centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 889I

Guía de Configuración segura para Oracle SaaS Fusion Applications

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 14:47:00 +02'00'

Pº de la Castellana 109, 28046 Madrid

NIPO: 083-23-181-5
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 FUSION APPLICATIONS

1.1 DESCRIPCIÓN DEL USO DE ESTA GUÍA

La principal utilidad de esta guía es identificar los servicios de Oracle SaaS Fusion que deben configurarse, cumpliendo con las distintas medidas de seguridad que establece el Esquema Nacional de Seguridad (ENS). 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 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, 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 de Oracle diseñada para ejecutar cualquier aplicación de forma más rápida y segura.

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 Fusion 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 Fusion Applications y la gestión del entorno donde se hospedan.

1.3 SERVICIOS DE ORACLE SAAS FUSION APPLICATIONS

A medida que el entorno empresarial sigue cambiando, de forma rápida e impredecible, las empresas y organizaciones usan software para ser más competitivas y satisfacer las demandas cambiantes de las partes interesadas. El software de aplicación en la nube proporciona innovación integrada y brinda la capacidad de respuesta más ágil dentro de un mercado dinámico.

Oracle Fusion Applications (OFA), en la modalidad SaaS de la nube de Oracle, ofrece la tecnología adecuada en el momento adecuado a través de una experiencia de usuario coherente y moderna. Esto facilita que los trabajadores completen sus tareas desde sus escritorios o en movimiento. Además, las aplicaciones integran una potente IA y aprendizaje automático para la automatización del trabajo manual y adquisición de nuevas capacidades comerciales que antes no eran posibles.

Una suite SaaS completa basada en una infraestructura de nube avanzada es una buena opción para obtener la agilidad y estar preparado para el crecimiento. No obstante, es posible que la organización, administración o negocio no esté listo para asumir toda la tecnología o todos los procesos comerciales disponibles en finanzas (ERP), SCM (Cadena de Suministros), HCM (Capital Humano) y CX (Ventas). Por eso es importante que la solución planteada facilite la modernización de los procesos empresariales clave y la activación de las funciones de las aplicaciones cuando se necesite.

Vista principal de Oracle Fusion Applications.

Oracle SaaS ofrece un conjunto completo de aplicaciones en la nube que brinda procesos consistentes y una única fuente de verdad en las funciones comerciales más importantes, desde la planificación de recursos empresariales, la gestión de la cadena de suministro y la gestión del capital humano hasta la publicidad y la experiencia del cliente.

Finalmente, el conjunto de servicios de Oracle Fusion basadas en la nube se compone de las siguientes aplicaciones:

a) **Planificación de recursos empresariales (ERP):** es un tipo de software usado por las organizaciones y enfocado a la administración de las actividades comerciales como la contabilidad, compras, gestión de proyectos, gestión de riesgos y cumplimiento y las operaciones de la cadena de suministro. Una suite ERP completa también incluye software de gestión del rendimiento empresarial que ayuda a planificar, presupuestar, predecir e informar sobre los resultados financieros de una organización.

b) **Gestión de la cadena de suministro (SCM):** es la gestión del flujo de bienes, datos y finanzas relacionados con un producto o servicio, desde la adquisición de materias primas hasta la entrega del producto en su destino final.

c) **Gestión del capital humano (HCM):** transforma las funciones administrativas tradicionales de los departamentos de recursos humanos como la contratación, formación, nómina, compensación y gestión del rendimiento en oportunidades para impulsar el compromiso, la productividad y el valor comercial.

d) **CX Sales:** la experiencia del cliente (CX) se refiere a cómo una empresa u organización interactúa con sus clientes en cada punto de su viaje de compra, desde marketing hasta ventas, servicio al cliente y en todos los puntos intermedios. En este punto concreto de interacción con el cliente, las herramientas de Oracle sales se centran en guiar a los vendedores con recomendaciones inteligentes que ayudan a concentrarse en los prospectos más valiosos en el momento adecuado.

Finalmente, en los siguientes apartados se describirán las funcionalidades de cada grupo de aplicaciones que forman parte de la suite Fusion de la nube de Oracle, y otros aspectos para tener en cuenta su implementación, con el objetivo de ampliar el conocimiento de estas desde un punto de vista global.

1.3.1 PLANIFICACIÓN DE RECURSOS EMPRESARIALES (ERP)

Los sistemas de planificación de recursos empresariales son plataformas completas e integradas, ya sea en las instalaciones o en la nube, que gestionan todos los aspectos de un negocio de distribución o basado en la producción. Además, los sistemas ERP admiten todos los aspectos de la gestión financiera, los recursos humanos, la gestión de la cadena de suministro y la fabricación con su función de contabilidad central.

Los sistemas ERP también brindan transparencia en su proceso comercial completo mediante el seguimiento de todos los aspectos de producción, logística y finanzas.

Por otro lado, ERP de Oracle Fusion Cloud es una suite completa que dispone de varias aplicaciones para la planificación de los recursos empresariales que, a diferencia de otros proveedores de software, las soluciones ERP de Oracle se han basado en la nube desde el principio, dotando de capacidades comerciales modulares basadas en Inteligencia Artificial (IA).

Finalmente, puede obtener más información sobre los sistemas ERP de Oracle consultando el siguiente enlace:

https://www.oracle.com/es/erp/what-is-erp/

A continuación, se describen las aplicaciones que forman parte de la suite de Oracle ERP basado en la nube.

1.3.1.1 FINANCIALS

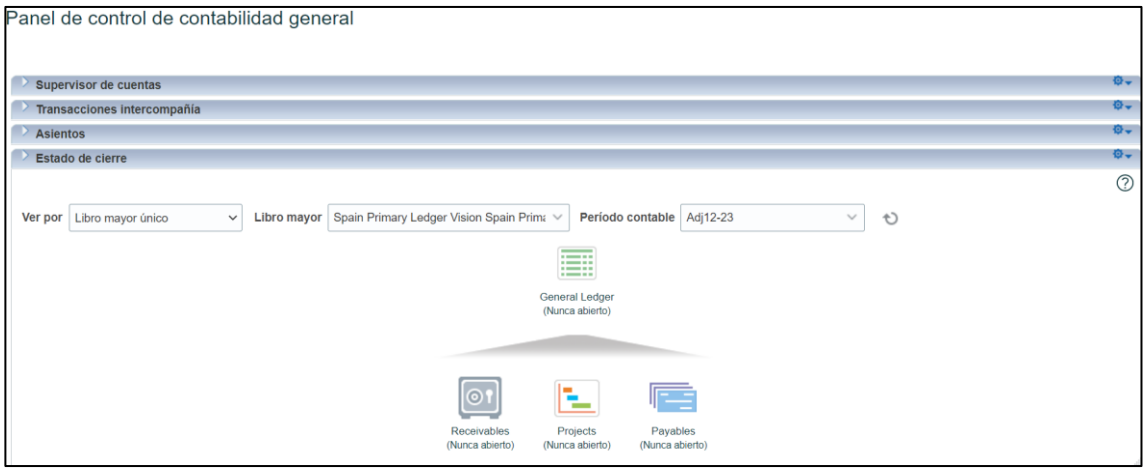
Las actividades financieras son las funciones comerciales relacionadas con el departamento de finanzas de una organización e incluyen módulos para contabilidad financiera, contabilidad auxiliar, centro de contabilidad, cuentas por pagar y cuentas por cobrar, gestión de ingresos, facturación, subvenciones, gestión de gastos, gestión de proyectos, gestión de activos, contabilidad de empresas conjuntas, y colecciones.

El software financiero utiliza capacidades analíticas y de informes para cumplir con los requisitos de informes de los órganos rectores y estados financieros periódicos para los reguladores gobernantes.

Por otro lado, otorga los mejores datos que aumentan la precisión de los pronósticos, acortando los ciclos de informes, simplificando la toma de decisiones y administrando mejor el riesgo y el cumplimiento. Oracle Fusion Cloud Financials es una plataforma financiera global que conecta y automatiza los procesos de gestión financiera, incluidas las cuentas por pagar, cuentas por cobrar, activos fijos, gastos e informes.

A continuación, se desarrollará una breve descripción de las funcionalidades que componen la plataforma de Oracle Cloud Financials:

a) **Accounting Hub:** el software de contabilidad administra y registra las transacciones financieras diarias de una organización, incluida la administración de activos fijos, la administración de gastos, la administración de ingresos, las cuentas por cobrar, las cuentas por pagar, la contabilidad auxiliar y los informes y análisis. Un sistema de contabilidad completo realiza un seguimiento de los activos, pasivos, ingresos y gastos de una organización. Estas transacciones luego llenan el libro mayor en tiempo real, brindando a los directores financieros, tesoreros y controladores acceso inmediato a datos financieros precisos en tiempo real.



Panel de control de contabilidad general.

El registro sistemático de estas transacciones financieras permite la producción de estados financieros trimestrales y anuales, incluidos balances, estados de resultados, estados de flujo de efectivo y estados de capital contable. El software de contabilidad es un componente clave de un sistema de planificación de recursos empresariales (ERP).

Puede obtener más información consultando el siguiente enlace de Oracle sobre qué es un software de contabilidad:

https://www.oracle.com/es/erp/what-is-accounting-software/

b) **Reporting and Analytics:** los informes y analíticas de Oracle brindan información gráfica para acelerar el proceso de toma de decisiones, mediante paneles totalmente configurables y entrega de información basada en eventos. Además, se pueden obtener respuestas oportunas con informes rápidos que se generan a partir de los datos financieros agregados previamente.

   Por otro lado, se puede evaluar rápidamente el estado de las tareas de cierre del periodo, incluido los libros mayores y los libros auxiliares y obtener nuevos conocimientos sobre la rentabilidad y los costos mediante el análisis de saldos de las cuentas del libro mayor en múltiples dimensiones.

   Finalmente, acceder a los informes utilizando múltiples dispositivos e identificar y resolver las excepciones rápidamente con paneles basados en funciones y alertas para las acciones que se deben realizar.

c) **Payables and assets:** las cuentas por pagar y activos de Oracle permite importar y registrar facturas de proveedores ágilmente con imágenes y reconocimiento óptico de caracteres. Procesar facturas y pagos para varias unidades de negocios en función de los permisos de las reglas de seguridad de transacciones y unidades de negocios.

El módulo de cuentas por pagar y activos dispone de pagos inteligentes a proveedores, gestión integral de efectivo y gestión integral de activos entre otras funcionalidades.

Panel de Facturas, dentro de la sección Cuentas a Pagar.

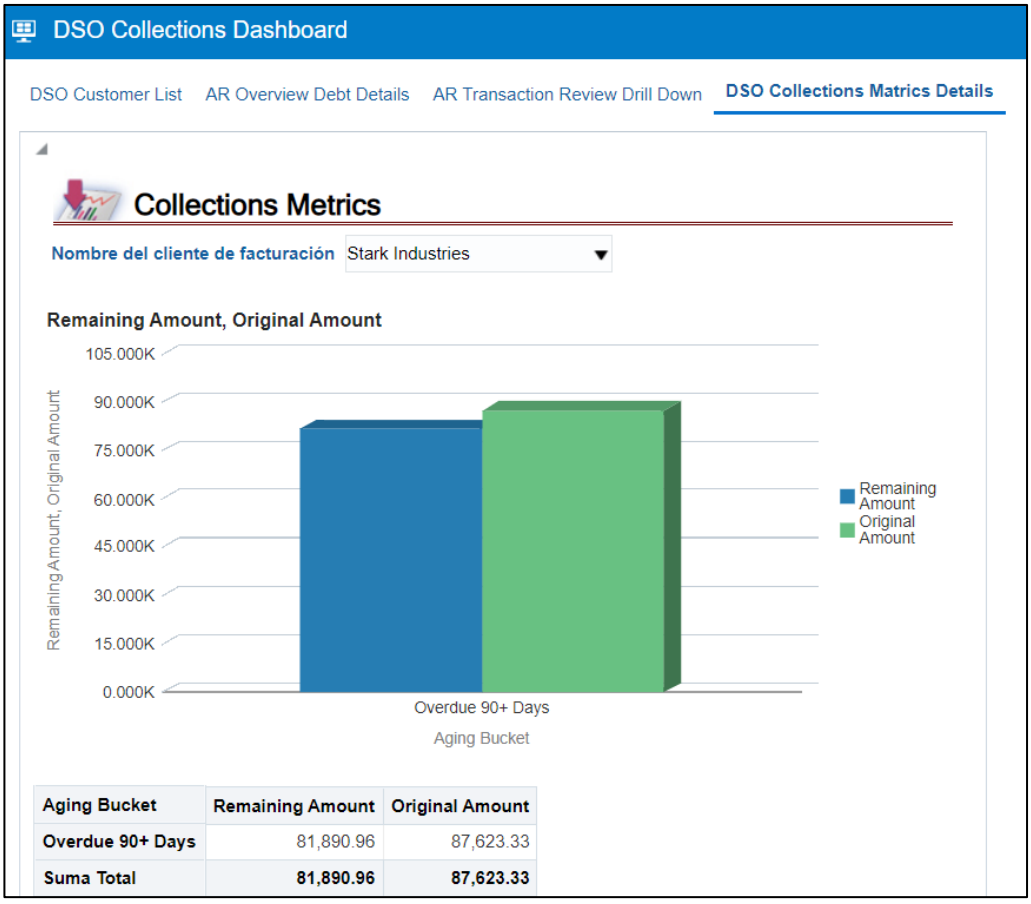
d) **Revenue Management:** la gestión de los ingresos permite automatizar la creación de contratos de clientes, obligaciones de desempeño, determinar y asignar los precios de transacción o el reconocimiento oportuno de ingresos.

e) **Receivables:** las cuentas por cobrar modelan a los clientes en función de cómo se realizan negocios utilizando el modelo de comunidad comercial. Compara las actividades de facturación, envío y pago entre las cuentas de los clientes estableciendo relaciones de cuentas de clientes según sea necesario.

Panel de Cuentas a Cobrar.

El módulo de cuentas por cobrar permite la toma de decisiones de crédito informadas con los perfiles y revisiones de crédito de los clientes. Además, permite generar rápidamente facturas y notas de crédito para ventas de suscripciones, productos y proyectos.

f) **Collections:** administrar las cuentas de alto riesgo calificando a los clientes según su capacidad de pago, para acelerar el proceso de cobro enviando automáticamente solicitudes de pago y llamadas de seguimiento a los agentes de cobro.



Collections Dashboard.

Es necesario asegurarse de que los clientes paguen rápidamente aplicando estrategias de cobro basadas en la puntuación de riesgo de cobro de cada cliente y mejorar el flujo de efectivo con compromiso de pago para clientes morosos. Evaluar el estado de las cuentas por cobrar utilizando métricas estándar de la industria, incluido los días de ventas pendientes, el promedio de días en mora, etc.

g) **Expense Management:** mediante un asistente digital fácil de usar, se puede reducir el trabajo manual para ingresar información con comandos de voz y enviando imágenes de recibos por mensaje de texto.

h) **Joint Venture Management:** la gestión de empresas conjuntas permite reducir el tiempo de cierre de fin de mes de días a horas, mediante el procesamiento basado en reglas de empresas conjuntas sin contacto. Por último, se puede minimizar los costos de resolución de disputas con registros de auditoría de definición de transacciones y empresas conjuntas.

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

https://www.oracle.com/uk/a/ocom/docs/applications/erp/oracle-joint-venture-management-cloud-ds.pdf

Finalmente, puede obtener más información sobre Oracle Fusion Cloud Financials consultando la hoja de datos financieros a través del siguiente enlace en inglés:

https://www.oracle.com/erp/financials-cloud/datasheet/

1.3.1.2 PROJECT MANAGEMENT

La gestión de proyectos de Oracle ayuda a planificar y realizar un seguimiento de los proyectos, asignando el talento adecuado, equilibrando la capacidad frente a la demanda y escalando los recursos hacia arriba o hacia abajo rápidamente a medida que cambian las necesidades.

La gestión de proyectos de Oracle es una solución dentro de Oracle Fusion Cloud ERP que brinda el control total del proyecto. La herramienta dispone de varias funciones que se describen a continuación:

a) **Plan, schedule and forecast:** Es posible planificar y programar los planes de proyecto críticos en un solo lugar, asignando los recursos correctos en el momento correcto. Permite generar, a su vez, presupuestos y previsiones de una manera rápida a partir de los planes de proyecto, planes de recursos o planes financieros existentes.

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

   https://www.oracle.com/uk/a/ocom/docs/applications/erp/planning-forecasting-scheduling-ds.pdf

b) **Resource management:** la gestión de recursos es una función de Project Management cuya finalidad consiste en encontrar el recurso exacto que necesita para el proyecto, filtrando por función, habilidades y ubicación.

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

   https://www.oracle.com/uk/a/ocom/docs/applications/erp/resource-management-ds.pdf

c) **Cost management and control:** Estandarizar la forma en que captura los costos en todas las funciones comerciales dentro de las aplicaciones de Oracle Cloud y los sistemas de terceros.

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

   https://www.oracle.com/uk/a/ocom/docs/applications/erp/cost-management-and-control-ds.pdf

d) **Billing and revenue management:** la gestión de facturación e ingresos maximiza el flujo de efectivo de la organización, satisfaciendo las necesidades de los clientes rápidamente con la facturación automatizada de proyectos.

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

   https://www.oracle.com/uk/a/ocom/docs/applications/erp/billing-and-revenue-ds.pdf

e) **Project asset management:** administrar proyectos de capital y calcular los costos acumulados para la construcción, instalación o adquisición de los activos fijos de la organización. Optimice los procesos de los proyectos de capital con flujos comerciales integrados para la creación de activos de capital, y se deben tomar las decisiones críticas del proyecto con información en tiempo real sobre las transacciones de activos de capital que requieren atención.

f) **Grant management:** mediante la gestión de subvenciones se controla completamente cómo se utilizan los fondos en el ciclo de vida posterior a la adjudicación para respaldar los proyectos patrocinados.

