centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 889H

Guía de Configuración segura para Oracle SaaS Enterprise Performance Management EPM

JULIO 2023

Catálogo de Publicaciones de la Administración General del Estado
https://cpage.mpr.gob.es

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

centro criptológico nacional

CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL, 2.5.4.97=VATES-S2800155J, ou=CENTRO CRIPTOLOGICO NACIONAL, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2023.07.04 14:46:09 +02'00'

Pº de la Castellana 109, 28046 Madrid

NIPO: 083-23-180-X
Fecha de Edición: julio de 2023

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

ÍNDICE

1. GUÍA DE CONFIGURACIÓN SEGURA PARA ORACLE SAAS ENTERPRISE PERFORMANCE MANAGEMENT (EPM)

1.1 DESCRIPCIÓN DEL USO DE ESTA GUÍA

La principal utilidad de esta guía es identificar los servicios de Oracle SaaS Enterprise Performance Management (EPM) que deben configurarse, cumpliendo con las distintas medidas de seguridad que establece el Esquema Nacional de Seguridad. Dichos servicios, en la modalidad SaaS de la nube pública de Oracle, son desplegados y configurados bajo la arquitectura de Oracle Cloud Infrastructure (OCI), para cargas de trabajo en la nube pública de Oracle, siguiendo las exigencias del Esquema Nacional de Seguridad (ENS).

Por un lado, se describe la Vigilancia continua como un principio básico del ENS y se recoge en un apartado independiente para la descripción de los pasos a seguir para el cumplimiento de dicho principio.

El principio de la Vigilancia continua permite la detección de actividades o comportamientos anómalos y su oportuna respuesta. Para ello, deberá realizarse una evaluación permanente del estado de la seguridad de los activos, permitiendo medir su evolución, detectando vulnerabilidades e identificando deficiencias de configuración.

Por otro lado, se describe, en otro apartado independiente (3.1.4) , aquellos procesos generadores de confianza en la nube que conforman un escenario completo de nube segura, a través de una implementación de configuración de elementos de seguridad como las credenciales o las conexiones seguras con el servicio de cualquier proveedor de nube.

La nomenclatura de los servicios descritos se documenta en el glosario de términos, incluido como anexo al documento. A su vez, se añaden referencias a la documentación oficial del fabricante con el objetivo de facilitar la lectura y comprensión por parte del usuario de esta guía.

Para finalizar, se incluye un resumen de las medidas detalladas anteriormente para realizar un control de la configuración a modo de “checklist”.

1.2 DEFINICIÓN DEL SERVICIO

Oracle Cloud Infrastructure (OCI), es la nube de última generación diseñada para ejecutar cualquier aplicación de forma más rápida y segura por menos.

El marco de adopción de OCI ayuda a las organizaciones a facilitar su transición a la nube y proporciona a los clientes una metodología para utilizar eficiencias incorporadas de Oracle Cloud, como los servicios SaaS EPM para la infraestructura de la nube de Oracle, la cual dispone de la Certificación de Conformidad con el Esquema Nacional de Seguridad.

Dentro de los modelos que ofrece OCI, esta guía se centrará en el modelo de Software como Servicio (SaaS).

a) **SaaS**: Es un tipo de modelo de entrega de software basado en la nube en el que el proveedor de la nube desarrolla y mantiene el software de las aplicaciones en la nube. Proporciona actualizaciones automáticas del mismo y lo pone a disposición de sus clientes a través de un navegador de internet con un sistema de pago por uso.

   El proveedor de la nube pública administra todo el hardware y el software tradicional, incluidos middleware, software de aplicaciones y seguridad. De este modo, los clientes de SaaS pueden reducir drásticamente los costos, implementar, ampliar y actualizar las soluciones empresariales con mayor rapidez de la que proporciona el mantenimiento de sistemas y software locales y predecir el costo total de propiedad con mayor precisión.

También se recogen las medidas de aplicación técnica que marca el ENS para la Categoría Alta, según las medidas a establecer en cada una de las aplicaciones que forman parte de la Suite de Oracle EPM Cloud y la gestión del entorno donde se hospedan.

1.3 SERVICIOS DE ORACLE SAAS ENTERPRISE PERFORMANCE MANAGEMENT (EPM)

El software Enterprise Perfomance Management (EPM) se refiere a los procesos diseñados para ayudar a las organizaciones a planificar, presupuestar, pronosticar e informar sobre el desempeño comercial, así como a consolidar y finalizar los resultados financieros. Las soluciones de EPM son utilizadas principalmente por los directores financieros y la oficina de finanzas, mientras que otras áreas funcionales, como recursos humanos, ventas, marketing y TI, utilizan EPM para la planificación operativa, la elaboración de presupuestos y la generación de informes.

Si bien a menudo está vinculado a los sistemas de planificación de recursos empresariales (ERP), el software EPM complementa el ERP al proporcionar información de gestión además de la parte superior de los datos operativos. En otras palabras, el ERP se encarga de operar el negocio, la actividad transaccional del día a día, y EPM se ocupa de administrar el negocio, analizar, comprender e informar sobre el negocio.

Hoy en día, el software EPM se considera fundamental para administrar todo tipo de organizaciones al vincular las métricas financieras y operativas con los conocimientos y, en última instancia, impulsar estrategias, planes y ejecución. Con el software EPM, los gerentes pueden impulsar un mejor desempeño en toda la organización al monitorear los resultados financieros y operativos contra los pronósticos y objetivos y usar análisis para reconocer tendencias clave y predecir resultados.

En un entorno de cambio constante, nuevos competidores e incertidumbre económica, EPM ofrece una herramienta para que las organizaciones gestionen sus negocios de manera ágil. Con finanzas a la cabeza, los procesos comerciales de EPM (modelado estratégico, planificación, consolidación y cierre, generación de informes y análisis del rendimiento) pueden ayudar a las organizaciones a comprender sus datos y utilizarlos para tomar mejores decisiones comerciales.

Oracle EPM Cloud proporciona procesos comerciales integrales para cumplir con los requisitos de la mayoría de las organizaciones y garantiza una experiencia ágil y conectada en múltiples procesos comerciales.

A continuación, se describen los procesos comerciales integrados en la herramienta basada en la nube de Oracle:

a) **Oracle Cloud EPM Platform:** es un marco de los componentes técnicos y funcionales compartidos entre los procesos de EPM en la nube. Permite tener una experiencia de usuario más unificada y una administración simplificada en distintas funciones de negocio.

b) **Oracle Cloud EPM Planning:** Oracle EPM Cloud ayuda a alinear la planificación en toda la organización basados en factores empresariales y orientados a objetivos. Mediante el desarrollo de previsiones ágiles para todas las líneas de negocio completamente integrados en finanzas y operaciones. Permite responder con mayor rapidez y eficacia a los cambios. Además, puede crear pronósticos a largo plazo para dinámicas comerciales impredecibles utilizando modelos de escenarios integrados y sofisticados.

c) **Oracle Cloud EPM Profitability and Cost Management:** comprende los productos o líneas de negocio de la organización y los costos, para tomar decisiones fundamentadas sobre la dirección que debe llevar la empresa. Puede crear modelos de asignación transparentes para análisis de rentabilidad, cálculo de costos de servicios compartidos, gestión financiera de IT, precios de transferencia de impuestos.

d) **Oracle Cloud EPM Financial Consolidation and Close:** Oracle EPM Cloud permite que las organizaciones se adapten rápidamente a los requisitos empresariales y de cumplimiento en constante cambio, al mismo tiempo que reducen el riesgo, mejorando los controles que brindan información más rápida, precisa y transparente para todas las partes interesadas, en cualquier momento y en cualquier lugar.

e) **Oracle Cloud EPM Account Reconciliation:** Oracle EPM Cloud permite automatizar las conciliaciones de cuentas y la conciliación de transacciones. Mejore la eficiencia y precisión de los estados financieros de la organización a la vez que permite abordar la seguridad y el riesgo típicamente asociados con el proceso.

f) **Oracle Cloud EPM Tax Reporting:** Oracle EPM Cloud se encarga de alinear los impuestos con los informes financieros corporativos, mejorando de esta manera la visibilidad y el cumplimiento. Tiene la capacidad de entregar procesos, previsión e informes corporativos transparentes segregado por país.

g) **Oracle Cloud EPM Narrative Reporting:** Oracle EPM Cloud permite a las organizaciones reinventar los informes narrativos. Las empresas de todos los tamaños pueden optimizar los procesos de generación de informes y combinar datos y narraciones de paquetes de informes financieros, de gestión y normativos, en un entorno seguro y colaborativo.

h) **Oracle Cloud EPM Freeform:** Oracle EPM Cloud facilita la toma de mejores decisiones con análisis multidimensionales, planificación, modelado e informes en Oracle Fusion Cloud Enterprise Perfomance Management (EPM). Oracle Cloud Freeform ofrece la conocida potencia y flexibilidad de Essbase con la escalabilidad y gobernanza de SaaS.

i) **Oracle Cloud EPM Enterprise Data Management:** Oracle EPM Cloud proporciona una plataforma única para administrar de manera flexible los datos empresariales incluyendo la gobernanza, visualización y gestión de jerarquías, mientras se mantiene la integridad de los datos y la alineación de las aplicaciones empresariales.

Finalmente, en los siguientes apartados se describirán las funcionalidades de las aplicaciones que forman parte de cada proceso comercial integrado en la solución de Oracle EPM Cloud.

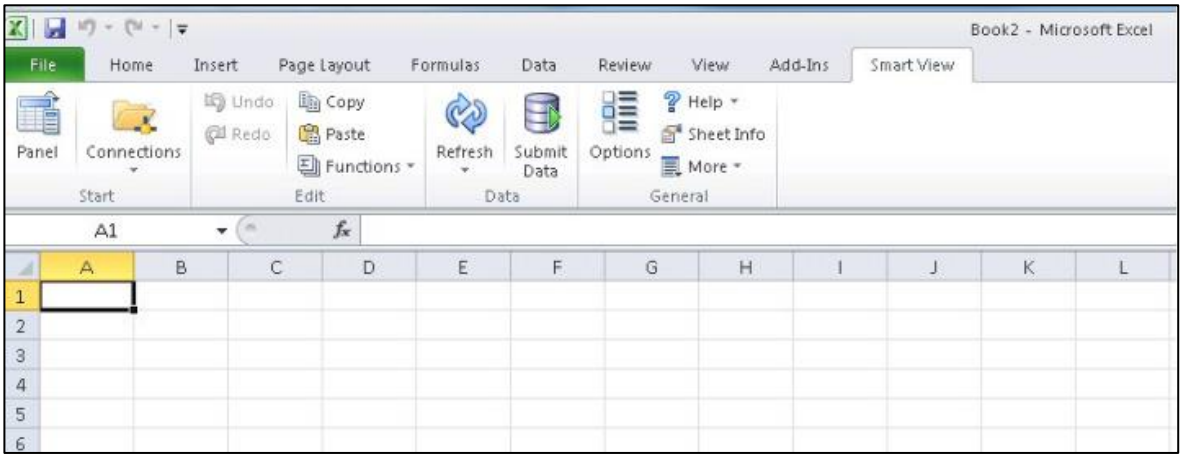
1.3.1 ORACLE CLOUD EPM PLATFORM

Es una plataforma que permite la gestión coherente de informes y metadatos en EPM y ERP en la nube de Oracle. Sirve como punto de acceso unificado y único entre los procesos de EPM y ERP, brindando una experiencia unificada de los procesos de negocio para el usuario.

1.3.1.1 ORACLE SMART VIEW FOR OFFICE

Permite integrar datos de ERP, gestión de rendimiento empresarial (EPM) e inteligencia empresarial (BI) directamente desde el origen de datos a Microsoft Word, PowerPoint, Excel y Outlook.

Mediante una interfaz fácil de manejar, proporciona potentes capacidades sin necesidad de escribir consultas complejas, pudiendo guardar de forma local o centralizada los análisis generados.



Smart View for Office.

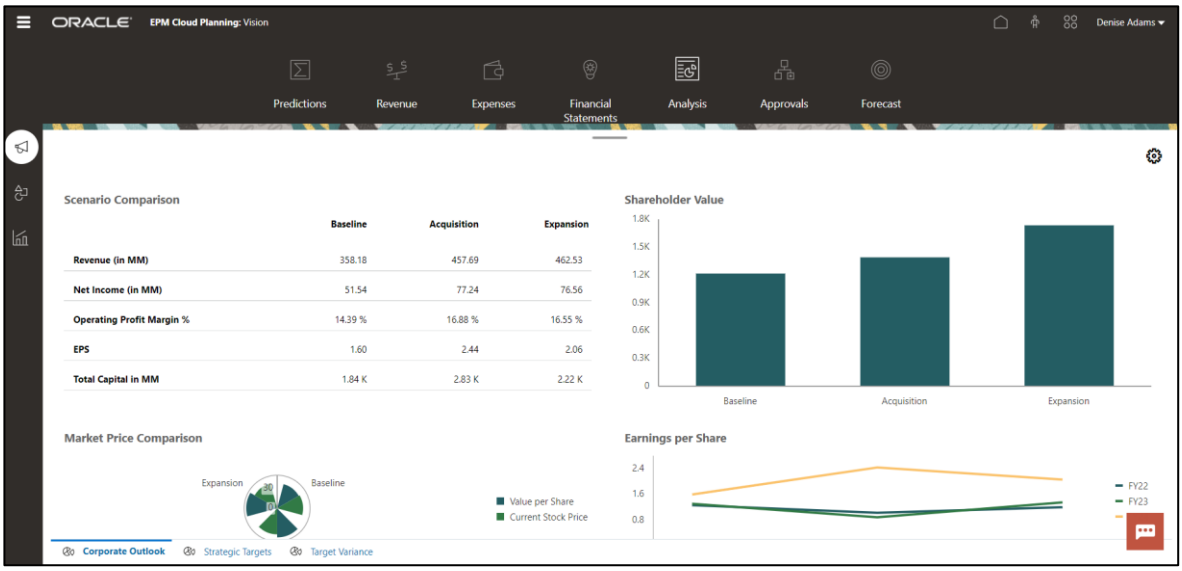
Además, los formularios flexibles permiten trabajar con las funciones de Excel para que los usuarios puedan aprovechar la clasificación, el filtrado y otras funciones nativas de la herramienta de Microsoft.

Finalmente, puede consultar más información relacionada con Oracle Smart View for Office a través del siguiente enlace de Oracle:

https://www.oracle.com/es/performance-management/smart-view-for-office/

1.3.1.2 ANALYTICS AND REPORTS

Los informes y analíticas de la plataforma de Oracle EPM Cloud permiten el uso de consolas y paneles de control con capacidades avanzadas de visualización y creación de gráficos. Los usuarios pueden crear fácilmente nuevos paneles de control con un diseñador puntual o manipular paneles de control existentes para soportar sus análisis y tareas.



Oracle EPM Cloud - Analysis.

Los informes que se pueden generar están dotados de inteligencia financiera integrada que permiten comprender mejor las variaciones. Además, permite el uso de forma interactiva para proporcionar análisis y obtener detalles, con la capacidad de cargar y enviar a los usuarios de manera programada.

Por otro lado, los principales indicadores clave de rendimiento (KPI) están disponibles para las partes interesadas a través de infolets en la pantalla de inicio del usuario.

Finalmente, puede acceder al contenido de los informes y análisis a través del escritorio, web o dispositivo móvil.

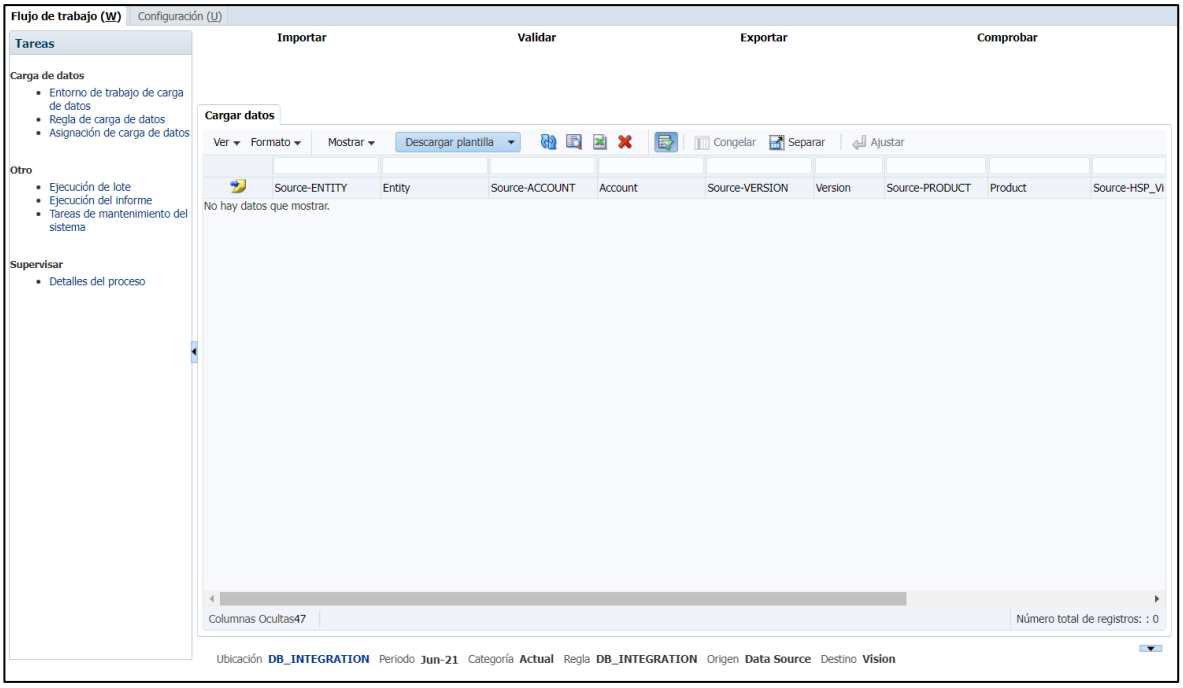
Puede consultar más información relacionada con Oracle Analytics and Reports a través del siguiente enlace de Oracle de Narrative Reporting:

https://www.oracle.com/es/performance-management/narrative-reporting/

1.3.1.3 DATA INTEGRATION

Puede integrar fácilmente los datos de varios tipos de aplicaciones de origen. Además, ofrece la capacidad de acceder a las transacciones detalladas subyacentes a los datos de la aplicación EPM y comprenderlas.

