华为云巴西金融行业监管遵从性指南

文档版本 3.0

发布日期 2024-09-30

华为云计算技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为云计算技术有限公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为云计算技术有限公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为云计算技术有限公司

地址： 贵州省贵安新区黔中大道交兴功路华为云数据中心 邮编：550029

网址： https://www.huaweicloud.com/intl/zh-cn

目 录

1 概述

1.1 背景与发布目的

随着技术的发展，对云计算的使用已经成为巴西金融机构的常态。云计算为金融机构的发展带来巨大的好处，但它也为金融机构创造了一个复杂的环境。为规范金融行业对于信息科技的运用，巴西国家货币委员会（The National Monetary Council，简称 CMN）和巴西中央银行（The Central Bank of Brazil，简称 BCB）发布了一系列监管要求，针对巴西金融机构的网络安全、信息技术风险管理等方面提供了相关监管要求。另外，巴西政府的第 8.771 号法令针对执行数据处理活动的实体提出了数据安全准则，巴西金融机构同样需要遵守该法令要求。

华为云作为云服务供应商，致力于协助金融客户满足这些监管要求，持续为金融客户提供遵从金融行业标准要求的云服务及业务运行环境。本文将针对巴西金融机构在使用云服务时通常需遵循的监管要求，详细阐述华为云将如何协助其满足监管要求。

1.2 适用的巴西金融监管要求简介

巴西国家货币委员会（CMN）

- **2021 年 2 月 26 日第 4.893 号决议（Resolution 4.893）**：本决议于 2021 年 7 月 1 日生效，规定了网络安全政策以及获得巴西中央银行许可的金融机构应遵守的数据处理、数据存储和云计算合同服务的要求。本决议废止并取代 2018 年 4 月 26 日第 4.658 号决议和 2019 年 9 月 26 日第 4.752 号决议。

巴西中央银行（BCB）

- **2021 年 4 月 28 日第 85 号决议（Resolution 85）**：本决议自 2021 年 8 月 1 日起生效，明确了巴西中央银行授权的支付机构应遵守的数据处理和存储以及云计算服务的网络安全政策和要求。本决议撤销 2018 年 8 月 16 日第 3.909 号决议和 2019 年 11 月 13 日第 3.969 号决议。

巴西政府

- **2016 年 5 月 11 日第 8.771 号法令（Decree 8.771）**：该法令规范了 2014 年 4 月 23 日第 12.965 号法律（互联网民事框架或“互联网民事框架”）文件，并提供了执行

数据处理活动的实体应遵守的数据安全准则，这些准则侧重于控制对个人数据的访问以及加密或等效保护措施的使用。

1.3 名词定义

- **华为云**

  华为云是华为的云服务品牌，致力于提供稳定可靠、安全可信、可持续创新的云服务。

- **服务提供商**

  根据外包安排向金融机构提供服务的实体以及实体的分支机构。

- **云计算**

  是指用一种模式，用于通过自助服务配置和按需管理，使网络能够访问可扩展且弹性的可共享物理或虚拟资源池（例如服务器、操作系统、网络、软件、应用程序和存储设备）。

- **客户内容数据**

  客户使用华为云服务过程中存储或处理的内容，包括但不限于数据、文件、软件、图像、音频、视频等类型的数据。

2 华为云安全与隐私合规

华为云继承了华为公司完备的管理体系以及 IT 系统的建设和运营经验，对华为云各项服务的集成、运营及维护进行主动管理，并持续改进。截至目前，华为云已获得**众多**全球性、区域性和行业特定的安全合规的权威认证，全力保障客户部署业务的安全。

关于更多华为云的安全合规信息以及获取相关合规证书，可参见华为云官网**“信任中心-合规中心”华为云部分标准类认证/鉴证示例：**

认证	描述
ISO27001	ISO27001 是目前国际上被广泛接受和应用的信息安全管理体系认证标准。该标准以风险管理为核心，通过定期评估风险和对应的控制措施来有效保证组织信息安全管理体系的持续运行。
ISO27017	ISO27017 是针对云计算信息安全的国际认证。ISO27017 的通过，表明华为云在信息安全管理能力达到了国际公认的最佳实践。
ISO27018	ISO27018 是专注于云中个人数据保护的国际行为准则。ISO27018 的通过，表明华为云已满足国际认可的公有云个人数据保护措施的要求，可保证客户个人数据安全。
TL 9000& ISO 9001	ISO 9001 是 ISO 9000 族标准所包括的一组质量管理体系核心标准之一，用于证实组织具有提供满足顾客要求和适用法规要求的产品的能力。 TL 9000 是一个建立在 ISO9001 基础上的，由全球电信业优质供应商联盟（QuEST Forum）针对全球信息和通讯技术（ICT）行业特定设计的、为 ICT 产品和服务供方提供的一套通用的质量管理体系要求。它包括了 ISO9001 的所有要求，ISO9001 将来的任何改动也会导致 TL9000 的改动。 华为云取得了 ISO9001 / TL9000 认证证书，表明华为云可以为您提供更快，更好和更具成本效益的服务。
ISO20000-1	ISO20000 是针对信息技术服务管理领域的国际标准，提供设计、建立、实施、运行、监控、评审、维护和改进服务管理体系的模型以保证服务供应商可提供有效的 IT 服务来满足

