Guía de Seguridad de las TIC
CCN-STIC 889J

Guía de Configuración segura de Oracle SaaS Fusion y EPM Applications bajo entorno EURA

Marzo 2025

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
2025.03.07 12:39:36 +01'00'

Pº de la Castellana 109, 28046 Madrid

NIPO: 083-25-058-9
Fecha de Edición: Marzo de 2025

ÍNDICE

1. GUÍA DE CONFIGURACIÓN SEGURA DE ORACLE SAAS FUSION Y EPM APLICACIONES BAJO ENTORNO EURA

1.1. DESCRIPCIÓN DEL USO DE ESTA GUÍA

La principal utilidad de esta guía es identificar los servicios de Oracle SaaS Fusión y EPM que deben configurarse, cumpliendo con las distintas medidas de seguridad que establece el Esquema Nacional de Seguridad (ENS) y bajo el paraguas de la solución de Oracle denominada *Acceso Restringido a la Unión Europea (EURA)* por sus siglas en inglés.

Dichos servicios en la modalidad SaaS de nube pública y/o soberana de Oracle, son desplegados y configurados bajo la arquitectura de Oracle Cloud Infrastructure (OCI), para cargas de trabajo en la nube pública/soberana de Oracle, siguiendo las exigencias del ENS.

Con la solución Oracle EURA, y el auge de las soluciones de informática en la nube y de SaaS, se afianza las cuestiones de transferencia y residencia de datos se han convertido en un tema de enorme relevancia para los clientes en la nube, sobre todo después de la adopción de nuevas leyes de privacidad, como el Reglamento General de Protección de Datos de la Unión Europea (UE) (RGPD).

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 último, esta guía incluye una aproximación, no objetivo de este documento, sobre el servicio de seguridad, configuración y vigilancia que Oracle ha introducido bajo el concepto de OCI *Landing Zone*, y en línea con los requerimientos de seguridad establecidos en el Esquema Nacional de Seguridad.

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 Infraestructura (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 Fusión y EPM para la infraestructura de la nube de Oracle, la cual dispone de la Certificación de Conformidad con el Esquema Nacional de Seguridad.

Dentro de los modelos que ofrece OCI, esta guía únicamente se centra 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 y/o soberana 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 poder 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 Fusión y EPM Aplicaciones y la gestión del entorno donde se hospedan.

1.3. SERVICIOS DE ORACLE SAAS FUSION Y EPM 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 Fusión Applications 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.

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.

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.

Oracle pone a su disposición una detallada guía de cada aplicativo mencionado anteriormente, así como la configuración de estos, la está disponible aquí (CCN-CERT) y con referencia *CCN-STIC-889I Guía de Configuración segura para Oracle SaaS Fusión Applications.*

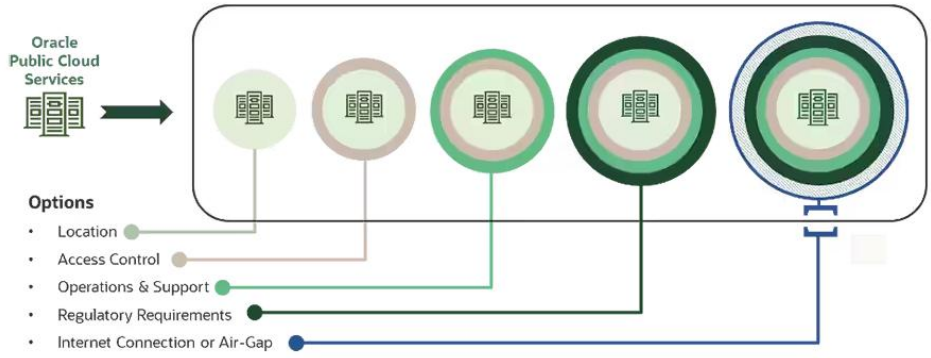
Respecto al servicio Oracle EPM, dicha solución brinda agilidad y conocimientos necesarios para obtener un rendimiento superior en cualquier condición del mercado. La gestión del rendimiento empresarial de Oracle EPM ayuda a modelar y planificar finanzas, recursos humanos, cadena de suministro y ventas,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

Oracle pone a su disposición una detallada guía de este aplicativo mencionado anteriormente, así como la configuración de este, la está disponible aquí (CCN-CERT) y con referencia *CCN-STIC-889H Guía de Configuración segura para Oracle SaaS Enterprise Performance Management EPM*.