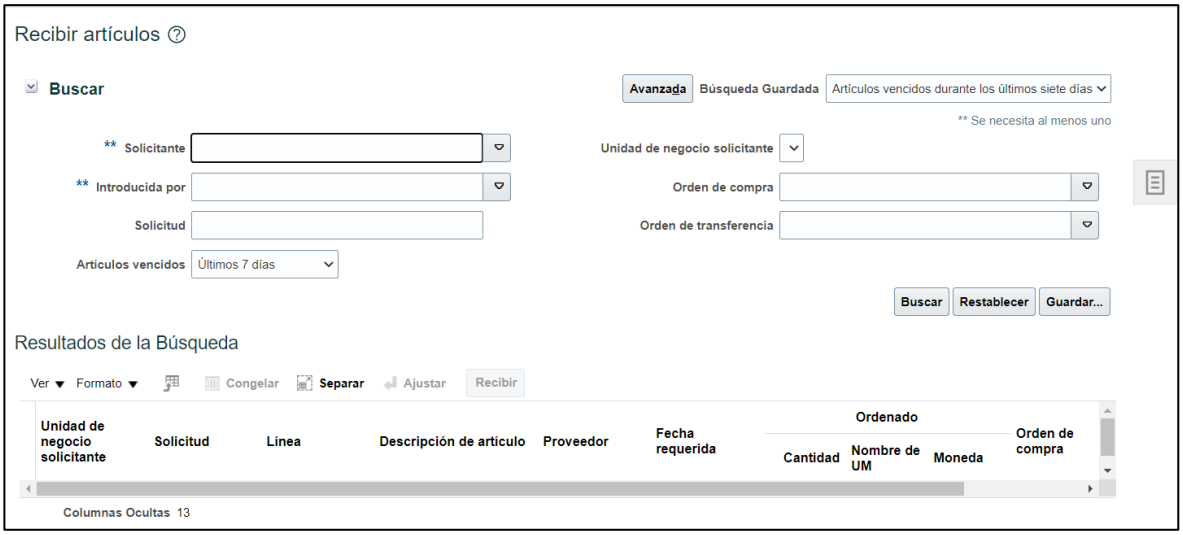
Puede obtener más información consultando el siguiente documento de Oracle en inglés:

https://www.oracle.com/uk/a/ocom/docs/applications/erp/oracle-grant-management-cloud-ds.pdf

1.3.1.3 PROCUREMENT

Es una suite integrada desde la fuente hasta la liquidación que automatiza los procesos comerciales, permitiendo el abastecimiento estratégico, mejorando la gestión de las relaciones con los proveedores y simplificando las compras, lo que da como resultado un menor riesgo, mejores ahorros y una mayor rentabilidad.

Oracle Procurement permite simplificar la compra realizada por los empleados y maximizar la adopción de los usuarios con una experiencia guiada similar a la de un consumidor. Además, mejora la conformidad del gasto, obteniendo ahorros en costos al dirigir las compras a los proveedores aprobados que ofrecen precios negociados.



Mis Recepciones, dentro de la sección Compras.

Finalmente, la solución de Oracle Procurement ofrece un mejor servicio al cliente, un procesamiento rápido de pedidos y una maximización de las tasas de ejecución con el cumplimiento consecutivo y el envío directo. Evita el agotamiento de stock en las ubicaciones mediante compras de reaprovisionamiento automatizado a la vez que se optimiza el flujo de caja.

Puede obtener más información consultando los siguientes documentos de Oracle en inglés:

a) Adquisición de autoservicio de Oracle Cloud.

https://www.oracle.com/uk/a/ocom/docs/applications/erp/oracle-self-service-procurement-cloud-ds.pdf

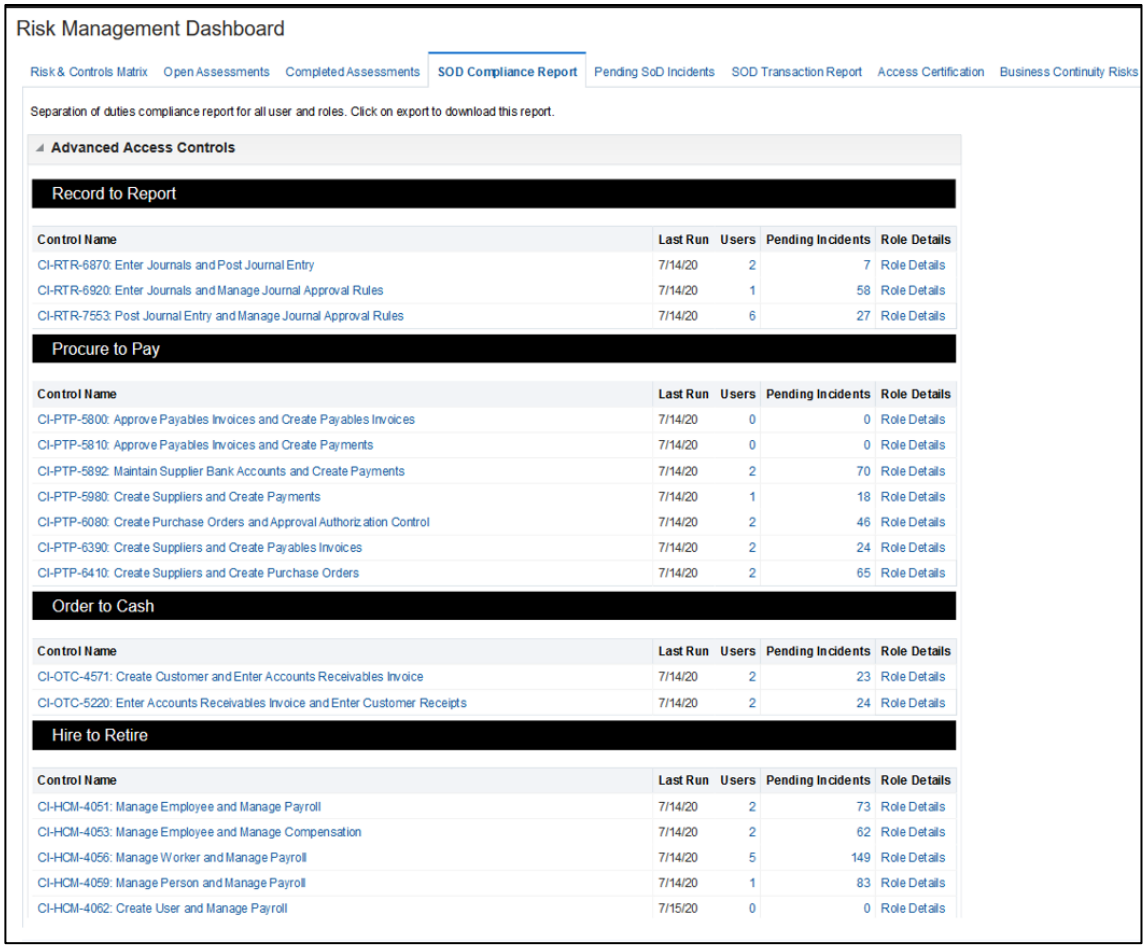
b) Compras de Oracle Cloud.

https://www.oracle.com/uk/a/ocom/docs/applications/erp/oracle-purchasing-cloud-ds.pdf

1.3.1.4 RISK MANAGEMENT AND COMPLIANCE

La solución de Oracle protege la organización de manera proactiva para generar confianza y resiliencia en medio de cambios e interrupciones constantes. La gestión de riesgos y cumplimiento de Oracle es una solución de seguridad y auditoría que controla el acceso de los usuarios a sus datos financieros de Oracle Cloud ERP, supervisa la actividad de los usuarios y facilita el cumplimiento de las normas de cumplimiento a través de la automatización.

Automatiza la supervisión y el control del acceso a los usuarios, diseñando roles de usuario seguros y compatibles durante la implantación. Utiliza una biblioteca de reglas de seguridad predefinidas para el aseguramiento de la compatibilidad de los roles antes de poner en marcha el sistema ERP.



Panel de Gestión de Riesgos.

Por otro lado, se puede controlar de forma continua la actividad de los usuarios con IA, controlando los cambios en configuraciones críticas y auditando las transacciones para la identificación de fraudes, errores e infracciones de políticas.

Finalmente, simplifica la elaboración de informes financieros y de conformidad, automatizando los flujos de trabajo de auditoría y conformidad y optimizando la gestión de riesgos empresariales (ERM).

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

https://www.oracle.com/uk/a/ocom/docs/applications/erp/oracle-risk-management-cloud-ds.pdf

1.3.1.5 ENTERPRISE PERFORMANCE MANAGEMENT (EPM)

Oracle EPM brinda la solución para obtener la agilidad y los conocimientos necesarios para obtener un rendimiento superior en cualquier condición del mercado. La gestión del rendimiento empresarial de Oracle Fusion Cloud ayuda a modelar y planificar finanzas, recursos humanos, cadena de suministro y ventas, optimizar el proceso de cierre financiero e impulsar mejores decisiones.

Puede obtener más información consultando la guía de seguridad CCN-STIC-XXX Guía de Configuración segura para Oracle SaaS Enterprise Performance Management (EPM).

1.3.2 GESTIÓN DE LA CADENA DE SUMINISTRO (SCM)

En el nivel más fundamental, la gestión de la cadena de suministro (SCM) es la gestión del flujo de bienes, datos y finanzas relacionados con un producto o servicio, desde la adquisición de materias primas hasta la entrega del producto en su destino final.

Aunque muchas personas equiparan la cadena de suministro con la logística, en realidad la logística es solo un componente de la cadena de suministro. Los sistemas SCM de base digital de hoy en día incluyen manejo de materiales y software para todas las partes involucradas en la creación de productos o servicios, cumplimiento de pedidos y seguimiento de información, como proveedores, fabricantes, mayoristas, proveedores de transporte y logística y minoristas.

Las actividades de la cadena de suministro abarcan el aprovisionamiento, la gestión del ciclo de vida del producto, la planificación de la cadena de suministro (incluidos la planificación de inventarios y el mantenimiento de los activos empresariales y las líneas de producción), la logística (incluidos el transporte y la gestión de la flota) y gestión de pedidos.

Puede obtener más información sobre la gestión de la cadena de suministro consultando el siguiente enlace de Oracle:

https://www.oracle.com/es/scm/what-is-supply-chain-management/

A continuación, se describen los principales módulos o aplicaciones que forman parte de la solución que ofrece Oracle SCM.

1.3.2.1 SUPPLY CHAIN PLANNING

El software de planificación de la cadena de suministro de Oracle admite los requisitos específicos de una amplia variedad de negocios en una plataforma unificada, incluidas empresas de fabricación y alta tecnología, organizaciones orientadas a proyectos, mayoristas y distribuidores, proveedores de atención médica y cadenas de suministro basadas en servicios.

A continuación, se describen los principales módulos o aplicaciones que componen la planificación de la cadena de suministro de Oracle:

a) **Oracle Demand Management:** se puede detectar y predecir la demanda para mejorar la visibilidad y utilizar reglas comerciales para segmentar dinámicamente la demanda. Además, se puede supervisar y detectar los cambios en las condiciones del mercado para evaluar el impacto e impulsar la rendición de cuentas al documentar las discusiones, decisiones y suposiciones del plan.

   Puede obtener más información relacionada con la gestión de la demanda consultando el siguiente documento de Oracle en inglés:

   https://www.oracle.com/uk/a/ocom/docs/applications/supply-chain-management/oracle-demand-management-cloud-ds.pdf

   Puede obtener más información relacionada con la automatización del reabastecimiento consultando el siguiente documento de Oracle en inglés:

   https://www.oracle.com/uk/a/ocom/docs/applications/oracle-replenishment-planning-solution-brief.pdf

b) **Replenishment planning:** habilitar el reabastecimiento basado en la demanda para que sea fácil y efectiva, impulsando un cumplimiento más preciso mediante políticas de inventario y reglas de consumo adaptadas a los segmentos de la demanda.

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

   https://www.oracle.com/uk/a/ocom/docs/applications/oracle-replenishment-planning-solution-brief.pdf

c) **Oracle Supply planning:** planificar y gestionar el material y la capacidad en las plantas, centros de distribución, proveedores y socios fabricantes por contrato en operaciones de fabricación discretas, basadas en procesos y basadas en proyectos.

   Puede obtener más información sobre la planificación del suministro a través de los detalles del producto, consultando el siguiente enlace de Oracle:

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

d) **Production scheduling:** programar la producción durante el día para maximizar el uso de los recursos de cuello de botella y los componentes disponibles. Reducir el inventario de trabajo en proceso, el desperdicio y las expediciones. Visualizar cómo se asignan las operaciones de órdenes de trabajo a los recursos. Arrastrar y soltar para simular la mejor respuesta a problemas o cambios, y liberar cronogramas para su ejecución en tiempo real.

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

   https://www.oracle.com/a/ocom/docs/applications/scm/oracle-production-scheduling-solution-brief.pdf

e) **Backlog management:** priorizar los pedidos abiertos para reducir los retrasos en las entregas, aumentar las ventas o alcanzar los objetivos de margen cuando cambie la oferta o la demanda. Simular múltiples alternativas de cumplimiento y seleccione las que mejor se adapten a sus objetivos comerciales.

Puede obtener más información en el siguiente documento de Oracle en inglés:

https://www.oracle.com/a/ocom/docs/applications/scm/oracle-order-backlog-management-solution-brief.pdf

f) **Oracle Sales and Operations Planning:** ajustar continuamente los planes operativos para cumplir con los objetivos de la organización y alinear la ejecución en toda la empresa con la planificación de ventas y operaciones (SOP).

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

https://www.oracle.com/uk/a/ocom/docs/applications/supply-chain-management/oracle-sales-and-operations-planning-cloud-ds.pdf

g) **Oracle Integrated Business planning and execution (IBPX):** proporciona capacidades de planificación integrales para las empresas de fabricación, lo que les permite alcanzar sus objetivos de rendimiento a largo, mediano y corto plazo. La solución de Oracle utiliza Internet de las cosas (IoT), inteligencia artificial (IA) y análisis prescriptivos para transformar los planes en ejecución. Proporciona un análisis hipotético de escenarios futuros y evalúa las alternativas para mantener o mejorar los objetivos comerciales de la empresa.

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/

h) **Oracle Supply chain collaboration:** detectar, analizar y resolver las interrupciones de la cadena de suministro dentro de la empresa y con los socios comerciales clave. Automatizar los procesos de manera inteligente para que toda la cadena de suministro sea más eficiente y receptiva. Lograr visibilidad de la cadena de suministro de varios niveles en toda la red.

Puede obtener más información consultando el siguiente enlace de Oracle:

https://www.oracle.com/es/scm/supply-chain-planning/supply-chain-collaboration/

i) **Supply chain visibility:** obtener una mejor visibilidad del suministro upstream tanto internamente como con proveedores estratégicos y fabricantes por contrato. Obtener alertas tempranas de expectativas no coincidentes y aprovechar la capacidad disponible del proveedor en sus planes de suministro.

1.3.2.2 FUSION CLOUD INVENTORY MANAGEMENT

Optimizar los niveles de inventario y el uso del capital de trabajo para reducir costos e impulsar una mayor satisfacción del cliente. Obtener visibilidad y control completos del flujo de productos en la organización y en las cadenas de suministro globales.

La solución Inventory Management basada en el Cloud de Oracle permite la gestión integral de materiales, la optimización del inventario y los niveles de servicio y determinar los costos y optimización de la rentabilidad.

Por un lado, la gestión integral de materiales garantiza una satisfacción de órdenes rápida y protege los ingresos mediante la automatización, optimización y control de las operaciones de inventario.

Por último, se puede realizar una determinación de costos exhaustiva, incluidos los costos indirectos de mano de obra y gastos generales para una planificación de inventario precisa. Obtener visibilidad de la estructura de costos y las operaciones de la cadena de suministro de la organización.

Puede obtener más información consultando el siguiente enlace de Oracle:

https://www.oracle.com/es/scm/product-tours/

1.3.2.3 MANUFACTURING

Optimizar la fabricación global de modo mixto con un sistema integrado de ejecución de fabricación, Manufacturing Execution System (MES). La integración de la cadena de suministros, el IoT y la IA incorporados simplifican la programación y la ejecución del taller, optimizando las decisiones y controlan la calidad y el costo.

La solución de Oracle Manufacturing basada en la nube permite las técnicas de fabricación discreta como, por ejemplo, la fabricación con procesos, fabricación en modo mixto, programación de la producción, operar en la cadena de suministro impulsada por proyectos o la fabricación por contrato o conectar la fábrica mediante dispositivos IoT.

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

https://www.oracle.com/es/scm/manufacturing/

1.3.2.4 MAINTENANCE

Optimizar las estrategias para la gestión de activos empresariales con mantenimiento de base condicionada que predice y responde a las necesidades de mantenimiento mediante el monitoreo continuo. Mejorar la eficiencia con una solución de mantenimiento inteligente e integrada que garantiza la disponibilidad de repuestos y mano de obra. Administrar los costos de infraestructura con software de mantenimiento escrito y optimizado para la nube.

