações incidirem sobre o operador de DP diretamente ou por contrato; permitir que o operador de DP em nuvem pública seja transparente em assuntos relevantes, de modo que os clientes possam selecionar serviços de tratamento de DP baseados em nuvem bem controlados; auxiliar o cliente que utiliza serviços em nuvem e o operador de DP em nuvem pública a realizarem um acordo contratual; prover aos clientes que utilizam serviços em nuvem um mecanismo para o exercício de direitos e responsabilidades de auditoria e conformidade, nos casos em que auditorias individuais do cliente que utiliza serviços em nuvem de dados hospedados em um ambiente de servidor virtualizado (nuvem) com várias partes possam ser impraticáveis tecnicamente e possam aumentar os riscos a estes controles de segurança de rede física e lógica no local.

Este documento pode auxiliar ao prover uma estrutura de conformidade comum para os provedores de serviços em nuvem pública, especialmente aqueles que operam em um mercado multinacional. Ele é projetado para que as organizações o utilizem como uma referência para selecionar controles de proteção de DP dentro do processo de implementação de um sistema de gestão de segurança da informação de computação em nuvem, com base na NBR ISO/IEC 27001, ou como documento de orientação para implementação de controles de proteção de DP comumente aceitos por organizações que atuam como operadores de DP em nuvem pública.

Em particular, este documento foi baseado na NBR ISO/IEC 27002, levando em consideração o (s) ambiente (s) de risco específico (s) decorrente (s) dos requisitos de proteção de DP que podem ser aplicados aos provedores de serviços de computação em nuvem pública que atuam como operadores de DP. Normalmente, uma organização que implementa a NBR ISO/IEC 27001 está protegendo seus próprios ativos de informação.

Entretanto, no contexto dos requisitos de proteção de DP para um provedor de serviços em nuvem pública que atua como um operador de DP, a organização está protegendo os ativos de informação que são confiados a ela pelos seus clientes. A implementação dos controles da NBR ISO/IEC 27002 pelo operador de DP em nuvem pública é adequada para esta finalidade e necessária.

Este documento incrementa os controles da NBR ISO/IEC 27002 para acomodar a natureza distribuída do risco e a existência de uma relação contratual entre o cliente que utiliza serviços em nuvem e o operador de DP em nuvem pública. Este documento incrementa os controles da NBR ISO/IEC 27002 de duas maneiras: as diretrizes para implementação aplicáveis à proteção de DP em nuvem pública são providas para determinados controles existentes na NBR ISO/IEC 27002; e o Anexo A que fornece um conjunto de controles adicionais e diretrizes associadas, destinados a tratar dos requisitos de proteção de DP em nuvem pública não abordados pelo conjunto de controle existente na NBR ISO/IEC 27002.

A maioria dos controles e diretrizes deste documento também se aplicará a um controlador de DP. Entretanto, o controlador de DP, na maioria dos casos, estará sujeito às obrigações adicionais não especificadas neste documento. É essencial que uma organização identifique seus requisitos para a proteção de DP.

Existem três fontes principais de requisitos, conforme descrito a seguir. Os requisitos legais, estatutários, regulatórios e contratuais, em que uma fonte é representada pelos requisitos e obrigações legais, estatutários, regulatórios e contratuais que uma organização, seus parceiros comerciais, contratados e provedores de serviços têm que atender, e suas responsabilidades socioculturais e seu ambiente operacional.

Convém observar se a legislação, regulamentos e cláusulas contratuais realizados pelo operador de DP podem requerer a seleção de controles específicos e também podem necessitar de critérios específicos para a implementação destes controles. Estes requisitos podem variar de uma jurisdição para outra.

Os riscos que são outras fontes derivadas da avaliação de riscos à organização associados aos DP, levando em consideração a estratégia e os objetivos globais de negócio da organização. Por meio de uma avaliação de riscos, as ameaças são identificadas, a vulnerabilidade e a probabilidade de ocorrência são avaliadas e o impacto potencial é estimado.

A NBR ISO/IEC 27005 fornece as diretrizes sobre a gestão de riscos na segurança da informação, incluindo recomendações sobre a avaliação do risco, aceitação do risco, comunicação do risco, monitoramento do risco e análise crítica do risco. A NBR ISO/IEC 29134 fornece diretrizes sobre a avaliação do impacto de privacidade.

