Global

Certificados	Infraestructura en la nube de Oracle	Aplicaciones Oracle
CSA STAR (Cloud Security Alliance Security Trust Assurance and Risk) Cloud Security Alliance (CSA) es una organización que promueve las mejores prácticas para brindar garantía de seguridad en la computación en la nube. La certificación CSA Security Trust, Assurance and Risk (STAR) prevé que un tercero de confianza realice una evaluación que confirme la implementación de los controles de seguridad necesarios. Esta evaluación se basa en CSA Cloud Controls Matrix (CCM) y los controles de SOC 2 e ISO/IEC 27001. Para obtener más información, consulte: https://cloudsecurityalliance.org/star/	SI	SI
ISO 9001ISO 9001: Quality Management Systems La Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC) forman el sistema especializado para la estandarización mundial. La familia de normas ISO 9001 se basa en una serie de principios de gestión de la calidad, incluido un fuerte enfoque en el cliente. Su objetivo es "ayudar a las organizaciones a demostrar su capacidad para proporcionar a los clientes productos y servicios de buena calidad de manera constante". Para obtener más información, consulte https://www.iso.org/iso-9001-quality-management.html	SI	NO
ISO/IEC 20000-1ISO/IEC 20000-1: Service Management Systems La Organización Internacional de Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC) redactaron el estándar del sistema de gestión de servicios (SMS) ISO/IEC 20000-1 reconocido internacionalmente. Su objetivo es ayudar a diseñar, hacer la transición, entregar y mejorar los servicios para cumplir con los requisitos de servicio acordados. Para obtener más información, consulte https://www.iso.org/standard/51986.html	SI	NO
ISO/IEC 27001ISO/IEC 27001: Information Security Management Systems La Organización Internacional de Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC) redactaron el estándar ISO/IEC 27001 reconocido internacionalmente. Su objetivo es proporcionar una guía para el establecimiento y la mejora continua de un sistema de gestión de seguridad de la información (SGSI) dentro del contexto de la organización. También incluye requisitos para la evaluación y el tratamiento de los riesgos de seguridad de la información adaptados a las necesidades de la organización. Para obtener más información, consulte https://www.iso.org/isoiec-27001-information-security.html	SI	SI
ISO/CEI 27017 La Organización Internacional de Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC) redactaron ISO/IEC 27017, un conjunto de directrices para los controles de seguridad de la información aplicables a la provisión y el uso de servicios en la nube. Su objetivo es proporcionar una guía de implementación adicional para los controles relevantes especificados en ISO/IEC 27002 y una guía que se relacione específicamente con los servicios en la nube. Para obtener más información, consulte https://www.iso.org/standard/54533.html	SI	SI
ISO/CEI 27018 La Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC) redactaron la norma ISO/IEC 27018, para ser utilizada junto con los objetivos y controles de seguridad de la información en ISO/IEC 27002. Su objetivo es crear un conjunto común de normas de seguridad. categorías y controles que puede implementar un proveedor de servicios de computación en la nube pública que actúe como un procesador de información de identificación personal (PII). Para obtener más información, consulte https://www.iso.org/standard/76559.html	SI	SI
ISO/CEI 27701 La Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC) redactaron el borrador ISO/IEC 27701. Su objetivo es brindar orientación para el establecimiento y la mejora continua de un Sistema de gestión de la información de privacidad (PIMS) que procesa información de identificación personal (IPI). Este estándar es una extensión de ISO/IEC 27001 e ISO/IEC 27002 para la gestión de la privacidad. Para obtener más información, consulte https://www.iso.org/standard/71670.html	SI	NO
PCI DSS El estándar de seguridad de datos de la industria de tarjetas de pago (PCI DSS) es un estándar de seguridad de la información para organizaciones que manejan las principales tarjetas de crédito . Su objetivo es fomentar y mejorar la seguridad de los datos de los titulares de tarjetas y facilitar la adopción generalizada de prácticas coherentes de seguridad de datos a nivel mundial. El estándar PCI DSS es obligatorio para las propias marcas de tarjetas, pero lo administra el Consejo de estándares de seguridad de la industria de tarjetas de pago (PCI SSC). Para obtener más información, consulte https://www.pcisecuritystandards.org/	SI	SI
SOC 1 El Sistema y Controles de Organización (SOC) es un programa del Instituto Americano de Contadores Públicos Certificados (AICPA). Tiene por objeto proporcionar informes de control interno sobre los servicios prestados por una organización de servicios. Un informe SOC 1 ayuda a las empresas a generar confianza en sus procesos y controles de prestación de servicios. La intención de estos informes se centra en los controles internos sobre la información financiera (ICFR). Para obtener más información, consulte https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/sorhome.html	SI	SI