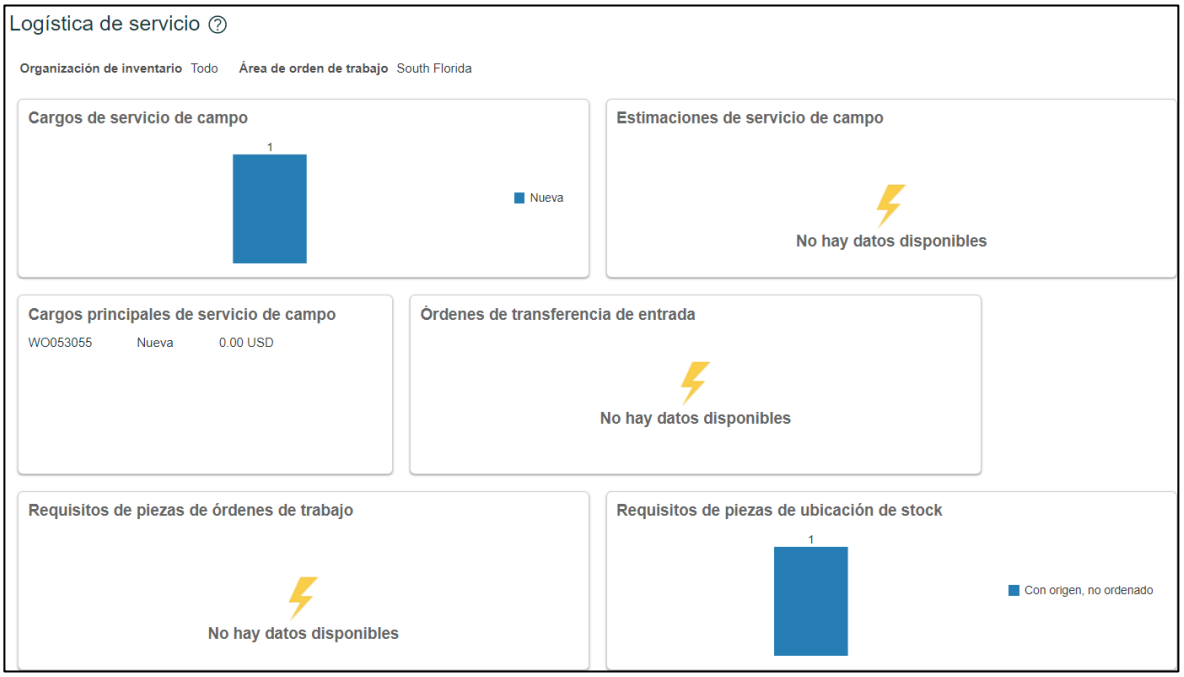
Puede obtener más información consultando el siguiente enlace de Oracle:

https://www.oracle.com/es/scm/maintenance/

1.3.2.5 ORDER MANAGEMENT

La solución de extremo a extremo omnicanal del pedido al cobro de Oracle organiza los pedidos en múltiples sistemas, simplifica la configuración de productos, permite precios dinámicos y el compromiso de pedidos global.

La solución de Oracle Orden Management permite la gestión de pedidos omnicanal que unifica la experiencia del cliente, realizar una gestión estratégica de precios para agrupar a los clientes en función de las características de compra y las sensibilidades de precios.



Panel de Logística de Servicio, dentro de Gestión de Órdenes.

Por otro lado, se puede simplificar la configuración de productos y servicios complejos personalizables mediante una experiencia de usuario intuitiva y visual. Además, se debe programar el envío desde el stock, el envío directo con fechas rápidas y fiables.

Puede obtener más información relacionada con Oracle Fusion Cloud Order Management consultando el siguiente enlace:

https://www.oracle.com/es/scm/order-management/

a) **Oracle Channel Revenue Management:** crear programas comerciales eficaces para aumentar los ingresos, los márgenes de beneficio y la cuota de mercado. La solución de promoción comercial de descuentos permite a las compañías optimizar el rendimiento del programa e impulsar la eficiencia de los canales automatizando los procesos y la liquidación en la nube.

   Puede obtener más información relacionada con Oracle Channel Revenue Managment consultando el siguiente enlace de Oracle:

   https://www.oracle.com/es/scm/order-management/channel-revenue-management/

1.3.2.6 LOGISTICS

Gestionar sin problemas el transporte sostenible, el comercio global y los procesos de distribución para maximizar el cumplimiento perfecto de los pedidos, minimizar los costos logísticos y, al mismo tiempo, adaptarse a las interrupciones del negocio y a los cambios en la cadena de suministro.

A continuación, se describen las distintos módulos o aplicaciones que forman parte de la solución de Oracle Logistics:

a) **Logistics Network Modeling:** con este se realiza un modelado de escenarios hipotéticos precisos para optimizar la red de transporte, se determina la mejor opción teniendo en cuenta el impacto en el tiempo y el costo de los cambios propuestos e impleméntalos fácilmente.

   Puede obtener más información consultando la ficha técnica de Oracle Logistics Network Modeling Cloud, a través del siguiente enlace en inglés:

   https://www.oracle.com/es/a/ocom/docs/applications/supply-chain-management/oracle-logistics-network-modeling-ds.pdf

b) **Warehouse Management:** transforma las operaciones de almacén para cumplir con los desafíos del mercado actual impulsado por la demanda, gestiona con éxito las operaciones de ejecución de pedidos complejas y obtiene una visibilidad total del inventario, desde el centro de distribución hasta el estante de la tienda.

   Puede obtener más información consultando el siguiente enlace de Oracle sobre Warehouse Management:

   https://www.oracle.com/es/scm/logistics/warehouse-management/

c) **Transportation Management:** gestiona toda la actividad de transporte en toda la cadena de suministro global. Combinando la facilidad de uso con las capacidades líderes del sector, Oracle Transportation Management y permite dirigir las operaciones logísticas de forma más eficiente, reducir los costos de flete y optimizar los niveles de servicio.

   Puede obtener más información relacionada con la solución Transportation Management, consultando el siguiente enlace de Oracle:

   https://www.oracle.com/es/scm/logistics/transportation-management/

d) **Transportation Operational Planning:** determina la mejor manera de satisfacer las necesidades de transporte, desde operaciones simples de punto a punto hasta complejas operaciones multimodales, de varios tramos y crossdocking para determinar las mejores opciones de ruta y optimizar la entrega rápida y el costo.

   Puede consultar la ficha técnica del producto de Oracle a través del siguiente enlace en inglés:

   https://www.oracle.com/es/a/ocom/docs/applications/supply-chain-management/oracle-transportation-operational-planning-ds.pdf

e) **Oracle Fleet Management:** garantiza la capacidad de cumplimiento en cuanto a pedidos y envíos con un enfoque integrado para gestionar los activos propios y los proveedores externos, lo que se traduce en envíos a tiempo, costos reducidos y una mayor satisfacción del cliente.

   Puede consultar la ficha técnica del producto de Oracle a través del siguiente enlace en inglés:

   https://www.oracle.com/es/a/ocom/docs/applications/supply-chain-management/oracle-fleet-management-ds.pdf

f) **Global Trade Management:** gestiona de forma centralizada los procesos de negocio relacionados con el comercio transfronterizo con la solución de cumplimiento global de Oracle. Empresas de todos los tamaños obtienen visibilidad y control incomparables de los pedidos y envíos, y se aseguran del cumplimiento de las normativas comerciales.

   Puede obtener más información relacionada con la solución de Oracle a través del siguiente enlace:

   https://www.oracle.com/es/scm/logistics/global-trade-management/

g) **Intelligent Technologies:** remodela la gestión logística mediante la aplicación de tecnologías adaptativas para impulsar la eficiencia en todo el proceso de transporte y distribución, responder rápidamente a las disrupciones y resolver problemas más rápidamente, lo que se traduce en mayor ahorro y un mejor servicio al cliente.

   Puede obtener más información sobre cómo Machine Learning dota de inteligencia a Transportation Management, a través del siguiente enlace de Oracle en inglés:

   https://www.oracle.com/scm/logistics/transportation-management/transportation-management-tour/

1.3.2.7 PRODUCT LIFECYCLE MANAGEMENT (PLM)

La solución de Oracle Cloud PLM o gestión del ciclo de vida del producto, acelera la innovación y la introducción de nuevos productos mediante la gestión eficiente de artículos, piezas, productos, documentos, requisitos, órdenes de cambio de ingeniería y flujos de trabajo de calidad en las cadenas de suministro globalizadas, y se integra a la vez y sin problemas en los sistemas de diseño asistido por ordenador (CAD).

Puede obtener más información relacionada con Oracle Product Lifecycle Management (PLM), consultando el siguiente enlace:

https://www.oracle.com/es/scm/product-lifecycle-management/

1.3.3 GESTIÓN DEL CAPITAL HUMANO (HCM)

Oracle Fusion Cloud HCM es una solución completa en la nube que conecta todos los procesos de recursos humanos (y todas las personas) de la organización. Oracle ayuda a crear una comunidad donde la gente se sienta valorada, escuchada y parte del grupo. Con una única experiencia de usuario y un solo modelo de datos, y reforzado gracias a unos procesos e infraestructura exentos de problemas, Oracle Cloud HCM puede ayudar a redefinir qué es lo mejor para los empleados de la organización.

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

https://www.oracle.com/es/human-capital-management/what-is-hcm/

A continuación, se describen los principales módulos y las funcionalidades de la solución que aporta Oracle en la gestión del capital humano.

1.3.3.1 ORACLE ME

Oracle ME (My Experience) forma parte de Oracle Fusion Cloud HCM. Se trata de la única plataforma completa de experiencia del empleado que ayuda al talento a conectarse a la organización, desarrollarse y dar lo mejor de sí mismo. Con una comprensión profunda de las necesidades, aspiraciones y particularidades de cada trabajador, se podrá diseñar experiencias que saquen lo mejor de cada persona.

Impulsa el cambio y refuerza la cultura organizativa, todo ello orientado y personalizado en función de los datos de los empleados gestionados en Oracle Cloud HCM.

Puede obtener más información relacionada con la plataforma Oracle ME consultando el siguiente enlace:

https://www.oracle.com/es/human-capital-management/employee-experience/tour/

A continuación, se describen los principales módulos de la plataforma Oracle ME.

a) **HCM Communicate:** controla la audiencia, contactando con los trabajadores de toda la organización sin depender de otros equipos ni poner en riesgo la confidencialidad de la información con soluciones de terceros.

   Para más información relacionada con HCM Communicate, consulte el siguiente enlace de Oracle:

   https://www.oracle.com/es/human-capital-management/employee-experience/oracle-me/communicate/

b) **Journeys:** impulsa el éxito ofreciendo orientación personalizada para ayudar a los empleados a abordar sus flujos de trabajo profesionales y personales, como incorporarse a un puesto de trabajo nuevo, buscar oportunidades laborales, trasladarse a un nuevo cargo o iniciar un nuevo proyecto. Todo ello con una única experiencia de usuario y un único sistema de registro: Oracle Fusion Cloud HCM.

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

https://www.oracle.com/es/human-capital-management/employee-experience/oracle-me/journeys/

c) **Touchpoints:** los empleados quieren sentirse escuchados y valorados todos los días. Oracle Touchpoints proporciona un canal de escucha y acción permanente entre empleados y gerentes que genera interacciones útiles para reforzar la confianza, mejorar la retención y fomentar el crecimiento.

Puede obtener más información consultando el siguiente enlace de Oracle:

https://www.oracle.com/es/human-capital-management/employee-experience/oracle-me/touchpoints/

d) **Connections:** conecta fácilmente con otras personas, ayuda a los trabajadores a encontrar y conectarse rápidamente con otras personas que tengan habilidades, intereses o experiencias específicas. Crea una red permitiendo a los trabajadores promover su marca personal destacando sus habilidades, logros y experiencia profesional.

1.3.3.2 HUMAN RESOURCES

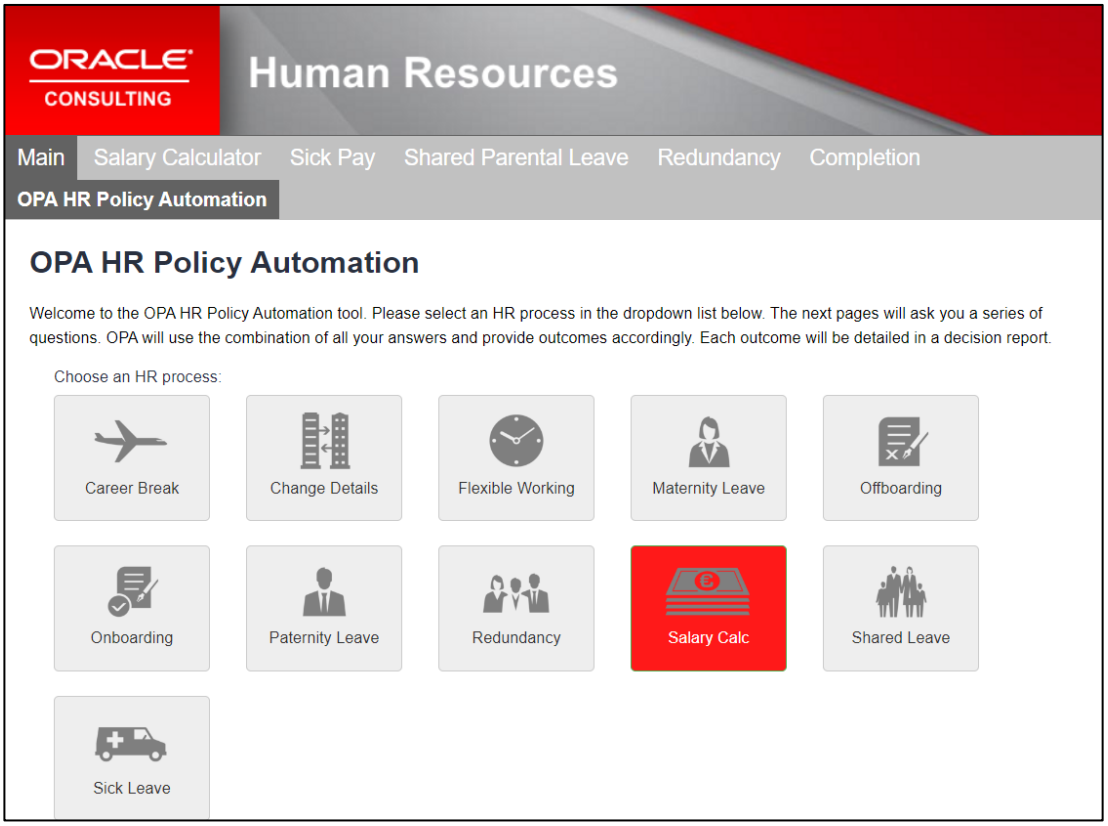
La suite de recursos humanos sirve para planificar, gestionar y optimizar los procesos globales de personas con una fuente de datos común. Tome mejores decisiones, personalice las experiencias de los empleados y aproveche los flujos de trabajo altamente configurables que ofrecen escalabilidad y localización.

a) **Funcionalidades clave:** Con esta se contrata, incorpora, gestiona y fomenta el compromiso de los trabajadores de acuerdo con las prácticas legales y de la empresa. Con la suite de recursos humanos, puede ofrecer a los trabajadores opciones seguras de autoservicio con capacidad de respuesta móvil para la gestión de datos personales, salarios y recibos, programas de beneficios e integración de directorios.

Puede obtener más información consultando el siguiente enlace de Oracle:

https://www.oracle.com/es/human-capital-management/hr/

b) **Oracle HR Help Desk:** ofrece servicios de RR.HH. rápidos, coherentes e inteligentes a todos los empleados. Oracle HR Help Desk es una solución de gestión de solicitudes de servicio escalable y unificada que facilita a los empleados encontrar respuestas sin el riesgo de que los datos confidenciales caigan en manos equivocadas.



Panel de Oracle Consulting.

Puede obtener más información consultando el siguiente enlace de Oracle:

https://www.oracle.com/es/human-capital-management/hr-help-desk/

c) **Oracle Advanced HCM Controls:** la gestión de riesgos de RR.HH. de Oracle incorpora las mejores prácticas de gestión con una solución de control de transacciones y acceso basada en IA. Automatiza el análisis de seguridad y optimiza las certificaciones de acceso para reforzar la protección frente a infracciones de privacidad, fraudes en nóminas y errores.

   Puede obtener más información relacionada con la solución Oracle Advanced HCM Controls, consultando el siguiente enlace:

   https://www.oracle.com/es/human-capital-management/advanced-hcm-controls/

d) **Digital Assistant for HCM:** proporciona comunicación y orientación a todas las preguntas de los empleados con soporte de IA conversacional a través de un bot conversacional de recursos humanos.

   Puede obtener más información con el asistente digital para HCM, a través del siguiente enlace de Oracle:

   https://www.oracle.com/es/human-capital-management/hr/digital-assistant/

1.3.3.3 TALENT MANAGEMENT

Se atrae a los mejores candidatos, aumentando la productividad y mejorando las decisiones con gestión del talento de extremo a extremo. Obtener, contratar, incorporar, gestionar el rendimiento, desarrollar carreras y planificar la sucesión, todo en un solo lugar.

A continuación, se va a detallar las principales funcionalidades de Oracle Talent Management:

a) **Oracle Recruiting:** Proporcionar experiencias atractivas a los candidatos y herramientas eficientes a los reclutadores. Oracle Recruiting, de Oracle Fusion Cloud Human Capital Management (HCM), es una solución completa y unificada que ayuda a los equipos a atraer y contratar a los profesionales adecuados.

   Puede obtener más información consultando el siguiente enlace de Oracle:

   https://www.oracle.com/es/human-capital-management/recruiting/

b) **Oracle Learning:** Desarrollar el talento con una solución de aprendizaje unificada y personalizada que reduce el riesgo de cumplimiento normativo y fortalece las habilidades del personal necesarias para innovar.

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

   https://www.oracle.com/es/human-capital-management/talent-management/learning/

c) **Oracle Compensation:** Promueve la equidad y ayuda a retener a los mejores talentos, independientemente de la ubicación, mediante el uso de datos en tiempo real para crear y modelar planes de compensación basados en sus propios requisitos únicos.

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

   https://www.oracle.com/es/human-capital-management/talent-management/compensation/

d) **Oracle Dynamic Skills:** Aprovecha la inteligencia artificial y la automatización para mantener al día las habilidades de la organización y respaldar las decisiones relacionadas con la planificación del talento.