Por otro lado, es posible la extracción, de forma segura, de datos de la aplicación EPM para la integración en otros entornos como un lago de datos, un almacén o un sistema operativo.



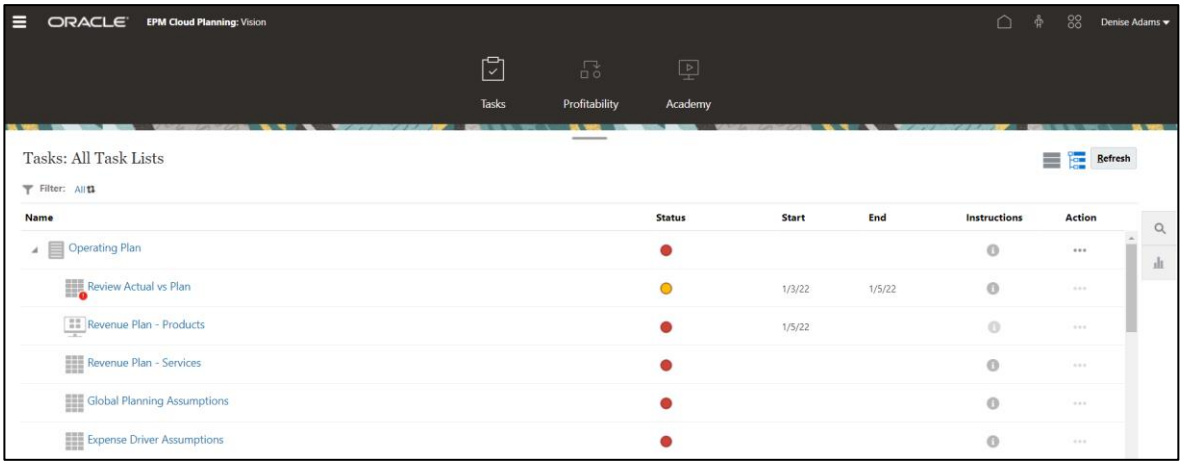
Oracle EPM Cloud - Data Integration.

Oracle EPM Cloud permite la automatización como una utilidad potente para la interacción con casi todas las necesidades administrativas de la organización. Por último, todo el contenido de Oracle EPM Cloud, incluido los formularios, informes y otros artefactos, se puede integrar con otras aplicaciones como Oracle Cloud ERP y otras aplicaciones de terceros. Esto proporciona capacidades completas para que los usuarios puedan acceder al contenido que necesitan, cuando lo necesiten y donde lo necesiten.

1.3.1.4 TASK MANAGEMENT

Permite orquestar procesos importantes con la gestión integrada de procesos y tareas. Las tareas pueden ser manuales o automatizadas y se pueden ejecutar cuando se completen las tareas precedentes o según hayan sido programadas. Las tareas clave de EPM, como proporcionar contenido para una divulgación financiera, requieren certificación.

La gestión de tareas de Oracle EPM Cloud admite certificaciones que se deben completar para que la tarea se pueda marcar como finalizada.

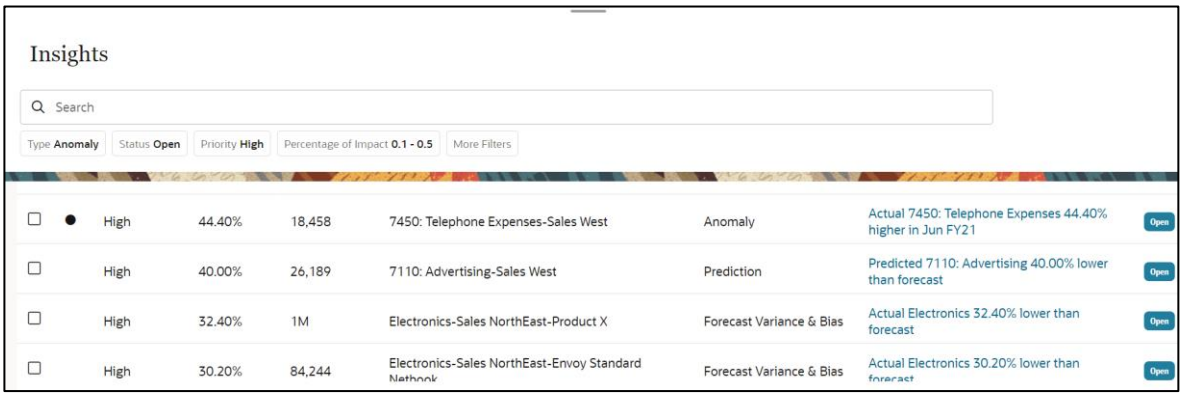


Oracle EPM Cloud - Tasks.

Además, los auditores a menudo revisan las tareas para completar un proceso de cierre financiero. La creación de un enlace de informes desde la gestión de tareas de Oracle EPM Cloud permite entregar informes con facilidad para su revisión por parte de los auditores.

1.3.1.5 INTELLIGENT PERFORMANCE MANAGEMENT (IPM)

IPM aplica la ciencia de datos y el aprendizaje automático para que los profesionales de finanzas puedan estar enfocados en los datos, las áreas claves del negocio y las oportunidades perdidas. Permite acelerar el análisis de los datos para agilizar la acción mediante estadísticas, usando la inteligencia artificial incorporada.



Oracle EPM Cloud - IPM.

Además, IPM permite identificar y aprovechar los patrones en los datos financieros y operativos de una organización para mejorar la precisión. Los usuarios pueden ejecutar predicciones sobre los datos reales más recientes y usarlos para la elaboración de los planes y toma de decisiones más oportunas y objetivas.

1.3.1.6 INTELLIGENT PROCESS AUTOMATION

Oracle EPM Cloud utiliza el poder de la automatización inteligente para realizar las tareas cuando se cumplen las condiciones, permitiendo acelerar y optimizar las consolidaciones y el proceso de cierre general, liberando al personal para realizar actividades de mayor valor añadido.

Reduce considerablemente el tiempo dedicado a los procesos de conciliación de cuentas con la automatización de transacciones para la confrontación, proporcionando estadísticas adicionales en la generación de informes.

1.3.1.7 LAST GENERATION USER EXPERIENCE

Mediante una interfaz intuitiva y atractiva, todos los procesos de negocio de EPM son accesibles a través de una sola página inicial que permite a los usuarios realizar todas las actividades necesarias de forma rápida y eficaz.

Oracle EPM Cloud ofrece flujos de navegación personalizados tanto a los usuarios como a los grupos de usuarios para ser guiados a través de las actividades necesarias para completar un determinado proceso de negocio.

Además, Oracle Digital Assistant para EPM permite aumentar la velocidad y la precisión del proceso de conciliación de cuentas.

1.3.1.8 MANAGEMENT

La administración de Oracle EPM Cloud Platform permite incorporar automáticamente las últimas capacidades tecnológicas en el entorno de la organización. Además, la administración permite la gestión de la seguridad que garantiza a los usuarios la seguridad de sus acciones, evitando al mismo tiempo el acceso a áreas a las que no se les ha otorgado permiso.

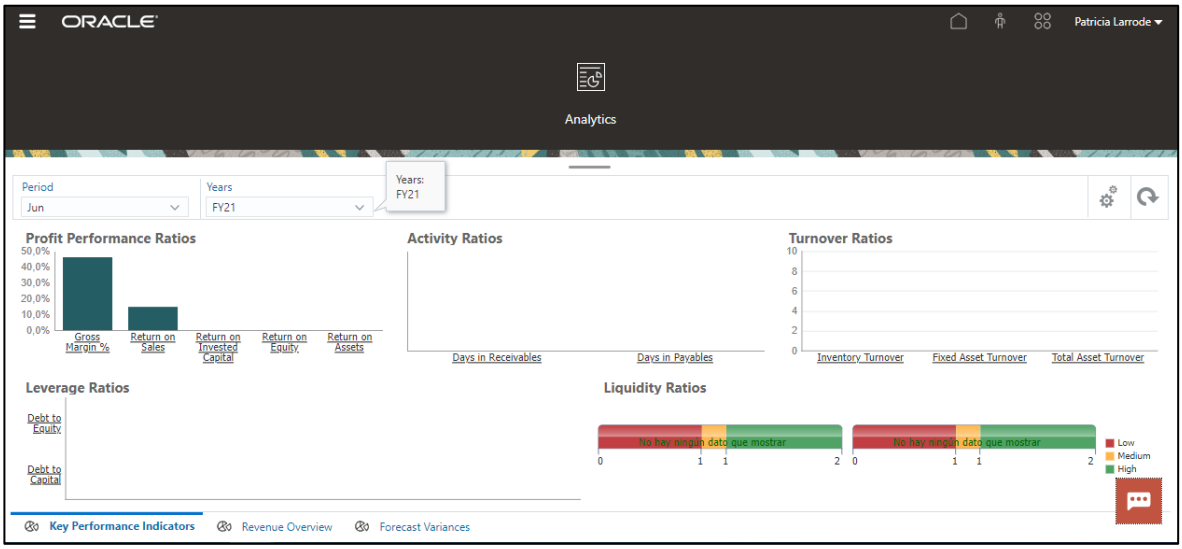
Oracle EPM Cloud - Consola Access Control.

La supervisión y la gestión completa de las aplicaciones del despliegue de EPM en la nube, permite a los administradores de IT mantener los procesos de negocio ágiles y optimizados en todas las operaciones.

1.3.2 ORACLE CLOUD EPM PLANNING

Para alinear la planificación de la organización, Oracle EPM Cloud dispone de las herramientas que responden a los cambios con agilidad y eficacia para todas las líneas de negocio.

Oracle Planning permite la toma de mejores decisiones creando planes basados en factores empresariales y orientados a objetivos. Puede conectar parte del negocio de la organización con un plan integrado en finanzas, operaciones y líneas de negocio.



Consola de Analytics.

A su vez, Oracle Planning permite realizar el modelado de formato libre a escala con EPM Freeform, creando varios modelos de escenarios posibles financieros y operativos complejos.

Por otro lado, Planning permite la planificación y ejecución empresarial integrada (IBPx) transformando los planes en ejecución y supervisando la actividad para la detección de eventos inesperados usando Internet of Things (IoT) e Inteligencia Artificial (IA).

Puede obtener más información relacionada con IBPx consultando el siguiente enlace de Oracle:

https://www.oracle.com/es/scm/supply-chain-planning/integrated-business-planning-execution/

Finalmente, puede capacitar a las finanzas para que se conviertan en datos impulsados por IPM, aplicando la ciencia de datos y el aprendizaje automático para aprovechar las oportunidades perdidas.

Puede obtener más información relacionada con Planning de Oracle Cloud EPM a través del siguiente enlace en inglés:

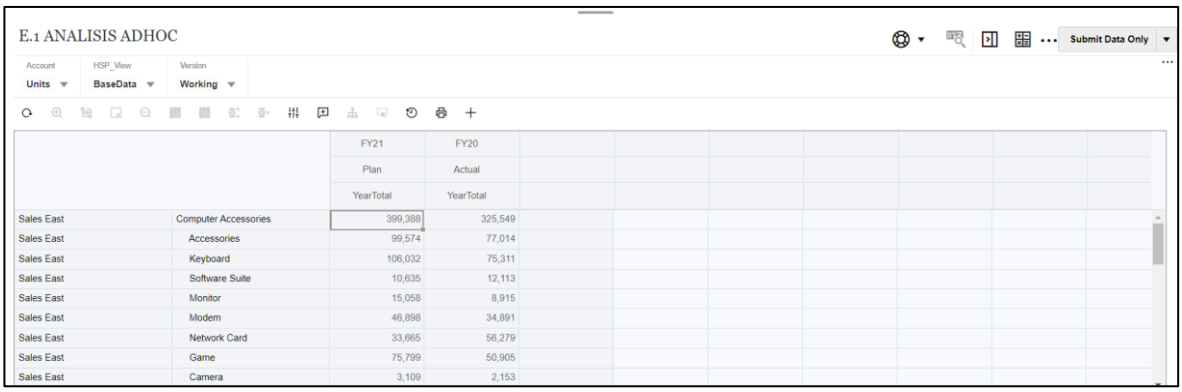
https://docs.oracle.com/en/cloud/saas/planning-budgeting-cloud/

1.3.3 ORACLE CLOUD EPM PROFITABILITY AND COST MANAGEMENT

Asignación de recursos de manera más eficiente para una comprensión más profunda de los costos y la rentabilidad para tomar decisiones más fundamentales sobre la dirección que debe llevar la empresa.

Oracle Cloud EPM Profitability and Cost Management permite el modelado flexible de los costos y la rentabilidad. Puede descubrir qué clientes, productos u otros segmentos del negocio de la organización son rentables y cuáles no lo son.

Por otro lado, puede asignar fácilmente el costo de los servicios compartidos a los departamentos y grupos que los utilizan.



Oracle EPM Cloud - Análisis Ad hoc.

Por último, puede analizar visualmente los datos más actuales mediante cuadros de mando totalmente configurables. Puede aprovechar los KPI y los gráficos prediseñados para realizar consultas como la curva de beneficios.

Puede obtener más información consultando el siguiente enlace de Oracle en inglés:

https://docs.oracle.com/en/cloud/saas/profit-cost-cloud/

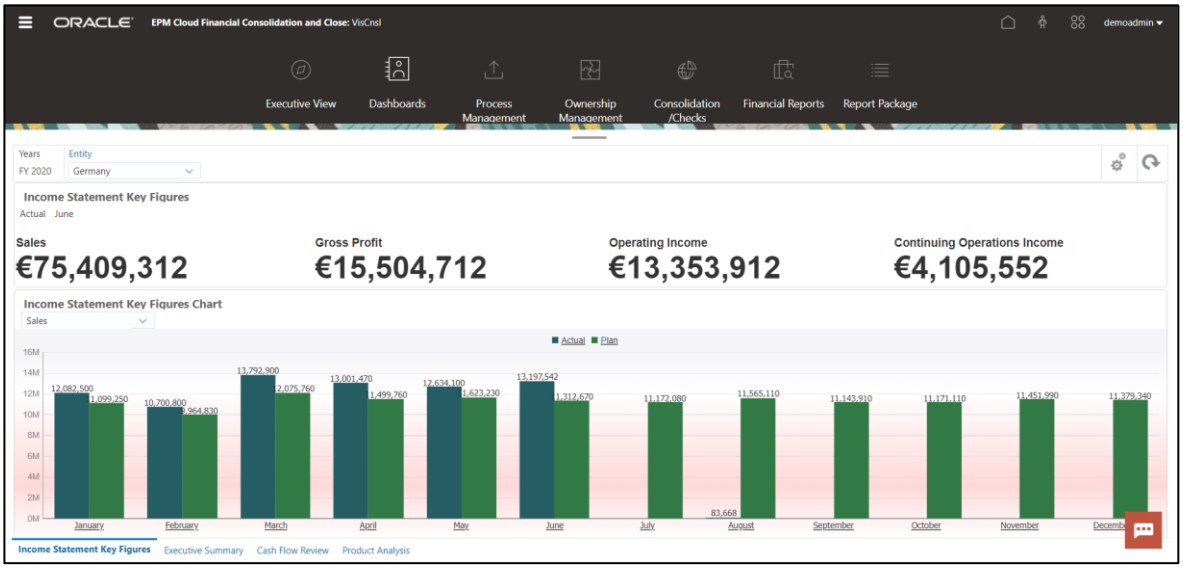
1.3.4 ORACLE CLOUD EPM FINANCIAL CONSOLIDATION AND CLOSE

Diseñado específicamente para administrar y mejorar de manera eficiente los procesos de consolidación y cierre.

Oracle Cloud EPM Financial Consolidation and Close integra las mejores prácticas para comenzar de manera ágil, mediante el cálculo automático para reducir la necesidad de personalización en el flujo de caja, el balance general, el estado de resultados, las transferencias o llamadas a la acción.

El servicio o aplicación permite realizar consolidaciones complejas, aumentando la precisión y la velocidad del proceso de cierre reclasificado. Ajusta y elimina datos para cualquier jerarquía con soporte de consolidación y trabaja fácilmente con resúmenes legales y de gestión complejos.

Además, permite la gestión del cierre mediante el seguimiento automático de métricas clave en toda la organización y la automatización inteligente de procesos (IPA), para aumentar el nivel de eficiencia con tecnologías avanzadas que automatizan las consolidaciones en segundo plano, disminuyendo el tiempo necesario para cumplir los requisitos de informes globales, incluidas las Normas Internacionales de Información Financiera (NIIF).



Dashboard Financial Consolidation and Close.

Finalmente, puede habilitar el cumplimiento de auditorías proporcionando transparencia para tareas como ajustes de diario con segregación forzada de funciones, cambio de datos, cálculos visibles y registro de actividad de los usuarios.