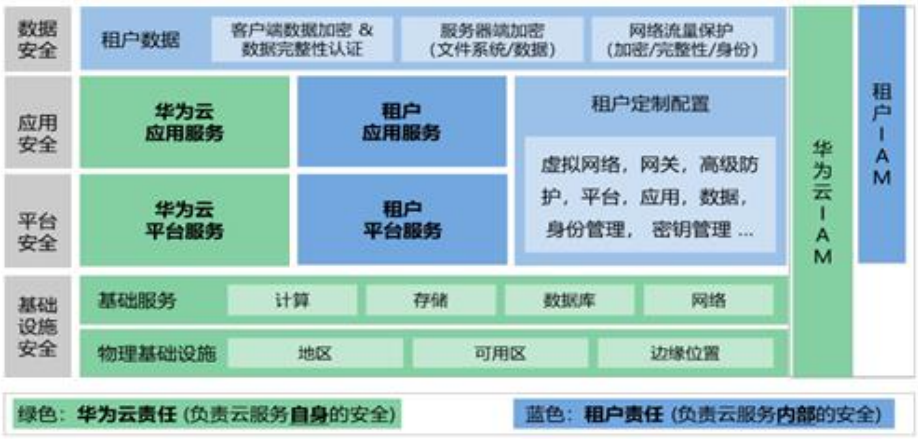
认证	描述
	客户和业务的需求。
ISO22301	ISO22301 是国际公认的业务连续性管理体系标准，通过对风险的识别、分析和预警来帮助组织规避潜在事件的发生，并且制定完备的“业务连续性计划”，有效地应对中断发生后的快速恢复，保持核心功能正常运行，将损失和恢复成本降至最低。
CSA STAR 认证	CSA STAR 认证是由标准研发机构 BSI（英国标准协会）和 CSA（云安全联盟）合作推出的国际范围内的针对云安全水平的权威认证，旨在应对与云安全相关的特定问题，协助云计算服务商展现其服务成熟度的解决方案。
ISO27701	ISO27701 规定了建立、实施、维护和持续改进隐私相关所特定的管理体系的要求。华为云通过 ISO27701 表明了其在个人数据保护具有健全的体制。
BS 10012	BS10012 是 BSI 发布的个人信息数据管理体系标准，BS10012 认证的通过表明华为云在个人数据保护上拥有完整的体系以保证个人数据安全。
ISO 29151	ISO29151 是国际个人身份信息保护实践指南。ISO29151 的通过，表明华为云实施国际认可的个人数据处理的全生命周期的管理措施。
PCI DSS	支付卡行业数据安全标准（PCI DSS）是由 JCB、美国运通、Discover、万事达和 Visa 等五家国际信用卡组织共同建立的一套支付卡行业数据安全标准，由支付卡行业安全标准委员会管理。它是世界上最权威、最严格的金融机构认证。
PCI 3DS	PCI 3DS 标准，旨在保护执行特定 3DS 功能或者存储 3DS 数据的 3DS 环境，支持 3DS 的实施。PCI 3DS 的评估对象为 3D 协议执行环境，包括访问控制服务器、目录服务器或 3DS 服务器功能；以及 3D 执行环境内和连接到环境所需要的系统组件，如防火墙、虚拟服务器、网络设备、应用等；除此之外，还会评估 3D 协议执行环境的过程、流程、人员管理等。
ISO 27799:2016	ISO/IEC 27799 是专注于医疗行业的信息安全管理体系，为医疗行业和其相关机构提供了关于如何更好地保护个人健康信息的保密性、完整性、可审计性和可用性的指导。 华为云是全球首个获得该认证的云服务商，表明华为云对医疗行业的理解和实践，对医疗行业信息安全的防护能力得到国际权威认可，能够更可靠的保障您的信息安全。
ISO 27034	ISO/IEC 27034 是国际标准化组织 ISO 通过的第一个关注建立安全软件程序流程和框架的标准，它清晰地定义了实际应用中软件系统面临的风险，同时为不同类型的软件开发组织提供了一套可以灵活应用的方法。华为云是全球首家获得

认证	描述
	ISO/IEC 27034 认证的云服务提供商，表明华为云具备在云服务中保持持续安全和合规的能力。
SOC 审计报告	SOC 审计报告是由第三方审计机构根据美国注册会计师协会（AICPA）制定的相关准则，针对外包服务商的系统和内部控制情况出具的独立审计报告。

3 华为云安全责任共担模型

在复杂的云服务业务模式中，云安全不再是某一方单一的责任，需要租户与华为云共同努力。基于此，华为云为帮助租户理解双方的安全责任边界、避免出现安全责任真空区而提出了责任共担模型。在模型中租户与华为云具体负责的区域可参见下图。

图 3-1 华为云责任共担模型



基于责任共担模型，华为云与租户主要承担如下责任：

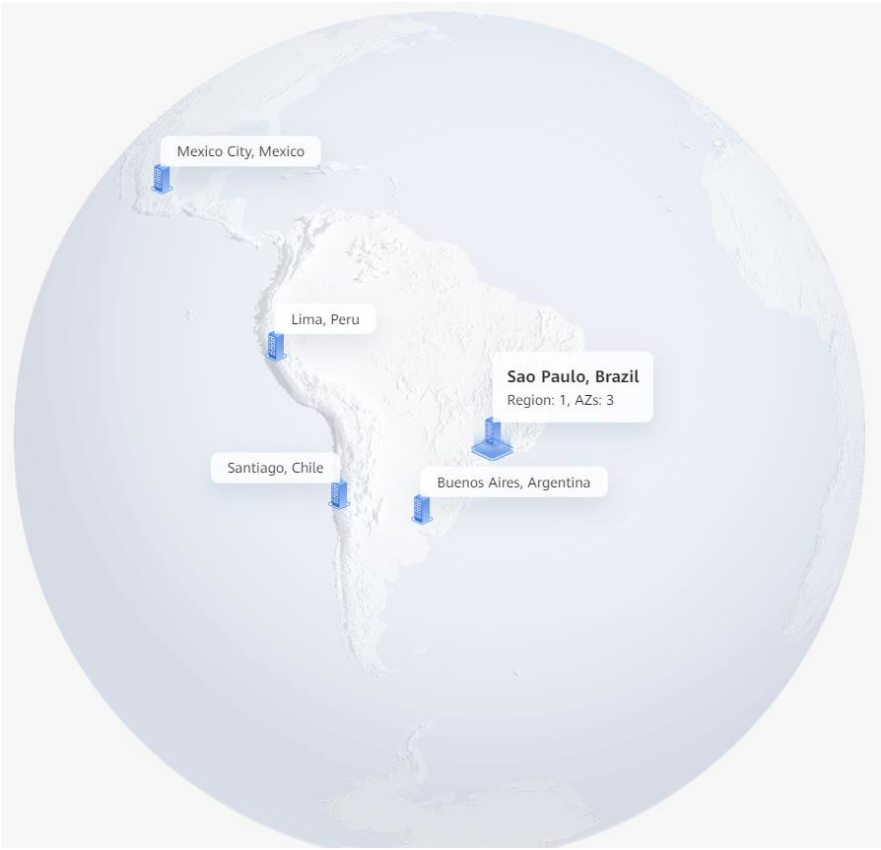
华为云：主要责任是研发并运维运营华为云数据中心的物理基础设施，华为云提供的各项基础服务、平台服务和应用服务，也包括各项服务内置的安全功能。同时，华为云还负责构建物理层、基础设施层、平台层、应用层、数据层和用户身份管理（IAM）层的多维立体安全防护体系，并保障其运维运营安全。