   Puede obtener más información consultando las funciones de Dynamic Skills a través del siguiente enlace de Oracle:

   https://www.oracle.com/es/human-capital-management/skills/

1.3.3.4 WORKFORCE MANAGEMENT

Alinea la estrategia comercial, reduce el riesgo de cumplimiento y despliega el personal con un mayor control a través de una solución totalmente integrada que vincula el tiempo, la mano de obra y la gestión de ausencias con datos de nómina, financieros y de personal.

Puede obtener más información relacionada con la gestión del personal consultando el siguiente enlace de Oracle:

https://www.oracle.com/es/human-capital-management/workforce-management/

1.3.3.5 PAYROLL

Apoya los innumerables requisitos en todas las organizaciones, trabajadores e industrias para permitir nóminas eficientes, conformes y configurables en todo el mundo, y aprovechar las integraciones predefinidas con sus proveedores de nóminas, que reducen la complejidad y el coste.

Puede obtener más información consultando el siguiente enlace de Oracle:

https://www.oracle.com/es/human-capital-management/payroll/

1.3.3.6 EMPLOYEE CARE PACKAGE

La pandemia ha puesto el mundo del revés, llevando a los equipos de RRHH a dar un paso al frente y liderar el cambio organizativo, garantizando al mismo tiempo la seguridad y productividad de los empleados. A medida que la situación evolucione, se pedirá a los empleados que hagan cosas nuevas, se adapten a nuevas estructuras y trabajen de nuevas formas.

La solución Employee Care Package de Oracle, incluye información sobre Vaccine at Work Journey. Estas soluciones que forman parte de Oracle Cloud HCM, ayudan a RRHH a mejorar la experiencia de sus empleados y brindan la seguridad, el soporte y las habilidades que se necesitan hoy y a medida que los planes continúan cambiando.

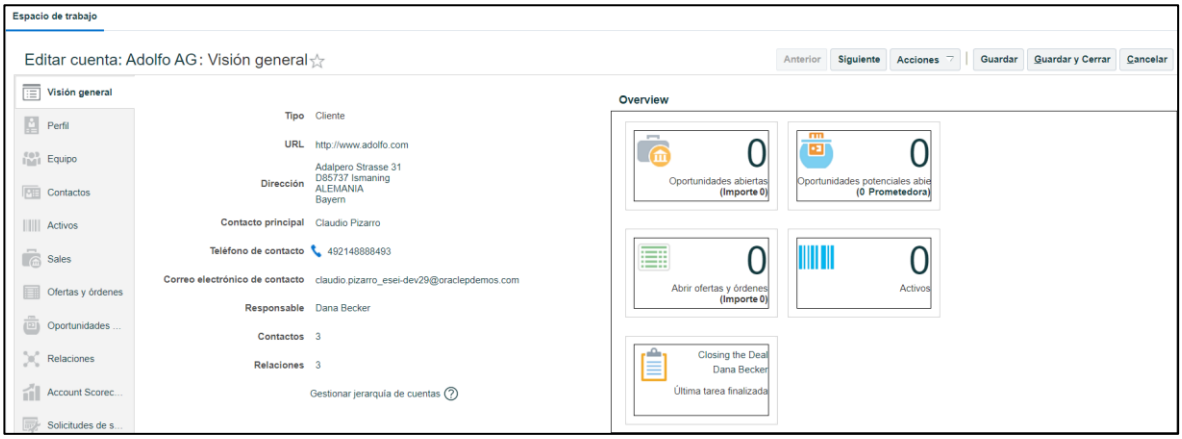
Puede obtener más información sobre la solución consultando el siguiente enlace de Oracle:

https://www.oracle.com/es/human-capital-management/employee-care-package/

1.3.4 CX SALES

La experiencia del cliente se extiende a todo el proceso de ventas, desde búsquedas en sitios web hasta navegar por sitios de comercio electrónico, varios canales digitales de servicio al cliente y experiencias en tienda, por nombrar algunos.

Es más fácil que nunca llevar el negocio a otra parte. Por lo tanto, brindar una gran experiencia durante cada interacción con el cliente es obligatorio para que éste compre, vuelva a comprar y siga siendo leal.



Espacio de trabajo, dentro de Ventas.

Oracle Sales guía a los vendedores con recomendaciones inteligentes que les ayudan a centrarse en los clientes potenciales más valiosos en el momento adecuado. Estas herramientas de venta CRM, basadas en aprendizaje automático, se centran en datos limpios y completos del cliente procedentes de fuentes internas y externas en las que los vendedores pueden confiar.

A continuación, se describen las principales funcionalidades de Oracle Sales a través de los siguientes módulos.

1.3.4.1 SALES AUTOMATION

Mejora la productividad de los vendedores y el éxito de las operaciones mediante la automatización de las tareas manuales y de introducción de datos. Ofrece a los vendedores rutas más rápidas a los registros críticos, para que puedan dedicar menos tiempo a actualizar el CRM o a buscar información y más tiempo a las ventas.

A continuación, se describen las aplicaciones y funcionalidades que aporta la solución de Oracle Sales automation:

a) **Oracle Sales Force Automation (SFA):** es una aplicación de automatización de ventas que recopila y conecta datos operativos y de clientes en un sistema CRM, para ayudar a los profesionales de ventas a comprender a sus clientes y automatizar las tareas durante todo el proceso de ventas.

   Puede obtener más información de la aplicación consultando el siguiente enlace de Oracle:

   https://www.oracle.com/es/cx/sales/sales-force-automation/

b) **Oracle Sales Perfomance Management:** la gestión del rendimiento de ventas de Oracle ofrece herramientas avanzadas para el pago de incentivos, la gestión de cuotas y la administración de territorios.

   Puede obtener más información consultando el siguiente enlace de Oracle:

   https://www.oracle.com/es/cx/sales/sales-performance-management/

c) **Oracle Sales Planning:** establece, analiza y ajusta cuotas individuales y de equipo para motivar a los vendedores a incrementar su agilidad. Oracle Sales Planning tiene las herramientas basadas en datos necesarias para aplicar un enfoque ascendente o descendente a la planificación de cuotas y utilizar análisis predictivos para mejorar el modelado e identificar asignaciones de territorio óptimas.

   Puede obtener más información de la aplicación consultando el siguiente enlace de Oracle:

   https://www.oracle.com/es/cx/sales/sales-planning-forecasting/

d) **Oracle Marketing:** es la solución de marketing integrada más completa disponible para lanzar programas de marketing multicanal y unificar todas las señales de marketing de clientes potenciales y clientes actuales en una sola vista. Esta solución ayuda a generar mayor retorno de las inversiones en marketing digital, a crear fidelidad con el cliente a través de un rendimiento superior de la campaña y permite tomar decisiones de rendimiento en tiempo real durante los ciclos críticos de la campaña.

i. **Oracle B2B Marketing:** Crea campañas de marketing multicanal dirigidas, optimiza actividades de generación de clientes potenciales, personaliza las comunicaciones de clientes actuales y clientes potenciales y automatiza las actividades de marketing.

   Puede obtener más información sobre Oracle B2B Marketing consultando el siguiente enlace:

   https://www.oracle.com/es/cx/marketing/b2b/

ii. **Oracle B2C Marketing:** simplifica la creación, ejecución y medición de campañas de marketing. Utiliza la inteligencia incorporada para captar el comportamiento de los clientes en tiempo real y producir así campañas de marketing B2C sofisticadas y a la vez eficientes.

   Puede obtener más información sobre Oracle B2C Marketing consultando el siguiente enlace de Oracle:

   https://www.oracle.com/es/cx/marketing/b2c/

1.3.4.2 COMMERCE

El comercio electrónico es el negocio de compra y venta de bienes y servicios a través de Internet. Los clientes de comercio electrónico pueden realizar compras desde sus ordenadores, así como desde otros puntos de contacto, incluidos smartphones, relojes inteligentes y asistentes digitales.

El comercio electrónico está en auge tanto en empresas B2C como en empresas B2B. En el comercio electrónico B2C, un minorista u otra empresa vende directamente a los clientes finales. En el comercio electrónico B2B, una empresa vende a otra. En ambos sectores, el objetivo para la mayoría de las empresas es permitir que los clientes compren lo que quieran, en cualquier momento, desde cualquier lugar, utilizando cualquier dispositivo digital.

Oracle Commerce es una gama completa de soluciones escalables en una plataforma unificada que ayuda a crear un exclusivo sitio de comercio electrónico y ofrece múltiples modelos de negocio de comercio electrónico, para generar rápidamente ingresos online.

A continuación, se explorará los módulos que ofrece la solución Commerce de Oracle CX Sales:

a) **Oracle B2B Commerce:** ofrece experiencias de comercio electrónico de autoservicio completas en los canales que prefieren los clientes. Esta solución de comercio digital unificada satisface las complejas demandas de las ventas B2B y escala los negocios en línea de una manera rentable.

   Puede obtener más información consultando el siguiente enlace de Oracle:

   https://www.oracle.com/es/cx/ecommerce/b2b/

b) **Oracle B2C Commerce:** ofrece experiencias de compra digital cuando y donde los clientes quieran interactuar con una marca. Esta solución unificada de comercio electrónico impulsa la fidelidad de los clientes en todos los canales.

   Puede obtener más información consultando el siguiente enlace de Oracle:

   https://www.oracle.com/es/cx/ecommerce/b2c/

c) **Oracle Content Management:** ayuda a todos los integrantes de la organización a gestionar, crear y activar diversos tipos de contenido, incluidos sitios web, documentos, videos y activos gráficos, en un sistema nativo en la nube.

Puede obtener más información sobre la gestión de contenido de Oracle CX Sales, consultando el siguiente enlace:

https://www.oracle.com/es/content-management/

1.3.4.3 CONFIGURE, PRICE, QUOTE (CQP)

Maximiza la rentabilidad de los negocios con precios y descuentos optimizados, mientras se crean propuestas precisas y dinámicas con facilidad. CPQ guía a los clientes a través de un proceso paso a paso para ingresar una orden de compra correctamente configurada y completamente detallada.

Puede consultar las funciones de Oracle CPQ en el siguiente enlace:

https://www.oracle.com/es/cx/sales/cpq/

1.3.4.4 SUBSCRIPTION MANAGEMENT

La gestión de suscripciones es el proceso de gestionar las suscripciones de los clientes y asegurarse de que su experiencia con el producto o servicio sea satisfactoria. El proceso comienza una vez que un cliente se registra para "suscribirse" a su producto o servicio, y finaliza cuando el cliente cancela la suscripción.

Las soluciones CRM de administración de suscripciones permiten a las organizaciones buscar nuevos modelos comerciales al ofrecer opciones dinámicas de precios/compras y propiedad a sus clientes. Puede consultar las funcionalidades de Subscription management en el siguiente enlace de Oracle:

https://www.oracle.com/es/cx/sales/subscription-management/

1.3.4.5 PARTNER RELATIONSHIP MANAGEMENT

Es un portal de socios de marca en el que los administradores de canal y los socios pueden colaborar, compartir y administrar clientes potenciales, registrar acuerdos y crear presupuestos. Esta solución integrada ofrece una experiencia de socio completa y conectada y ayuda a las empresas a desarrollar sus canales de ventas para socios de cara a aumentar los ingresos.

Puede consultar las funcionalidades de Oracle Partner relationship management en el siguiente enlace:

https://www.oracle.com/es/cx/sales/partner-relationship-management/

2. DESPLIEGUE SEGURO PARA ORACLE SAAS FUSION APPLICATIONS

Para realizar un despliegue en la infraestructura de Oracle en la nube es necesario disponer de una cuenta cloud que se asocie a un tenant. Los pasos para crear un tenant en Oracle son descritos en la guía de seguridad "CCN-STIC-889A Guía de Configuración segura para IAM y servicios de seguridad", donde se puede encontrar más información.

2.1 ENTORNOS DE ORACLE SAAS FUSION APPLICATIONS

Un entorno es una plataforma en la que se aprovisionan las aplicaciones. El entorno proporciona un interfaz de gestión para las aplicaciones instaladas. Los entornos se distinguen por entornos de producción o entornos de preproducción. A continuación, se describen los conceptos más importantes que engloban las aplicaciones de Oracle Fusion:

a) **Entorno de producción:** admite las operaciones de negocio diarias en tiempo real de los usuarios autorizados. A una familia de entornos se le asigna un entorno de producción para su aprovisionamiento.

b) Entornos de preproducción.

   i. **Entorno de prueba:** se utiliza para la ubicación temporal antes del despliegue de la aplicación en producción y para la validación de las actualizaciones de mantenimiento antes de que se aplique el mismo mantenimiento al entorno de producción. El entorno de prueba es asignado por una familia de entornos.

   ii. **Entorno de desarrollo:** también denominado entorno de prueba adicional o ATE se utiliza normalmente como sandboxes de desarrollo individuales o colaborativos para el desarrollo de extensiones o integraciones con otras aplicaciones. Por el contrario, la organización debe solicitar a Oracle el número de entornos que necesita.

c) **Familia de entornos:** agrupación lógica de entornos configurada para facilitar la gestión de los entornos relacionados. La familia de entornos garantiza el mantenimiento, la actualización y la aplicación de parches en todas sus aplicaciones en los mismos niveles.

d) **Integración:** se refiere a los servicios que se aprovisionan con las aplicaciones suscritas para ampliar la funcionalidad de las aplicaciones de Fusion. La función de integraciones de la gestión del entorno permite detectar y gestionar estos servicios desde un único lugar.

   Para obtener más información sobre la gestión de integraciones, consulte el siguiente enlace de Oracle:

   https://docs.oracle.com/es-ww/iaas/Content/fusion-applications/manage-integrations.htm

2.2 DESCRIPCIÓN DE LAS FUNCIONES DE OCI UTILIZADAS PARA LA GESTIÓN DEL ENTORNO DE ORACLE SAAS FUSION APPLICATIONS

La gestión del entorno de las aplicaciones Fusion de Oracle se basa en OCI y aprovecha sus servicios para proporcionar funciones como autenticación y autorización, eventos y supervisión. Al gestionar los entornos de las aplicaciones Fusion, se interactuará con OCI, por lo que resulta

útil comprender los conceptos fundamentales de OCI descritos en las guías de seguridad CCN-STIC de Oracle publicadas por el CCN. A continuación, se guiará al lector por las guías de seguridad que hacen referencia a los conceptos fundamentales de OCI:

a) CCN-STIC-889A Guía de Configuración segura para IAM y servicios de seguridad: para obtener más información sobre los conceptos de compartimentos, regiones, identificación y autorización de recursos.

b) CCN-STIC-889B Guía de Configuración segura para Monitorización y gestión: para obtener más información sobre los servicios de eventos y supervisión.

2.3 FLUJO DE TRABAJO PARA LA GESTIÓN DEL ENTORNO DE LAS APLICACIONES DE ORACLE SAAS FUSION APPLICATIONS

El siguiente flujo de trabajo describe las principales tareas para comenzar a trabajar con la gestión del entorno de las aplicaciones Fusion de Oracle:

a) **Solicitud de suscripción para Fusion Applications:** se debe solicitar una suscripción para el uso de las aplicaciones de Oracle Fusion con el proveedor.

b) **Activación del pedido:** para empezar a utilizar el servicio de Oracle Fusion Applications se debe activar el pedido. La activación de órdenes asocia la suscripción a una cuenta de Oracle.

c) **Inicio de sesión en el tenant de Oracle Cloud Infrastructure:** al iniciar sesión, automáticamente será redirigido a la Consola de Oracle Cloud solo con las nuevas órdenes de aplicaciones específicas. Si la orden incluye otras aplicaciones de Oracle Cloud que no aparecen al conectarse, se podrán gestionar desde la Consola de aplicaciones clásicas.

   Para obtener más información sobre el uso de la Consola de Oracle Cloud, consulte el siguiente enlace de Oracle:

   https://docs.oracle.com/es-ww/iaas/Content/GSG/Concepts/applications-home-page.htm

d) **Creación de familia de entornos:** desde la Consola de Oracle Cloud, en el separador de Aplicaciones, se gestiona la creación de entornos para la nueva suscripción.

   Para obtener más información sobre cómo planificar una familia de entornos, consulte el siguiente enlace de Oracle:

   https://docs.oracle.com/es-ww/iaas/Content/fusion-applications/plan-environment-family.htm

e) **Creación de entorno:** una vez creada una familia de entornos es necesario crear un entorno específico. Cuando el entorno esté listo, se podrá utilizar las aplicaciones.

   Para obtener más información para la planificación de un entorno específico, consulte el siguiente enlace de Oracle:

   https://docs.oracle.com/es-ww/iaas/Content/fusion-applications/plan-environment.htm

f) **Adición de usuarios:** opcionalmente, puede agregar más usuarios para trabajar con la gestión de entornos de aplicaciones Fusion de Oracle. Para obtener más información, consulte el siguiente enlace:

https://docs.oracle.com/es-ww/iaas/Content/applications-manager/add-apps-users.htm

3. CONFIGURACIÓN SEGURA PARA ORACLE SAAS FUSION APPLICATIONS

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 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. Adicionalmente, se establecerá la necesidad de que el uso del sistema quede registrado para detectar y reaccionar ante una incidencia de seguridad o fallo del sistema pudiendo configurarlo en Oracle mediante el Servicio OCI Identity and Access Management (OCI IAM) para la gestión del entorno de las aplicaciones Fusion de Oracle, y desde la Consola de Seguridad para el establecimiento de roles y cuentas de usuario dentro de las aplicaciones Fusion de Oracle.

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 gestionadas de tal forma que deban 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.

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. Además, se asegurará la existencia de una lista actualizada de usuarios autorizados y mantenida por el administrador del sistema o administrador de seguridad del sistema.

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, en la nube de Oracle, los usuarios de implementación o configuración de los servicios de Oracle SaaS Fusion Applications suelen ser diferentes de los usuarios consumidores de las aplicaciones disponibles en el Cloud de Oracle una vez implementadas y configuradas.