Puede obtener más información consultando el siguiente enlace de Oracle en inglés:

https://docs.oracle.com/en/cloud/saas/financial-consolidation-cloud/index.html

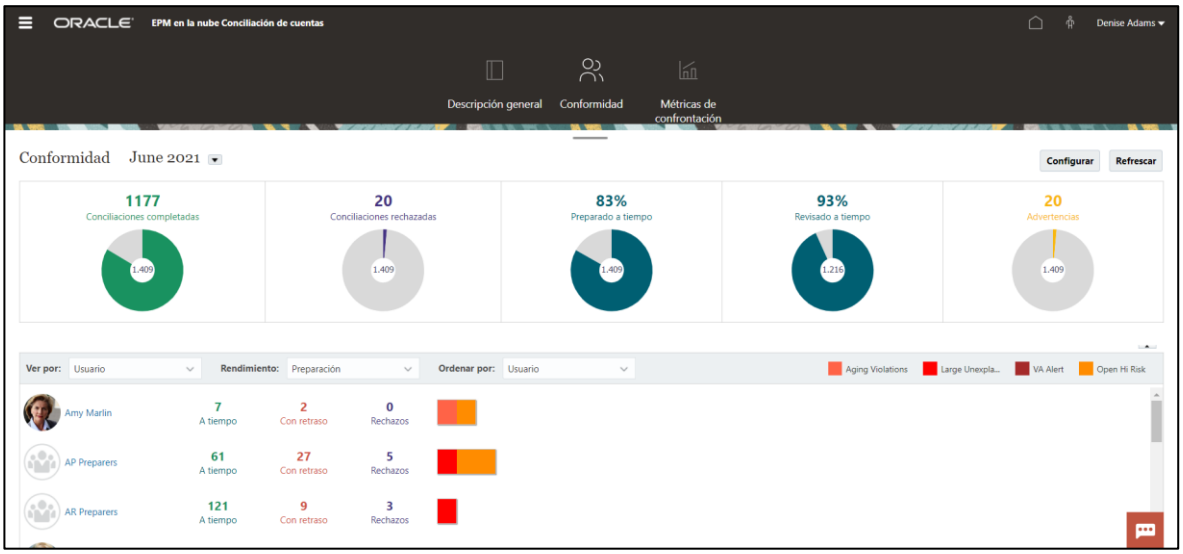
1.3.5 ORACLE CLOUD EPM ACCOUNT RECONCILIATION

Oracle Cloud EPM Account Reconciliation permite cerrar de manera ágil las conciliaciones de cuentas y la comparación de transacciones, para mejorar la eficiencia y precisión de los estados financieros de la organización, mientras aborda la seguridad y el riesgo típicamente asociado con el proceso.

Las conciliaciones de alto volumen de transacciones y trabajo intensivo requieren características sofisticadas de conciliación de transacciones. El motor de coincidencia automática puede coincidir con millones de transacciones en minutos.

Por otro lado, cada organización tiene una estrategia diferente sobre cuántos y qué tan detallados deben ser sus formatos de conciliación. Además, puede definir reglas y perfiles de cuenta que contenga calificación de riesgo, las asignaciones de flujo de trabajo o la moneda que se usará.

Puede mejorar la eficacia del ciclo cerrado con paneles operativos y de cumplimiento. Se podrá ver las conciliaciones abiertas, atrasadas o con vencimiento, así como los detalles de variación y añadir comentarios sobre ellas.



Panel de Conformidad en Oracle Cloud EPM Account Reconciliation.

El depósito de documentos seguro garantiza que las conciliaciones no se extravíen ni se pierdan proporcionando una capacidad de auditoría global. La evidencia de las conciliaciones se audita y registra en la aplicación para satisfacer las necesidades de cumplimiento.

Finalmente, puede modernizar el cierre financiero mediante la conexión integrada con Oracle Cloud EPM. Existen conexiones a otros procesos comerciales de Oracle Cloud EPM y aplicaciones de ERP, como Oracle Cloud ERP, E-Business Suite o SAP ERP para obtener datos y metadatos de muchas fuentes.

Puede obtener más información consultando el siguiente enlace de Oracle en inglés:

https://docs.oracle.com/en/cloud/saas/account-reconcile-cloud/index.html

1.3.6 ORACLE CLOUD EPM TAX REPORTING

Los cálculos de los impuestos utilizan los datos más actuales brindando una mayor precisión y velocidad, accediendo directamente a los datos financieros del libro mayor o del sistema de consolidación financiera.

La escala de generación automática de los impuestos se calcula des del nivel más bajo, por entidad legal, hasta la declaración fiscal consolidada con los requisitos de las NIIF.

Puede obtener más información relacionada consultando el siguiente enlace de Oracle en inglés:

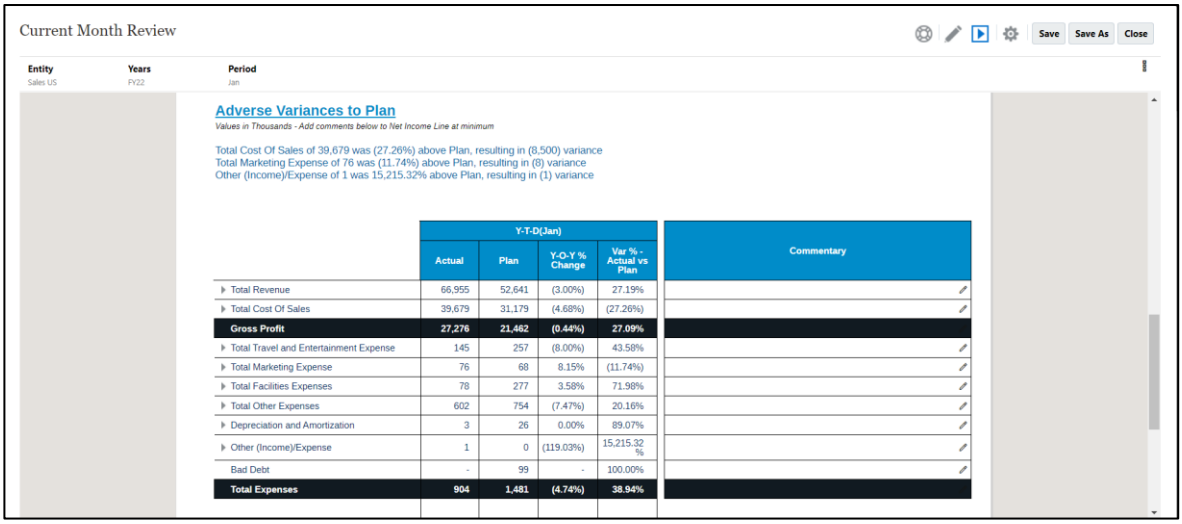
https://docs.oracle.com/en/cloud/saas/tax-reporting-cloud/

1.3.7 ORACLE CLOUD EPM NARRATIVE REPORTING

Para optimizar los procesos de generación de informes y combinación de datos y narraciones en un entorno seguro y colaborativo para las organizaciones, Oracle Cloud dispone del servicio EPM Narrative Reporting.

Por un lado, puede acceder a los sistemas de registro directamente para trabajar con datos que siempre estén actualizados desde fuentes de Oracle y de terceros.

Además, no es necesario volver a crear los informes existentes, ya que puede traer sus propios informes narrativos actuales de Microsoft Word, PowerPoint o PDF, así como informes basados en Excel a través de un proceso constante y controlado, en el que puede involucrar a varios autores de informes.



Reports de Narrative Reporting.

Por otro lado, puede crear libros de informes ejecutivos o de registro financiero, accediendo a los informes desde cualquier lugar mediante dispositivos móviles, web o Microsoft Office.

Finalmente, puede producir informes país por país para los reguladores fiscales, cumpliendo con los mandatos de generación de informes basados en XBRL y publicarlos en múltiples formatos reglamentarios.

Puede obtener más información relacionada consultando el siguiente enlace de Oracle en inglés:

https://docs.oracle.com/en/cloud/saas/enterprise-performance-reporting-cloud/index.html

1.3.8 ORACLE CLOUD EPM FREEFORM

Oracle EPM Cloud ofrece la potencia y flexibilidad de Essbase con la gobernanza y escalabilidad de la modalidad SaaS de OCI, para la toma de decisiones mediante análisis multidimensionales, planificaciones, modelado e informes.

Puede usar aplicaciones de planificación e informes a medida, hecho para usuarios comerciales, para la toma de decisiones sin ayuda de profesionales de IT o consultores.

La planificación operativa y financiera permite el modelado a gran escala, de forma libre y ad-hoc para los planificadores operativos. Los informes unificados satisfacen múltiples necesidades de informes internos y externos y acceso centralizado a través de múltiples procesos comerciales de EPM y sistemas ERP.

Por otro lado, puede importar cubos de Essbase y modelos de Excel locales para compartir en una plataforma segura basada en la nube, aprovechando el conjunto diverso de herramientas integradas de generación de informes y análisis, incluidos paneles, web y Oracle Smart View para Office basado en Excel.

Finalmente, puede analizar múltiples fuentes de datos para los análisis avanzados y complejos, conectando cada parte del negocio con las soluciones de planificación e informes personalizados de múltiples sistemas ERP y EPM.

Puede obtener más información consultando el siguiente enlace de Oracle en inglés:

https://docs.oracle.com/en/cloud/saas/freeform/index.html

1.3.9 ORACLE ENTERPRISE DATA MANAGEMENT

Para administrar los datos empresariales mientras se mantiene la integridad de los datos y la alineación de las aplicaciones empresariales de la organización, Oracle EPM Cloud dispone de la siguiente herramienta para la transformación empresarial ágil.

Gestione el cambio empresarial mediante la gestión de datos empresariales, incluyendo la gobernanza de datos de la organización, la visualización de datos de cambio y la gestión de jerarquías. Además, puede gestionar los cambios de elementos de datos maestros de la empresa agilizando las solicitudes, validando datos inmediatamente, visualizando el impacto de los cambios o simplificando los envíos.

Por otro lado, puede colaborar y ser coautor en tiempo real, realizar seguimiento de la actividad mediante hilos de conversación, etiquetando participantes, otorgando permisos granulares para el acceso a datos u optimizando el flujo de trabajo automatizado.

Finalmente, puede distribuir los cambios al resto de aplicaciones, automatizando las integraciones con la API REST y proporcionar transparencia proporcionando registros de auditoría.

Puede obtener más información relacionada consultando la siguiente documentación de Oracle en inglés:

https://docs.oracle.com/en/cloud/saas/enterprise-data-management-cloud/index.html

2. DESPLIEGUE SEGURO PARA ORACLE ENTERPRISE PERFORMANCE MANAGEMENT (EPM)

Para realizar un despliegue en la infraestructura de Oracle en la nube y los servicios de Oracle Enterprise Perfomance Management (EPM), es necesario realizar una serie de pasos que se describen a continuación.

2.1 ACTIVACIÓN DE UNA SUSCRIPCIÓN A ORACLE EPM CLOUD

Al adquirir una suscripción a Oracle Enterprise Perfomance Management Cloud como cliente nuevo en Oracle Cloud Infrastructure (OCI), Oracle le enviará un correo electrónico que identifica los pasos necesarios para activar la suscripción.

Nota: si es la primera vez que accede a los productos de Oracle Cloud Infrastructure, consulte la guía de seguridad CCN-STIC 889A Guía de Configuración segura para IAM y servicios de seguridad, para crear y formalizar un tenant en Oracle Cloud.

Los suscriptores a Oracle EPM Cloud necesitan una cuenta de Oracle Fusion Cloud Enterprise Performance Management para activar la orden.

Puede obtener más información mediante las instrucciones que proporciona Oracle para los clientes nuevos, a través del siguiente enlace:

https://docs.oracle.com/cloud/help/es/epm-common/CGSAD/idcs_activate_epm_subscription_first_time.htm

Por otro lado, para los clientes existentes, pueden obtener más información e instrucciones de activación de la suscripción a Oracle EPM Cloud, a través del siguiente enlace:

https://docs.oracle.com/cloud/help/es/epm-common/CGSAD/idcs_activate_epm_subscription_existing_user.htm

Finalmente, para los clientes de Oracle EPM Cloud que estén corriendo sobre Oracle Cloud Classic, pueden adquirir suscriciones adicionales que usen Oracle Cloud Classic, sin necesidad de activación inicial. Oracle crea los entornos de EPM Cloud del usuario y les envía correos electrónicos con los detalles de sus entornos y las credenciales de acceso a Mis Servicios (Classic).

Puede consultar más información relacionada con los conceptos clave de las suscripciones de Oracle Cloud en el siguiente enlace:

https://docs.oracle.com/cloud/help/es/epm-common/CGSAD/idcs_opc_key_concepts.htm

2.2 CREACIÓN DE CUENTAS ADMINISTRADORAS DE DOMINIO DE IDENTIDAD Y DEL SERVICIO

El administrador de la cuenta puede delegar las actividades de configuración mediante la creación de Administradores de Dominio de Identidad y Administradores del Servicio.

El Administrador de Dominio de Identidad no es un rol funcional de Oracle Cloud Enterprise Perfomance Management (EPM). Sin embargo, este rol permite a los usuarios trabajar con el proceso de negocio.

Para acceder a un proceso de negocio y trabajar en él, se debe otorgar a los usuarios uno de los cuatro roles funcionales que puede consultar en el siguiente enlace de Oracle:

https://docs.oracle.com/cloud/help/es/epm-common/CGSAD/4_managing_epm_cloud_users_roles_predefined_roles.htm

Nota: en la actualidad, Oracle fusiona IDCS y OCI IAM en un único servicio de nube para la autenticación, gestión de acceso, gestión de derechos e inicio de sesión único. Mediante el servicio de OCI IAM, el cliente puede disponer del control en la capa de acceso a los servicios y recursos de Oracle Cloud como, por ejemplo:

- Autenticación federada, social, delegada, adaptativa y multifactorial.
- Gestión de acceso, ciclo de vida de identidad manual o automatizado.
- Gestión de derechos de acceso sobre los recursos.
- Inicio de sesión único, federado, puertas de enlace, proxies, almacenamiento de contraseñas, etc.

Listado completo de dichos recursos y descripción de los mismos se puede encontrar en el siguiente enlace:
https://docs.oracle.com/es-ww/iaas/Content/Identity/getstarted/identity_domains.htm#overview

Cada instancia del servicio IAM de OCI se administra como dominios de identidad en la Consola de OCI. Un dominio de identidad es un servicio de administración de acceso e identidad autónomo para abordar la autenticación y gestión de derechos y privilegios sobre los recursos de la nube de Oracle de manera segura.

Debido a este cambio, y en concreto para la administración de los aplicativos de SaaS, la gestión de identidades y accesos se llevará también a cabo dentro de estos dominios de identidad en la Consola de la nube de Oracle. Esta gestión se realizaba, anteriormente, en Mis Servicios.

Además, permite una fácil administración de usuarios, grupos y acceso, API amigables para desarrolladores, cobertura de aplicaciones a través de servidores proxy, puentes, puertas de enlace que ofrecen SSO, informes y auditorías integrados sobre la actividad y el riesgo, etc.

Puede obtener más información sobre el servicio OCI IAM con dominios de identidad consultando el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/Content/Identity/home.htm

Por otro lado, el rol de Administrador de Servicio es el rol funcional más completo de Oracle EPM Cloud. Los usuarios que tengan este rol tienen acceso a la consola de Oracle Identity Cloud para OCI y al portal Mis Servicios para Classic y también para OCI. Este rol permite ver a los usuarios de Oracle EPM Cloud y gestionar sus roles predefinidos para los entornos en los que son administradores del servicio. Sin embargo, no pueden crear usuarios.

Para crear Administradores del Dominio de Identidad y Administradores del Servicio, se deben realizar los siguientes pasos que se describen a continuación:

a) Acceder a Mis Servicios (OCI) como administrador de la cuenta o Administrador del Dominio de Identidad.

b) En el menú de navegación, haga clic en Usuarios y, a continuación, en Identidad (principal).

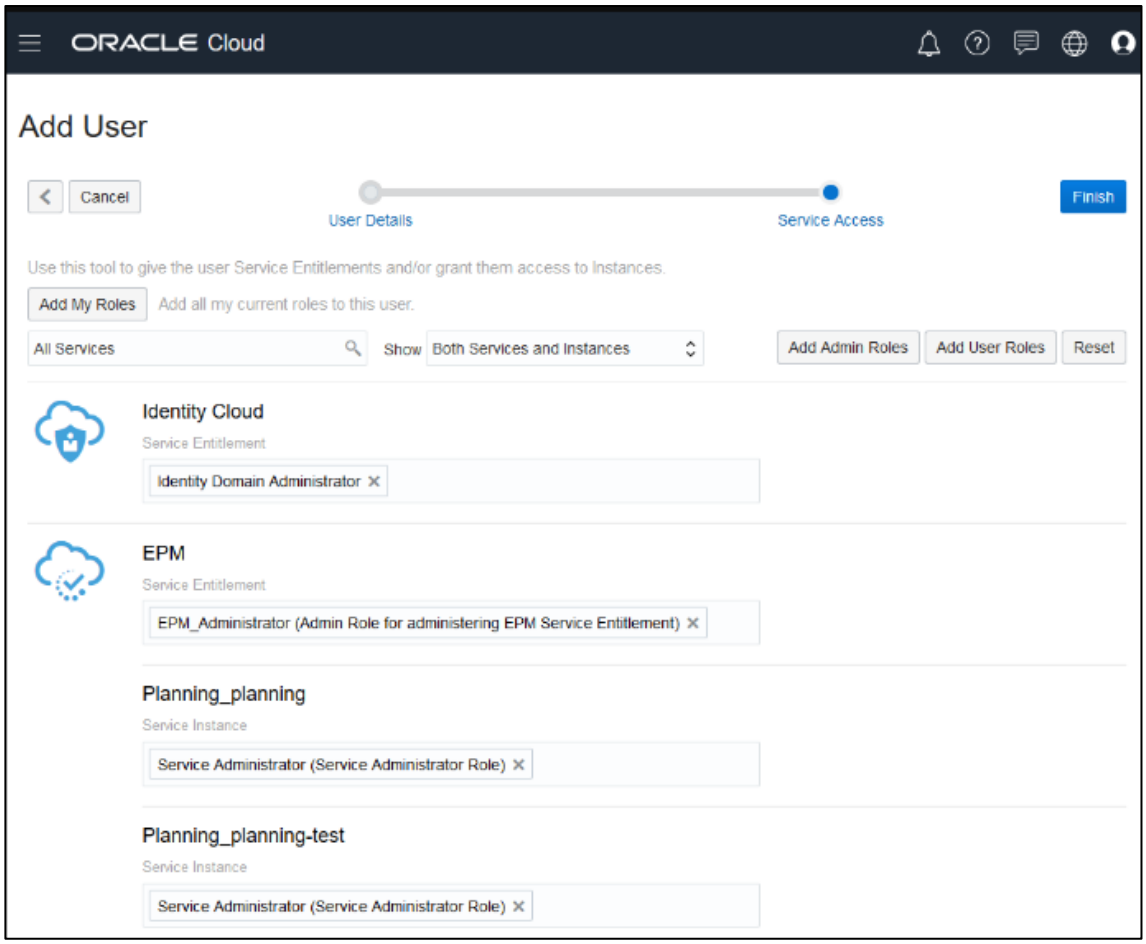
c) Haga clic en agregar.

d) En detalles del usuario, introduzca la información necesaria del usuario y, a continuación, haga clic en Siguiente.

e) En Acceso al servicio, seleccione uno o más roles para asignar:

   i. Administrador de Dominio de Identidad en Identity Cloud.

ii. Administrador del Servicio para cada instancia del servicio.