租户：主要责任是在租用的华为云基础设施与服务之上定制配置并且运维运营其所需的虚拟网络、平台、应用、数据、管理、安全等各项服务，包括对华为云服务的定制配置和对租户自行部署的平台、应用、用户身份管理等服务的运维运营。同时，租户还负责其在虚拟网络层、平台层、应用层、数据层和 IAM 层的各项安全防护措施的定制配置、运维运营安全、以及用户身份的有效管理。

关于华为云与租户的安全责任详情，可参考华为云已发布的《华为云安全白皮书》。

4 华为云全球基础设施

华为云目前已陆续在全球多个国家或地区开服。华为云的基础设施采用在全球部署多个地理区域（Region）和多可用区（AZ）的模式，华为云能够在多个地理区域内或同一地域内多个可用区之间灵活替换计算实例和存储数据，每个可用区都是一个独立故障维护域，也就是各可用区物理上是隔离的。在巴西，华为云已部署“LA-Sao Paulo1”Region，拥有 3 个可用区（AZ）。用户可充分利用这些地理区域和可用区，规划应用系统在云上的部署和运行。基于多个可用区进行应用的分布式部署，可保证在大多故障情况下系统都能连续运行。关于更多关于华为云基础设施的信息，参见华为云官网**“全球基础设施”**。



5 华为云如何遵从及协助客户满足 CMN《第 4.893 号决议》和 BCB《第 85 号决议》的要求

巴西国家货币委员会于 2021 年 2 月 26 日发布了《第 4.893 号决议》。该决议从网络安全政策、数据处理、数据存储和云计算服务的外包、通用要求等领域提出对**巴西中央银行许可的金融机构**的网络安全管理相关要求。

巴西中央银行于 2021 年 4 月 8 日发布了《第 85 号决议》。该决议规定了巴西中央银行授权的支付机构应遵从的网络安全政策和数据处理和存储以及云计算服务的要求。

金融机构在遵循《第 4.893 号决议》和《第 85 号决议》要求时，华为云作为云服务供应商，可能会参与到要求所涉及的部分活动中。以下内容将总结《第 4.893 号决议》和《第 85 号决议》中与云服务供应商相关的控制要求，并阐述华为云作为云服务供应商，会如何帮助金融机构满足这些控制要求。

注：《第 4.893 号决议》和《第 85 号决议》除适用对象不同之外，与云服务提供商相关的控制要求的条款编号以及内容基本一致。因此，针对华为云作为云服务提供商如何遵从及协助金融机构满足这些要求，在本章节进行合并阐述。

5.1 网络安全政策

原文编号	控制域	具体控制要求	华为云的应答
2、3	网络安全政策的实施	2.金融机构必须实施并维护旨在确保所使用数据和信息系统的保密性、完整性和可用性的原则和指南的网络安全政策。 3. 网络安全政策至少必须包括： I-机构的网络安全目标； II-为减少机构对事件	客户应制定并实施网络安全政策，明确网络安全目标、信息安全措施、事件管理流程、业务连续性管理流程、数据分类标准等。作为云服务提供商，华为云参照 ISO27001 构建了完善的信息安全管理体系，制定了华为云整体的信息安全策略，其中明确了信息安全管理组织的架构与职责，信息安全体系文件的管理办法，以及信息安全的重点关注方向和目标，包括：资产安全、访问控制、密码学、物理安全、操作安全、通信安全、系统开

原文编号	控制域	具体控制要求	华为云的应答
		的脆弱性和解决其他网络安全目标而采取的程序和控制； III-具体的控制措施，包括针对信息可追溯性的控制措施，旨在确保敏感信息的安全性； IV-记录、分析原因和影响，以及控制与机构活动相关的事件的影响； V-下列指引：a）制定反映业务连续性测试中考虑的事件的场景；b）定义了针对预防和处理事件的程序和控制措施，这些程序和控制应由处理敏感数据或信息或与机构的运营活动相关的第三方提供商采用；c）根据数据和信息的相关性对其进行分类。 d) 定义用于评估事件相关性的参数： VI - 在机构内传播网络安全文化的机制 VII - 主动与第 IV 节中提到的其他机构分享有关相关事件的信息	发安全、供应商管理、信息安全事件管理、以及业务连续性。全方位保护客户系统和数据的保密性、完整性和可用性。
6、9、10	事件的行动和响应计划	6.金融机构必须制定事件的行动和响应计划，以保障网络安全政策的执行。 9.第 2 条所述的网络安全政策以及第 6 条所述事件的行动和响应计划必须得到董事会的批准，如果没有董事会，则须经高级	客户应制定事件的行动和响应计划，并得到董事会的批准。另外，定期对网络安全政策和事件的行动和响应计划进行更新。作为云服务提供商： **（1）**华为云内部制定了安全事件管理机制，并持续优化该机制。安全事件响应流程清晰定义了在事件响应过程中负责各个活动的角色和职责。华为云日志大数据分析系统具备海量日志快速收集、处理、实时分析的能力，