El usuario de implementación puede realizar todas las tareas de configuración y seguridad, como restablecer contraseñas y otorgar privilegios adicionales para sí mismo o para otros. También puede restringir los privilegios de los usuarios de implementación según las necesidades de configuración del entorno.

Para ello, se puede asignar roles de trabajo y roles abstractos a los usuarios de configuración mediante la Consola de Seguridad. A continuación, se describen los roles que pueden ser asignados:

a) Application Diagnostic Administrator.

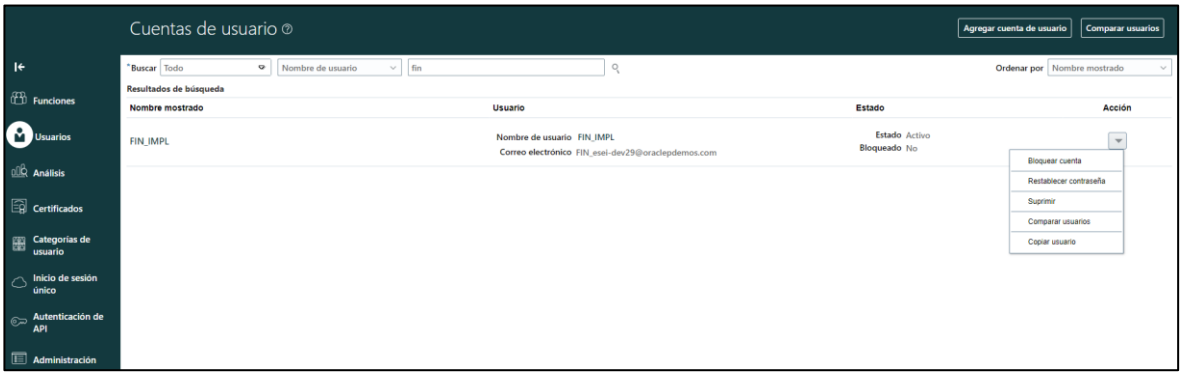
b) Application Implementation Consultant.

c) Employee.

d) IT Security Manager.

Nota: el rol abstracto Application Implementation Consultant tiene acceso sin restricciones a una gran cantidad de datos. Por lo tanto, asigne este rol solo a aquellos usuarios de implementación que realicen una amplia gama de tareas de implementación y manejen los datos de configuración en todos los entornos.

La página Cuentas de usuario se encuentra en Consola de Seguridad → Usuarios y proporciona resúmenes de las cuentas de usuario que seleccione para revisar.



Cuentas de Usuario en Consola de Seguridad.

La información que se puede obtener se enumera a continuación:

a) Inicio de sesión del usuario, nombre y apellido.

b) Si la cuenta se encuentra activa o bloqueada y fecha de vencimiento de la contraseña del usuario.

c) También puede proporcionar la siguiente información:

   i. Información del trabajador asociado, si la cuenta de usuario se creó junto con un registro de trabajador en Human Capital Management, puede incluir también el número de persona, el gerente, el cargo y la unidad comercial.

ii. Información del grupo, si la cuenta de usuario fue creada junto con un registro de grupo en CRM.

La página de cuentas de usuario de la Consola de Seguridad también sirve como puerta de entrada a las acciones de administración de cuentas que puede realizar:

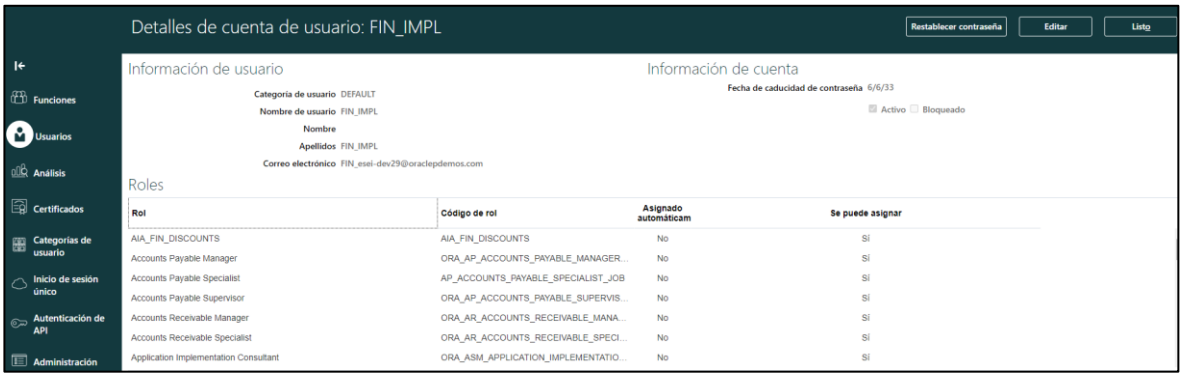
a) Revisar detalles, editar o eliminar roles existentes.

b) Añadir nuevos roles.

c) Bloqueo de cuentas.

d) Restablecimiento de contraseñas.

Finalmente, para revisar los detalles completos de una cuenta de usuario existente, debe navegar por la siguiente ruta Consola de Seguridad → Usuarios → Detalles de cuenta de usuario.



Detalles de Cuenta de Usuario en Consola de Seguridad.

Desde los detalles de la cuenta de usuario, se puede obtener información del usuario, información de la cuenta y una tabla que enumera los roles asignados al usuario.

Para obtener más información sobre cómo agregar cuentas de usuario, puede consultar el siguiente enlace de Oracle en inglés:

https://docs.oracle.com/en/cloud/saas/applications-common/23a/facsa/add-user-accounts.html

3.1.1.2 REQUISITOS DE ACCESO

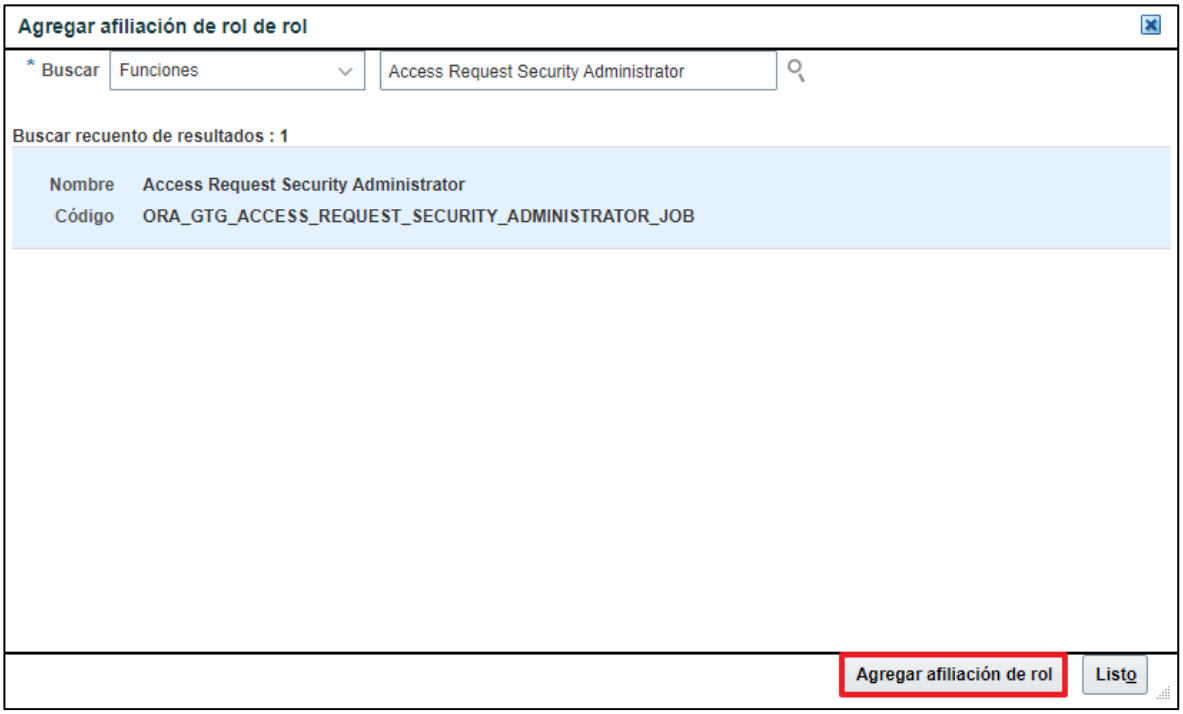
Los requisitos de acceso se aplican atendiendo a la necesidad de que los recursos del sistema queden protegidos con algún mecanismo que impida su utilización, salvo a las organizaciones que disfruten de los derechos de acceso suficientes a ellos.

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.).

Mediante la Consola de Seguridad, Oracle implementa el control acerca de quién tiene acceso a los servicios Fusion a través de la asignación directa de roles predefinidos o roles a medida de los usuarios.



Asignación de Roles desde el apartado Usuarios de la Consola de Seguridad.

Por otro lado, el administrador de Seguridad tiene acceso a los roles y privilegios predefinidos que están disponibles para su asignación. Sin embargo, se debe evaluar la necesidad del usuario antes de asignar roles y privilegios que pueda dar acceso completo a todos los datos y funciones provocando un problema de seguridad.

Para asignar roles a un usuario existente, puede consultar el siguiente enlace de Oracle en inglés:

https://docs.oracle.com/en/cloud/saas/applications-common/23a/facsa/assign-roles-to-an-existing-user.html

Para copiar roles de un usuario a otro, puede consultar el siguiente enlace de Oracle en inglés:

https://docs.oracle.com/en/cloud/saas/applications-common/23a/facsa/copy-roles-from-one-user-to-another.html

Se puede usar el acceso basado en la ubicación para controlar el acceso de los usuarios a las tareas y los datos según sus funciones y direcciones IP de los dispositivos desde los que se conectan.

https://docs.oracle.com/en/cloud/saas/applications-common/23a/facsa/enable-and-disable-location-based-access.html

Finalmente, Oracle dispone del servicio Oracle Database Vault para el control de acceso a las bases de datos.

Oracle Database Vault, para Fusion Cloud Service, está destinado a aumentar la seguridad de los servicios en la nube al proteger los datos de la aplicación contra el acceso de usuarios de base de datos privilegiados. Además, controla las operaciones confidenciales dentro de Oracle Fusion Cloud mediante la autorización de múltiples factores:

a) Formación de reinos que actúan como cortafuegos dentro de Oracle Fusion Cloud.

b) Restricción de acceso a los datos de aplicación tanto para el DBA como para los usuarios.

c) Crea fuertes controles de acceso sobre cuándo y dónde se puede acceder a las aplicaciones.

d) Protección contra cambios no autorizados en la base de datos y aplicaciones.

e) Privilegios temporales y roles específicos de las bases de datos para el descubrimiento y la generación de informes.

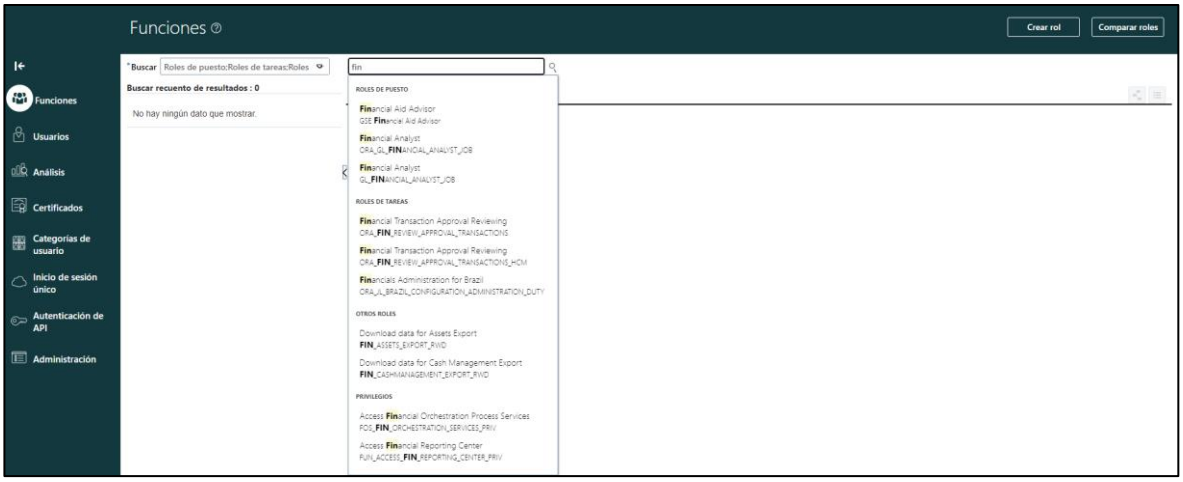
No obstante, existen ciertos límites de uso para Oracle Database Vault for Fusion Cloud Service:

a) Oracle no proporciona almacenamiento adicional. El servicio usa el almacenamiento bajo los servicios adquiridos de Oracle Fusion Cloud.

b) La futura expansión del servicio para Fusion Cloud Service puede estar sujeta a cuotas adicionales.

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.



Asignación de Roles y Funciones desde la Consola de Seguridad.

Oracle Fusion Applications define los siguientes tipos de roles para establecer un control de acceso basado en roles (RBAC) gestionado desde la Consola de Seguridad:

a) **Roles de trabajo:** representan los trabajos que los usuarios realizan en una organización como, por ejemplo, General Accountant y Accounts Receivables Manager.

b) **Roles abstractos:** representan a los usuarios en la empresa independientemente de los trabajos que realicen. Puede asignar roles abstractos directamente a los usuarios para proporcionar acceso a un conjunto de funciones estándar. Ejemplos de roles abstractos se pueden encontrar como Enterprise Resource Planning Self-Service User y Project Team Member.

c) **Roles de servicio:** representan una colección lógica de privilegios que otorgan acceso a las tareas que alguien realiza como parte de un trabajo. Algunas características del rol de servicio son:

   i. Agrupar múltiples privilegios de funciones de seguridad.

   ii. Heredar privilegios agregados y otros roles de servicio.

   iii. Se pueden copiar y editar.

   Algunos ejemplos de roles de servicio que se pueden encontrar incluyen Budget Review y Account Balance Review.

   Puede obtener más información relacionada con los roles de servicio consultando el siguiente enlace de Oracle en inglés:

   https://docs.oracle.com/en/cloud/saas/applications-common/23a/facsa/duty-role-components.html

d) **Privilegios agregados:** son un tipo de rol que combinan el privilegio funcional para una tarea o deber individual con las políticas de seguridad de datos relevantes. Las funciones que agregan privilegios pueden otorgar el acceso para incluir flujos de tareas, páginas de aplicaciones, áreas de trabajo, tableros, informes, programas por lotes, etc.

   Los privilegios agregados difieren de los roles de servicio en los siguientes aspectos:

   i. Todos los privilegios agregados están predefinidos. No se pueden crear, modificar ni copiar.

   ii. No heredan ningún tipo de rol adicional.

   Puede obtener más información relacionada con los privilegios agregados consultando el siguiente enlace de Oracle en inglés:

   https://docs.oracle.com/en/cloud/saas/applications-common/23a/facsa/aggregate-privileges.html

La mayoría de los roles son una jerarquía o colección de otros roles. Los roles abstractos, de trabajo o de servicio heredan privilegios agregados. Sin embargo, los roles de servicio pueden agregar otros roles de servicio, además de privilegios agregados.

Nota: además de los privilegios agregados y los roles de servicio, los roles de trabajo y los roles abstractos reciben directamente muchos privilegios de seguridad de funciones y políticas de seguridad de datos. Puede explorar la estructura completa de un rol de trabajo o abstracto desde la Consola de Seguridad.

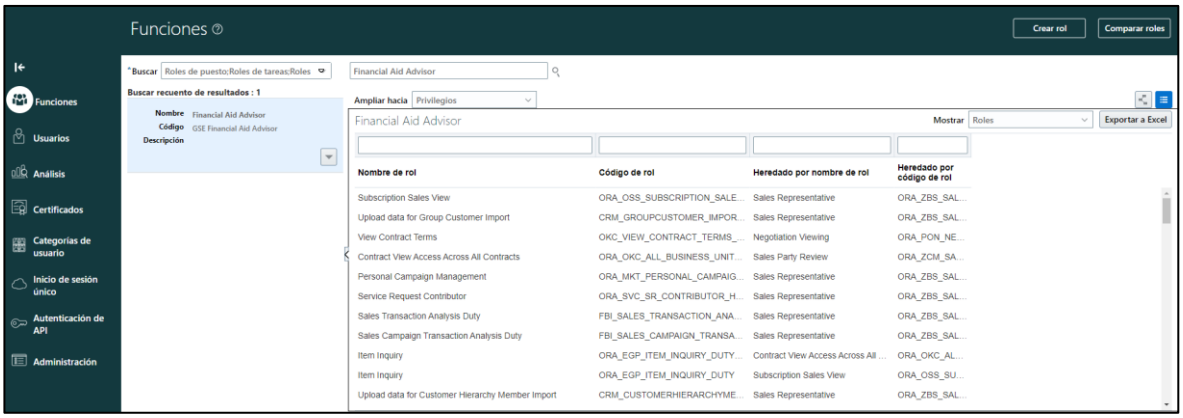
Por último, se puede consultar la siguiente tabla donde se recogen todos los roles asociados a las distintas aplicaciones que forman parte de la suite de Oracle Fusion Applications, incluido los roles comunes a todas las aplicaciones.