2. ACCESO RESTRINGIO A LA UNION EUROPEA (EURA)

A medida que avanza la transformación de la nube, las empresas, el sector público y las industrias reguladas, incluidos los servicios financieros, en toda la Unión Europea (UE) están interesados en la soberanía digital sobre sus datos, para poder definir dónde residen sus datos y quién tiene acceso a ellos. Las tendencias del mercado en la UE han llevado a una creciente necesidad de una infraestructura en la nube diseñada en la UE, ubicada en la UE, operada por personal de la UE y que cumpla con los requisitos de la UE, incluidos:

- Panorama dinámico de cumplimiento normativo
- Requisitos políticos
- Mitigación de riesgos (percibidos y reales)



Servicios de protección para la soberanía de la nube

En respuesta a estas tendencias, Oracle ha lanzado el servicio en la nube de acceso restringido de la UE para aplicaciones Oracle Fusion, una solución de servicio en la nube diseñada para abordar las preocupaciones de privacidad y soberanía de los datos de los clientes de la UE de dos maneras críticas:

1. Aseguramiento que todas las instancias de servicio al cliente, datos de clientes y datos de diagnóstico residan únicamente en centros de datos de la UE.

2. Restringe el acceso del personal de Oracle a los datos de los clientes y a los datos de diagnóstico solo a personal residente en la UE.

Los prospectos con una estrategia de gobierno de datos de ubicación y/o necesidades de demostrar una mitigación proactiva de riesgos pueden aprovechar EURA para Oracle Fusion y EPM Applications para cumplir con esos requisitos.

Abajo se detalla algunos de sus principales beneficios operaciones y sus ventajas, asi como a la seguridad, en cuanto al gobierno del dato, inherente a la solucion EURA establecida por Oracle para los servicios SaaS listados anteriormente.

2.1. SOBERANIA DEL DATO

Al restringir el almacenamiento de datos a los centros de datos de la UE y al acceso del personal de Oracle, EU Restricted Access Cloud Service potencia a los clientes de la UE con un mayor control sobre sus datos. EU Restricted Access Cloud Service funciona exclusivamente en centros de datos de la UE.

Oracle EURA procesa y almacena todos los datos de clientes y conjuntos de datos derivados que puedan contener información de clientes, como archivos de rastreo y logs de servicio, de acuerdo con las restricciones de EURA relativas a la residencia y el acceso a datos.

Este modelo de gobernanza para las regiones de nube soberana de Oracle en la Unión Europea, diseñado de modo que las entidades de nube soberana funcionen de forma independiente, sin posibilidad de transferir datos de clientes fuera de la UE.

2.2. ACCESO A DATOS

Se han implementado controles para garantizar que solo el personal de la UE tenga acceso al servicio en la nube y a los datos de los clientes a efectos de la gestión del servicio. Los controles de acceso limitan solo al personal de Oracle, no se aplican a los usuarios finales de los clientes. Estos controles de acceso verifican que el personal de Oracle trabaja en la UE. Además, al iniciar sesión de forma remota desde ubicaciones que no sean de Oracle, se inician y se aplican procesos de validación geográfica para verificar en todo momento que el personal de Oracle esté físicamente presente en la UE todo el tiempo.

2.3. RECUPERACION ANTE DESASTRES

La recuperación ante desastres se proporciona normalmente desde un entorno de servicio de EURA designado que es independiente del entorno de servicio de EURA principal.