Quanto às políticas corporativas, enquanto muitos aspectos abrangidos por uma política corporativa são derivados de obrigações legais e socioculturais, uma organização também pode escolher, voluntariamente, ir além dos critérios que são derivados dos requisitos legais. Os controles podem ser selecionados deste documento (que inclui, por referência, os controles da NBR ISO/IEC 27002, criando um conjunto combinado de controle de referência para o setor ou aplicação especificado pelo escopo).

Se requerido, os controles também podem ser selecionados de outros conjuntos de controle, ou novos controles podem ser projetados para atender a necessidades específicas, conforme apropriado. Um serviço de tratamento de DP fornecido por um operador de DP em nuvem pública pode ser considerado uma aplicação de computação em nuvem em vez de um setor por si só. Entretanto, o termo específicos do setor é utilizado neste documento, uma vez que este é o termo convencional utilizado em outras normas da série ISO/IEC 27000.

A seleção de controles depende de decisões organizacionais com base nos critérios para aceitação do risco, nas opções para tratamento do risco e na abordagem geral da gestão de riscos aplicada à organização, e de acordos contratuais, de seus clientes e de seus fornecedores. A seleção de controles também está sujeita aos regulamentos e legislações nacionais e internacionais pertinentes.

Quando os controles neste documento não forem selecionados, é necessário que esta informação seja documentada, com justificativa pela omissão. Além disso, a seleção e a implementação de controles dependem da função real do provedor de nuvem pública no contexto de toda a arquitetura de referência de computação em nuvem (ver ISO/IEC 17789). Muitas organizações diferentes podem ser envolvidas no fornecimento de serviços de infraestrutura e de aplicação em um ambiente de computação em nuvem.

Em algumas circunstâncias, os controles selecionados podem ser exclusivos para uma categoria de serviço específica da arquitetura de referência de computação em nuvem. Em outros casos, pode haver funções compartilhadas na implementação de controles de segurança. Os acordos contratuais precisam especificar claramente as responsabilidades de proteção de DP de todas as organizações envolvidas em prover ou utilizar os serviços em nuvem, incluindo o operador de DP em nuvem pública, seus subcontratados e o cliente que utiliza serviços em nuvem.

Os controles neste documento podem ser considerados princípios de diretrizes e aplicáveis à maioria das organizações. Eles são explicados com mais detalhes a seguir, juntamente com as diretrizes para implementação. A implementação pode ser simplificada se os requisitos para a proteção de DP tiverem sido considerados no projeto do sistema de informações, serviços e operações do operador de DP em nuvem pública. Esta consideração é um elemento do conceito que é muitas vezes denominado Privacidade por Projeto.

Este documento pode ser considerado um ponto de partida para o desenvolvimento de diretrizes de proteção de DP. É possível que nem todos os controles e diretrizes contidos neste código de prática sejam aplicáveis. Além disso, controles e diretrizes adicionais não incluídos neste documento podem ser requeridos.

Quando documentos forem desenvolvidos contendo diretrizes ou controles adicionais, pode ser útil incluir referências cruzadas às Seções deste documento, quando aplicável, para facilitar a verificação da conformidade por auditores e parceiros de negócio. Os DP têm um ciclo de vida

natural, desde a sua criação e origem, armazenamento, tratamento, uso e transmissão, até a sua eventual destruição ou obsolescência.

Os riscos aos DP podem variar durante o seu tempo de vida, porém a proteção de DP permanece importante em algumas etapas de todos os estágios. Os requisitos de proteção de DP precisam ser levados em consideração quando os sistemas de informações existentes e novos forem gerenciados por meio do seu ciclo de vida. Este documento possui uma estrutura similar à da NBR ISO/IEC 27002.

Nos casos em que os objetivos e controles especificados na NBR ISO/IEC 27002 são aplicáveis sem a necessidade de quaisquer informações adicionais, somente uma referência à NBR ISO/IEC 27002 é fornecida. Controles adicionais e diretrizes para implementação associadas, aplicáveis à proteção de DP para provedores de serviços de computação em nuvem, são descritos no Anexo A.