Servicio	Aplicaciones	Roles
Características comunes	Todas las aplicaciones	https://docs.oracle.com/en/cloud/saas/applications-common/23a/oacsm/index.html
Planificación de recursos empresariales (ERP)	Accounting Hub	https://docs.oracle.com/en/cloud/saas/financials/23a/oaahm/index.html
	Financials	https://docs.oracle.com/en/cloud/saas/financials/23a/oafrm/index.html
	Procurement	https://docs.oracle.com/en/cloud/saas/procurement/23a/oapcm/index.html
	Project Management	https://docs.oracle.com/en/cloud/saas/project-management/23a/oapjm/index.html
	Risk Management	https://docs.oracle.com/en/cloud/saas/risk-management/23a/farsr/index.html
Gestión de la cadena de suministro (SCM)	Manufacturing and Supply Chain Materials Management	https://docs.oracle.com/en/cloud/saas/supply-chain-management/23a/fammm/index.html
	Order Management	https://docs.oracle.com/en/cloud/saas/supply-chain-management/23a/farom/index.html
	Product Management	https://docs.oracle.com/en/cloud/saas/supply-chain-management/23a/faspm/index.html
	Supply Chain Planning	https://docs.oracle.com/en/cloud/saas/supply-chain-management/23a/fasvc/index.html
Gestión del capital humano (HCM)	HCM Talent Management	https://docs.oracle.com/en/cloud/saas/human-resources/23a/oawpm/index.html
Sales CX	Enterprise Contracts	https://docs.oracle.com/en/cloud/saas/sales/23a/oaecm/index.html
	Sales Automation	https://docs.oracle.com/en/cloud/saas/sales/23a/oaicm/index.html
	Customer Experience	https://docs.oracle.com/en/cloud/saas/sales/23a/oaslm/index.html

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 las 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, se podrá conceder, alterar o anular la autorización de acceso a los recursos, conforme a los criterios establecidos por su responsable. Además, se establecerá una política específica de acceso remoto, requiriéndose autorización expresa.



Apartado de Funciones, dentro de la Consola de seguridad.

De forma predeterminada, Oracle Fusion Applications niega el acceso a los datos a todos los usuarios. Configurar las políticas de seguridad pone a disposición de los usuarios el acceso a los datos por los siguientes medios:

a) Políticas que definen las concesiones disponibles a través de roles aprovisionados.

b) Políticas definidas en el código de aplicación.

Por otro lado, los roles que brindan acceso a los datos pueden ser generados en función de los perfiles de seguridad de HCM. Los roles de datos y los perfiles de seguridad HCM permiten definir los conjuntos de instancias especificados en las políticas de seguridad de los datos.

Cuando proporciona un rol de trabajo a un usuario, el rol de trabajo limita el acceso a los datos en función de las políticas de seguridad de datos de los roles de servicio heredados. Cuando proporciona un rol de datos a un usuario, el rol de datos limita el acceso a los datos del rol de trabajo heredado a una dimensión de datos.

La seguridad de los datos consiste en la concesión de privilegios otorgados condicionalmente a un rol y utilizados para controlar el acceso a los datos.

Un privilegio es una única acción del mundo real en un único objeto comercial. Una política de seguridad de datos es la concesión de un conjunto de privilegios a un principal beneficiario que le permite realizar acciones sobre un objeto dato o un grupo de atributos que cumplan con una condición dada basada en una cláusula WHERE, que especifica el acceso dentro de una dimensión particular como, por ejemplo, una unidad de negocio a la que está autorizado el usuario.

Finalmente, los conjuntos de datos a los que puede acceder un usuario se definen mediante la creación y el aprovisionamiento de roles de datos. La seguridad de datos de Oracle se integra con Oracle Platform Security Services (OPSS), para autorizar a los usuarios o roles con acceso a los datos.

Puede obtener más información relacionada con los perfiles de seguridad de HCM consultando el siguiente enlace de Oracle en inglés:

https://docs.oracle.com/en/cloud/saas/human-resources/23a/ochus/overview-of-securing-oracle-hcm-cloud.html

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.

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.

Oracle Fusion Applications permite la creación de una política de contraseñas que configura reglas y condiciones para el uso de contraseñas por parte de todos los usuarios de la organización. Además, puede definir una política de contraseñas para una categoría de usuario que se aplique a todos los usuarios pertenecientes a una categoría de usuario.

Una categoría de usuario es un grupo o conjunto de usuarios que permite agruparlos en función de los diversos requisitos funcionales y operativos.

Puede obtener más información relacionada con las categorías de los usuarios a través del siguiente enlace de Oracle en inglés:

https://docs.oracle.com/en/cloud/saas/applications-common/23a/facsa/overview-of-user-categories.html

La creación de una política de contraseñas permite definir o establecer los siguientes valores:

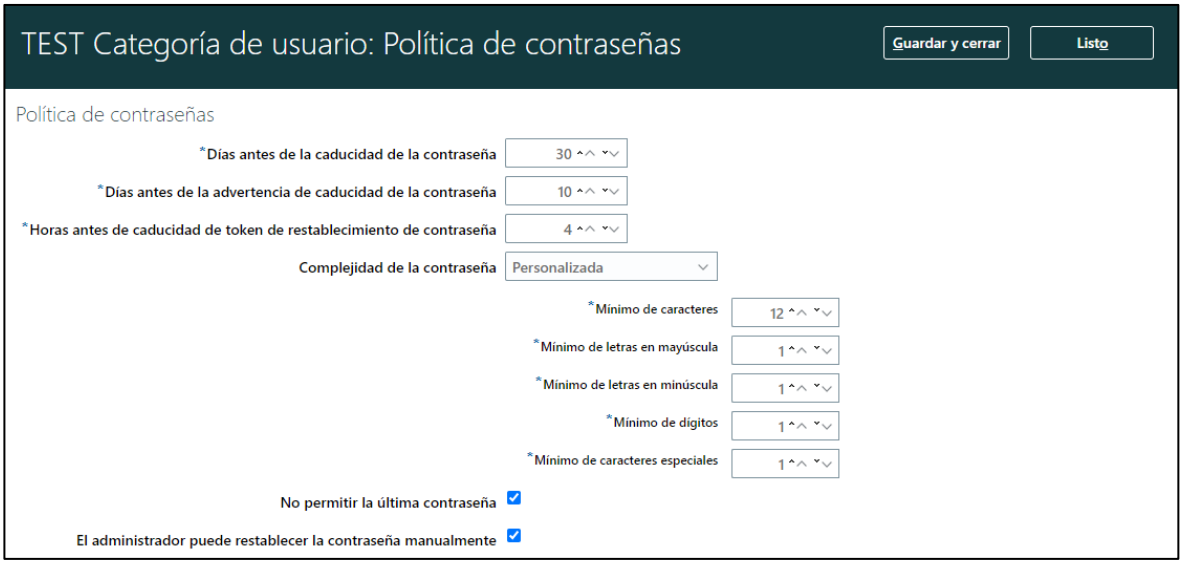
a) **Días antes de la caducidad de la contraseña:** define el número de días que una contraseña sigue siendo válida.

b) **Días antes de la advertencia de caducidad de la contraseña:** define el número de días antes de la caducidad de la contraseña de un usuario para recibir una advertencia de restablecimiento de la contraseña.

c) **Horas antes de la expiración del token de restablecimiento de contraseña:** define la cantidad de horas dentro de las cuales un usuario debe responder a una notificación para restablecer la contraseña.

La política de contraseñas permite configurar la complejidad de la misma. Además, se puede configurar para evitar que el usuario no reutilice la última contraseña y restablecer la contraseña de un usuario por parte de un administrador.

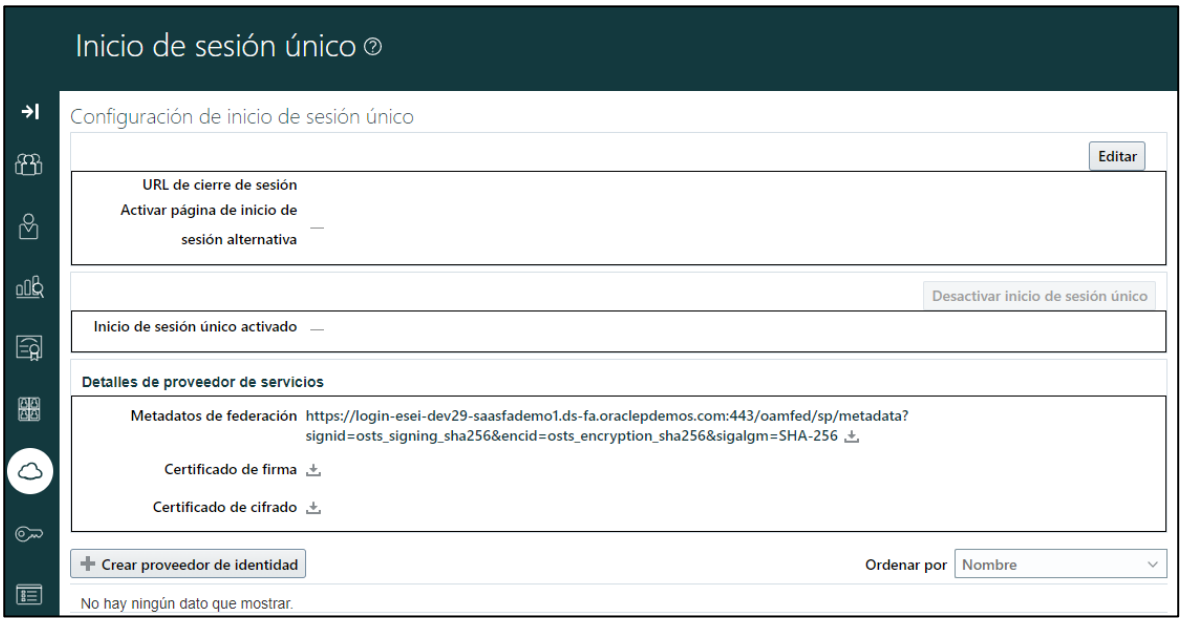
Para la Categoría Alta, se recomienda establecer una política contraseña personalizada con una longitud de al menos 12 caracteres y con la máxima complejidad posible que se pueda establecer. La complejidad de la contraseña se configura desde la Consola de Seguridad → Categorías de usuario → seleccione una categoría del usuario → Política de contraseñas → Editar, para establecer los siguientes valores recomendados que se aprecian en la siguiente imagen.



Política de Contraseñas desde la Consola de Seguridad.

Además, es posible que los usuarios accedan a diferentes aplicaciones internas y externas para realizar sus tareas. Es posible que requieran acceso a diferentes aplicaciones alojadas por socios, vendedores y proveedores.

Para ello, puede proporcionar a los usuarios una experiencia de inicio de sesión único fluida cuando configura Oracle Fusion Applications como un proveedor de servicios de inicio de sesión único. Desde la Consola de Seguridad → Inicio de sesión único, puede administrar los proveedores de identidad para que puedan verificar a los usuarios sin tener que almacenar la información.



Panel de Inicio de Sesión Único.

Uno de los pasos más importantes para agregar un proveedor de identidad es importar el contenido de metadatos del proveedor de identidad. El archivo de metadatos contiene la información de autenticación y también los certificados firmados y encriptados del proveedor de identidad.

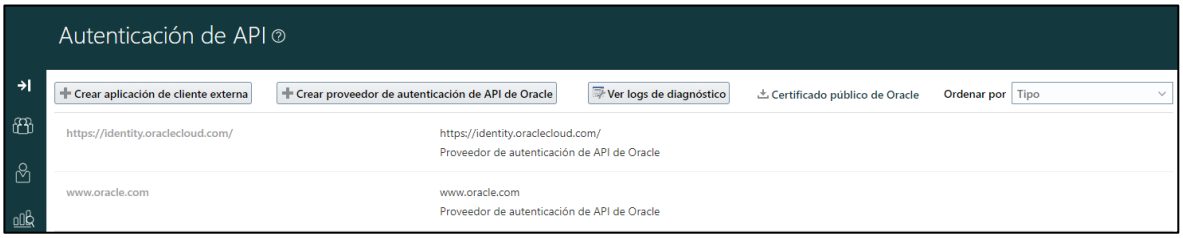
Puede obtener más información relacionada con la configuración de inicio de sesión único consultando el siguiente enlace de Oracle en inglés:

https://docs.oracle.com/en/cloud/saas/applications-common/23a/facsa/configure-single-sign-on.html

Por otro lado, una cuenta del sistema es una cuenta utilizada para integrar aplicaciones de Oracle Fusion Applications con aplicaciones de terceros. Estas cuentas no se encuentran asociadas a ningún usuario, pero debe tener funciones de acceso a las API de REST.

La cuenta del sistema utiliza la autenticación básica para autenticar a los usuarios incluso si el inicio de sesión único está habilitado. La política de contraseñas de la Consola de Seguridad se aplica a las cuentas del sistema y, por lo tanto, la contraseña de esta cuenta caduca según la política de contraseñas definida.

Las tareas críticas, como las operaciones por lotes o las sincronizaciones de datos, deben continuar sin interrupción ni necesidad de volver a autenticarse a intervalos. Para admitir tales tareas, debe definir parámetros personalizados para la autenticación. Desde la Consola de Seguridad, puede definir un token web JSON (JWT) que las API REST pueden usar para automatizar la autenticación del sistema sin tener que autenticarse manualmente.



Autenticación de API desde la Consola de Seguridad.

También es posible la configuración de la autenticación de la API de salida mediante el protocolo de autorización OAuth de tres patas. Puede obtener más información consultando el siguiente enlace de Oracle en inglés:

https://docs.oracle.com/en/cloud/saas/applications-common/23a/facsa/configure-outbound-api-authentication-using-three-legged-oauth.html

Por último, los usuarios de aplicaciones de terceros pueden acceder a un servicio de Oracle Fusion Applications si la autenticación entrante está configurada para ellos. Se puede utilizar un proveedor de autenticación de la API de Oracle para configurar la autenticación de entrada para dichos usuarios. Para ello, es necesario disponer de un certificado público y un emisor de confianza que contenga los tokens.

Puede obtener más información relacionada con la configuración de la autenticación de entrada a través del siguiente enlace de Oracle en inglés:

https://docs.oracle.com/en/cloud/saas/applications-common/23a/facsa/configure-inbound-authentication.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 INVENTARIO DE ACTIVOS

Esta medida obliga a mantener un inventario actualizado de todos los elementos del sistema, detallando su naturaleza e identificando a su responsable; es decir, la persona que es responsable de las decisiones relativas al mismo.

La política formal de protección de la información de Oracle proporciona pautas para toda la clasificación de la información de Oracle y requisitos mínimos de manipulación para cada clasificación.

Desarrollar y mantener un inventario preciso del sistema es un elemento necesario y efectivo para la gestión de la seguridad de los sistemas de información general. La política de inventario de activos de sistemas de información de Oracle requiere que las líneas de negocio, pueda mantener inventarios precisos y completos de sistemas de información, hardware y software. Esta política se aplica a todos los activos de información mantenidos en cualquier sistema de Oracle, incluidos los sistemas empresariales y los servicios en la nube.

3.1.2.2 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.

Antes de la aplicación de las configuraciones, parches y actualizaciones de seguridad, se preverá un mecanismo para revertirlos en caso de aparición de efectos adversos.

Oracle ejecuta automáticamente el mantenimiento en los entornos para aplicar actualizaciones de funciones y parches de seguridad a las aplicaciones, según el programa de políticas de mantenimiento que se escoja. Durante algunos tipos de mantenimiento, no se puede acceder al entorno ni a todas las aplicaciones que se ejecutan en el entorno durante la ventana de mantenimiento.

Por otro lado, Oracle notificará con antelación los próximos tiempos de mantenimiento. No obstante, Oracle pone a disposición del cliente elegir cuándo y con qué frecuencia se produce el mantenimiento en sus entornos, aunque algunas aplicaciones tienen programas de mantenimiento estipulados contractualmente.

Al crear una familia de entornos, se define una política de mantenimiento para todos los entornos de la familia. Algunos aspectos de la política se pueden personalizar por entorno.

Oracle dispone de varios tipos de mantenimiento:

a) Programa de mantenimiento trimestral.

   Oracle lanza nuevas funciones y mejoras importantes cuatro veces al año y las aplica en la actualización trimestral. Estas actualizaciones son obligatorias para todos los clientes y se aplican al entorno según los meses de mantenimiento trimestrales que haya seleccionado. Se puede elegir entre los siguientes programas de mantenimiento para recibir las actualizaciones:

   i. Enero/abril/julio/octubre

   ii. Febrero/mayo/agosto/noviembre

   iii. Marzo/junio/septiembre/diciembre

Nota: Oracle Fusion Cloud Payroll tiene períodos de mantenimiento obligatorios en febrero/mayo/agosto/noviembre. Si la familia de entornos incluye este servicio, no se podrá cambiar los meses de mantenimiento.

b) Aplicación de parches mensual.

   La aplicación de parches mensual es una oferta opcional que se puede elegir. Al seleccionar la aplicación de parches mensual, los entornos reciben correcciones de bugs cada mes. No obstante, se suministrará trimestralmente la entrega de nuevas funciones para el entorno, aunque cada mes se reciban correcciones de bugs.

Nota: después de crear una familia de entornos, puede activar o desactivar la aplicación de parches mensual. No puede cambiar el programa de mantenimiento trimestral.

Finalmente, para modificar la frecuencia del servicio de mantenimiento consulte el siguiente enlace de Oracle en inglés:

https://docs.oracle.com/en/cloud/get-started/subscriptions-cloud/mmocs/modifying-frequency-service-maintenance.html

3.1.2.3 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.

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.

Por otro lado, la aplicación técnica de la presente medida de seguridad se encuentra en la gestión de la familia de entornos. Los entornos de no producción son entornos de prueba y desarrollo usados normalmente para la ubicación temporal antes del despliegue de la aplicación en producción, y para la validación de las actualizaciones de mantenimiento antes de que se aplique el mismo mantenimiento al entorno de producción.

Oracle facilita la validación de las actualizaciones periódicas poniendo a disposición de los clientes material de preparación con al menos 30 días de antelación. Este material describe toda nueva funcionalidad añadida.