2.4. SEGREGACION DE DATOS

Los entornos de servicio de EURA se suministran en los mismos centros de datos que los entornos de servicio de aplicación de Fusion que no tienen el servicio de EURA. No hay ninguna segregación física entre los dos tipos de entornos, lo que significa que pueden compartir la misma infraestructura.

Sin embargo, los entornos de servicios EURA están separados de forma lógica, lo que aprovecha las funciones de seguridad de Oracle Gen 2 Cloud. Estos controles lógicos de segregación están diseñados para aplicar restricciones de acceso del personal con sede en la UE no solo a través de la política operativa, sino también a través de controles de acceso y controles de seguridad de la red, como los hosts bastión con derechos separados y controlados para todos los servidores que alojan el servicio EURA.

Personal residente en la UE tienen roles únicos, limitados y específicamente creados para la identificación de ellos con el fin de que sea este personal el que pueda acceder a los datos de cliente en caso de ser necesario (servicio Break Glass como se indica más adelante en detalle).

2.5. ACCESO A LOS DATOS Y TRANSFERENCIA DE ESTOS

El entorno de servicio de EURA está diseñado para restringir el acceso a su contenido y a los logs de aplicación al personal de Oracle con sede en la UE.

Todo personal de Oracle que tenga acceso a un entorno de servicio de EURA, el lugar de trabajo asignado a dicho personal se valida con una lista de países de la UE. Todo acceso autorizado es revisado frecuentemente, en caso de que un empleado desempeñara otras tareas no relacionadas con el servicio EURA, este dejaría automáticamente de poder acceder a dicha plataforma.

Además, cualquier acceso remoto a través de VPN, los controles de validación geográfica requieren que los miembros del personal de Oracle estén físicamente presentes en la UE (según lo determinado por su dirección IP aparente) al conectarse al entorno de servicio de EURA.

Esta lista de países aprobados incluye a los estados miembros de la UE.

A fecha de publicación de esta guía los servicios EURA están disponible en un limitado número de países de la Unión Europea, en los que se incluye el centro de datos localizado en Madrid (España).

2.6. ACCESO ESCORTED

En caso de que la solución de problemas requiera la ayuda de un empleado con una aptitud avanzada, no disponible en un empleado de la UE, el empleado de la UE puede compartir su pantalla a través de un canal seguro y recibir orientación del empleado no perteneciente a la UE con el fin de solucionar el problema en un espacio corto de tiempo. El empleado no perteneciente a la UE no puede recibir derechos de conexión ni proporcionar orientación que recupere datos de clientes fuera del entorno de EURA.

Un número limitado de empleados de Oracle con un rol de super-administrador para el sistema de aprovisionamiento de Fusion Cloud Service puede tener acceso a las credenciales del entorno de servicio EURA de un cliente. El sistema de aprovisionamiento almacena estas credenciales para realizar la configuración inicial del entorno del cliente (antes de que su contenido se almacene en el entorno) y cualquier operación de actualización posterior aprobada a instancias de servicio de EURA.

2.7. SOPORTE TECNICO

Las solicitudes de servicio (SR) serán gestionadas por ingenieros de soporte que operen desde ubicaciones de la UE. En la medida en que proporcione su contenido como parte de un anexo a una solicitud de servicio enviada a *My Oracle Support* (MOS), dicho contenido se alojará en nuestros sistemas de soporte global, pero los ingenieros de soporte que operen desde ubicaciones dentro de la UE únicamente podrán acceder a dicho contenido

2.8. SOLUCIONES AVANZADAS DE EURA

Además de los controles corporativos y específicos del servicio de Oracle disponibles en las soluciones de Oracle, Oracle EURA pone a su disposición funciones la siguiente seguridad adicional.