Consola Mis Servicios (OCI) para asignar roles.

f) Haga clic en Finalizar.

2.3 CREACIÓN DE UNA INSTANCIA DE ORACLE EPM CLOUD

La suscripción activada a Oracle Cloud Enterprise Performance Management otorga el derecho a crear una instancia que incluye dos entornos:

a) Un entorno para alojar la versión de prueba de un proceso de negocio.

b) Un entorno para alojar la versión de producción de un proceso de negocio.

Al crear una instancia, Oracle Fusion Cloud Enterprise Perfomance Management crea automáticamente los entornos.

Sin embargo, para crear una instancia de Oracle EPM Cloud, es necesario el rol de administrador de la cuenta de Cloud. A continuación, se describen los pasos para crear una instancia EPM Cloud:

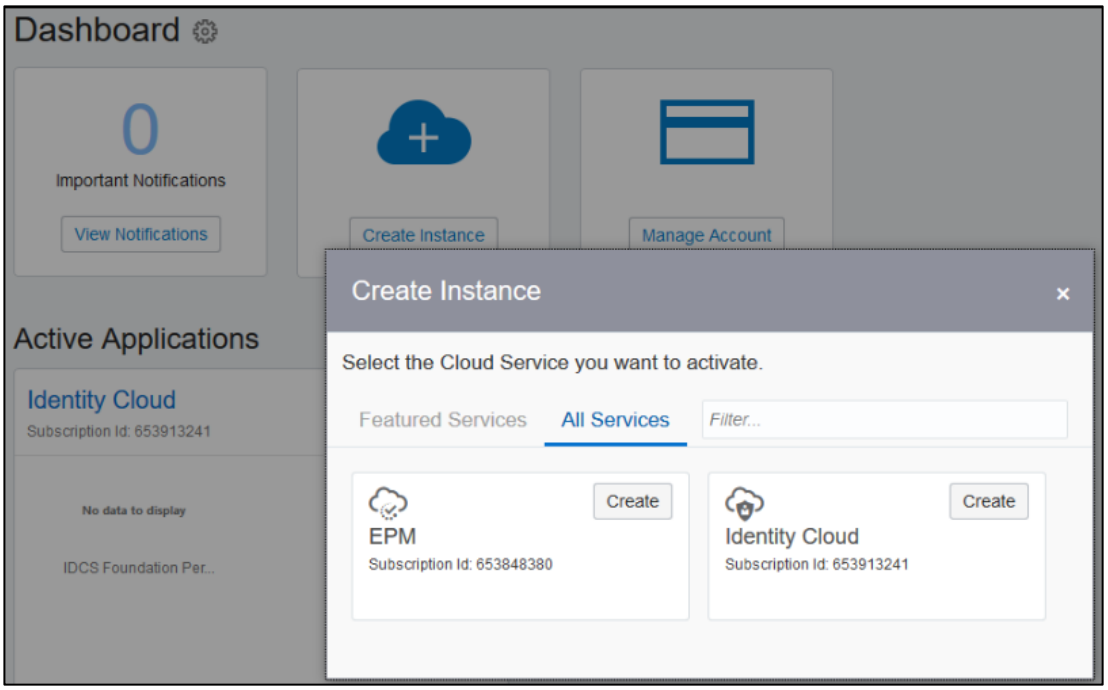
a) Puede crear la instancia directamente desde el correo electrónico que haya recibido tras activar el servicio e iniciar sesión. No obstante, es posible hacerlo accediendo a Mis Servicios (OCI).

Puede obtener más información consultando el siguiente enlace de Oracle:

https://docs.oracle.com/cloud/help/es/epm-common/CGSAD/idcs_log_int_cloud_account.htm

b) Una vez dentro, haga clic en Crear instancia.

c) En crear instancia, haga clic en Crear en el mosaico EPM.



Panel para la creación de una instancia.

d) Haga clic en Configuración.

e) En Centro de datos, seleccione un centro de datos cercano a la mayoría de los usuarios.

f) En Nombre, introduzca un nombre para este entorno. Este nombre forma parte de la URL para el acceso al entorno, por lo que los usuarios tienen que poder identificarlo fácilmente.

Puede obtener más información consultando los patrones de URL de OCI en el siguiente enlace de Oracle:

https://docs.oracle.com/cloud/help/es/epm-common/CGSAD/1_epm_cloud_accessing_sample_urls_oci.htm

g) Haga clic en Revisar.

h) Haga clic en Finalizar para enviar la solicitud de creación del entorno. Una vez creado el entorno, el mosaico de la aplicación EPM se agregará a Mis Servicios (OCI).

i) Puede ver los detalles de la instancia y del entorno haciendo clic en el nombre del mosaico.

3. CONFIGURACIÓN SEGURA PARA ORACLE SAAS ENTERPRISE PERFORMANCE MANAGEMENT (EPM)

Las medidas de seguridad se dividen en tres grupos, Marco Organizativo, Marco Operacional y Medidas de Protección del Esquema Nacional de Seguridad. En los siguientes puntos, se detallan los grupos Marco Operacional y Medidas de Protección con las medidas que aplican en la Categoría Alta del ENS.

3.1 MARCO OPERACIONAL

Este grupo está formado por las medidas a tomar en cuenta para proteger la operación del sistema como un conjunto integral de componentes para un fin. Para lograr el cumplimiento de los principios básicos y requisitos mínimos establecidos, se aplicarán las medidas de seguridad indicadas en este anexo, las cuales serán proporcionales a las dimensiones de seguridad relevantes en el sistema a proteger y la categoría del sistema de información a proteger.

Se considera, en este sentido, que la organización ha dispuesto todos aquellos mecanismos de control físico necesarios, con objeto de evitar el acceso a la nube existentes por parte de personal no autorizado.

3.1.1 CONTROL DE ACCESO

El conjunto de medidas que establece el Control de Acceso cubre todas las acciones que, bien preparatorias o ejecutivas, están orientadas a determinar qué o quién puede o no acceder a un recurso del sistema mediante una determinada acción. Con el cumplimiento de todas las medidas, se garantizará que nadie accederá a recursos sin la debida autorización.

3.1.1.1 IDENTIFICACIÓN

Esta medida especifica los mecanismos para garantizar que las entidades (usuarios o procesos) identificados en el sistema cuenten con un identificador único. Cuando el usuario disponga de diferentes roles frente al sistema, recibirá identificadores singulares para cada perfil o rol que vaya a desempeñar, de forma que se recaben siempre los correspondientes registros de actividad, delimitándose los privilegios correspondientes a cada perfil.

La identificación del usuario se traduce en la necesidad de crear cuentas únicas e inequívocas para cada usuario y servicio. Dichas cuentas deberán ser inhabilitadas cuando se den una serie de condicionantes:

a) El usuario deje la organización.

b) Cese en la función para la cual se requería dicha cuenta.

c) La persona que lo autorizó emita una orden en contra.

d) Las cuentas se retendrán durante el periodo necesario para atender a las necesidades de trazabilidad de los registros de actividad asociados a las mismas.

Por otro lado, la identificación del usuario permitirá singularizar a la persona asociada al mismo, utilizando los datos de identificación por el sistema, para determinar los privilegios del usuario conforme a los requisitos de control de acceso. Por último, se asegurará la existencia de una lista actualizada de usuarios autorizados y mantenida por el administrador del sistema o administrador de seguridad del sistema.

Oracle Fusion Cloud Enterprise Performance Management implanta varias capas de seguridad. Los componentes de seguridad de la infraestructura, de cuya implantación y gestión se encarga Oracle, crean entornos de Oracle EPM Cloud seguros.

Oracle EPM Cloud garantiza la seguridad con los siguientes mecanismos que permiten que solo los usuarios autorizados puedan acceder al servicio.

a) Inicio de sesión único (SSO)

b) Acceso basado en roles a los entornos

El inicio de sesión único y la seguridad basada en roles se controlan a través de Oracle Identity Management, que define un dominio de seguridad para cada entorno y la identificación unívoca que singulariza a la persona o proceso asociado con la cuenta. Tras un inicio de sesión correcto, el acceso al servicio se determina por el rol asignado al usuario.

Finalmente, los usuarios que necesiten acceder a un entorno deben tener una cuenta en el dominio de identidad asociado al entorno. El rol predefinido otorgado al usuario determina lo que el usuario puede hacer en el entorno.

3.1.1.2 REQUISITOS DE ACCESO

Los requisitos de acceso se aplican atendiendo a la necesidad de que los recursos del sistema queden protegidos con algún mecanismo que impida su utilización, salvo a las organizaciones que disfruten de los derechos de acceso suficientes a ellos.

Estos derechos se controlarán y asignarán atendiendo a la política y normativa de seguridad de la organización, a través de la persona responsable de dicha determinación y haciendo uso de mínimo privilegio.

Principalmente se controlará el acceso a los componentes del sistema y sus ficheros o registros de configuración. Además, todos los usuarios autorizados deben tener un conjunto de atributos de seguridad (privilegios) que puedan ser mantenidos individualmente.

Los privilegios de acceso se implementarán para restringir el tipo de acceso que un usuario puede tener (lectura, escritura, modificación, borrado, etc.).

Por otro lado, los servicios de Oracle EPM Cloud utilizan un conjunto común de roles funcionales predefinidos para controlar el acceso a los entornos.

El acceso a los entornos se otorga mediante la asignación de roles a los usuarios. Los Administradores de Dominio de Identidad y los Administradores del Servicio de Oracle EPM Cloud, pueden usar la consola de Oracle Cloud Identity para asignar roles predefinidos a los usuarios.

Para obtener más información relacionada con la asignación de roles con Identity Cloud Service, consulte el siguiente enlace de Oracle:

https://docs.oracle.com/cloud/help/es/epm-common/CGSAD/idcs_assign_roles_gen2.htm

Finalmente, las aplicaciones de Oracle EPM Cloud permiten crear grupos de usuarios. Puede definir usuarios de dominio de identidad u otros grupos como, por ejemplo, grupos para Planning, Módulos de Planning, FreeForm, Financial Consolidation and Close o Enterprise Profitability and Cost Managemen. La información de un grupo de cada entorno se mantiene de forma independiente.

Puede obtener más información relacionada con la administración del control de acceso para Oracle EPM Cloud, a través del siguiente enlace de Oracle en inglés:

https://docs.oracle.com/en/cloud/saas/enterprise-performance-management-common/pappm/index.html

3.1.1.3 SEGREGACIÓN DE FUNCIONES Y TAREAS

La segregación de funciones y tareas que establece el ENS se basa en establecer un control de acceso de forma que se exija la concurrencia de dos o más personas para realizar tareas críticas, anulando la posibilidad de que un solo individuo autorizado, pueda abusar de sus derechos para cometer alguna acción ilícita. Además, siempre que sea posible, la misma persona no aunará funciones de configuración y mantenimiento del sistema, ni funciones de auditoría o supervisión con cualquier otra función.

Todos los servicios de Oracle EPM Cloud que no sean Oracle Enterprise Data Management Cloud utilizan un conjunto común de cuatro roles funcionales predefinidos para controlar el acceso a los entornos de servicio:

a) Administrador del servicio

b) Usuario avanzado

c) Usuario

d) Visor

El acceso que un rol predefinido otorga a un entorno depende del tipo de servicio. Por ejemplo, el rol Usuario Avanzado en Planning permite gestionar la seguridad de las reglas de negocio y controlar el proceso de aprobación, mientras que el mismo rol en Tax Reporting permite ejecutar la automatización de impuestos e importar datos.

Los roles predefinidos de Oracle EPM Cloud son jerárquicos. El acceso otorgado a través del rol inferior es heredado por el rol de nivel superior. Por ejemplo, los Administradores de Servicio, además del acceso que solo tienen ellos, heredan el acceso otorgado a los roles Usuario Avanzado, Usuario y Visor.

Nota: el comportamiento de todos los roles predefinidos que no sea el rol de Administrador del Servicio se ve afectado por la opción Aplicar Seguridad, definida a nivel de dimensión en el proceso de negocio. Al desactivar la opción Aplicar Seguridad, las dimensiones quedan desprotegidas, lo que permite que todos los usuarios asignados a roles predefinidos accedan a los datos y escriban en ellos en los miembros de dimensión.

Oracle recomienda que seleccione la opción Aplicar Seguridad a nivel de dimensión para aplicar la seguridad.

Por otro lado, además de los roles funcionales, todos los servicios de Oracle EPM Cloud usan el rol Administrador de Dominio de Identidad para realizar tareas de gestión del dominio de identidad.

El Administrador de Dominio de Identidad no hereda los privilegios de acceso otorgados a través de roles funcionales. Para acceder a las funciones de servicio, se debe otorgar uno de los cuatro roles funcionales al Administrador de Dominio de Identidad.

Nota: el Administrador de Dominio de Identidad gestiona tanto el entorno de producción como el de prueba de todos los servicios que pertenecen a un dominio de identidad. Un usuario que solo tenga asignado el rol Administrador de Dominio de Identidad no se cuenta en el recuento de licencias de usuarios designados. Solo los usuarios que tengan asignados los roles predefinidos de Oracle EPM Cloud se cuentan en el recuento de licencias de usuarios designados.

A continuación, se reúnen los roles funcionales por aplicaciones y una breve descripción de la función que desempeñan:

Servicio o aplicación	Roles	Descripción
Planning, Planning Modules y Freeform	Administrador del servicio	Realiza todas las actividades funcionales de Planning, Planning Modules o de FreeForm, incluso otorgar roles a usuarios.
	Usuario Avanzado	Visualiza e interactúa con los datos. Este rol otorga acceso de alto nivel a varias áreas funcionales dentro de un entorno.
	Usuario	Introduce datos en formularios y los envía para su aprobación, analiza los formularios con funciones ad hoc y controla la capacidad de ir a los detalles del sistema de origen.
	Visor	Visualiza y analiza datos mediante formularios y herramientas de acceso a datos.
Profitability and Cost Management	Administrador del servicio	Realiza todas las actividades funcionales en un entorno.

Servicio o aplicación	Roles	Descripción
	Usuario Avanzado	Controla el proceso de desarrollo y ejecución de modelos. Este rol otorga acceso de alto nivel a varias áreas funcionales dentro de un entorno. Los usuarios Avanzados pueden realizar todas las actividades que puede realizar un Visor. Además, un usuario avanzado puede realizar estas tareas: • Crea cuadrículas ad hoc y escribe en las cuadrículas ad hoc y los datos de carga con Data Integration. • Crea, borra y copia datos de PDV. • Crea y ejecuta integraciones. • Crea modelos. • Crea y edita curvas de perfil.
	Usuario	Introduce datos donde se soliciten datos al usuario, ejecuta herramientas analíticas e informes y diseña reglas y cálculos. Los usuarios pueden realizar todas las tareas que pueden realizar los visores. Un Usuario puede realizar estas operaciones adicionales: • Realiza las funciones ad hoc, pero no puede escribir en las cuadrículas ad hoc o los datos de carga con Data Integration. • Obtiene detalles. • Crea, modifica y suprime reglas. • Realiza la edición masiva de reglas. • Ejecuta el balance de reglas. • Ejecuta validaciones. • Ejecuta cálculos, vistas y suprime el historial de cálculos.
	Visor	Ve y analiza los datos.

Servicio o aplicación	Roles	Descripción
Financial Consolidation and Close	Administrador del Servicio	Realiza todas las actividades funcionales de Financial Consolidation and Close, incluido otorgar roles a los usuarios. • Acceder a todas las tareas, las plantillas del Gestor de tareas y los programas. • Crear y administrar tipos de tarea, tipos de integración, atributos y tipos de alerta. • Generar y gestionar informes del Gestor de datos adicionales y del Gestor de tareas. • Definir y desplegar juegos de datos adicionales y gestionar periodos de recopilación de datos. • Gestionar formularios de datos adicionales.

Servicio o aplicación	Roles	Descripción
	Usuario Avanzado	Visualiza e interactúa con los datos. Este rol otorga acceso de alto nivel a varias áreas funcionales de Financial Consolidation and Close. Un Usuario Avanzado puede realizar las siguientes actividades: • Crear y mantener formularios, hojas de trabajo de Oracle Smart View for Office, reglas de negocio, listas de tareas e informes de Financial Reporting. • Consolidar los datos según sea necesario para las entidades a las que tiene acceso. • Controlar el proceso de aprobaciones, realizar acciones en unidades de consolidación y asientos a los que tiene acceso de modificación y asignar propietarios y revisores para la organización de la que está a cargo. • Importar datos. • Crear y guardar Smart Slices. • Crear y gestionar tareas, plantillas, tipos de tareas y programas del Gestor de tareas. • Definir y desplegar juegos de datos adicionales. • Definir formularios de datos adicionales y modificar los datos del formulario.