Finalmente, a una familia de entornos se le asigna un entorno de prueba para el aprovisionamiento. Los entornos de desarrollo se usan normalmente como sandboxes de desarrollo individuales o colaborativos para el desarrollo de extensiones como, informes, páginas e interfaces o integraciones con otras aplicaciones.

3.1.2.4 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”.

El software de protección deberá ser capaz de analizar todo fichero procedente de fuentes externas y las bases de datos de detección de código dañino deben permanecer permanentemente actualizadas.

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.

El equipo de operaciones de Oracle Cloud utiliza una variedad de métodos para prevenir, detectar y erradicar el malware, mediante la implementación de software antivirus/malware en sistemas relevantes utilizados por los servicios de Oracle Cloud.

El malware detectado se elimina o se pone en cuarentena automáticamente. Las definiciones de virus y malware son actualizadas con frecuencia, y los sistemas cliente aplicables están configurados para realizar actualizaciones de definición y exploraciones en tiempo real.

3.1.2.5 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 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 en conformidad con los acuerdos contractuales y responsabilidades reglamentarias tal y como se definen en el Acuerdo de Procesamiento de Datos para los servicios de Oracle.

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.

3.1.2.6 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.

La auditoría se utiliza para monitorizar la actividad del usuario y todos los cambios de configuración, seguridad y datos que se han realizado en una aplicación. La auditoría implica registrar y recuperar información relacionada con la creación, modificación y eliminación de objetos comerciales. También se registran todas las acciones realizadas sobre los objetos de negocio y los valores modificados.

La información de auditoría se almacena sin ninguna intervención del usuario ni ninguna acción explícita del usuario. Puede utilizar políticas de auditoría para seleccionar objetos comerciales y atributos específicos para auditar. La decisión de crear políticas generalmente depende del tipo de información a auditar y del nivel de detalle requerido para el reporte.

Para obtener más información relacionada con la configuración de la auditoría para las aplicaciones de Oracle Fusion Cloud, consulte el siguiente enlace de Oracle en inglés:

https://docs.oracle.com/en/cloud/saas/applications-common/23a/facia/set-up-auditing-for-oracle-fusion-applications.html

Por otro lado, es necesario habilitar la funcionalidad de auditoría para las aplicaciones de Oracle Cloud Fusion, donde debe configurar también los objetos comerciales y seleccionar los atributos antes de habilitar la función de auditoría.

Nota: de manera predeterminada, la auditoría está deshabilitada para todas las aplicaciones.

Para habilitar y administrar la auditoría, debe disponer del rol con el privilegio asignado de Administrar Políticas de Auditoría (FND_MANAGE_AUDIT_POLICIES_PRIV).

Además, puede consultar el siguiente enlace de Oracle en inglés para la configuración de los atributos de los objetos comerciales:

https://docs.oracle.com/en/cloud/saas/applications-common/23a/facia/audit-configuration-for-business-object-attributes.html

Finalmente, es posible que los usuarios puedan designar temporalmente a otros usuarios para que se hagan pasar por sus perfiles y realicen tareas en su nombre en las aplicaciones. Para ello, Oracle proporciona la función de auditoría de suplantación activada por defecto, incluso cuando la función de auditoría está deshabilitada para una aplicación.

Puede obtener más información sobre la auditoría de suplantación en el siguiente enlace de Oracle en inglés:

https://docs.oracle.com/en/cloud/saas/applications-common/23a/facia/impersonation-audit.html

3.1.2.7 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.

Por defecto, los entornos de Fusion Applications están protegidos por claves de cifrado gestionadas por Oracle. Al suscribirse al servicio Oracle Break Glass, se le ofrece la función de claves gestionadas por el cliente que permite proporcionar y gestionar las claves maestras de cifrado que protegen sus entornos.

La suite de aplicaciones Fusion aprovecha el servicio de OCI Vault que permite crear y gestionar claves de cifrado, para proteger los datos almacenados en reposo en los entornos de producción y de prueba. Si la organización dispone de la suscripción a Oracle Break Glass, puede configurar claves para el entorno durante la creación su creación o puede agregar la clave a un entorno existente.

Nota: si agrega la configuración de una clave en un entorno existente, el cifrado del entorno se producirá durante el siguiente ciclo de mantenimiento programado.

Oracle recomienda crear almacenes independientes para entornos de producción y entornos de no producción. En el almacén asignado al entorno de no producción, puede crear claves independientes para los entornos de prueba y desarrollo.

La principal ventaja de crear almacenes independientes permite la rotación independiente de claves para entornos de producción y no producción. Además, existe un número limitado de claves por almacén. Disponer de almacenes separados proporciona un recuento independiente para los entornos de producción y no producción.

A continuación, se enumeran las posibles acciones a realizar en la gestión de las claves y almacenes:

a) Gestión de claves y configuración de acceso.

b) Creación de almacenes y claves.

c) Visualización del estado y los detalles de la clave.

d) Rotación de claves.

e) Activación y desactivación de claves.

f) Supresión de claves.

Todas las acciones citadas anteriormente pueden ser consultadas a través del siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/Content/fusion-applications/manage-security-key-management.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 Fusion Applications.

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. Los sensores NIDS se implementan en modo de prevención de intrusiones (IPS) o modo de detección de intrusiones (IDS) en la red, para monitorizar y bloquear el tráfico de red sospechoso para que no llegue a la red interna.

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.

Los registros se generan para actividades relevantes para la seguridad en los sistemas operativos. Los sistemas están configurados para registrar actividades de seguridad predeterminadas como acceso a la información o programas, eventos del sistema, alertas, mensajes de la consola y errores del sistema.

Oracle revisa los registros con fines forenses e incidentes de ciberseguridad. Las actividades anómalas identificadas se incorporan al proceso de gestión de incidentes. Los registros de seguridad se almacenan dentro del sistema de gestión de eventos e información de seguridad en un entorno nativo, y almacenado de acuerdo con las políticas internas de Oracle.

Dichos registros se conservan en línea por un mínimo de un año para las operaciones de seguridad interna de Oracle Cloud Services.

Por otro lado, el cliente puede realizar un seguimiento del estado de los servicios desde la página de Detalles del Servicio:

a) **Supervisión de uso y métricas comerciales:** puede monitorizar los datos de uso para determinar si las asignaciones de recursos del servicio están infrautilizadas o sobre utilizadas.

   i. **Visualización de métricas de nivel de derecho:** si las métricas de nivel de derecho se encuentran habilitadas, éstas son mostradas en la Consola de Aplicaciones para algunos servicios. Los datos de uso de nivel de derecho se muestran como un gráfico y las métricas históricas se detallan en la tabla inferior al gráfico. Además, los datos son recopilados cada día para el servicio actual durante los últimos 7 días por defecto.

   ii. **Supervisión del estado y porcentaje de disponibilidad de un servicio:** el sistema calcula el porcentaje de disponibilidad como el número de horas que el servicio ha estado activo, dividido por 24 horas. Por lo tanto, la consulta sobre el porcentaje de disponibilidad siempre será inferior al 100% para el día en que se ha realizado dicha consulta.

   iii. **Supervisión del estado y porcentaje de disponibilidad de una instancia de servicio:** si la organización está suscrita para crear instancias de un servicio en Oracle Cloud, puede ver el uso histórico y el estado de cada instancia desde el mosaico Estado, en la página Detalles del Servicio.

b) **Visualización de métricas de facturación:** la página Métricas de Facturación muestra un gráfico basado en intervalos de tiempo que contiene las métricas relevantes para el servicio seleccionado.

Los datos en el gráfico se muestran en función de los parámetros de medición que seleccione, para mostrar los cargos por uso y excedentes para el servicio y el recurso seleccionado. Por último, puede descargar las métricas en formato CSV y establecer alertas para controlar el saldo de la cuenta.

Puede obtener más información relacionada con la configuración de las alertas para el saldo de la cuenta consultando el siguiente enlace de Oracle en inglés:

https://docs.oracle.com/en/cloud/get-started/subscriptions-cloud/mmocs/set-alert-your-account-balance.html

c) **Visualización del uso de recursos para una suscripción de servicio:** puede ver el uso de los recursos para un servicio desde la Consola de Aplicaciones. La página Cuotas de Recursos, muestra información sobre los recursos adquiridos, los saldos restantes y las fechas de inicio y finalización de la compra.

Puede obtener más información relacionada con la visualización del uso de recursos para una suscripción de servicio, consultando el siguiente enlace de Oracle en inglés:

https://docs.oracle.com/en/cloud/get-started/subscriptions-cloud/mmocs/view-resource-usage-service-subscription.html

d) **Exportación de datos de métricas:** puede exportar los datos de uso que se muestran en el gráfico para servicios medidos, servicios no medidos y derechos, a un archivo con formato CSV desde la página Métricas.

e) **Descarga de informes:** desde la página Documentos de la Consola de Aplicaciones, puede descargar informes relacionados con las suscripciones de la organización. Puede descargar diferentes categorías de informes, como métricas de uso, facturas o incidentes, siempre que estén disponibles. Por último, los informes para descargar están disponibles en formatos como PDF, MS Word y Open XML.

Finalmente, puede obtener más información para consultar cómo visualizar y exportar métricas y uso de recursos o descargar informes, consultando el siguiente enlace de Oracle en inglés:

https://docs.oracle.com/en/cloud/get-started/subscriptions-cloud/mmocs/monitoring-service-status-and-utilization.html

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 mantiene la sesión activa durante un periodo predefinido, que se denomina período de tiempo de espera de la sesión. En este período, el usuario se autentica para usar la aplicación y establece una sesión. Durante la sesión, no es necesario volver a autenticarse. Sin embargo, por motivos de seguridad, las sesiones pueden caducar debido a varias razones y tiempos de espera:

a) **Tiempo de espera de la vida útil de la sesión:** una vez que el usuario se ha autenticado en la aplicación, si está trabajando activamente en ella, su sesión permanece activa durante un periodo de 8 horas.

b) **Tiempo de espera de inactividad de la sesión:** el tiempo de espera considera el tiempo transcurrido desde la última vez que se envió una solicitud al servidor de aplicaciones. Pasados 10 minutos, se recibirá un mensaje con la opción para extender la sesión. Si ésta no se extiende, la sesión cerrará.

c) **Tiempo de espera de sesión inactiva:** mide el tiempo de espera que deja la aplicación inactiva. Pasados 30 minutos, se recibirá un mensaje para reiniciar la sesión.

d) **Tiempo de espera de inactividad del navegador:** mide el tiempo de espera que deja el navegador inactivo. Después de 30 minutos, la sesión finalizará.

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.

El acceso de los clientes al sistema es principalmente a través de internet. Oracle usa la capa de transporte estándar de la industria usa el protocolo de seguridad (TLS), para el acceso a Oracle Cloud Service. Las conexiones TLS son negociadas por al menos una encriptación de 128 bits como mínimo y 2048 bits para las claves privadas usadas para generar la clave de cifrado.

Se recomienda disponer de los últimos navegadores validados por Oracle para el uso de sus aplicaciones, ya que son compatibles con los métodos de cifrado más seguros.

Nota: la lista de navegadores certificados para cada versión de un programa de Oracle se puede encontrar en el Portal de soporte al cliente (My Oracle Support) en la nube.

Los clientes también pueden acceder a los servicios de Oracle Cloud mediante un servicio VPN o Fastconnect habilitado para Ipsec.

Nota: el uso de la VPN y Fasconnect requieren de una suscripción adicional. Póngase en contacto con el fabricante para obtener más información.

Por otro lado, para la comunicación entre aplicaciones de los servicios de Oracle Cloud pueden usarse los certificados. Puede usar la página Certificados en el área funcional de la Consola de Seguridad para trabajar con certificados en cualquiera de los dos formatos: PGP y X.509.

Puede obtener más información relacionada con los tipos de certificado, firmas, importación y exportación o eliminación de certificados consultando el siguiente enlace de Oracle en inglés:

https://docs.oracle.com/en/cloud/saas/applications-common/23a/facsa/overview-of-certificates.html

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 CALIFICACIÓN DE LA INFORMACIÓN

Para calificar la información se estará a lo establecido legalmente sobre la naturaleza de la misma. La política de seguridad establecerá quién es el responsable de cada información manejada por el sistema y recogerá, directa o indirectamente, los criterios que en cada organización determinarán el nivel de seguridad requerido.

El responsable de cada información seguirá los criterios determinados para asignar a cada información el nivel de seguridad requerido, y será responsable de su documentación y aprobación formal. El responsable de cada información en cada momento tendrá en exclusiva la potestad de modificar el nivel de seguridad requerido.

Por otro lado, Oracle clasifica la información en cuatro clases:

a) Información pública.

b) Información interna.

c) Información restringida.

d) Información altamente restringida.

La información pública no es confidencial y, por tanto, no es necesario que lo sea para Oracle. Además, la información interna de Oracle debe permanecer confidencial para Oracle.

Además, la información restringida y la altamente restringida debe permanecer confidencial para Oracle y el acceso a la misma quedará restringida en base a la necesidad de conocer. Adicionalmente, también se deben cumplir los requisitos adicionales para el manejo de información clasificada.

Oracle dispone de requisitos formales para administrar la retención de datos. Estas políticas operativas definen los requisitos por tipo de datos y categoría, incluidos ejemplos de registros en varios departamentos de Oracle. La retención de datos de los clientes en los servicios en la nube es controlada por el cliente y está sujeto a los términos de su contrato.

Los datos del cliente se clasifican en una de las dos principales categorías de información confidencial de Oracle, con el fin de limitar el acceso para la distribución y manejo de dichos datos. Oracle mantiene la información confidencial de acuerdo con las condiciones del pedido del cliente.

3.2.3.2 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.

Periódicamente, Oracle realiza copias de seguridad del contenido de la instancia de los servicios de Oracle Cloud en el entorno de producción, para minimizar las pérdidas de datos en caso de incidente. Las copias de seguridad se almacenan en el sitio principal utilizado para proporcionar los servicios en el Cloud de Oracle y también puede almacenarse en una ubicación alternativa con fines de retención.

Una copia de seguridad de producción generalmente se conserva en línea o fuera de línea durante un período de al menos 60 días posteriores a la fecha en que se realiza la copia de seguridad.

Por otro lado, para la restauración de las copias de seguridad, Oracle normalmente no actualiza, ni inserta, ni elimina o restaura los datos de un cliente en su nombre. Sin embargo, con carácter excepcional y siempre sujeto a la autorización por escrito, Oracle puede ayudar a los clientes a restaurar sus datos perdidos.

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).

Para el cumplimiento de esta medida, Oracle dispone de la solución de seguridad WAF for Fusion, basada en la nube de segunda generación y administrada por Oracle de manera gratuita para los clientes de Fusion alojados en OCI. WAF for Fusion funciona como un control de seguridad adicional que proporciona protección activa contra ataques dirigidos en la capa 7.

La solución permite monitorizar y detectar fuentes de tráfico HTTP y HTTPS maliciosas para ayudar a proteger las aplicaciones, cargas de trabajo y datos críticos de Fusion de ataques DDoS, así como los 10 principales riesgos OWASP y otras amenazas de aplicaciones web. Además, WAF está integrado e implementado en las instancias de OCI Load Balancer que se ejecutan frente a las aplicaciones de Fusion.

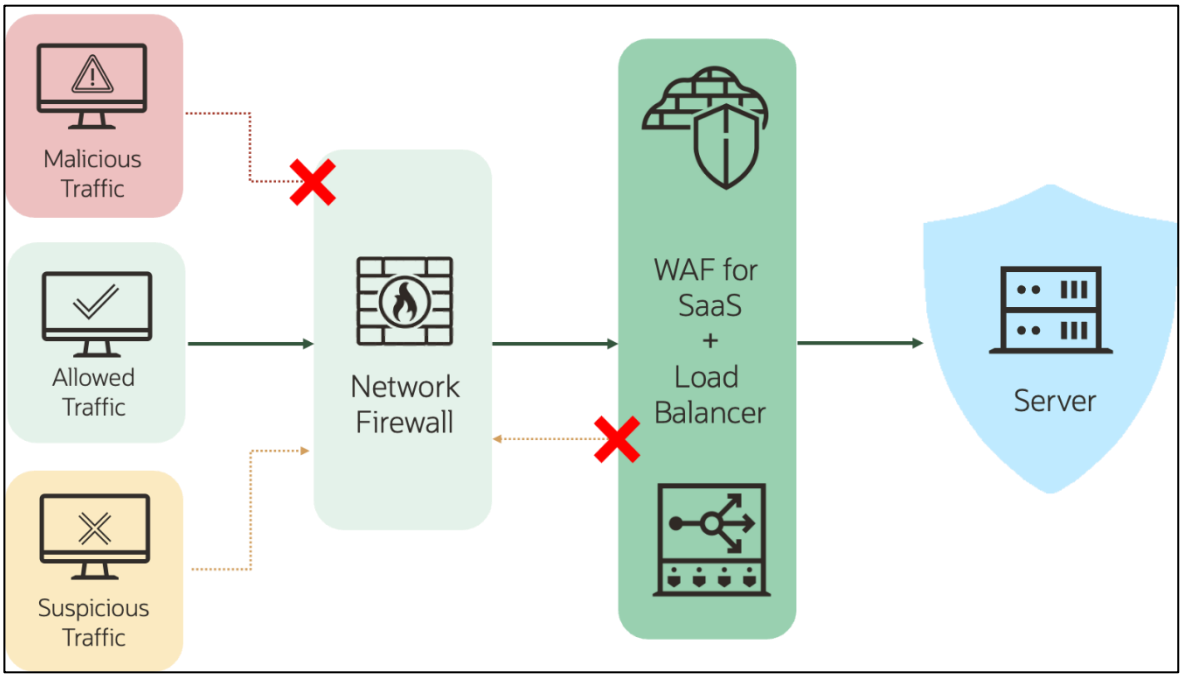


Diagrama de WAF Para Fusion.