2.8.1 Oracle Break Glass for Fusion

Break Glass for Fusion permite a los clientes restringir y controlar el acceso de Oracle a los datos de cliente almacenados en la base de datos de Oracle Fusion Cloud Service. Mediante el uso de Oracle Break Glass for Fusion Cloud Service, los clientes pueden controlar el acceso a cada nivel de datos de la base de datos de Oracle Fusion Cloud Service. Con Break Glass, los profesionales de Oracle no podrán acceder al entorno de nube del cliente para solucionar problemas a menos que cuenten con la aprobación del cliente.

Además, los datos estáticos están protegidos con el uso de Oracle Transparent Data Encryption (TDE) Security Cloud Service y Oracle Database Vault. Oracle requiere la clave maestra de cifrado de datos transparente (TDE) para que un cliente pueda operar una base de datos con Oracle Fusion Cloud Service, pero conserva solo una copia de la última clave proporcionada por el cliente.

- Los datos de cliente alojados en la base de datos se cifran de forma estática mediante TDE, y el acceso se registra y se audita mediante Database Vault.
- Break Glass tiene límite de tiempo; protege los datos de clientes y es precisa la aprobación del cliente para que los profesionales de Oracle puedan acceder al entorno.
- Break Glass solo proporciona acceso temporal. Las credenciales de acceso se restablecen mediante programáticamente después del transcurso de un tiempo preconfigurado (96 horas).
- El acceso a Break Glass se audita y registra, y los informes están disponibles.

Los clientes pueden cargar, eliminar o restaurar su clave de cifrado maestro de TDE desde la consola de aplicaciones.

Información adicional sobre esta solución puede ser encontrada en este enlace: https://docs.oracle.com/search/?q=breaking+glass

2.8.2 Oracle Data Masking Cloud Service

Las empresas corren el riesgo de exponer datos confidenciales al copiar datos de producción en entornos que no sean de producción para desarrollar nuevas aplicaciones, ejecutar pruebas o realizar análisis de datos. Sin embargo, para realizar pruebas reales, los usuarios que no sean de producción deben acceder a conjuntos de datos representativos.

Oracle Data Masking reduce este riesgo sustituyendo los datos confidenciales originales por datos ficticios para que se puedan compartir de forma segura con usuarios que no sean de producción.

Con Oracle Data Masking, los clientes pueden:

- **Limitar la proliferación de datos confidenciales**: las crecientes amenazas a la seguridad han aumentado la necesidad de las empresas de limitar la exposición de información confidencial. Al mismo tiempo, copiar datos de producción con fines no relacionados con la producción, como pruebas y desarrollo, está provocando la proliferación de datos confidenciales, la ampliación del límite de seguridad y cumplimiento normativo y el incremento de la probabilidad de que se produzcan filtraciones de datos.
- **Compartir solo lo necesario**: a menudo, las empresas tienen que compartir un conjunto de datos de producción con actores internos y externos por diversos motivos. En algunos casos, resulta

eficaz extraer y compartir una parte o un subconjunto de información en lugar de compartir todo el conjunto de datos de producción.

- **Aplicar la minimización de datos:** los reglamentos en relación con la privacidad de datos, como el RGPD, promulga principios de minimización de datos. La limitación de información confidencial en entornos que no sean de producción puede ayudar a abordar estos principios, ya que a estos entornos a menudo acceden más usuarios y con más privilegios que en los sistemas de producción habituales.

Información adicional sobre esta solución puede ser encontrada en este enlace: https://docs.oracle.com/en-us/iaas/Content/fusion-applications/manage-security-data-masking.htm

2.8.3 Acceso restringido a la base de datos y funciones "trae tu propia clave" (BYOK) para Enterprise Performance Management

La función "trae tu propia clave" (en ingles Bring Your Own Key, BYOK) mejora la seguridad de Oracle Fusion Cloud y EPM al permitir a los clientes proporcionar su propia clave, que se utiliza para cifrar la clave de acceso a la base de datos. Esta función está disponible para todos los clientes de Oracle Fusion Cloud y EPM, no solo para los aprovisionados en entornos de Oracle EURA.