SOC 2 El Sistema y Controles de Organización (SOC) es un programa del Instituto Americano de Contadores Públicos Certificados (AICPA). Tiene por objeto proporcionar informes de control interno sobre los servicios prestados por una organización de servicios. Un informe SOC 2 describe la información relacionada con los controles internos de seguridad, disponibilidad, integridad del procesamiento, confidencialidad o privacidad de una organización de servicios. Criterios de confianza. La intención de este informe es brindar información detallada y garantías sobre los controles relevantes para la seguridad, la disponibilidad y la integridad del procesamiento de los sistemas utilizados para procesar los datos de los usuarios y la confidencialidad y privacidad de la información procesada por estos sistemas. Para obtener más información, consulte https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/sorhome.html	SI	SI
SOC 3 El Sistema y Controles de Organización (SOC) es un programa del Instituto Americano de Contadores Públicos Certificados (AICPA). Tiene por objeto proporcionar informes de control interno sobre los servicios prestados por una organización de servicios. Un informe SOC 3 describe información relacionada con los controles internos de seguridad, disponibilidad, integridad del procesamiento, confidencialidad o privacidad de una organización de servicios. Estos informes son más cortos que los informes SOC 2 y tienen menos detalles. Para obtener más información, consulte https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/sorhome.html	SI	SI

AMERICAS

Certificados	**Infraestructura en la nube de Oracle**	**Aplicaciones Oracle**
Departamento de Defensa DISA SRG La Guía de requisitos de seguridad informática en la nube (CC SRG) de la Agencia de sistemas de información de defensa (DISA) describe cómo el Departamento de Defensa de EE. UU. (DoD) evaluará la postura de seguridad de los proveedores de servicios en la nube (CSP) que no pertenecen al DoD. Además, CC SRG explica cómo los CSP que no pertenecen al DoD pueden demostrar que cumplen con los controles y requisitos de seguridad antes de manejar cualquier dato del DoD. CC SRG prevé la siguiente categorización: Nivel de impacto 2: Datos borrados para publicación pública (nota: el nivel 1 se combinó con el nivel 2) Nivel de impacto 4: información no clasificada controlada (CUI) a través de la red de enrutador de protocolo de Internet no seguro (NIPRNet). CUI incluye información de salud protegida (PHI), información de privacidad (PII) y datos controlados de exportación (nota: el nivel 3 se combinó con el nivel 4) Nivel de impacto 5: CUI de mayor sensibilidad, información de misión crítica o NSS sobre NIPRNet Nivel de impacto 6: datos clasificados a través de la red secreta de enrutadores de protocolo de Internet (SIPRNet) Para obtener más información, consulte https://dl.dod.cyber.mil/wp-content/uploads/cloud/zip/U_Cloud_Computing_SRG_V1R4.zip	SI	SI
FedRAMP El Programa Federal de Gestión de Riesgos y Autorizaciones (FedRAMP) es un programa del gobierno de EE. UU. diseñado para proporcionar un enfoque estándar para la evaluación de la seguridad, la autorización y el control continuo de los productos y servicios en la nube. La Oficina de Administración y Presupuesto (OMB, por sus siglas en inglés) indica a las agencias federales de EE. UU. que aprovechen FedRAMP para garantizar que exista seguridad al acceder a productos y servicios en la nube. FedRAMP utiliza la publicación especial 800-53 del Instituto Nacional de Estándares y Tecnología (NIST), que proporciona un catálogo de controles de seguridad para todos los sistemas de información federales de EE. UU. FedRAMP requiere que los proveedores de servicios en la nube (CSP) reciban una revisión de seguridad independiente realizada por una organización de evaluación de terceros (3PAO) para garantizar que las autorizaciones cumplan con la Ley Federal de Gestión de Seguridad de la Información (FISMA). Para obtener más información, consulte https://marketplace.fedramp.gov/#!/products?sort=productName&productNameSearch=oracle	SI	SI
HITRUST LCR Health Information Trust Alliance (HITRUST) es una organización que representa a la industria de la salud. HITRUST creó y mantiene el Marco de Seguridad Común (CSF), un marco contra el cual los proveedores de servicios en la nube (CSP) y las entidades de salud cubiertas pueden demostrar el cumplimiento de los requisitos de la Ley de Portabilidad y Responsabilidad de Seguros Médicos (HIPAA) de EE. UU. Para obtener más información, consulte https://hitrustalliance.net/	SI	NO
HIPAA La Ley de Portabilidad y Responsabilidad de los Seguros Médicos de 1996 (HIPAA) es una ley federal de EE. UU. Requiere la creación de estándares nacionales para proteger la información sensible de salud del paciente de ser divulgada sin el consentimiento o conocimiento del paciente. Para obtener más información, consulte https://www.hhs.gov/hipaa/	SI	SI
HIPAA El Programa de gestión de autorizaciones y riesgos de Texas (TX-RAMP) es "un marco para recopilar información sobre la postura de seguridad de los servicios en la nube y evaluar las respuestas para el cumplimiento de los controles y la documentación requeridos". Para obtener más información, consulte https://dir.texas.gov/texas-risk-and-authorization-management-program-tx-ramp	NO	SI