Las políticas de capa 7 dentro de WAF for Fusion se componen de un conjunto de reglas que admiten controles de acceso, capacidades protección del conjunto de reglas básicas de OWASP y limitación de velocidad, sin impactar en el rendimiento y la escalabilidad de las aplicaciones de Fusion.

Nota: las políticas y los registros solo estarán disponibles para el equipo de seguridad en la nube de SaaS de Oracle.

Estas políticas funcionan para los casos de uso comunes que van desde el bloqueo de intentos maliciosos de inundar un servicio en línea de solicitudes, hasta la protección contra solicitudes dirigidas específicas que intentan hacerse cargo de los sistemas de una aplicación. A continuación, se describen algunos ejemplos:

a) Los portales de contratación de HCM son un almacén de información personal atractivo para los actores maliciosos, ya que pueden desactivar el servicio o bien exfiltrar los datos de los clientes a través de un ataque DDoS.

WAF for Fusion puede inspeccionar dichos patrones de ataque y aplicar reglas de limitación de velocidad para denegar o redirigir las solicitudes de tráfico que superen un umbral de intervalo.

b) Las herramientas de CX Customer Relationship Management a menudo brindan oportunidades para que los clientes potenciales acepten contenido de servidores comprometidos o de dudosa reputación. WAF for Fusion puede mitigar ataques Cross Site Scripting (XSS) y SQL injection y garantizar que el tráfico que llega a las aplicaciones Fusion provenga de servidores confiables.

c) WAF for Fusion permite detectar y bloquear intentos de explotación de ejecución remota de código (RCE), mediante su capacidad para brindar información detallada de las solicitudes y respuestas como, inserción de valores en sus registros de errores, parámetros de aplicaciones web y campos de encabezado HTTP.

Finalmente, WAF for Fusion está integrado con SIEM de Oracle SaaS Cloud Security y recibe registros de WAF para la monitorización. Los registros enriquecen las capacidades de detección de SIEM y Oracle Security Operations Center (SOC) recibe alertas cuando se detectan comportamientos anómalos, para tomar las medidas correctivas adecuadas.

4. MECANISMOS DE VIGILANCIA

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.

Oracle se enfoca en ayudar a reducir el riesgo al proporcionar un conjunto integral de capacidades de seguridad simples, prescriptivas e integradas que pueden ayudar a las organizaciones a asegurar su tenant de OCI. El enfoque de servicios de seguridad integrados reduce la carga de los clientes, permitiéndoles concentrarse en mejorar su negocio principal.

Oracle cuenta con centros de operaciones y monitorización globales (Global Nerve Centre, GNC) que siguen un enfoque follow-the-sun 24x7. Estos centros están conectados a los pods de producción, proporcionando visibilidad al minuto de los componentes del entorno. Los GNC se encargan de supervisar y garantizar la estabilidad de los pods así como de gestionar los eventos de los clientes y las comunicaciones proactivas en caso de incidencia.

Las capacidades de detección y prevención están marcadas por un equipo dedicado 24x7x365 en cada GNC.

Entre los servicios de seguridad proporcionados por Oracle, se encuentra Cloud Guard, para ayudar a los clientes a monitorizar, identificar, lograr y mantener una sólida postura de seguridad en Oracle Cloud. Puede usar el servicio para examinar sus recursos en OCI en busca de debilidades de seguridad relacionadas con la configuración y actividades de riesgo.

Puede obtener más información sobre el servicio consultando el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/cloud-guard/home.htm

Tras la detección de una amenaza, Cloud Guard puede sugerir, ayudar o tomar medidas correctivas, según la configuración proporcionada por el cliente.

Las características de Cloud Guard permiten obtener vistas consolidadas de las políticas de seguridad de IaaS y SaaS. Utilice las configuraciones preconfiguradas y personalizadas para monitorizar violaciones de seguridad en aplicaciones SaaS.

Por otro lado, Oracle Cloud Guard Fusion Applications Detector amplía el servicio de Oracle Cloud Guard, más allá de la gestión de posturas de seguridad en la nube, para que OCI también pueda monitorizar las aplicaciones de Oracle Fusion Cloud, ofreciendo a los clientes una vista consolidada de las políticas de seguridad.

El servicio está disponible primero para Oracle Fusion Cloud Human Capital Management (HCM) y Oracle Fusion Cloud Enterprise Resource Planning (ERP). La herramienta proporciona configuraciones preconfiguradas y personalizadas, o "recetas", para monitorizar posibles violaciones de seguridad en las aplicaciones. Los detectores activan alertas en respuesta a cambios de configuración confidenciales relacionados con los privilegios de los usuarios que afectan el acceso a datos importantes, incluida la adición, eliminación o modificación de datos y privilegios de funciones para roles y usuarios, así como cambios en objetos confidenciales.

La receta del detector de actividad de aplicaciones Cloud Guard Fusion (administrada por Oracle) es una plantilla lista para usar (OOTB) y no se puede modificar. Los clientes pueden clonar y editar sus propias reglas; por ejemplo, pueden modificar un nombre, cambiar el nivel de riesgo, filtrar un usuario específico para monitorear sus actividades, deshabilitar una regla, etc.

Finalmente, los clientes de Oracle Fusion deben optar por habilitar Cloud Guard dentro de tu tenant de OCI. Una vez que Cloud Guard está habilitado, hay un flujo de registro objetivo dentro de Cloud Guard que requiere que los clientes proporcionen la URL de su pod y las credenciales del usuario del servicio, creadas previamente dentro de la aplicación Fusion. Una vez que se crea el objetivo y se adjunta la receta de la aplicación Fusion, la monitorización se activa automáticamente y los problemas de actividad del usuario de la aplicación Fusion activarán alertas.

Sin embargo, Cloud Guard no proporciona integración SIEM directa. Los clientes pueden hacer uso de eventos y funciones de OCI, como el servicio de notificación, el servicio de funciones y otros, para integrar Cloud Guard con SIEM de terceros. Estos servicios están descritos en las guías de seguridad publicadas por el CCN de Oracle Cloud Infrastructure, en la modalidad IaaS y PaaS.

5. ESCENARIO COMPLETO DE NUBE SEGURA

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:

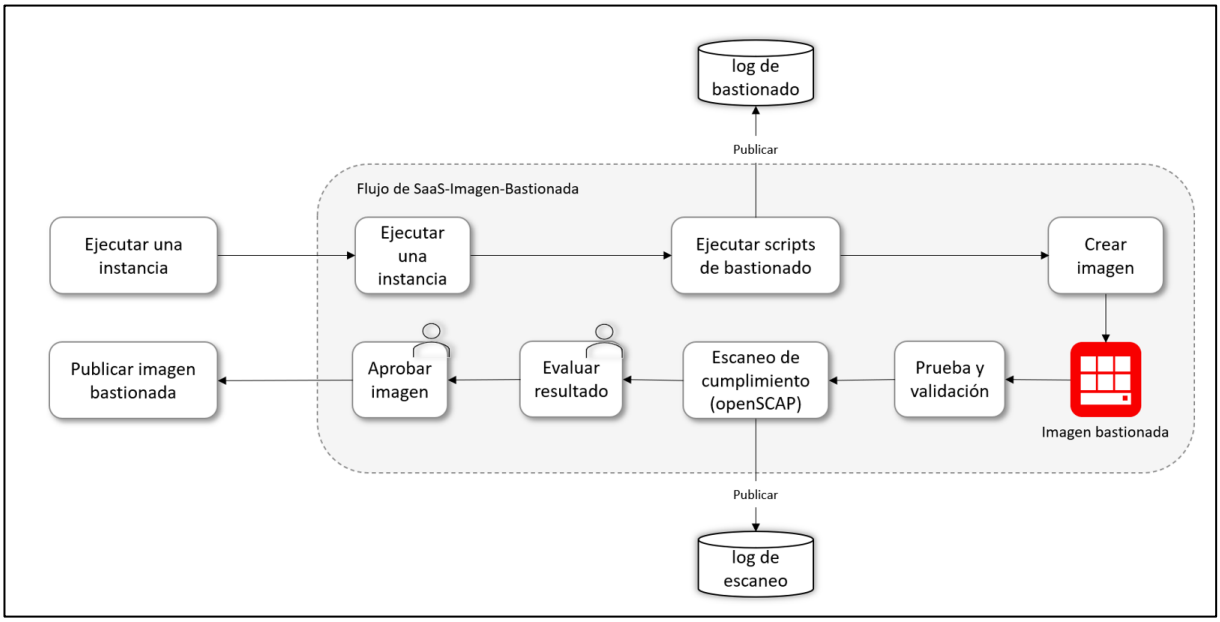


Diagrama para la elaboración de la imagen bastionada.

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.

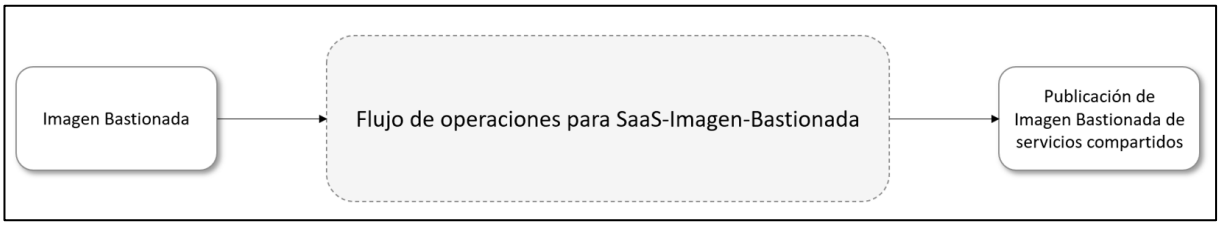


Diagrama de una imagen bastionada de servicios compartidos.

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.

6. GLOSARIO

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

Término	Definición
AIDE	Advanced Intrusion Detection Environment.
API	Application Programming Interfaces.
ATE	Application Test Environment.
B2B	Business-to-Business.
B2C	Business-to-Consumer.
CAD	Computer Aided Design.
CapEx	Capital Expenditures.
CCN	Centro Criptológico Nacional.
CDaaS	Content Delivery as a Service.
CIS	Center for Internet Security.
CQP	Configure, Price, Quote.
CRM	Customer Relationship Management.
CX	Customer Experience.
DDoS	Distributed Denial of Service.
DISA	Defense Information Systems Agency.
DoS	Denial of Service.

Término	Definición
ELSA	Enterprise Linux Security Advisory.
ENS	Esquema Nacional de Seguridad.
EPM	Enterprise Perfomance Management.
ERM	Enterprise Risk Management.
ERP	Enterprise Resource Planning.
GDS	Global Desktop Strategy.
GIS	Geographical Information System.
HCM	Human Capital Management.
IA	Inteligencia Artificial.
IaaS	Infrastructure as a Service.
IAM	Identity and Access Management.
IBPX	Integrated Business Planning and Execution.
IDCS	Identity Cloud Service.
IDS	Intrusion Detection System.
IEC	International Electrotechnical Commission.
IoT	Internet of Things.
IPS	Intrusion Prevention System.
ISO	International Organization for Standardization.
JRE	Java Runtime Environment.
JSON	JavaScript Object Notation.
JWT	JSON Web Token.
KPI	Key Perfomance Indicator.
LDAP	Lightweight Directory Access Protocol.
LoB	Line of Business.
MES	Manufacturing Execution System.
NIDS	Network Intrusion Detection System.
NIST	National Institute of Standards and Technology.
OAuth	Open Authorization.
OCI	Oracle Cloud Infrastructure.
OCID	Oracle Cloud Identifier.
OFA	Oracle Fusion Applications.
OKE	Oracle Container Engine for Kubernetes.
OKEOM	OKE Oracle-Managed.
OOTB	Out-Of-The-Box.
OpEx	Operating Expenses.
OPSS	Oracle Platform Security Services.
Oracle ME	Oracle My Experience.
OS	Operating System.
OTP	One-Time Password.
OWASP	Open Web Application Security Project.
PaaS	Platform as a Service.
PAM	Pluggable Authentication Module.

Término	Definición
PAR	Pre-Authenticated Request.
PCI-DSS	Payment Card Industry Data Security Standard.
PGP	Pretty Good Privacy.
PLM	Product Lifecycle Management.
RBAC	Role based Access control.
RCE	Remote code execution.
RPM	Red Hat Package Manager.
S&OP	Sales and Operations.
SaaS	Software as a Service.
SCIM	System for Cross-domain Identity Management.
SCM	Supply Chain Management.
SFA	Sales Force Automation.
SFC	System File Checker.
SIEM	Security Information and Event Management.
SOC	Security Operations Center.
SQL	Structured Query Language.
SSO	Single Sign-On.
STIG	Security Technical Implementation Guide.
TLS	Transport Layer Security.
VCN	Virtual Cloud Network.
VMI	Windows Management Instrumentation.
VPN	Virtual Private Network.
WAF	Web Application Firewall.
WSUS	Windows Server Update Service.
XSS	Cross Site Scripting.

7. 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 han configurado cuentas únicas e inequívocas para cada usuario y servicio, recibiendo identificadores singulares para cada perfil o rol que vaya a desempeñar.	☐Si ☐No	☐Si ☐No
		Observaciones:	
op.acc.2	Requisitos de acceso	Aplica	Cumple
	Se han gestionado los requisitos de acceso de los usuarios desde la Consola de Seguridad.	☐Si ☐No	☐Si ☐No
		Observaciones:	
	Se ha configurado el acceso basado en la ubicación de los dispositivos de los usuarios.	☐Si ☐No	☐Si ☐No
		Observaciones:	
	Se ha gestionado el acceso a las bases de datos desde Oracle Database Vault para Fusion Cloud Service.	☐Si ☐No	☐Si ☐No
		Observaciones:	

Control ENS	Medidas y Configuración	Estado	
op.acc.3	Segregación de funciones y tareas	Aplica	Cumple
	Se han asignado los roles necesarios para el acceso a los servicios de Oracle Cloud Fusion desde la Consola de Seguridad.	☐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 servicios de Oracle Fusion Cloud mediante la gestión de roles en la Consola de Seguridad, manteniendo los siguientes principios: • Mínimo privilegio. • Necesidad de conocer. • Capacidad para autorizar.	☐Si ☐No	☐Si ☐No
		Observaciones:	
op.acc.5	Mecanismos de autenticación	Aplica	Cumple
	Para un escenario de acceso local a los servicios de Oracle Cloud Fusion, se ha creado una política de contraseña compleja con una longitud de al menos 12 caracteres.	☐Si ☐No	☐Si ☐No
		Observaciones:	
	Para un escenario SSO a los servicios de Oracle Cloud Fusion, se ha configurado el inicio de sesión único con un proveedor de servicios SSO.	☐Si ☐No	☐Si ☐No
		Observaciones:	
	Se ha configurado la autenticación de la API de salida mediante el protocolo de autorización OAuth de tres patas.	☐Si ☐No	☐Si ☐No
		Observaciones:	

Control ENS	Medidas y Configuración	Estado	
	Se ha utilizado un proveedor de autenticación de la API de Oracle para configurar la autenticación de entrada para usuarios de aplicaciones de terceros.	☐Si ☐No	☐Si ☐No
		Observaciones:	
op.exp	Explotación		
op.exp.4	Mantenimiento y actualizaciones de seguridad	Aplica	Cumple
	Se ha configurado una política de mantenimiento para todos los entornos de la familia de Oracle Cloud Fusion.	☐Si ☐No	☐Si ☐No
		Observaciones:	
op.exp.5	Gestión de cambios	Aplica	Cumple
	Se está gestionando los entornos de no producción para el desarrollo de informes, páginas e interfaces o integraciones con otras aplicaciones.	☐Si ☐No	☐Si ☐No
		Observaciones:	
op.exp.8	Registro de la actividad	Aplica	Cumple
	Se ha habilitado la funcionalidad de auditoría para las aplicaciones de Oracle Cloud Fusion.	☐Si ☐No	☐Si ☐No
		Observaciones:	

Control ENS	Medidas y Configuración	Estado	
	Se ha configurado los objetos comerciales y los atributos de las aplicaciones de Oracle Cloud Fusion.	☐Si ☐No	☐Si ☐No
		Observaciones:	
	Se está revisando periódicamente la auditoría de suplantación que proporciona Oracle.	☐Si ☐No	☐Si ☐No
		Observaciones:	
op.exp.10	Protección de claves criptográficas	Aplica	Cumple
	Se ha suscrito al servicio de Oracle Break Glass para la gestión de las claves de cifrado.	☐Si ☐No	☐Si ☐No
		Observaciones:	
	Se han creado almacenes independientes para entornos de producción y entornos de no producción. Para los entornos de no producción, se han creado claves independientes para los entornos de prueba y desarrollo.	☐Si ☐No	☐Si ☐No
		Observaciones:	
	Se está gestionando periódicamente la rotación de las claves de los almacenes creados para los distintos entornos de Oracle Cloud Fusion.	☐Si ☐No	☐Si ☐No
		Observaciones:	

Control ENS	Medidas y Configuración	Estado	
op.mon	Monitorización del sistema		
op.mon.2	Sistema de métricas	Aplica	Cumple
	Se está realizando un seguimiento del estado de los servicios mediante la supervisión de uso de los recursos, métricas comerciales y métricas de facturación.	☐Si ☐No	☐Si ☐No
		Observaciones:	
mp	Medidas de protección		
mp.com	Protección de las comunicaciones		
mp.com.2	Protección de la integridad y de la autenticidad	Aplica	Cumple
	Se dispone de los últimos navegadores validados por Oracle para el uso de las aplicaciones de Oracle Cloud Fusion.	☐Si ☐No	☐Si ☐No
		Observaciones:	
mp.si	Protección de los soportes de información		
mp.info	Protección de la información		
mp.info.6	Copias de seguridad	Aplica	Cumple
	En caso de pérdida de datos, se está gestionando con el proveedor Oracle la restauración de los mismos.	☐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