Todos los datos de la base de datos relacional se cifran cuando están estáticos, y la clave proporcionada por el cliente se utiliza para cifrar las credenciales de acceso a la base de datos. El cliente se encarga de la gestión de esta clave.

Esta función se puede utilizar junto con la de acceso restringido a la base de datos, que proporciona acceso restringido a los datos del cliente por parte de los DBA del cliente y los empleados de desarrollo de Oracle. Con la función de acceso restringido a la base de datos activada, el cliente controla y autoriza los accesos. Todos los accesos a la base de datos del cliente se auditan y pueden ser visualizados por el cliente.

Oracle permite a los clientes de EPM restringir y controlar el acceso de Oracle a los datos de clientes almacenados en la base de datos relacional del servicio en la nube de EPM. Cuando se active, los profesionales de Oracle no podrán acceder al entorno de nube del cliente para solucionar ningún problema a menos que cuenten con la aprobación del cliente.

- Además, los datos estáticos están protegidos con el cifrado de datos transparente de Oracle.
- El acceso a la base de datos relacional tiene límite de tiempo; protege los datos de clientes y es precisa la aprobación del cliente para que los profesionales de Oracle puedan acceder al entorno.
- Una vez permitido por el cliente, el acceso a la base de datos relacional se audita y registra, y los informes de acceso se ponen a disposición de los administradores de servicio del cliente.

Información adicional sobre esta solución puede ser encontrada en este enlace: https://docs.oracle.com/en-us/iaas/Content/KeyManagement/Concepts/keyoverview.htm

3. DESPLIEGUE SEGURO PARA ORACLE SAAS FUSION Y EPM

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-889I Guía de Configuración segura para Oracle SaaS Fusión Applications”, y “CCN-STIC-889H Guía de Configuración segura para Oracle SaaS Enterprise Performance Management EPM”.

En ambas guias, en su segunda sección, se cubre en detalle un despligue seguro para Oracle SaaS para los servicios Fusión y EPM respectivamente.

4. CONFIGURACIÓN SEGURA PARA ORACLE SAAS FUSIÓN Y EPM 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.

Esta sección y cada sub-sección indicada en esta cuarta sección esta desarrolla en más detalle en las guías de configuración segura publicadas para Oracle SaaS Fusión Aplicaciones y Oracle SaaS EPM respectivamente.

Las guías están disponibles en la página oficilal del CCN en el siguiente enlace:

https://www.ccn-cert.cni.es/es/guias.html

- *CCN-STIC-889I Guía de Configuración segura para Oracle SaaS Fusión Aplicaciones,*
- *CCN-STIC-889H Guía de Configuración segura para Oracle SaaS Enterprise Performance Management EPM*.

4.1. 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.

4.1.1. 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).

4.1.1.1. 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.

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.

4.1.1.2. 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.

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

4.1.1.3. 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.

4.1.1.4. 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. Los privilegios se limitarán de forma que los usuarios sólo accederán al conocimiento de aquella información requerida para cumplir sus obligaciones.

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.

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.

4.1.1.5. 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".

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.

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.

4.1.2. 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.

4.1.2.1. 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.

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.

4.1.2.2. 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.

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.

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.

4.1.2.3. 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.

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.

Por otro lado, la aplicación técnica de la presente medida de seguridad se encuentra en la gestión de la familia de entornos.

4.1.2.4. 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 “programa maligno” (*malware* en inglés).

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.

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

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

4.1.2.5. 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.

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

4.1.2.6. 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 información se realiza el evento, tipo de evento y resultado del evento (fallo o éxito).

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 estos 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.

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.

4.1.2.7. 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.

La suite de aplicaciones 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.

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.

4.1.3. 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.

4.1.3.1. 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.

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.

4.1.4. 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.

4.1.4.1. 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 utilizan 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.

4.1.4.2. 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.

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.

4.2. 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 estas 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.