原文编号	控制域	具体控制要求	华为云的应答
		管理层批准。 10. 网络安全政策和事件的行动和响应计划必须至少每年记录并修订一次。	支持与第三方安全信息和事件管理系统如 ArcSight、Splunk 对接。该系统统一收集所有物理设备、网络、平台、应用、数据库和安全系统的管理行为日志和各安全产品及组件的威胁检测告警日志，持续的监控和实时分析保证对安全事件的及时发现。此外鉴于安全事件处理的专业性和紧迫性，华为云拥有 7*24 的专业安全事件响应团队以及对应的安全专家资源池来应对。华为云制定安全事件的定级原则和升级原则，根据安全事件对客户业务的影响程度进行事件定级，并根据安全事件的通报机制启动客户通知流程，将事件通知客户。当发生严重的安全事件，已经或可能对大量客户造成严重影响时，华为云可通过公告在最快的时间内将事件的相关信息通知客户。通知的信息至少包括事件的描述、起因、影响、华为云已采取的措施、建议客户采取的措施等。在事件解决后，华为云会根据具体情况向客户提供事件报告。 **（2）**为应对云环境中复杂的安全风险，华为云制定了各类的专项应急预案，每年会对重大的安全风险场景进行应急演练，从而在发生此类安全事件时，快速削减可能产生的安全风险，保障网络韧性。同时，根据内部信息安全管理体系和业务连续性管理体系的要求，每年定期对所有体系文件进行审核及做出必要的更新。华为云维护了突发事件下应联系的联系人名单，在得到人员变更通知后，将第一时间及时更新。

5.2 数据处理、数据存储和云计算服务的外包

原文编号	控制域	具体控制要求	华为云的应答
12、14	服务供	12.金融机构在聘用数	客户在外包数据处理、数据存储和云

原文编号	控制域	具体控制要求	华为云的应答
	应商评估	据处理、数据存储和云计算等相关服务之前，必须对第三方提供商能力进行验证，以确保: a)遵守现行法律法规； b)机构对将由第三方提供商处理或存储的数据和信息的访问权； c)第三方提供商处理或存储的数据和信息的保密性、完整性、可用性和恢复； d)遵守机构要求的认证，以履行拟承包的服务； e)机构可以获取第三方提供商聘请的专业独立审计师提供的报告，这些报告与合同服务中使用的程序和控制有关的报告； f)提供足够的资料和管理资源，以监控拟外包的服务； g)通过物理或逻辑控制，识别和分离与机构客户有关的数据；和 h)旨在保护机构客户数据和信息的访问控制的质量。 14. 聘用第 12 条所述服务的机构，对聘用服务的可靠性、完整性、可用性、安全性和保密性负责，并对现行法律法规的遵守负责。	计算等相关服务之前，必须对服务供应商的能力进行验证，包括数据安全、认证、审计报告、服务监控、数据隔离、访问控制等方面。作为云服务供应商，华为云在上述方面的情况如下： **（1）适用法律法规的遵循：**华为云业务的开展遵循华为公司“一国一策，一客一策”的战略，在遵从客户所在国家或地区的安全法规以及行业监管要求的基础上，参考业界优秀实践从组织、流程、规范、技术、合规、生态和等方面建立并管理完善、高可信、可持续的安全保障体系，并与有关政府、客户及行业伙伴以开放与合作的方式，共同应对云安全挑战，助力客户的安全需求。 **（2）客户的访问权：**客户拥有对其数据的所有权和控制权，华为云提供的产品和服务，可让客户确定其内容数据将存储在何处，并支持用户对华为云资源和数据的访问。 **（3）数据安全：**数据安全指对用户数据信息资产的机密性、完整性、可用性、持久性，以及可追溯性等方面的全面保护。华为云高度重视用户的数据信息资产，把数据保护作为华为云安全策略的核心。华为云将继续遵循数据安全生命周期管理的业界先进标准，在身份认证、权限管理、访问控制、数据隔离、数据传输、数据存储、数据删除、物理销毁等方面，采用优秀的技术、实践和流程，为用户提供有效的数据保护能力，保障用户对其数据的隐私权、所有权和控制权不受侵犯。有关华为云如何遵守 LGPD 的更多信息，请参考**《华为云巴西 LGPD 遵从性指南》**。 **（4）认证：**华为云已通过 ISO27001、ISO27017、ISO27018、SOC、CSA STAR 等多项国际安全与隐私保护认证，更多信息请参见本白皮书“2.华为云安全与隐私合规”。 **（5）审计报告：**第三方测评公司会定期对华为云展开保密性、安全充分性

原文编号	控制域	具体控制要求	华为云的应答
			和合规性的审核并出具第三方审计报告。关于第三方审计报告的获取的要求，可以根据实际情况在客户签订的协议中约定。 **（6）服务监控：**华为云的**云监控服务（Cloud Eye Service，简称 CES）**为用户提供一个针对**弹性云服务器（Elastic Cloud Server，简称 ECS）**、带宽等资源的立体化监控平台。云监控服务提供实时监控告警、通知以及个性化报表视图，精准掌握业务资源状态。用户可以自主设置告警规则和通知策略，以便及时了解各服务的实例资源运行状况和性能。 **（7）数据隔离：**华为云各服务产品和组件从设计之初规划并实施了合理的隔离机制，避免客户间有意或无意的非授权访问、篡改等行为，降低数据泄露风险。以数据存储为例，华为云的块存储、对象存储、文件存储等服务均将客户数据隔离作为重要特性。 **（8）访问控制：**华为云的**统一身份认证服务（IAM）**为客户提供云上资源访问控制。使用 IAM，客户管理员可以管理用户账号，并且可以控制这些用户账号对客户名下资源具有的操作权限。当客户企业存在多用户协同操作资源时，使用 IAM 可以避免与其他用户共享账号密钥，按需为用户分配最小权限，也可以通过设置登录验证策略、密码策略、访问控制列表来助力用户账户的安全。通过以上方式，实现对特权和紧急账号的有效管控。客户也可通过**云审计服务（CTS）**作为辅助，为用户提供云服务资源的操作记录，供用户查询、审计和回溯使用。
15	与监管机构的沟通	数据处理、数据存储、云计算等相关服务的外包，必须由金融机构与巴西中央银行进行沟通。 第 1 段 标题中提到的沟通必须包括以下	在外包数据处理、数据存储、云计算等相关服务之前，客户应与巴西中央银行进行沟通。沟通的内容包括服务提供商的公司名称，要聘用的服务，以及可提供服务和可存储、处理和管理数据的国家/地区的说明。金融机构客户向巴西中央银行发出的沟通是金融机构客户独立完成的一项行动，但