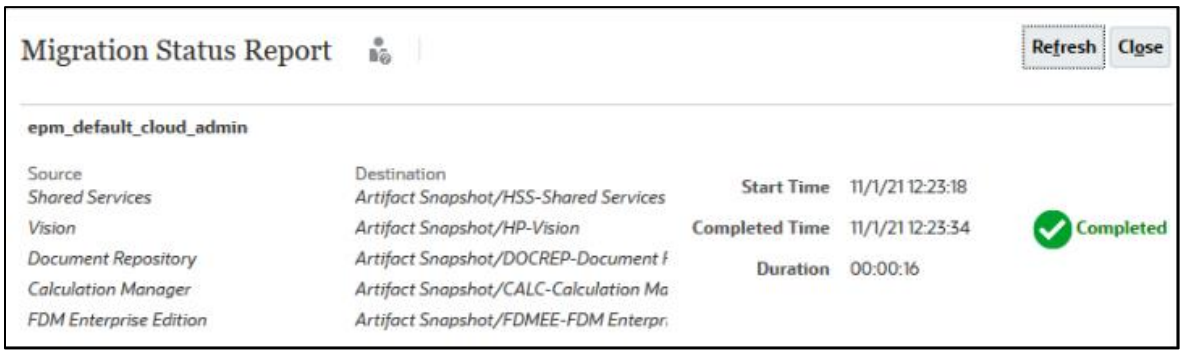
Servicio o aplicación	Roles	Descripción
	Usuario	Las actividades que puede realizar un Usuario son las siguientes: • Introducir y enviar datos para su aprobación, analizar formularios con funciones ad hoc y controlar la capacidad de obtención de detalles del sistema de origen. • Crear y enviar para su aprobación los asientos de los miembros de dimensión para los que tienen derechos Modify (modificación). • Acceder a Data Management (para crear una integración, ejecutar una integración y obtener detalles) y cargar datos si al usuario se le otorga un rol de aplicación que garantiza dicho acceso. • Modificar el estado de las tareas, crear y modificar alertas, comentarios y preguntas del Gestor de tareas. • Acceder a los paneles del Gestor de tareas y del Gestor de datos adicionales. • Introducir y editar datos en los formularios de datos adicionales.
	Visor	Las tareas que puede realizar un Visor son las siguientes: • Ver y analizar los datos mediante formularios y cualquier herramienta de acceso a datos, como informes, Smart Slice y registros, si se han concedido al usuario derechos de acceso a objetos relacionados, como los formularios de datos y las cuadrículas ad hoc (el usuario no puede crear estos objetos). Un usuario que solo tiene acceso de vista no puede acceder al cubo de consolidación o de tipos. • Ver programas del Gestor de tareas y datos del formulario de datos adicionales.

Servicio o aplicación	Roles	Descripción
Account Reconciliation	Administrador del Servicio	Configura el sistema y gestiona la totalidad del proceso de conciliación. Estos usuarios tienen acceso sin restricciones a todas las funciones de Account Reconciliation con la posibilidad de ver todas las conciliaciones.
	Usuario Avanzado	Agrega y mantiene perfiles y crea conciliaciones a partir de esos perfiles, pero solo si los perfiles están dentro del filtro de seguridad del usuario.
	Usuario	Prepara y revisa las vistas o conciliaciones de cuentas o los comentarios de las conciliaciones.
	Visor	Ve las conciliaciones.
Narrative Reporting	Administrador del Servicio	Realiza todas las actividades funcionales, incluido la asignación de roles predefinidos a usuarios de Narrative Reporting.
	Usuario Avanzado	• Crea paquetes de informes y definiciones de informes de gestión. • Crea carpetas, incluidas carpetas de nivel raíz. • Crea y mantiene todos los artefactos, como modelos, dimensiones y asignación de datos.
	Usuario	Ve los artefactos de Narrative Reporting a los que tiene acceso el usuario.
	Visor	Ve los informes y otros artefactos a los que tiene acceso el usuario. Es el rol mínimo necesario para iniciar sesión en un entorno y utilizarlo.
Enterprise Data Management	Administrador del Servicio	Realiza todas las actividades funcionales. Crea aplicaciones, vistas y actualiza datos. Realiza tareas administrativas que incluye la asignación de roles funcionales a los usuarios.
	Usuario	Crea vistas y aplicaciones y trabaja con cadenas de datos.

Para finalizar, Oracle EPM Cloud usa una cuenta de usuario definida de forma interna denominada epm_default_cloud_admin (también puede aparecer como SYSTEM en algunas interfaces de usuario e informes). Esta cuenta, reservada para uso interno de Oracle EPM Cloud, no se puede utilizar para acceder a entornos de Oracle EPM Cloud desde Internet.

Oracle EPM Cloud usa la cuenta SYSTEM internamente para realizar acciones del sistema, como la copia de seguridad diaria.

Por ejemplo, en el informe "Estado de la migración" se muestra epm_default_cloud_admin como el usuario que ha creado Artifact Snapshot durante el mantenimiento diario.



Oracle EPM Cloud - Migration Status Report.

3.1.1.4 PROCESO DE GESTIÓN DE DERECHOS DE ACCESO

El proceso de gestión de derechos de acceso a Oracle debe limitar los mismos, aplicando los principios de mínimo privilegio, necesidad de conocer y capacidad de autorizar dentro de las dimensiones de la Integridad, Confidencialidad, Autenticidad y Trazabilidad.

Los privilegios de cada usuario se reducirán al mínimo estrictamente necesario para cumplir sus obligaciones. De esta forma se acotan los daños que pudiera causar a una organización, de forma accidental o intencionada. Los privilegios se limitarán de forma que los usuarios sólo accederán al conocimiento de aquella información requerida para cumplir sus obligaciones. Sólo y exclusivamente el personal con competencia para ello, podrá conceder, alterar o anular la autorización de acceso a los recursos, conforme a los criterios establecidos por su responsable.

Por otro lado, el acceso a los procesos de negocio de Oracle Enterprise Performance Management Cloud se controla de forma estricta mediante el uso de roles predefinidos. Estos roles determinan el acceso funcional que tiene cada usuario en un proceso de negocio.

Además, los administradores del servicio pueden usar la funcionalidad de Control de Accesos para crear grupos que incluyan a los usuarios del dominio de identidad o a otros grupos. La asignación de permisos a estos grupos permite a los Administradores de Servicio otorgar permisos a varios usuarios a la vez, lo cual reduce la sobrecarga administrativa.

Finalmente, la asignación de permisos en el nivel de aplicación solo puede mejorar los derechos de acceso de los usuarios; ninguno de los privilegios que haya otorgado un rol predefinido puede restringirse mediante los permisos asignados en el nivel de aplicación. De esta forma se cumplen los requisitos de control de acceso basado en roles (RBAC).

3.1.1.5 MECANISMOS DE AUTENTICACIÓN

Dentro de los procesos habituales en el manejo de los sistemas de la información, el relativo a la autenticación corresponde al primero a llevar a efecto. Antes de acceder a datos, gestionar recursos o tratar servicios es necesario indicar al sistema "quién eres". Además, antes de activar el mecanismo de autenticación, el usuario debe reconocer que ha recibido y aceptado las obligaciones que implica su tenencia, custodia, protección y confidencialidad.

Las credenciales estarán bajo el control exclusivo del usuario y se activarán una vez estén bajo su control efectivo. A su vez, deben cambiar con una periodicidad marcada por la política de seguridad de la organización.

Las credenciales serán inhabilitadas, pudiendo ser regeneradas, cuando conste o se sospeche su pérdida, compromiso o revelación a entidades (personas, equipos o procesos) no autorizados o cuando la entidad termina su relación con el sistema.

Antes de autorizar el acceso, la información presentada por el sistema debe ser la mínima imprescindible para que el usuario pueda autenticarse, evitando todo aquello que pueda, directa o indirectamente, revelar información sobre el sistema o la cuenta, sus características, operación o estado.

Según establece el propio Esquema Nacional de Seguridad, en el nivel alto, se prohíbe el uso de autenticadores basados en el empleo exclusivo de claves concertadas y se exige, para ello, el uso de claves de un solo uso (OTP) o bien el uso de certificados o certificados en dispositivo físico, que empleen algoritmos acreditados por el Centro Criptológico Nacional y que Oracle cumple disponiendo del Certificado de cumplimiento con el ENS en su Categoría Alta.

Dado que el servicio Oracle EPM Cloud será accesible por los usuarios a través de un acceso público en Internet, las consideraciones de acceso local (usuarios de la organización) y acceso remoto (usuarios externos) quedarán unificadas debido a que la validación y autenticación siempre se va a producir en el punto de acceso público.

A efectos de esta guía, se tiene también en consideración la autenticación de tipo local que puede realizarse en los servicios de Infraestructura en la nube de Oracle desde dichos puestos de trabajo dentro de las dimensiones de la Integridad, Confidencialidad, Autenticidad y Trazabilidad.

El Esquema Nacional de Seguridad tiene en cuenta la aplicación de medidas diferentes atendiendo a la criticidad de servicios y sistemas. Ya desde el nivel más bajo es necesaria la prevención de los ataques para evitar intentos reiterados contra los sistemas de autenticación, limitando el número de intentos y que estos queden registrados, tanto los intentos satisfactorios como los erróneos.

Por otro lado, para los entornos de Oracle EPM Cloud, puede configurar un inicio de sesión único para autenticar usuarios que pertenecen a un proveedor de identidad compatible con SAML 2.

Nota: Oracle EPM Cloud solo soporta el inicio de sesión único iniciado por un proveedor de servicio (SP); no soporta un inicio de sesión iniciado por un proveedor de identidad (IdP).

Los usuarios utilizan las credenciales de inicio de sesión único de acceso a los recursos de red de su organización para autenticarse una vez en el entorno de Oracle EPM Cloud y, posteriormente, acceder fácilmente a otros entornos en la nube configurados con el mismo proveedor de identidad.

Puede utilizar cualquier proveedor de identidad SAML 2.0 (como Oracle Identity Federation, Microsoft Active Directory Federation Services 2.0+, Okta, Ping Identity PingFederate y Shibboleth Identity Provider) para establecer el inicio de sesión único.

Puede obtener más información sobre la gestión del inicio de sesión único de Oracle a través del siguiente enlace en inglés:

https://docs.oracle.com/en/cloud/get-started/subscriptions-cloud/csimg/managing-oracle-single-sign.html

También puede obtener más información relacionada con la adición de un proveedor de identidad SAML para la versión de OCI (Gen2), a través del siguiente enlace de Oracle en inglés:

https://docs.oracle.com/en/cloud/paas/identity-cloud/uaids/add-saml-identity-provider.html

Nota: Oracle debe acceder a sus entornos para solucionar los problemas. Este acceso es muy seguro y está regulado. Solo se permite el acceso a los entornos de Oracle EPM Cloud a un grupo concreto de empleados de Oracle, que han realizado una formación especial relacionada con la gestión de los entornos de los clientes. En este acceso se usa la autenticación de varios factores y se realiza una auditoría de todos los accesos.

Además, para la autenticación local mediante credenciales de Oracle EPM Cloud, se recomienda establecer una política contraseña personalizada con una longitud de al menos 12 caracteres y con la máxima complejidad posible que se pueda establecer.

Finalmente, puede configurar políticas de inicio de sesión que permite a los Administradores de Dominio de Identidad, Administradores de Seguridad y Administradores de Aplicaciones definir los criterios que debe utilizar Oracle Identity Cloud Service, para determinar si permite o impide que un usuario inicie sesión en Oracle EPM Cloud.

Puede obtener más información relacionada con las políticas de inicio de sesión consultando el siguiente enlace de Oracle en inglés:

https://docs.oracle.com/en/cloud/paas/identity-cloud/uaids/understand-sign-policies.html

3.1.2 EXPLOTACIÓN

Se incluyen en este apartado, todas aquellas medidas designadas como parte de la explotación de los servicios. El ENS define, a través de ellas, una serie de procesos tanto para el control como para la gestión que deberán llevarse a cabo por parte de las entidades.

Las medidas atienden a diferentes tareas que deberán ser llevadas a la práctica por el departamento de informática.

3.1.2.1 MANTENIMIENTO Y ACTUALIZACIONES DE SEGURIDAD

Para mantener el equipamiento físico y lógico que constituye el sistema, se aplicará lo siguiente:

a) Se atenderá a las especificaciones de los fabricantes en lo relativo a instalación y mantenimiento de los sistemas, lo que incluirá un seguimiento continuo de los anuncios de defectos.

b) Se dispondrá de un procedimiento para analizar, priorizar y determinar cuándo aplicar las actualizaciones de seguridad, parches, mejoras y nuevas versiones. La priorización tendrá en cuenta la variación del riesgo en función de la implantación o no de la actualización.

c) El mantenimiento solo podrá realizarse por personal debidamente autorizado.

Además, para la aplicación de la categoría alta del ENS, antes de poner en producción una nueva versión o una versión parcheada, se debe realizar pruebas en un entorno de prueba controlado y consistente en configuración al entorno de producción. Las nuevas instalaciones deben funcionar correctamente y no disminuir la eficacia de las funciones necesarias para el trabajo diario.

Nota: para Oracle, la priorización se basará en la gravedad asignada, siguiendo la evaluación estándar Common Vulnerability Scoring System y el posible impacto de negocio en función de la implantación o no de la actualización.

Oracle lanza una revisión que contiene correcciones de errores, optimización de código y actualizaciones de funciones el primer viernes del mes. Oracle aplica esta revisión al entorno de prueba del servicio durante el siguiente periodo de mantenimiento diario tras el lanzamiento de la revisión. Normalmente, a los entornos de producción se les aplican parches el tercer viernes de cada mes.

a) **Actualizaciones mensuales de entornos:** Oracle informa a los administradores del servicio sobre las actualizaciones que incluye cada revisión. En el caso de las versiones de parches secundarias, Oracle suele enviar notificaciones con una semana de antelación antes de aplicarlas en el entorno de prueba. Respecto a las actualizaciones principales, Oracle envía una notificación con dos meses de antelación.

Nota: Oracle notifica las actualizaciones principales con una semana de antelación a su aplicación al entorno de producción. No obstante, el calendario de las actualizaciones se encuentra actualizado continuamente en el Cloud Portal, accesible al administrador del servicio designado.

b) **Mantenimiento diario:** cada entorno de Oracle Enterprise Performance Management Cloud requiere hasta una hora al día para realizar el mantenimiento rutinario. Los administradores del servicio pueden seleccionar y cambiar la mejor hora para iniciar el proceso de mantenimiento.

En el sitio web “Preparación para la versión de Oracle Cloud”, hay publicado un documento que proporciona información detallada sobre la actualización de servicio instalada actualmente. Entre la información que puede estar disponible en este sitio web, se incluyen anuncios y nuevas funciones, cambios de comportamiento y defectos corregidos que puede consultar en el siguiente enlace de Oracle en inglés:

https://www.oracle.com/webfolder/technetwork/tutorials/tutorial/readiness/home/index.html

Por otro lado, el mantenimiento diario es un proceso automatizado que realiza las siguientes operaciones:

a) Crea una instantánea de mantenimiento denominada Artifact Snapshot.

b) Aplica cualquier parche necesario como actualizaciones mensuales, parches semanales y parches puntuales.

c) Ajusta las configuraciones como cachés.

d) Analiza todas las actividades realizadas y los registros creados durante las últimas 24 horas para crear un informe de actividad.

e) La nueva instantánea de mantenimiento reemplaza a la anterior.

Oracle recomienda descargar la instantánea a diario para realizar copias de seguridad del entorno.

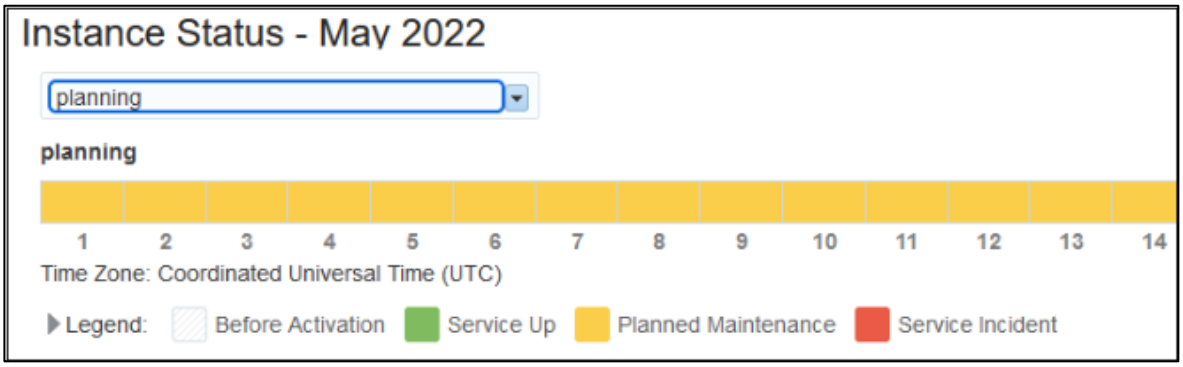
Los entornos de Oracle Enterprise Performance Management Cloud se paran durante el mantenimiento diario para crear copias de seguridad de Essbase y aplicar los parches necesarios. Luego de esto, el entorno se reinicia y solo está disponible para los administradores del servicio mientras el proceso de mantenimiento lleva a cabo copias de seguridad de la base de datos.

Dado que los entornos no están disponibles para los usuarios durante el periodo de mantenimiento, el administrador del servicio debe identificar un periodo de una hora en el que nadie utilice el servicio. Se cerrará la sesión de cualquier usuario conectado y se perderán los datos sin guardar.

Nota: para permitir a los usuarios guardar sus datos, Oracle EPM Cloud muestra una notificación de mantenimiento inminente 15 minutos antes de que el proceso de mantenimiento comience. Puede que algunos servicios realicen operaciones de mantenimiento adicionales. Por ejemplo, Módulos de Planning, Account Reconciliation y Financial Consolidation and Close pueden necesitar un tiempo de mantenimiento adicional para la actualización del contenido.

Finalmente, la hora de inicio del mantenimiento predeterminada está entre las 10:00 p.m. y la 1:00 a.m. hora local del centro de datos que aloja el entorno. Si no restablece la hora de inicio predeterminada para un entorno, Oracle la establecerá aleatoriamente para que comience entre las 10:00 p.m. y la 1:00 a.m., hora local del centro de datos. Después de seleccionar una hora de inicio del mantenimiento, Oracle respeta la selección.