4.2.1. 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.

4.2.1.1. 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. Sin embargo, por motivos de seguridad, las sesiones pueden caducar debido a varias razones y tiempos de espera.

4.2.2. 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.

4.2.2.1. 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 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.

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

4.2.3. 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.

4.2.3.1. CALIFICACIÓN DE LA INFORMACIÓN

Para calificar la información se estará a lo establecido legalmente sobre la naturaleza de esta. 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.

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.

4.2.3.2. 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.

4.2.4. 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.

4.2.4.1. 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).

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.

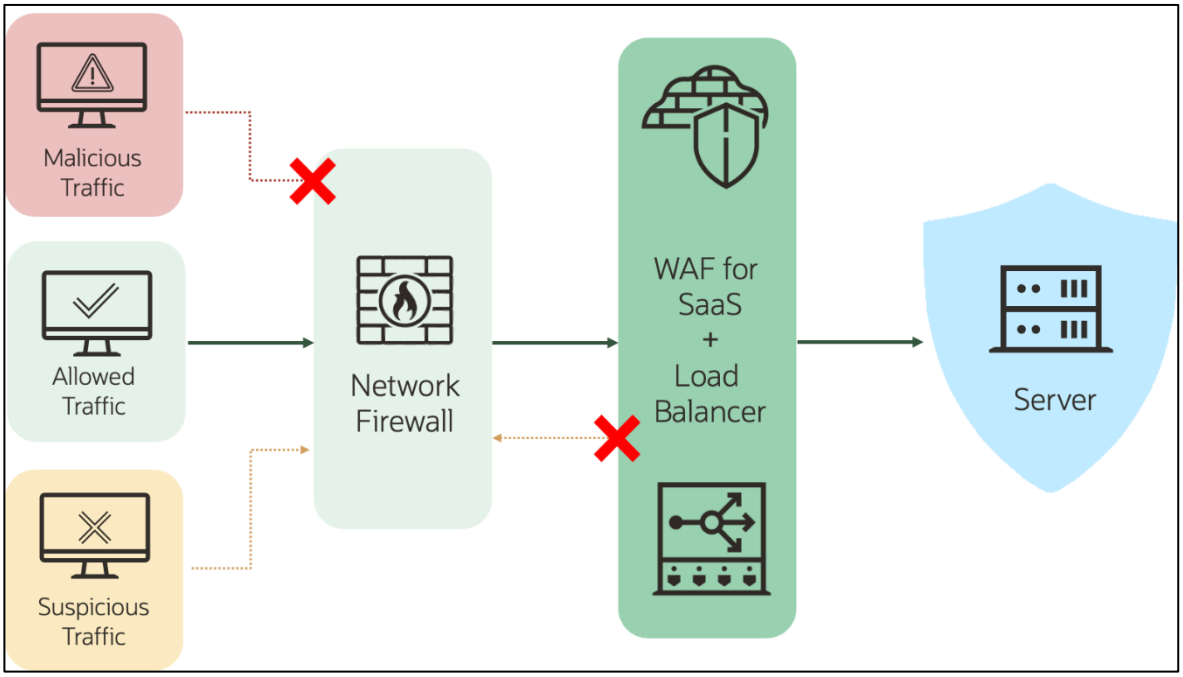


Diagrama de WAF Para Fusion.

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.

5. 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, se enfoca en ayudar a reducir el riesgo al proporcionar un conjunto integral de capacidades de seguridad.

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, brindando 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.

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

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

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.

6. ESCENARIO COMPLETO DE NUBE SEGURA

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.

Informacion en detalle, en su sección quinta, sobre el escenario completo de nube segura es desarrollada en la guía de seguridad “CCN-STIC-889I Guía de Configuración segura para Oracle SaaS Fusión Applications”, y “CCN-STIC-889H Guía de Configuración segura para Oracle SaaS Enterprise Performance Management EPM”.