原文编号	控制域	具体控制要求	华为云的应答
		信息： I-拟签约的第三方供应商名称； II-拟外包的相关服务； III-如果是国外承包时，则根据第 16 条第 III 项的规定，指定可提供服务和可储存、处理和管理数据的国家和每个国家的地区。	金融机构客户可以利用华为云在官网和**《华为云用户协议》**中提供的信息来满足其要求。
16	巴西境外的外包	外包境外提供的数据处理、数据存储和云计算相关服务，必须具备以下条件: I-巴西中央银行与可能提供服务的国家的监管机构之间存在信息交换协议； II-进行外包的机构必须确保提供本条所述服务不会对其自身的运作造成损害，也不会阻止巴西中央银行的行动； III-进行外包的机构必须在其签约之前定义可提供服务和可储存、处理和管理数据的国家和每个国家的地区；和 IV-进行外包的机构必须在合同不可能继续或合同终止的情况下准备业务连续性的备选方案。	对于在巴西境外提供的云计算服务，客户应查看巴西中央银行发布的与不同国家的**谅解备忘录（MoU）清单**。此列表显示了与巴西中央银行存在信息交换协议的监管机构。若未达成协议，客户应请求巴西中央银行的授权。另外，客户应保证外包服务不会阻碍对自身的运作和巴西中央银行的行动，并确定提供服务和数据处理所涉及的国家/地区，以及合同终止情况下的业务连续性安排。为配合客户满足监管要求，作为云服务提供商： **（1）**华为云不用客户数据做商业变现，在用户协议中明确表示除非是为用户提供必要的服务，或者为遵守适用的法律法规或政府机关的约束性命令，否则不会访问或者使用用户的内容。此外，华为云遵守巴西《通用数据保护法 LGPD》所述的数据保护原则。有关华为云如何遵守 LGPD 的更多信息，请参考**《华为云巴西 LGPD 遵从性指南》**。 **（2）**华为云目前已陆续在全球多个国家或地区开服。华为云的基础设施采用在全球部署多个地理区域（Region）和多可用区（AZ）的模式，华为云能够在多个地理区域内或同一地域内多个可用区之间灵活替换计算实例和存储数据，每个可用区都是一个独立故障维护域，也就是各可用区物理上是隔离的。用户可充分利用这些地理区域和可用区，规划应用系统在云上的

原文编号	控制域	具体控制要求	华为云的应答
			部署和运行。基于多个可用区进行应用的分布式部署，可保证在大多故障情况下系统都能连续运行。关于更多关于华为云基础设施的信息，参见华为云官网“**全球基础设施**”。 **（3）**在服务协议终止时，客户可通过华为云提供的**对象存储迁移服务（Object Storage Migration Service，简称 OMS）**和**主机迁移服务（Server Migration Service，简称 SMS）**，将内容数据从华为云中迁移出去，如迁移至本地数据中心。
17	服务协议	数据处理、数据存储、云计算相关服务合同必须包括: I-指明可以提供服务和可储存、处理和管理数据的国家和地区； II-为传输和存储第 I 项所述数据而采取的安全措施； III-在合同生效期间，隔离数据和访问控制，以保护客户的信息； IV-合同终止时的义务: a)将第 I 项引用的数据转移给新的第三方提供商或进行外包的机构；b)在完成 a 项所述的数据传输及确认接收数据的完整性和可用性确认，由被替换的第三方提供商删除第 I 项中提及的数据； V-进行外包的机构可以访问： a)第三方提供商提供的信息，用于验证符合第 I、III 项；b)第	客户应与服务提供商签订具有法律效力服务协议，并保证协议条款的合法性和适宜性。 为配合客户满足监管要求：华为云提供了线上的**《华为云用户协议》**以及**《华为云服务等级协议》**，其中规定了所提供服务内容和服务水平，以及华为云的职责。同时，华为云也制定了线下合同模板，可根据不同客户的需求进行定制化，客户及其监管机构对华为云的审计和监督权益，华为云会根据实际情况在与客户签订的协议中进行约定。

原文编号	控制域	具体控制要求	华为云的应答
		12 条第 II 项 d、e 项所述专业独立审计提供的证明和报告的有关资料；c)第 12 条第 II 项 f 项所述用于监控所提供服务的适当信息和管理资源; VI-如果分包服务被视为与进行外包的机构有关，第三方提供商有义务通知进行外包的机构； VII-允许巴西中央银行访问与提供服务相关的合同和条款、与所提供服务相关的文件和信息、存储的数据及其处理信息、数据和信息的备份以及数据和信息的访问代码； VIII-根据巴西中央银行的决定，进行外包的机构采取的措施；以及 IX-第三方提供商有义务随时向进行外包的机构通报可能影响所提供服务或遵守现行法律法规的限制。	