Nos casos em que os controles necessitam de orientações adicionais aplicáveis à proteção de DP para provedores de serviços de computação em nuvem, isto é provido sob o título Orientações para implementação da proteção de DP em nuvem pública. Em alguns casos, outras informações relevantes que incrementem as orientações adicionais são fornecidas, sob o título outras informações para proteção de DP em nuvem pública.

Conforme mostrado na tabela abaixo, estas orientações e informações específicas do setor estão incluídas nas categorias especificadas na NBR ISO/IEC 27002. Os números das Seções, que foram alinhados com os números das Seções correspondentes na NBR ISO/IEC 27002, estão indicados na tabela abaixo. Este documento deve ser utilizado em conjunto com a NBR ISO/IEC 27001, e os controles adicionais especificados no Anexo A devem ser considerados para adoção como parte do processo de implementação de um sistema de gestão de segurança da informação baseado na NBR ISO/IEC 27001.

Localização das diretrizes específicas do setor e outras informações para implementação de controles

Número da Seção	Título	Observações
5	Políticas de segurança da informação	Diretrizes para implementação específicas do setor e outras informações são providas.
6	Organização da segurança da informação	Diretrizes para implementação específicas do setor são providas.
7	Segurança em recursos humanos	Diretrizes para implementação específicas do setor e outras informações são providas.
8	Gestão de ativos	Diretrizes adicionais para implementação específicas do setor ou outras informações não são providas.
9	Controle de acesso	Diretrizes para implementação específicas do setor são providas, juntamente com uma referência cruzada do(s) controle(s) no Anexo A.
10	Criptografia	Diretrizes para implementação específicas do setor são providas.
11	Segurança física e do ambiente	Diretrizes para implementação específicas do setor são providas, juntamente com uma referência cruzada do(s) controle(s) no Anexo A.
12	Segurança nas operações	Diretrizes para implementação específicas do setor são providas.
13	Segurança nas comunicações	Diretrizes para implementação específicas do setor são providas, juntamente com uma referência cruzada do(s) controle(s) no Anexo A.
14	Aquisição, desenvolvimento e manutenção de sistemas	Diretrizes adicionais para implementação específicas do setor ou outras informações não são providas.
15	Relacionamento na cadeia de suprimento	Diretrizes adicionais para implementação específicas do setor ou outras informações não são providas.
16	Gestão de incidentes de segurança da informação	Diretrizes para implementação específicas do setor são providas.
17	Aspectos de segurança da informação na gestão da continuidade do negócio	Diretrizes adicionais para implementação específicas do setor ou outras informações não são providas.
18	Conformidade	Diretrizes para implementação específicas do setor são providas, juntamente com uma referência cruzada do(s) controle(s) no Anexo A.

De acordo com a NBR ISO/IEC 27002, cada categoria de controle principal contém: um objetivo do controle, declarando o que é para ser alcançado; e um ou mais controles que podem ser aplicados para alcançar o objetivo do controle. As descrições do controle estão estruturadas conforme o descrito a seguir.

O controle estabelece a declaração de controle específica para atender ao objetivo do controle. As diretrizes para implementação da proteção de DP em nuvem pública proveem informações mais detalhadas para apoiar a implementação do controle e atender aos objetivos do controle.

As diretrizes podem não ser totalmente adequadas ou suficientes em todas as situações e podem não atender aos requisitos específicos de controle da organização. Os controles alternativos ou adicionais, ou outras formas de tratamento de risco (evitando, transferindo ou aceitando riscos) podem, portanto, ser apropriados.

Outras informações para proteção de DP em nuvem pública proveem informações adicionais que podem ser consideradas, como considerações legais e referências a outras normas. O controle e as diretrizes para implementação associadas e outras informações especificadas na NBR ISO/IEC 27002 são aplicáveis. As seguintes diretrizes específicas do setor também são aplicáveis.

Para as diretrizes para implementação da proteção de DP em nuvem pública, convém que as políticas de segurança da informação sejam incrementadas por uma declaração referente ao suporte e comprometimento em atingir o compliance com a legislação e os termos contratuais de proteção de DP aplicáveis acordados entre o operador de DP em nuvem pública e seus clientes (clientes que utilizam serviços em nuvem).

Convém que os acordos contratuais atribuam claramente as responsabilidades entre o operador de DP em nuvem pública, seus subcontratados e o cliente que utiliza serviços em nuvem, levando em consideração o tipo de serviço em nuvem em questão (por exemplo, um serviço de uma categoria IaaS, PaaS ou SaaS da arquitetura de referência de computação em nuvem).