Además, debido al mantenimiento diario planificado, el estado del entorno en la consola Mis servicios se muestra siempre como Planned Maintenance (en amarillo) incluso si el entorno no tiene ningún mantenimiento planificado para el día.



Estado del entorno desde la consola Mis Servicios.

Para establecer la hora de inicio del mantenimiento de un entorno, consulte la siguiente documentación de Oracle:

https://docs.oracle.com/cloud/help/es/epm-common/CGSAD/6_house_keeping_tasks_understand_service_maintenance_time.htm

3.1.2.2 GESTIÓN DE CAMBIOS

Esta medida contempla el mantenimiento de un control continuo de los cambios realizados en el sistema, de forma que exista una planificación de los cambios para reducir el impacto sobre la prestación de los servicios afectados. La información que se registra para cada petición de cambio debe ser suficiente para que quien deba autorizarlos no tenga dudas al respecto, facilitando la gestión.

Las pruebas de preproducción, siempre que sea posible realizarlas, se deben efectuar en equipos equivalentes a los de producción. Mediante un análisis de riesgos se determinará si los cambios son relevantes para la seguridad del sistema y una vez implementado un cambio, se deben realizar pruebas de aceptación convenientes.

Por último, antes de la aplicación de los cambios, se debe tener en cuenta la posibilidad de revertirlos en caso de la aparición de efectos adversos, teniendo que comunicar todos los fallos en el software y hardware al responsable designado en la organización de seguridad. Todos los cambios en el sistema deberán ser documentados, incluyendo una valoración del impacto y que dicho cambio supone en la seguridad del sistema.

La aplicación técnica de la presente medida de seguridad tiene relación con la recomendación de Oracle para la descarga diaria de los snapshots que realiza automáticamente durante los periodos de mantenimiento fijados por el administrador o bien, por Oracle.

Además, puede consultar la herramienta de Funciones de Oracle EPM Cloud para ver una lista de funciones que se lanzan cada mes para el proceso de negocio de Oracle EPM Cloud, a través del siguiente enlace de Oracle:

https://docs.oracle.com/cloud/help/es/epm-common/CGSAD/1_about_epm_cloud_new_features_tool.htm

3.1.2.3 PROTECCIÓN FRENTE A CÓDIGO DAÑINO

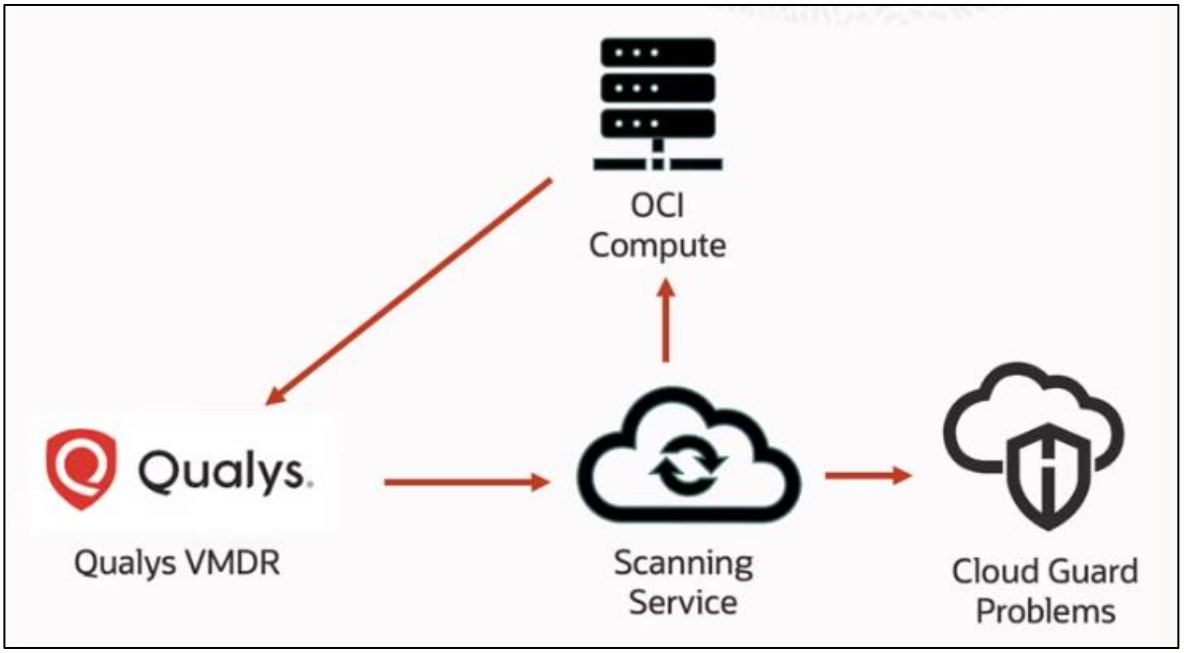
Para la protección de los sistemas frente a código dañino, el ENS establece que se debe disponer de mecanismos de prevención y reacción frente a este tipo de amenazas como, virus, gusanos, programas espías, más conocidos por su terminología inglesa “spyware” y en general, todo lo conocido como “malware”.

Por último, se deben realizar escaneos periódicos, realizar revisiones preventivas del sistema, establecer una lista blanca y disponer de capacidad de respuesta en caso de un incidente.

Para cumplir el requisito de la gestión de amenazas y vulnerabilidades, Oracle utiliza QualysGuard de Qualys para detectar vulnerabilidades de seguridad.

QualysGuard ofrece datos de inteligencia de seguridad que facilita los procesos de conformidad de seguridad de Oracle.

El uso de QualysGuard garantiza que los servidores de Internet, los sitios web y las aplicaciones web estén actualizados y configurados de forma segura frente a ataques malintencionados. También permite garantizar que no haya malware cargado en los blogs y las páginas de foros, así como que los formularios web no incluyan posibles riesgos de pirateo informático.



Arquitectura funcional de Qualys y OCI.

El servicio de análisis de vulnerabilidades de OCI ha ofrecido escaneo nativo de instancias de cómputo OCI desde su lanzamiento inicial. Sin embargo, Oracle ofrece en la actualidad una opción integrada de Qualys para las instancias Oracle EPM Cloud que aprovechan el mismo motor de exploración de vulnerabilidades.

3.1.2.4 GESTIÓN DE INCIDENTES

Esta medida indica la necesidad en las organizaciones de disponer de procesos frente a incidentes con un alto impacto en la seguridad de los sistemas, incluyendo:

a) Un proceso integral para hacer frente a los incidentes que puedan tener un impacto en la seguridad del sistema, que incluya el informe de eventos de seguridad y debilidades, detallando los criterios de clasificación y el escalado de la notificación.

b) La gestión de incidentes que afecten a datos personales tendrá en cuenta lo dispuesto en el Reglamento General de Protección de Datos; la Ley Orgánica 3/2018, de 5 de diciembre, en especial su disposición adicional primera, así como el resto de normativa de aplicación, sin perjuicio de los requisitos establecidos en este real decreto.

c) Soluciones de ventanilla única para la notificación de incidentes al CCN-CERT, que permita la distribución de notificaciones a las diferentes entidades de manera federada, utilizando para ello dependencias administrativas jerárquicas.

d) Detección y respuesta mediante la implantación de medidas urgentes, incluyendo la detención de servicios, el aislamiento del sistema afectado, la recogida de evidencias y protección de los registros.

e) Reconfiguración dinámica para detener, desviar o limitar ataques, acotando los daños.

Los programas de Seguridad Corporativa de Oracle están diseñados para proteger tanto los datos de Oracle como los de los clientes, tales como:

a) Los sistemas críticos en los que confían los clientes para los servicios Cloud, soporte técnico y otros servicios.

b) El robo o la alteración maliciosa del código fuente de Oracle y otros datos confidenciales.

c) Información personal y otra información confidencial que Oracle recopila en el curso de su negocio, incluido el cliente, datos de socios, proveedores y empleados que residen en los sistemas IT internos de Oracle.

Las políticas de seguridad de Oracle cubren la gestión de la seguridad tanto para las operaciones internas de Oracle como para los servicios de Oracle. Proporciona a sus clientes y se aplica a todo el personal de Oracle, como empleados y contratistas. Estas políticas están alineadas con los estándares ISO/IEC 27002:2022, ISO/IEC 27001:2013 que guían a todas las áreas de seguridad dentro de Oracle.

Las prácticas recomendadas por Oracle se reflejan en los estándares de seguridad emitidos por la Organización Internacional de Normalización (ISO), el Instituto Nacional de Estándares y Tecnología de los Estados Unidos (NIST) y otras fuentes de la industria.

Oracle ha implementado una amplia variedad de controles de seguridad preventivos, detección y correctivos con el objetivo de proteger activos de información.

Por otro lado, Oracle evaluará y responderá a cualquier evento cuando haya la sospecha de que los datos de los clientes administrados por Oracle han sido vulnerados. La política de respuesta e informes de incidentes de seguridad de Oracle define los requisitos para informar y responder a eventos e incidentes.

Esta política autoriza a la organización Global Information Security (GIS) para proporcionar una dirección general para la prevención, identificación, investigación y resolución de incidentes dentro de las líneas de negocio de Oracle (LoB). Tras el descubrimiento de un incidente, Oracle define un plan de respuesta a incidentes para una investigación de incidentes rápida y eficaz que permita dar una respuesta y recuperación de manera contundente y en el menor tiempo posible.

En base al Acuerdo de Procesamiento de Datos, en caso de que Oracle determine la confirmación de un incidente de seguridad que involucre la información personal de los clientes procesada por Oracle, éstos serán notificados de inmediato, sin demoras indebidas y, a más tardar, en un plazo de 24 horas, en conformidad con los acuerdos contractuales y responsabilidades reglamentarias.

Finalmente, aquella información sobre los intentos o sospechas de incidentes se considera información confidencial de Oracle y no se comparte públicamente. El historial de incidentes de Oracle es confidencial y tampoco se comparte públicamente.

3.1.2.5 REGISTRO DE LA ACTIVIDAD

Esta medida del ENS establece que se deben registrar las actividades de los usuarios del sistema, de forma que:

a) Se genere un registro de auditoría para saber quién realiza la actividad, cuándo la realiza y sobre qué.

b) Se realicen revisiones periódicas de los registros de actividad en busca de patrones anormales.

c) El sistema deberá disponer de una referencia de tiempo para facilitar las funciones de registro de eventos y auditoría.

d) En la documentación de seguridad del sistema se deberán indicar los eventos de seguridad que serán auditados y el tiempo de retención de los registros antes de ser eliminados.

e) Los registros de actividad y, en su caso, las copias de seguridad de los mismos solamente podrán ser accedidos o eliminarse por personal debidamente autorizado.

f) El sistema deberá implementar herramientas para analizar y revisar la actividad del sistema y la información de auditoría, en búsqueda de comprometimientos de la seguridad posibles o reales. Además, se dispondrá de un sistema automático de recolección de registros, correlación de eventos y respuesta automática ante los mismos.

En la arquitectura OCI (Gen 2), Identity Cloud Service de Oracle EPM Cloud proporciona informes de auditoría y de inicio de sesión generados para rangos predefinidos de 30, 60 o 90 días. También puede generar estos informes para un rango de fechas personalizado y descargarlos como archivos CSV. A continuación, se muestra los distintos informes de auditoría disponibles:

a) **Informe de Acceso a Aplicaciones:** proporciona información sobre los usuarios que han iniciado sesión, la fecha de inicio de sesión, la aplicación en la que han iniciado sesión y si el inicio de sesión se ha realizado correctamente.

b) **Informe de Privilegios de Roles de Aplicación:** en este informe se documentan los cambios en los roles predefinidos. En cada fila del informe se incluye:

   i. El entorno donde se ha realizado el cambio de rol.

   ii. El beneficiario o usuario al que se le ha asignado un rol o cuya asignación al rol se ha anulado.

   iii. El rol asignado o cuya asignación se ha anulado.

   iv. El usuario que ha asignado o anulado el rol.

   v. La fecha y hora de asignación o anulación del rol.

Por otro lado, existen informes de inicios de sesión disponibles desde Identity Cloud Service, que proporciona al usuario informes de inicio de sesión generados para rangos predefinidos de 30, 60 o 90 días, pudiendo generar dichos informes en un rango de fechas personalizados y descárgalos en formato CSV.

En este informe se muestran todos los usuarios que han iniciado sesión correctamente en Identity Cloud Service y el proveedor que mantiene las credenciales usadas para iniciar sesión en Identity Cloud Service. La información disponible y trazable de los informes de Inicio de Sesión es la siguiente:

a) ID del usuario que ha iniciado sesión.

b) Registro de hora del intento de inicio de sesión.

c) Proveedor de inicio de sesión, que es el atributo UserNamePassword en el caso de Oracle Identity Cloud Service o el nombre del proveedor de SAML.

Los informes disponibles son los siguientes:

a) **Informe de Intentos de Inicio de Sesión Incorrectos:** se muestran todos los usuarios que no han conseguido iniciar sesión en Identity Cloud Service, revelando el ID del usuario, registro de hora del intento de inicio de sesión y comentarios sobre el motivo del fallo del intento de inicio de sesión.

b) **Informe de Usuarios Inactivos:** se muestran los usuarios que no hayan iniciado sesión en Identity Cloud Service durante un periodo de tiempo seleccionado. Revela información sobre el ID del usuario, fecha del último inicio de sesión, nombre completo del usuario y correo electrónico.

Finalmente, para acceder a los informes de auditoría y de usuarios en Identity Cloud Service, puede consultar el siguiente enlace de Oracle:

https://docs.oracle.com/cloud/help/es/epm-common/CGSAD/idcs_audit_login_reports.htm

Para el acceso a informes de auditoría y de usuarios mediante REST API de Identity Cloud Service, puede consultar el siguiente enlace de Oracle:

https://docs.oracle.com/cloud/help/es/epm-common/CGSAD/idcs_audit_login_reports_rest_apis.htm

3.1.2.6 PROTECCIÓN DE CLAVES CRIPTOGRÁFICAS

Tal y como establece el ENS, el uso de claves criptográficas debe estar asegurado durante todo su ciclo de vida, desde la generación, transporte, custodia, archivado tras su retirada y su destrucción final, y que, además de establecer su aislamiento de los medios de explotación durante su generación y que su archivado será realizado en medios aislados de los de explotación exige la utilización de programas evaluados o dispositivos criptográficos certificados, así como la utilización de algoritmos acreditados por el CCN.

Para cumplir el requisito del cifrado de datos estáticos, Oracle Enterprise Performance Management Cloud utiliza el cifrado de datos transparente (TDE) para cifrar todos los datos en el nivel del tablespace. Cada tablespace tiene su propia clave de cifrado.

Las claves de cifrado se cifran con una clave maestra. La clave maestra se cifra con cifrado AES-256 y se rota de forma periódica. En entornos Classic, la clave maestra se almacena en una instancia de Oracle Wallet. En entornos de OCI (Gen 2), se almacena en un módulo de seguridad de hardware (HSM) para una mayor seguridad. Además, en entornos OCI (Gen 2), el espacio de tablas solo está cifrado con AES-256.

Por otro lado, los entornos de Oracle EPM Cloud OCI (Gen 2) usan el cifrado de Block Volume con AES-256 para cifrar todos los datos del sistema de archivos, incluidos los datos de Essbase.

Puede obtener más información relacionada con el cifrado y la protección de las claves criptográficas en la guía de seguridad CCN-STIC 889A Guía de Configuración segura para IAM y servicios de seguridad.

Finalmente, todas las credenciales de usuario de Oracle EPM Cloud se almacenan en un formato seguro. Esto incluye credenciales que se han proporcionado al conectarse, así como las credenciales suministradas durante la creación de los flujos de navegación y las conexiones de orígenes de datos.

Además, puede exigir el uso de un archivo de contraseñas cifrado para cumplir el requisito de evitar el uso de información confidencial de texto sin formato al conectarse a EPM Automate. Utilice el comando encrypt de EPM Automate para crear un archivo que almacene la contraseña cifrada.

Puede obtener más información consultando el siguiente enlace de Oracle:

https://docs.oracle.com/cloud/help/es/epm-common/CEPMA/epm_auto_encrypt.htm

3.1.3 SERVICIOS EN LA NUBE

Según establece el ENS, para la protección de servicios en la nube, los sistemas que suministran un servicio en la nube a organismos del sector público deberán cumplir con el conjunto de medidas de seguridad en función del modelo de servicio en la nube que presten: Software como Servicio (Software as a Service, SaaS), Plataforma como Servicio (Platform as a Service, PaaS) e Infraestructura como Servicio (Infrastructure as a Service, IaaS) definidas en las guías CCN-STIC que sean de aplicación.

3.1.3.1 PROTECCIÓN DE SERVICIOS EN LA NUBE

La medida de seguridad indica que cuando se utilicen servicios en la nube suministrados por terceros, los sistemas de información que los soportan deberán ser conformes con el ENS o cumplir con las medidas desarrolladas en una guía CCN-STIC que incluirá, entre otros, requisitos relativos a:

a) Auditoría de pruebas de penetración (pentesting).

b) Transparencia.

c) Cifrado y gestión de claves.

d) Jurisdicción de los datos.

Además, cuando se utilicen servicios en la nube suministrados por terceros, estos deberán estar certificados bajo una metodología de certificación reconocida por el Organismo de Certificación del Esquema Nacional de Evaluación y Certificación de Seguridad de las Tecnologías de la Información, como es el caso de Oracle.

La configuración de seguridad de los sistemas que proporcionan estos servicios deberá realizarse según la correspondiente guía CCN-STIC de Configuración de Seguridad Específica, orientadas tanto al usuario como al proveedor, tal y como se recoge en la presente guía de seguridad CCN-STIC-XXX_Guía de Configuración segura para Oracle SaaS Enterprise Performance Management (EPM).