5.3 通用要求

原文编号	控制域	具体控制要求	华为云的应答
19	业务连续性管理政策	金融机构必须确保其依照现行法规实施的风险管理政策，包括与业务连续性有关的事项：	客户应制定业务连续性管理政策。作为云服务提供商： （1）华为云内部制定了安全事件管理机制，并持续优化该机制。安全事件响应流程清晰定义了在事件响应过程

原文编号	控制域	具体控制要求	华为云的应答
		I-第 3 条第 IV 项所提到的相关网络安全事件的处理； II-云计算服务相关数据处理、数据存储和外包中断时应遵循的程序，包括考虑更换第三方提供商和恢复机构正常运行的场景；和 III-第 3 条第 V 项 a 点中提及的业务连续性测试中考虑的事件场景。	中负责各个活动的角色和职责。华为云日志大数据分析系统具备海量日志快速收集、处理、实时分析的能力，支持与第三方安全信息和事件管理系统如 ArcSight、Splunk 对接。该系统统一收集所有物理设备、网络、平台、应用、数据库和安全系统的管理行为日志和各安全产品及组件的威胁检测告警日志，持续的监控和实时分析保证对安全事件的及时发现。此外鉴于安全事件处理的专业性和紧迫性，华为云拥有 7*24 的专业安全事件响应团队以及对应的安全专家资源池来应对。华为云制定安全事件的定级原则和升级原则，根据安全事件对客户业务的影响程度进行事件定级，并根据安全事件的通报机制启动客户通知流程，将事件通知客户。当发生严重的安全事件，已经或可能对大量客户造成严重影响时，华为云可通过公告在最快的时间内将事件的相关信息通知客户。通知的信息至少包括事件的描述、起因、影响、华为云已采取的措施、建议客户采取的措施等。在事件解决后，华为云会根据具体情况向客户提供事件报告。 （2）为应对云环境中复杂的安全风险，华为云制定了各类的专项应急预案，每年会对重大的安全风险场景进行应急演练，从而在发生此类安全事件时，快速削减可能产生的安全风险，保障网络韧性。同时，根据内部信息安全管理体系和业务连续性管理体系的要求，每年定期对所有体系文件进行审核及做出必要的更新。华为云维护了突发事件下应联系的联系人名单，在得到人员变更通知后，将第一时间及时更新。
20	业务连续性管理程序	金融机构为符合现行法规而采取的风险管理程序，必须包括与业务连续性有关的事项： I-为减轻第 3 条第 IV 项所述相关事件的影	客户应建立业务连续性管理机制，明确有关服务的恢复目标及最小恢复策略，制定危机管理流程，包括危机的响应、处置和通报。作为云服务提供商： **（1）**为向客户提供持续、稳定的云服务，华为云遵循 ISO22301 业务连续性

原文编号	控制域	具体控制要求	华为云的应答
		响以及合同中相关数据处理、数据存储和云计算服务中断而采取的处理措施； II-第 I 项所述中断的活动或有关服务规定的恢复或恢复正常的期限；和 III-及时向巴西中央银行通报第 I 项中所述构成金融机构危机状况的相关事件和相关服务中断，以及恢复活动的程序。	管理国际标准的要求，建立了一套完善的业务连续性管理体系。在该体系框架的要求下，华为云定期开展业务影响分析、识别关键业务、确定关键业务的恢复目标及最小恢复水平。在识别关键业务的过程中，将业务中断对客户的影响程度作为判断关键业务的一个重要标准。 **（2）**华为云根据内部业务连续性管理体系的要求，定期开展风险评估，识别并分析支撑云服务持续运行的关键资源所面临的潜在风险。针对突出风险，华为云进一步考虑突发事件发生的场景，并制定应对各种突发事件场景的危机管理程序，以最大程度地降低突发事件的影响。危机管理程序中详细规定了突发事件的预警和报告流程、事件升级流程、应急预案启动的条件、事件进展的通报流程、内外部沟通流程等。 **（3）**为配合客户满足通知的要求，华为云内部制定了完善的事件管理和客户通知通报流程，若华为云底层基础平台发生事件，相关人员将依据流程分析事件的影响，若事件已对或即将对云服务客户产生影响时，华为云将启动通知通报机制，将事件通知客户。通知的内容包括但不限于：事件的描述、起因、影响、华为云已采取的措施、建议客户采取的措施等。根据内部的客户通知通报流程，在底层基础平台发生严重事件，已经或可能对大量客户造成严重影响时，华为云可通过公告在最快的时间内将事件的相关信息通知客户。

6 华为云如何遵从及协助客户满足巴西政府《第8.771号法令》的要求

巴西政府于2016年5月11日发布了《第8.771号法令》。该规定从网络安全、记录、个人资料和私人通信的保护等领域提出了对数据保护相关要求。

金融机构在遵循《第8.771号法令》要求时，华为云作为云服务供应商，可能会参与到要求所涉及的部分活动中。以下内容将总结《第8.771号法令》中与云服务供应商相关的控制要求，并阐述华为云作为云服务供应商，会如何帮助金融机构满足这些控制要求。

6.1 网络安全

原文编号	控制域	具体控制要求	华为云的应答
5	网络安全	负责传输、交换或路由活动的当事方必须应遵守适当提供服务和应用所必需的技术要求，其目的是保持其稳定性、安全性、完整性和功能性。 (1)上段提到的必要技术要求是来自： I-处理网络安全问题，例如对限制发送大量消息（垃圾邮件）和拒绝服务攻击； II-处理网络干扰的特殊情况，例如在主路由中断和紧急情况下的备用路由。	在处理网络安全问题和网络干扰的特殊情况时，客户应遵守必需的技术要求以保持其服务和应用的稳定性、安全性、完整性和功能性。作为云服务提供商，为配合客户满足监管要求： **（1）**华为云为客户**DDoS高防（Advanced Anti-DDoS，简称AAD）**。针对DDoS攻击，华为云提供多种安全防护方案，AAD服务提供了DDoS原生基础防护（Anti-DDoS流量清洗）、DDoS原生高级防护和DDoS高防三个子服务。AAD可服务于华为云和非华为云的主机，用户可以通过修改DNS解析或对外服务地址为高防IP，将恶意攻击流量引流到高防IP清洗，助力重要业务不被攻击中断。华为云的防DDoS攻击服务提供精细化的抵御DDoS攻击的功能，包