Por exemplo, a atribuição de responsabilidade pelos controles da camada de aplicação pode diferir, dependendo se o operador de DP em nuvem pública está fornecendo um serviço de SaaS ou, em vez disso, está fornecendo um serviço de PaaS ou IaaS sobre o qual o cliente que utiliza serviços em nuvem pode construir ou estender em camadas suas próprias aplicações. Em algumas jurisdições, o operador de DP em nuvem pública está diretamente sujeito à legislação de proteção de DP.

Em outros locais, a legislação de proteção de DP é aplicável somente ao controlador de DP. Um mecanismo para assegurar que o operador de DP em nuvem pública está obrigado a apoiar e gerenciar o compliance é provido pelo contrato entre o cliente que utiliza serviços em nuvem e o operador de DP em nuvem pública.

O contrato pode requerer conformidade com auditoria independente, aceitável ao cliente que utiliza serviços em nuvem, por exemplo, por meio da implementação dos controles pertinentes neste documento e na NBR ISO/IEC 27002. Para as diretrizes para implementação da proteção de DP em nuvem pública, convém que medidas sejam implementadas para conscientizar os funcionários da organização, quando pertinente, sobre as possíveis consequências ao operador de DP em nuvem pública (por exemplo, consequências legais, perda de negócio e danos à marca ou de reputação), ao membro da equipe (por exemplo, consequências disciplinares) e ao titular de DP (por exemplo, consequências físicas, materiais e emocionais) na violação das regras e

procedimentos de privacidade ou de segurança, especialmente aqueles que tratam da manipulação de DP.

Para as outras informações para proteção de DP em nuvem pública, em algumas jurisdições, o operador de DP em nuvem pública pode estar sujeito a sanções legais, incluindo multas substanciais diretamente da autoridade local de proteção de DP. Em outras jurisdições, convém que o uso de normas como este documento, na preparação do contrato entre o operador de DP em nuvem pública e o cliente que utiliza serviços em nuvem, auxilie a estabelecer uma base para sanções contratuais por violação de regras e procedimentos de segurança.

No contexto das categorias de serviço da arquitetura de referência de computação em nuvem, o cliente que utiliza serviços em nuvem pode ser responsável por alguns ou todos os aspectos do gerenciamento de acesso para usuários que utilizam serviços em nuvem sob seu controle. Quando apropriado, convém que o operador de DP em nuvem pública permita que o cliente que utiliza serviços em nuvem gerencie o acesso dos usuários sob seu controle, por exemplo, fornecendo direitos administrativos para gerenciar ou encerrar o acesso.

Convém que os procedimentos para registro e cancelamento do usuário tratem a situação quando o controle de acesso do usuário estiver comprometido, como a corrupção ou o comprometimento de senhas ou outros dados de registro do usuário (por exemplo, como resultado de uma divulgação involuntária). As jurisdições individuais podem impor requisitos específicos relativos à frequência de verificações para credenciais de autenticação não utilizadas.

Convém que as organizações que operam nessas jurisdições assegurem que elas atendam a estes requisitos. Convém que o operador de DP em nuvem pública forneça informações ao cliente que utiliza serviços em nuvem referentes às circunstâncias em que ele utiliza a criptografia para proteger os DP que ele trata.

Convém que o operador de DP em nuvem pública também forneça informações ao cliente que utiliza serviços em nuvem sobre quaisquer capacidades que ele fornece que possam auxiliar o cliente que utiliza serviços em nuvem a aplicar sua própria proteção criptográfica. Em algumas jurisdições, pode ser requerido aplicar a criptografia para proteger tipos específicos de DP, como dados de saúde relativos a um titular de DP, números de registro de residentes, números de passaporte e números de licença de motorista.

Como citar esse artigo:

PRADO FILHO, Hayrton Rodrigues do. A gestão da proteção de dados pessoais (DP) em nuvens públicas. REVISTA DIGITAL AdNORMAS, ano 4, n. 157, maio 2021.

Disponível em: https://www.revistaadnormas.com.br/2021/05/04/a-gestao-da-protecao-de-dados-pessoais-dp-em-nuvens-publicas