3.1.4 MONITORIZACIÓN DEL SISTEMA

El ENS establece al respecto de esta norma que los sistemas estarán sujetos a medidas de monitorización de su actividad. El sistema de monitorización debe disponer de herramientas de detección o de prevención de intrusión, así como poder recopilar los datos necesarios atendiendo a la categoría del sistema para conocer el grado de implantación de las medidas de seguridad que apliquen, de las detalladas en el Anexo II y, en su caso, para proveer el informe anual requerido por el artículo 32 del RD 311/2022, de 3 de mayo, por el que se regula el ENS.

3.1.4.1 DETECCIÓN DE INTRUSIÓN

La medida indica que se debe disponer de herramientas de detección o de prevención de intrusión que incluya reglas y procedimientos de respuesta a las alertas generadas por el sistema de detección o prevención de intrusiones.

Oracle Cloud Services utiliza sistemas de detección de intrusos en la red (NIDS) para proteger el entorno.

Las alertas NIDS se enrutan a un sistema de monitorización centralizado que es administrado por los equipos de operaciones de seguridad las 24 horas del día y los 365 días del año.

3.1.4.2 SISTEMA DE MÉTRICAS

Según el ENS, atendiendo a la categoría de seguridad del sistema, se recopilarán los datos necesarios para conocer el grado de implantación de las medidas de seguridad que resulten aplicables y, en su caso, para proveer el informe anual requerido. Además, se recopilarán los datos precisos que posibiliten evaluar el comportamiento del sistema de gestión de incidentes y para conocer la eficiencia del sistema de seguridad, en relación con los recursos consumidos, en términos de horas y presupuesto.

El Informe de Actividad y los Registros de Acceso se utilizan para supervisar lo que ocurre en los entornos de Oracle EPM Cloud. El Informe de Actividad permite a los administradores del servicio conocer cuál es el uso de la aplicación. También ayuda a optimizar el diseño de la aplicación mediante la identificación de solicitudes de usuario, scripts de cálculo, formularios, informes, etc. Hay disponibles dos versiones del informe: una versión HTML y una versión JSON.

Oracle EPM Cloud conserva los informes de actividad solo de los últimos 60 días y, por tanto, se recomienda descargar y crear copias de seguridad en un equipo local para analizar las tendencias históricas.

El informe de actividad se genera automáticamente en estas tres situaciones:

a) Cada día durante el mantenimiento diario del servicio.

b) Cada vez que se envíe o proporcione comentarios.

c) Cada vez que se ejecute el comando resetService de EPM Automate para reiniciar un entorno.

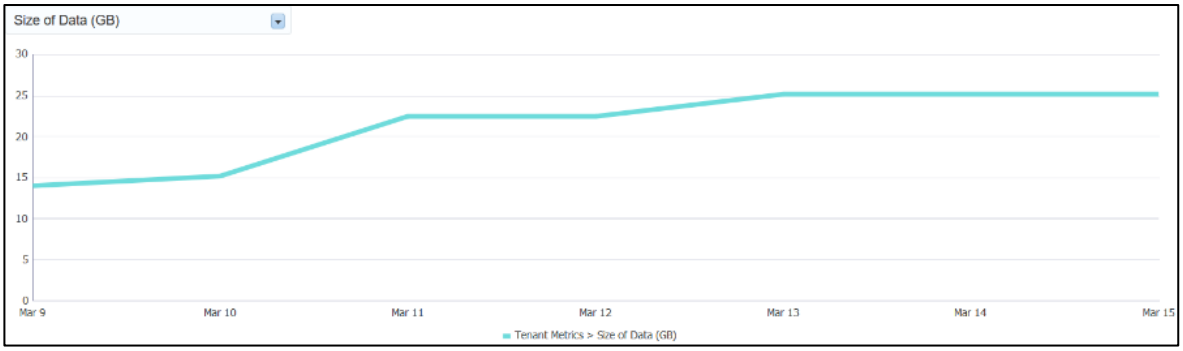
Oracle EPM Cloud genera un Informe de Actividad adicional cada vez que un usuario envía comentarios mediante la utilidad para proporcionar comentarios. Este informe permite a los usuarios reportar incidencias. Además, muestra información enviada como, por ejemplo, capturas de pantalla y descripción de problemas.

Nota: No se puede acceder a la versión JSON del Informe de Actividad desde el servicio. Utilice el comando downloadFile de EPM Automate para descargarlo. Los Informes de Actividad de Narrative Reporting se generan y almacenan en el servidor de Narrative Reporting. Si bien no se puede acceder a los Informes de Actividad desde las pantallas de Narrative Reporting, se pueden descargar con el comando downloadFile de EPM Automate.

Puede obtener más información sobre los Informes de Actividad dependiendo del proceso de negocio y de los componentes usados, a través del siguiente enlace de Oracle:

https://docs.oracle.com/cloud/help/es/epm-common/CGSAD/6_house_keeping_tasks_monitoring_service_activity_rep_access_logs.htm

Por otro lado, el apartado Métricas de negocio dentro del portal Mis Servicios (OCI) y Mis Servicios (Classic) muestra información que ayuda a supervisar el número de usuarios únicos accediendo al sistema, el tiempo promedio de respuesta de la interfaz del usuario y el tamaño de los datos de los entornos de Oracle EPM Cloud.



Métricas de negocio en formato gráfico.

Por último, puede supervisar las métricas de negocio del tamaño de los datos en formato gráfico, formato tabla o como formato del valor más reciente. La información que se puede obtener de las métricas ayuda a la supervisión del número de usuarios únicos que han iniciado sesión en el entorno, en un día o en un periodo determinado. A su vez, puede supervisar el tiempo promedio de respuesta de la interfaz del usuario para verificar el rendimiento del entorno o supervisar el tamaño de los datos para verificar que cumple los límites predefinidos.

3.2 MEDIDAS DE PROTECCIÓN

Este grupo de medidas cubre el espectro de aplicación de mecanismos más amplios en cuanto a dimensión. No obstante, debe tenerse en consideración que incluye una gran variedad de las mismas y que son aplicables desde las más puramente procedimentales, a las puramente físicas o a las de aplicación técnica.

Solo éstas últimas se tendrán en consideración para su implementación en la presente guía y de ellas solo un número limitado es de aplicación sobre las funcionalidades de la nube.

Se considera, en este sentido, que la organización ha dispuesto todos aquellos mecanismos de control físico necesarios, con objeto de evitar el acceso a la nube existentes por parte de personal no autorizado.

3.2.1 PROTECCIÓN DE LOS EQUIPOS

Las medidas de protección de los equipos cubren todos aquellos mecanismos que son necesarios para garantizar una configuración de seguridad válida para el sistema, así como para mantener la propia privacidad del trabajo desarrollado.

Dentro de las medidas, se articula la aplicación de mecanismos de índole tecnológica y otras de tipo física, aunque esta guía de seguridad se encuentra orientada a una Infraestructura en la nube y se tienen en consideración aquellas medidas que, siendo establecidas para un puesto de trabajo, le es de completa aplicación, por ejemplo, la necesidad de realizar un bloqueo o cierre de la sesión establecida en el tenant por inactividad.

3.2.1.1 BLOQUEO DEL PUESTO DE TRABAJO

Dentro de la protección de los equipos, esta medida es la única de aplicación al contemplar el puesto de trabajo como la sesión establecida al tenant de la organización y no como un puesto físico, con lo que se debe establecer el bloqueo de la sesión para impedir el acceso no autorizado.

Esta medida contempla la desconexión de la sesión pasado un cierto tiempo de inactividad.

Oracle dispone de un servicio que finaliza automáticamente las sesiones de usuario inactivas una vez transcurridos 75 minutos. Además, Smart View finaliza las sesiones tras 75 minutos o el tiempo de espera de la sesión HTTP, que se puede modificar con la comprobación del sistema de Smart View.

Se recomienda establecer en 5 minutos la finalización de las sesiones de usuario inactivas.

3.2.2 PROTECCIÓN DE LAS COMUNICACIONES

El conjunto de medidas orientadas a la protección de las comunicaciones tiene como objetivo proteger la información en tránsito, así como dotar de los mecanismos necesarios para la detección y bloqueo de intrusos en una red.

Aunque fundamentalmente tienen un alcance mayor en cuanto a la implementación de sistemas de electrónica de red y control perimetral que aporta la infraestructura en la nube de Oracle, determinadas medidas pueden ser aplicables y gestionadas desde alguno de los servicios que ofrece OCI.

3.2.2.1 PROTECCIÓN DE LA INTEGRIDAD Y DE LA AUTENTICIDAD

Esta medida indica que, en comunicaciones con puntos exteriores al dominio propio de seguridad, se asegurará la autenticidad del otro extremo del canal de comunicación antes de intercambiar información.

Se prevendrán ataques activos garantizando que al ser detectados se activarán los procedimientos previstos de tratamiento del incidente. Se considerarán ataques activos:

a) La alteración de la información en tránsito.

b) La inyección de información espuria.

c) El secuestro de la sesión por una tercera parte.

Se aceptará cualquier mecanismo de identificación y autenticación de los previstos en el ordenamiento jurídico y en la normativa de aplicación. Además, se emplearán redes privadas virtuales cifradas cuando la comunicación discurra por redes fuera del propio dominio de seguridad, empleando algoritmos y parámetros autorizados por el CCN, preferentemente, con dispositivos hardware en el establecimiento y utilización de la red privada virtual y productos certificados conforme a lo establecido en el ENS.

Por otro lado, Oracle cumple con el requisito de una comunicación de datos cifrada. Oracle EPM Cloud utiliza TLS 1.2 con un algoritmo hash criptográfico SHA-2/SHA-256 para proteger la comunicación en los exploradores, Oracle Smart View for Office y EPM Automate. Todas las sesiones de EPM Cloud están cifradas.

Además, se cifra la información de sesión almacenada en las cookies y el ID de sesión se genera de forma aleatoria para garantizar la seguridad.

Puede obtener más información relacionada con los niveles de cifrado y del tiempo de espera de la sesión en el siguiente enlace de Oracle:

https://docs.oracle.com/cloud/help/es/epm-common/CGSAD/6_house_keeping_tasks_session_timeout_encryption.htm

3.2.3 PROTECCIÓN DE LA INFORMACIÓN

Este conjunto de medidas trata todo lo relacionado con la protección de la información, desde lo dispuesto por las diferentes leyes nacionales y de la Unión Europea acerca de los datos personales, así como las distintas dimensiones que alcanzan cada uno de los aspectos relacionados con la información, su clasificación, accesos, responsables, tratamiento, almacenamiento, limpieza o destrucción, cuando ésta ya no sea necesaria.

Siendo uno de los activos más valiosos para cualquier organización, la información debe protegerse para garantizar la confidencialidad, disponibilidad e integridad de los datos.

Para ello, la información debe ser clasificada e identificada para la aplicación de las medidas necesarias y adecuadas para su preservación. Sin embargo, la mayoría de estas medidas presentan un carácter más organizativo y procedimental, aunque también existen medidas de carácter técnico para permitir la comprobación de dimensiones como la autenticidad de la procedencia y la integridad de la información.

3.2.3.1 COPIAS DE SEGURIDAD

El ENS establece que deben realizarse copias de seguridad que permitan recuperar datos perdidos de manera accidental o intencionadamente, con una antigüedad determinada por la normativa interna de la organización. Los procedimientos de respaldo establecidos indicarán la frecuencia de las copias, los requisitos de almacenamiento en el propio lugar, los requisitos de almacenamiento en otros lugares y los controles para el acceso autorizado a las copias de respaldo.

Además, los procedimientos de copia de seguridad y restauración deben probarse regularmente. Su frecuencia dependerá de la criticidad de los datos y del impacto que cause la falta de disponibilidad. Al menos, una de las copias de seguridad se almacenará de forma separada en lugar diferente, de tal manera que un incidente no pueda afectar tanto al repositorio original como a la copia simultáneamente.

Cada día, durante el mantenimiento operativo del entorno, Oracle realiza una copia de seguridad del contenido del entorno para crear una instantánea de mantenimiento, llamada Artifact Snapshot, de los datos y artefactos existentes.

Los administradores del servicio pueden utilizar la instantánea de mantenimiento para recuperar artefactos y datos, por ejemplo, definiciones de formularios, informes, etc., del día anterior al que se eliminaron del servicio tras el último periodo de mantenimiento operativo. Si es necesario, también pueden utilizarla para restaurar el entorno al estado en el que estaba durante el último mantenimiento operativo.

Sin embargo, los siguientes artefactos no se incluyen en la instantánea de mantenimiento:

a) Los archivos que se hayan cargado en el entorno, incluidas las instantáneas que haya cargado.

b) Los archivos que ha creado mediante la exportación de artefactos del entorno.

c) Datos de auditoría. Las instantáneas de todos los procesos de negocio que no sean de Planning, Planning Modules, Profitability and Cost Management y Enterprise Profitability and Cost Management incluyen información de auditoría.

d) Datos de la consola de trabajos. Para Planning, Planning Modules, FreeForm y Enterprise Profitability and Cost Management, los datos de la consola de trabajos no se incluyen en la instantánea.

e) Datos de tabla temporal de Data Management. Para exportar e importar estos datos, use los comandos exportDataManagement e importDataManagement de EPM Automate o la interfaz de scripts de mantenimiento del sistema de Data Management.

Se recomienda que, para crear una copia idéntica de un entorno, incluidos los datos de auditoría, los datos de la consola de trabajos, los datos de la tabla temporal de Data Management y las instantáneas y archivos almacenados, use el comando cloneEnvironment de EPM Automate o la función Clonar Entorno.

Nota: los archivos XML incluidos en las instantáneas de Oracle EPM Cloud, utilizan un formato privativo definido por Oracle. Este formato puede cambiar para admitir los cambios que se produzcan en las versiones de EPM Cloud. Cualquier proceso o utilidad personalizados que use no deberían depender del formato XML que quede sin cambiar en las versiones de EPM Cloud.

La retención, archivado o recuperación de las instantáneas diarias varía según el entorno en el que esté operando:

a) Entornos Classic:

i. Oracle archiva las instantáneas diarias de los últimos 3 días. Se debe solicitar a Oracle las instantáneas de los entornos de producción y de pruebas.

ii. Oracle archiva las instantáneas semanales de los últimos 60 días. Se debe solicitar a Oracle las instantáneas de los entornos de producción y de pruebas.

Puede obtener más información relacionada con la solicitud de una copia de seguridad anterior de un entorno, a través del siguiente enlace de Oracle:

https://docs.oracle.com/cloud/help/es/epm-common/TSEPM/sop_request_restore_environment_backup.htm

b) **Entornos de OCI (Gen 2):** las instantáneas diarias se archivan en Oracle Object Storage. Las instantáneas del entorno de producción se conservan durante 60 días, mientras que las instantáneas del entorno de prueba se conservan durante 30 días.

El usuario puede usar operaciones de autoservicio con los comandos listBackups y restoreBackup de EPM Automate para comprobar y copiar las instantáneas de copia de seguridad disponibles de Object Storage en el entorno de los últimos 60 días para entornos de producción y de los últimos 30 días para los entornos de prueba.

Nota: es responsabilidad del cliente archivar las copias de seguridad durante el tiempo que exija su organización. Para ello, descargue las instantáneas diarias con el comando downloadfile de EPM Automate y archívelas en un almacenamiento local o en la nube. También puede archivar instantáneas en Oracle Object Storage con el comando copyToObjectStorage de EPM Automate.

Puede obtener un script de ejemplo para descargar instantáneas diarias y almacenarlas en una ubicación de almacenamiento local, a través del siguiente enlace de Oracle:

https://docs.oracle.com/cloud/help/es/epm-common/CEPMA/sample_script_1.htm

Puede consultar un script de ejemplo para archivar instantáneas diarias en Oracle Object Storage, a través del siguiente enlace de Oracle:

https://docs.oracle.com/cloud/help/es/epm-common/CEPMA/sample_script_15_object_store.htm

Nota: si el tamaño total de todas las instantáneas excede los 150 GB, se empieza a suprimir las instantáneas creadas en los últimos 60 días, pero de hace más de 48 horas y empezando por la más antigua, hasta que el tamaño total de las instantáneas sea inferior a 150 GB. La instantánea de mantenimiento diario, independientemente de su tamaño, se conservará siempre. Si la instantánea de mantenimiento supera los 150 GB, solo se mantiene ésta y se suprime el resto de las instantáneas. Además, Narrative Reporting solo conserva la instantánea actual (EPCRS_Backup.tar.gz) del entorno. Los archivos de registro de proceso de Data Management se conservan solo durante siete días.

Por otro lado, se puede consultar el siguiente enlace de Oracle para ver cómo realizar una copia de seguridad de la instantánea de mantenimiento para servicios que no sean Narrative Reporting:

https://docs.oracle.com/cloud/help/es/epm-common/CGSAD/5_maint_snapshot_back_up_to_local.htm

Para restaurar artefactos y datos de la aplicación a partir de una instantánea de los servicios que no forman parte de Narrative Reporting, puede consultar el siguiente enlace:

https://docs.oracle.com/cloud/help/es/epm-common/CGSAD/5_maint_snapshot_restore_artifacts_data.htm

Finalmente, para descargar, cargar o restaurar una instantánea de copia de seguridad en el entorno de Narrative Reporting, consulte el siguiente enlace de Oracle:

https://docs.oracle.com/cloud/help/es/epm-common/CGSAD/5_maint_snapshot_back_up_to_local_eprcs_only.htm

3.2.4 PROTECCIÓN DE LOS SERVICIOS

Las medidas de protección de los servicios deben hacer frente a las amenazas que puedan sufrir servicios tan críticos como el correo electrónico o las aplicaciones web de una organización, dotando a los mismos de aquellos mecanismos o tecnologías que los protejan frente a las amenazas externas.

3.2.4.1 PROTECCIÓN FRENTE A LA DENEGACIÓN DE SERVICIO

El ENS exige para esta medida el despliegue de tecnologías para prevenir ataques conocidos, así como la correcta planificación de sistemas con capacidad para atender la carga prevista con capacidad de escalado. Además, se establecerá un sistema de detección y tratamiento de ataques de denegación de servicio (DoS y DDoS).