原文编号	控制域	具体控制要求	华为云的应答
			括但不限于 Ping Flood、 SYN Flood、UDP Flood、Challenge Collapsar、HTTP Flood 、DNS Flood。用户只需根据租用带宽及业务模型自助配置防护阈值，系统检测到攻击后就会实时通知用户并进行有效防御。 **（2）**华为云 **Web 应用防火墙服务（WAF）**是结合了华为多年攻防经验和一系列针对性优化算法的高级 Web 应用防火墙。采用正则规则和语义分析的双引擎架构对 SQL 注入、跨站攻击、命令和代码注入、目录遍历、扫描器、恶意 bot、webshell、CC 等攻击实现实时的高性能防护。华为云 WAF 给用户提供简便的管理界面，用户可根据自身业务需要进行相关防护设置，亦可在集中的管理界面上查看防护日志并对误报的事件进行处理。 **（3）**客户可以使用华为云提供的**弹性负载均衡（Elastic Load Balance，简称 ELB）**服务，实现不同区域之间的负载平衡。ELB 将访问流量自动分发到多台弹性云服务器，扩展应用系统对外的服务能力，实现更高水平的应用程序容错性能。 **（4）**客户可依赖华为云数据中心集群的多地域（Region）和多可用区（AZ）架构实现其业务系统的容灾和备份，数据中心按规则部署在全球各地，客户可通过两地互为灾备中心，如一地出现故障，系统在满足合规政策前提下自动将客户应用和数据转离受影响区域，保证业务的连续性。同时，华为云还部署了全局负载均衡调度中心，客户的应用在数据中心实现 N+1 部署，即便在一个数据中心故障的情况下，也可以将流量负载均衡到其他中心。

6.2 记录、个人资料和私人通信的保护

原文编号	控制域	具体控制要求	华为云的应答
13	访问控制	连接和应用程序提供商在保管、存储和处理个人数据和私人通信时必须遵守以下安全标准指南： I-建立对数据访问的严格控制；通过对某些具有访问权限和具有专有访问权限的人规定责任； II-为记录的访问提供认证机制，例如使用双重认证系统，以确保负责数据处理的人员的个性化； III-创建连接和应用程序记录的详细访问日志。这些记录应包括访问的时间和持续时间、涉及的由公司指定的员工或负责人的身份以及被访问的文件； IV-使用记录管理解决方案，通过技术手段保证数据的不可侵犯性（如加密或等效保护措施）。	客户应建立访问控制管理机制，设定与职责匹配的用户权限，采用安全的身份认证和数据加密技术，并对用户访问通过日志进行记录。作为云服务提供商，为配合客户满足监管要求： **（1）**客户可通过华为云的**统一身份认证服务（IAM）**对使用云资源的用户账号进行管理。每一位华为云客户在华为云都拥有唯一可辨识的用户 ID，此外，华为云还提供多种用户身份验证机制，包括账号密码、多因素认证等。 • IAM 支持客户的安全管理员根据需求来设置不同强度的密码策略和更改周期，防止用户使用简单密码或长期使用固定密码而导致账号泄露。此外，IAM 还支持客户的安全管理员设置登录策略，避免用户密码被暴力破解或者因为访问钓鱼页面等而导致账号信息泄露。 • IAM 同时支持多因子认证机制。多因子认证是用户登录控制台时，除密码认证外，增加的另一层安全认证保护，以增强账号安全性。用户可选择是否启用。如启用，用户在密码认证通过后，还将收到一次性短信认证码进行二次认证。用户修改密码、手机等敏感信息时，IAM 默认启用多因子认证，保证用户账号安全。 • 如果用户有安全可靠的外部身份认证服务商，可以将 IAM 服务的联邦认证外部用户映射成华为云的临时用户，并访问用户的华为云资源。IAM 可以按层次和细粒度授权，管理员可以基于用户的工作职责规划使用云资源的权限，还可以通过设置用户访问云服务系统的安全策略，例如设置访问控制列表来限制未信任网络的恶意接入。 **（2）**华为云的**云审计服务（CTS）**，可提供对各种云资源操作记录的收

原文编号	控制域	具体控制要求	华为云的应答
			集、存储和查询功能，可用于支撑安全分析、合规审计、资源跟踪和问题定位等常见应用场景。 **（3）**华为云内部建立了运维和运营账号管理机制。华为云运维人员接入华为云管理网络对系统进行集中管理时，需使用唯一可辨识的员工身份账号，用户账号均配置了强密码安全策略，且密码定期更改，以防止暴力破解密码。此外，华为云还采用双因子认证对华为云运维人员进行身份认证，如 USB key、Smart Card 等。所有运维账号由 LDAP 集中管理，通过统一运维审计平台集中监控并进行自动审计,以实现从创建用户、授权、鉴权到权限回收的全流程管理,并根据不同业务维度和相同业务不同职责，实行 RBAC 权限管理，保证不同岗位不同职责人员限定只能访问本角色所管辖的设备。
16	安全标准披露	有关应用程序和连接提供商采用的安全标准的信息应以清晰易懂的方式向任何相关方披露，最好通过其网站披露，同时尊重商业秘密的保密权。	客户应向相关方披露其所采用的安全标准信息。作为云服务提供商： **（1）**华为云在官网上发布了其所提供产品的功能、安全特性以及使用到的标准技术的说明，具体请参见华为云官网“**帮助中心**”。 **（2）**华为云已通过 ISO27001、ISO27017、ISO27018、SOC、CSA STAR 等多项国际安全与隐私保护认证，关于更多华为云的安全合规信息以及获取相关合规证书，可参见华为云官网“**信任中心-合规中心**”。

7 客户可选择的额外安全措施

华为云理解客户的网络安全与数据保护需求，并结合自身丰富网络安全与数据安全实践及技术能力，提供了额外安全措施供客户选择。额外安全措施涵盖网络、数据库、安全、管理与部署工具等产品，相关产品的数据保护、数据删除、网络隔离、权限管理、容灾备份、安全审计等功能可帮助客户加强客户内容安全。

产品名称	产品介绍	助力领域
统一身份认证服务 Identity and Access Management (IAM)	IAM 提供适合企业级组织结构的用户账号管理服务，为企业用户分配不同的资源及操作权限。用户通过使用访问密钥获得基于 IAM 的认证和鉴权后，以调用 API 的方式访问华为云资源。 IAM 可以按层次和细粒度授权，保证同一企业租户的不同用户在使用云资源上得到有效管控，避免单个用户误操作等原因导致整个云服务的不可用，确保租户业务的持续性。	数据处理、数据存储和云计算服务的外包 记录、个人资料和私人通信地保护
云审计服务 Cloud Trace Service (CTS)	CTS 为用户提供一个针对弹性云服务器、带宽等资源的立体化监控平台。CES 提供实时监控告警、通知以及个性化报表视图，精准掌握业务资源状态。需要强调的是，CES 的监控对象是基础设施的资源使用数据，不监控或触碰租户数据。	数据处理、数据存储和云计算服务的外包 记录、个人资料和私人通信地保护
云监控服务 Cloud Eye Service (CES)	CES 为用户提供一个针对弹性云服务器、带宽等资源的立体化监控平台。CES 提供实时监控告警、通知以及个性化报表视图，精准掌握业务资源状态。用户可以自主设置告警规则和通知策略，以便及时了解各服务的实例资源运行状况和性能。	数据处理、数据存储和云计算服务的外包
数据加密服务 Data Encryption Workshop	DEW 是一款综合的云上数据加密服务。它可以提供专属加密、密钥管理、凭据管理、密钥对管理等服务，安全可靠的为您解决了数据安全、密钥安全、密钥管理复杂等问题。其密钥由硬件安全模块（Hardware Security Module，	数据处理、数据存储和云计算服务的外包 记录、个人资料和

产品名称	产品介绍	助力领域
(DEW)	HSM） 保护，并与多个华为云服务集成。用户也可以借此服务开发自己的加密应用。	私人通信地保护 网络安全
数据库安全服务 Database Security Service (DBSS)	DBSS 是一个智能的数据库安全服务，基于机器学习机制和大数据分析技术，提供数据库审计，SQL 注入攻击检测，风险操作识别等功能，保障云上数据库的安全。包括用户行为发现审计、多维度分析、实时告警、提供精细化报表、敏感数据保护、审计日志备功能。 数据库安全审计提供的旁路模式数据库审计功能，可以对风险行为进行实时审计和告警。同时，通过生成满足数据安全标准的合规报告，可以对数据库的内部违规和不正当操作进行审计及定位追责。	数据处理、数据存储和云计算服务的外包
企业主机安全服务 Host Security Service (HSS)	HSS 是以工作负载为中心的安全产品，旨在解决现代混合云、多云数据中心基础架构中服务器工作负载的独特保护要求。它集成了主机安全、容器安全和网页防篡改。	网络安全 记录、个人资料和私人通信地保护
DDoS 防护 Advanced Anti-DDoS (AAD)	AAD 服务在企业重要业务连续性方面提供了有力保 障。当用户的服务器遭受大流量 DDoS 攻击时，DDoS 高防可以保护用户业务持续可用。DDoS 高防通过高防 IP 代理源站 IP 对外提供服务，将恶意攻击流量引流到高防 IP 进行清洗，确保重要业务不被攻击中断。DDos 高防服务于华为云、非华为云及 IDC 的互联网主机。	网络安全
Web 应用防火墙服务 Web Application Firewall （WAF）	WAF 通过对 HTTP(S)请求进行检测，识别并阻断 SQL 注入、跨站脚本攻击、网页木马上传、命令/代码注入、文件包含、敏感文件访问、第三方应用漏洞攻击、CC 攻击、恶意爬虫扫描、跨站请求伪造等攻击，保护 Web 服务安全稳定。 在 WAF 管理控制台将网站添加并接入 WAF，即可启用 WAF。启用之后，您网站所有的公网流量都会先经过 WAF，恶意攻击流量在 WAF 上被检测过滤，而正常流量返回给源站 IP，从而确保源站 IP 安全、稳定、可用。 WAF 支持云模式和独享模式两种部署方式。	网络安全
弹性负载均衡 Elastic Load Balance （ELB）	客户可以使用华为云提供的 ELB，实现不同区域之间的负载平衡。ELB 将访问流量自动分发到多台弹性云服务器，扩展应用系统对外的服务能力，实现更高水平的应用程序容错性能。	网络安全

8 结语

本文描述了华为云如何为客户提供遵从巴西金融行业监管要求的云服务，并表明华为云遵守巴西国家货币委员会（CMN）、巴西中央银行（BCB）和巴西政府发布的重点监管要求，有助于客户详细了解华为云对巴西金融行业监管要求方面的合规性，让客户安全、放心地通过华为云服务存储、处理客户内容数据。同时，本文也在一定程度上指导客户如何在华为云上设计、构建和部署遵从巴西金融行业监管要求的安全的云环境，帮助客户更好地与华为云共同承担起相应的安全责任。

本白皮书仅供一般性参考，不具备任何法律效力或构成任何形式的法律建议，客户应酌情评估自身使用云服务的情况，并负责确保在使用华为云时对相关巴西金融行业监管要求的遵从性。

9 版本历史

日期	版本	描述
2024 年 9 月	3.0	法规更新和例行刷新
2022 年 4 月	2.0	合规要求更新
2020 年 12 月	1.0	首次发布