En entornos OCI (Gen 2), el Web Application Firewall (WAF) satisface el requisito de proteger Oracle EPM Cloud de una variedad de ataques a la capa de aplicación, como cross-site scripting y SQL injection. El servicio WAF está disponible out-of-the-box.

Para obtener más información sobre el servicio WAF de OCI, consulte la guía de seguridad CCN-STIC 889A Guía de Configuración segura para IAM y servicios de seguridad.

4. ESCENARIO COMPLETO DE NUBE SEGURA PARA ORACLE SAAS

Con el fin de aumentar la confianza en la nube, se describen aquellos procesos generadores de confianza en la nube que conforman un escenario completo de nube segura, a través de una implementación de configuración de elementos de seguridad como las credenciales o las conexiones seguras con el servicio de cualquier proveedor de nube.

En este sentido, Oracle dispone de una imagen SaaS-Imagen-Bastionada, elaborada a partir de las últimas actualizaciones de seguridad y del fortalecimiento del sistema operativo para los servicios SaaS integrados en OCI. Además, contiene agentes de servicios compartidos para el registro, seguridad, inteligencia del sistema, autenticación o el escalado de privilegios.

Los equipos de servicio de SaaS pueden importar una imagen bastionada en su tenant y usarla para lanzar una instancia de cómputo OCI o un nodo de trabajo OKE. SaaS-Imagen-Bastionada puede usarse como imagen base para crear su propia imagen personalizada.

A continuación, se describen los beneficios de uso de SaaS-Imagen-Bastionada de Oracle:

a) Aprobar y agilizar las auditorías de cumplimiento.

b) Facilidad en la transición al patrón SaaS-on-OCI.

c) Integración sin fricciones con servicios compartidos.

d) Entrega más rápida a producción.

Oracle dispone de distintos tipos de imágenes bastionadas para los distintos tipos necesidades de los clientes de SaaS:

a) Imagen Bastionada.

   El equipo de Oracle toma la última imagen OCI OS (VMI), aplica las configuraciones de refuerzo de PCI-DSS y trabaja para aplicar DISA STIG y C2S. Posteriormente, se toma una instantánea del resultado creando una imagen bastionada.

   La imagen bastionada es usada por el equipo de Oracle para crear otras imágenes, recogiendo todas las correcciones de vulnerabilidades de seguridad conocidas hasta la fecha. Si surge una nueva vulnerabilidad después de que se publique una imagen SaaS-Imagen-Bastionada, a través de las publicaciones mensuales, se corregirán las vulnerabilidades de seguridad pendientes. Las correcciones de seguridad se recogerán en la siguiente imagen de sistema operativo OCI (VMI) más reciente y será usada de nuevo como imagen bastionada.

La imagen bastionada se crea a través de los flujos de bastionado, prueba, validación y publicación, tal y como se muestra en el diagrama a continuación:

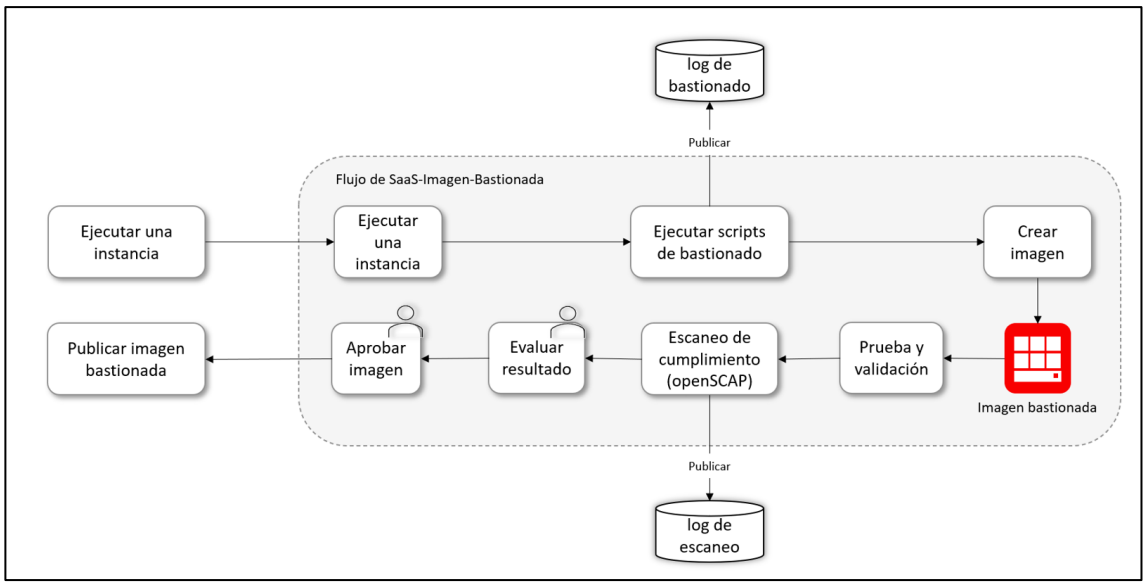


Diagrama para la elaboración de la imagen bastionada.

b) Imagen Bastionada de servicios compartidos.

Oracle lanza una instancia con la imagen bastionada y agrega agentes o clientes de servicio compartido configurados y se toma una instantánea del resultado combinado. Esta imagen se publica a través de PAR (Pre-Authenticated Requests) para la implementación general de máquinas virtuales del servicio SaaS.

Para obtener más información del uso de solicitudes autenticadas previamente, consulte el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/Content/Object/Tasks/usingpreauthenticatedrequests.htm

El flujo de trabajo que crea la imagen bastionada de servicios compartidos es idéntico a la canalización de la Imagen Bastionada que, además de la securización, instala y configura los servicios compartidos. Antes de la publicación de la imagen, ésta es validada por los clientes, propietarios y agentes de servicios compartidos.

Diagrama de una imagen bastionada de servicios compartidos.

c) Servicio OKE Oracle-Managed (OKEOM).

Para habilitar la imagen bastionada para Oracle Kubernetes Engine (OKE), el equipo de Oracle toma la imagen bastionada y agrega la personalización para OKE. Posteriormente se realiza una instantánea del resultado combinado.

La imagen de OKEOM se publica a través de PAR para que los equipos de servicio de SaaS la implementen en un nodo de trabajo de OKE. La imagen se crea a través de un proceso similar al que se usa para crear otras imágenes SaaS-Imagen-Bastionada.

Diagrama imagen bastionada OKEOM.

d) Imagen Windows.

El equipo de Oracle proporciona la imagen bastionada de Windows tomando como referencia el CIS y la generaliza usando sysprep.

Puede obtener más información consultando el siguiente enlace de Oracle para la creación de imágenes personalizadas de Windows:

https://docs.oracle.com/es-ww/iaas/Content/Compute/References/windowsimages.htm

Además, es posible crear y personalizar una imagen SaaS-Imagen-Bastionada atendiendo a las necesidades de los clientes, usando como base la imagen bastionada por el equipo de Oracle. En la actualidad, el equipo de Oracle ha estado apoyando las siguientes imágenes personalizadas de los clientes:

a) SaaS Bastion Service.

b) FA OCI.

c) Commerce.

A continuación, se enumeran las características que ofrece una imagen SaaS-Imagen-Bastionada:

a) **Diseñadas sobre imágenes de Oracle Linux:** las imágenes bastionadas se crean con la última imagen base de Oracle Linux que pone a disposición el equipo de OCI. Todos los paquetes se instalan con las últimas versiones disponibles en el repositorio de Oracle Linux Yum.

Puede obtener más información consultando las imágenes de Oracle en el siguiente enlace en inglés:

https://docs.oracle.com/en-us/iaas/images/

b) **Seguridad y cumplimiento:** la imagen base, ya bastionada, primordial para todas las imágenes SaaS-Imagen-Bastionada, se protege a través de varios scripts de bastionado, incluido el creado por SaaS Cloud Security.

Todas las imágenes se escanean a través del escáner de configuración de código abierto OpenSCAP, teniendo en cuenta las siguientes referencias:

i. Estándar de seguridad de datos de la industria de tarjetas de pago (PCI-DSS).

ii. Base de referencia de las Guías de implementación técnica de seguridad de la Agencia de sistemas de información de defensa (DISA STIG).

iii. Línea de base de servicios comerciales en la nube (C2S) del gobierno de EE. UU.

iv. Referencia de Oracle Enterprise Linux Security Advisory (ELSA).

v. Línea de base personalizada por Oracle.

c) **Preconfiguración de servicios compartidos:** las imágenes SaaS-Imagen-Bastionada de servicios compartidos y OKEOM están instaladas y preconfiguradas con agentes de servicios compartidos para los patrones arquitectónicos integrados de SaaS en OCI, que satisfacen los estándares de seguridad en la nube de SaaS y los requisitos de cumplimiento. La imagen incluye el proceso de arranque inteligente, que integra automáticamente su host con los servicios compartidos.

d) **Optimización para OKE:** la imagen SaaS-Imagen-Bastionada para OKEOM está optimizada para los nodos trabajadores de OKE que ejecutan servicios administrados por Oracle. Además, la imagen se basa en la imagen bastionada de base y tiene todas las capacidades de servicios compartidos.

La imagen OKEOM tiene la siguiente personalización:

i. Instalación de paquetes RPM adicionales.

ii. Establecimiento del modo SELinux en permisivo para permitir la comunicación entre nodos.

Puede obtener más información relacionada con la configuración de SELinux consultando el siguiente enlace de Oracle en inglés:

https://docs.oracle.com/en/operating-systems/olcne/1.1/start/selinux.html

Finalmente, se enumeran los requisitos necesarios para el uso de imágenes SaaS-Imagen-Bastionada:

a) Disponer de todas las conectividades requeridas para los servicios compartidos de imágenes SaaS-Imagen-Bastionada:

i. El tenant debe estar incluida en la lista blanca como OCI dev o Prod Tenancy.

ii. La VCN debe usar rangos de IP de OCI Prod o Dev. La mayoría de los servicios compartidos no permiten el acceso desde rangos de IP públicos de OCI que usan clientes externos.

iii. La VCN debe tener la configuración de salida hacia los puntos finales del servicio compartido, para la instancia lanzada desde una imagen SaaS-Imagen-Bastionada.

b) Las imágenes bastionadas están diseñadas para las siguientes circunstancias:

i. El servicio del cliente está basado en la arquitectura o patrón SaaS-on-OCI.

ii. El cliente es propietario del tenant y operado por Oracle.

5. GLOSARIO

A continuación de describen una serie de términos, acrónimos y abreviaturas en materia de seguridad utilizados en esta guía.

Término	Definición
AES	Advanced Encryption Standard.
AIDE	Advanced Intrusion Detection Environment.
BI	Business Intelligence.
C2S	Consumer-to-Service.
CCN	Centro Criptológico Nacional.
CDaaS	Content Delivery as a Service.
CIS	Center for Internet Security.
DDoS	Denial of Service.
DISA	Defense Information Systems Agency.
ELSA	Enterprise Linux Security Advisory.
ENS	Esquema Nacional de Seguridad.
EPM	Enterprise Performance Management.
ERP	Enterprise Resource Management.
Gen2	Generation 2.
GIS	Geographical Information System.
HCM	Human Capital Management.
HSM	Hierarchical Storage Manager.
IA	Inteligencia Artificial.
IaaS	Infrastructure as a Service.
IAM	Identity and Access Management.
IBPx	Integrated Business Planning and Execution.
IDCS	Identity Cloud Service.
IdP	Identity Provider.
IDS	Intrusion Detection System.
IEC	International Electrotechnical Commission.
IoT	Internet of Things.
IPA	Intelligence Process Automation.
IPM	Intelligent Performance Management.
IPS	Intrusion Prevention System.
ISO	International Organization for Standardization.
IT	Information Technology.
KPI	Key Performance Indicator.
LoB	Line of Business.
NIDS	Network Intrusion Detection System.
NIST	National Institute of Standards and Technology.
OCI	Oracle Cloud Infrastructure.

Término	Definición
OKE	Oracle Container Engine for Kubernetes.
OKEOM	OKE Oracle-Managed.
OOTB	Out-of-the-box.
OTP	One-Time Password.
PaaS	Platform as a Service.
PAM	Pluggable Authentication Module.
PAR	Pre-Authenticated Request.
PCI-DSS	Payment Card Industry Data Security Standard.
RBAC	Role Based Access Control.
RPM	Red Hat Package Manager.
SaaS	Software as a Service.
SAML	Security- Assertion Markup Language.
SELinux	Security-Enhanced Linux.
SFC	System File Checker.
SHA	Secure Hash Algorithm.
SIEM	Security Information and Event Management.
SP	Service Provider.
SSO	Single Sign-On.
STIG	Security Technical Implementation Guide.
TDE	Transparent Data Encryption.
TLS	Transport Layer Security.
VCN	Virtual Cloud Network.
WAF	Web Application Firewall.
WMI	Windows Management Instrumentation.
XBRL	eXtensible Business Reporting Language.

6. RESUMEN Y APLICACIÓN DE MEDIDAS

El siguiente cuadro, resume las medidas de seguridad a implementar para valorar el nivel de cumplimiento.

Control ENS	Medidas y Configuración	Estado	
op	Marco operacional		
op.acc	Control de Acceso		
op.acc.1	Identificación	Aplica	Cumple
	Se ha configurado el inicio de sesión único (SSO) y/o cuentas locales en Oracle Identity Management para la autenticación de las cuentas de usuario.	☐Si ☐No	☐Si ☐No
		Observaciones:	
op.acc.2	Requisitos de acceso	Aplica	Cumple
	Se han gestionado los requisitos de acceso de los usuarios mediante la asignación de grupos de usuarios.	☐Si ☐No	☐Si ☐No
		Observaciones:	
op.acc.3	Segregación de funciones y tareas	Aplica	Cumple
	Se han creado los grupos de seguridad basados en roles funcionales y disponibles en Oracle Cloud EPM, garantizando la concurrencia de dos o más personas para realizar las tareas más críticas.	☐Si ☐No	☐Si ☐No
		Observaciones:	

Control ENS	Medidas y Configuración	Estado	
	Se ha seleccionado la opción Aplicar seguridad a nivel de dimensión en el proceso de negocio.	☐Si ☐No	☐Si ☐No
		Observaciones:	
op.acc.4	Proceso de gestión de derechos de acceso	Aplica	Cumple
	Se han gestionado los derechos de acceso de los usuarios a los Grupos mediante la asignación de los roles funcionales desde el Control de acceso, manteniendo los siguientes principios: • Mínimo privilegio. • Necesidad de conocer. • Capacidad para autorizar.	☐Si ☐No	☐Si ☐No
		Observaciones:	
op.acc.5	Mecanismo de autenticación	Aplica	Cumple
	Se ha utilizado un proveedor de identidad SAML 2.0 para la configuración del inicio de sesión único.	☐Si ☐No	☐Si ☐No
		Observaciones:	
	Se ha configurado la complejidad de las contraseñas para las cuentas locales, estableciendo un valor de longitud mínimo de 12 caracteres.	☐Si ☐No	☐Si ☐No
		Observaciones:	

Control ENS	Medidas y Configuración	Estado	
op.exp	Explotación		
op.exp.4	Mantenimiento	Aplica	Cumple
	Se están descargando las instantáneas diarias para realizar copias de seguridad del entorno.	☐Si ☐No	☐Si ☐No
		Observaciones:	
	Se ha establecido la hora de inicio predeterminado del mantenimiento ajustándose a las necesidades de la organización.	☐Si ☐No	☐Si ☐No
		Observaciones:	
op.exp.5	Gestión de cambios	Aplica	Cumple
	Se está consultando y registrando las funciones de Oracle EPM Cloud para ver los cambios y novedades para el proceso de negocio de la organización.	☐Si ☐No	☐Si ☐No
		Observaciones:	
op.exp.8	Registro de la actividad	Aplica	Cumple
	Se están revisando y almacenando los distintos informes de auditoría disponibles.	☐Si ☐No	☐Si ☐No
		Observaciones:	

Control ENS	Medidas y Configuración	Estado	
op.exp.10	Protección de claves criptográficas	Aplica	Cumple
	Se está usando un archivo de contraseñas cifrado al conectarse a EPM Automate mediante el comando encrypt.	☐Si ☐No	☐Si ☐No
		Observaciones:	
op.mon	Monitorización del sistema		
op.mon.2	Sistema de métricas	Aplica	Cumple
	Se está supervisando de forma activa el número de usuarios únicos, el tiempo promedio de respuesta de la interfaz del usuario y el tamaño de los datos de los entornos de Oracle EPM Cloud.	☐Si ☐No	☐Si ☐No
		Observaciones:	
	Se está descargando los informes de actividad en un equipo local para el análisis de las tendencias históricas.	☐Si ☐No	☐Si ☐No
		Observaciones:	

Control ENS	Medidas y Configuración	Estado	
mp	Medidas de protección		
mp.eq	Protección de los equipos		
mp.eq.2	Bloqueo de puesto de trabajo	Aplica	Cumple
	Se ha establecido en 5 minutos la caducidad de las sesiones de usuario inactivas.	☐Si ☐No	☐Si ☐No
		Observaciones:	
mp.info	Protección de la información		
mp.info.6	Copias de seguridad	Aplica	Cumple
	Se están creando copias idénticas del entorno mediante el comando cloneEnviroment de EPM Automate o mediante la función Clonar entorno.	☐Si ☐No	☐Si ☐No
		Observaciones:	
	Se están almacenando localmente o a través del servicio de Oracle Object Storage las copias de seguridad del entorno durante el tiempo que exija la organización.	☐Si ☐No	☐Si ☐No
		Observaciones:	

PUBLICACIONES DE DEFENSA

GOBIERNO DE ESPAÑA MINISTERIO DE DEFENSA SUBSECRETARÍA DE DEFENSA SECRETARÍA GENERAL TÉCNICA SUBDIRECCIÓN GENERAL DE PUBLICACIONES Y PATRIMONIO CULTURAL