7. ORACLE LANDING ZONE

En esta sección se realiza una aproximación a la solución de configuración segura integrada con los servicios en el tenant de Oracle Cloud y dentro del servicio de OCI llamado Oracle Enterprise Landing Zone (OELZ versión 2).

La seguridad y conformidad regulatoria en la nube debe ser considera de forma holística y no como algo único que afecta a las soluciones de Oracle SaaS descriptas en este documento. Pero como un conjunto orquestado de servicios entorno a una seguridad integral en cada capa, con un marcado acento de cumplimiento regulatorio, y todo configurado desde su origen a través de la solución OELZ.

Una Landing Zone (LD) es un conjunto de servicios y componentes que se despliegan en el tenant de Oracle Cloud Infrastructure (OCI) para establecer una base segura y ampliable para ejecutar cargas de trabajo empresariales. Algunos casos de sus beneficios incluyen:

a) **Arquitecturas multinube**.

b) **Gobernanza y cumplimiento**: OELZ v2 proporciona un conjunto de políticas y guías incorporadas para ayudar a garantizar que su entorno de OCI cumpla con los estándares del sector, como ISO27001 y PCI DSS.

c) Automatización y escalabilidad

7.1 Seguridad, Cumplimiento y Center for Internet Security (CIS)

OELZ incluye políticas y guías incorporadas que ayudan a la implementación de un entorno en OCI, donde se tenga una base sólida para lograr los objetivos de conformidad de seguridad. Los controles de seguridad implementados en OELZ incluyen recomendaciones que pueden ayudarle a alcanzar el nivel 1 de conformidad de CIS 1.2.

El Center for Internet Security (CIS) es una organización que establece prácticas globales de referencia para proteger los sistemas y datos de TI. El objetivo de CIS es prevenir y mitigar las nuevas amenazas cibernéticas que se identifican en la industria.

Para obtener una lista de los controles de seguridad que se incluyen en OELZ y como estos controles se podrían conectar con los establecidos en el Esquema Nacional de Seguridad (ENS), se puede consultar Controles de seguridad de nivel 1 de CIS 1.2.

7.2 Módulos Avanzados de Configuración en LLDD

Oracle pone a disposición a través de la plataforma GitHub diferentes tipos de módulos (o plantillas) avanzos de seguridad dentro de CIS LLDD (Landing Zones) para desplegar en la plataforma Oracle Cloud Infrastructure. Las CIS LLDD se ensamblan a partir de módulos y plantillas que el cliente puede utilizar en su configuración por defecto o bifurcar el repositorio y personalizar para sus propios escenarios.

Desde la perspectiva de la arquitectura, en el front-end, la plantilla proporciona una interfaz gráfica fácil de usar a través de OCI Resource Manager, lo que la hace muy atractiva para los equipos que comienzan con el paradigma de infraestructura como código (IaC).

A continuación, indicamos los módulos disponibles y donde se ubican en GitHub. Cada repositorio tiene un archivo README.md que menciona los demás repositorios de la colección y que es conveniente leer antes de ejecutar cualquier actividad.

Gestión de identidad y acceso	
Módulos	Compartimentos (Compartments)
	Políticas (Policies)
	Grupos (Groups)
	Grupos dinámicos (Dynamic Groups)
GitHub: https://github.com/oracle-quickstart/terraform-oci-cis-landing-zone-iam	

Redes	
Módulos	Redes centrales (Core networking)
	Cortafuegos de red (Firewall)
	ALB (Application Load Balancer)
GitHub: https://github.com/oracle-quickstart/terraform-oci-cis-landing-zone-networking	

Gobernanza	
Modulo	Redes Etiquetas (Tags)
GitHub: https://github.com/oracle-quickstart/terraform-oci-cis-landing-zone-governance	

Gestión de identidad y acceso	
Módulos	Guardia de la nube (Cloud Guard)
	Zonas de seguridad (Security Zones)
	KMS (Vaults)
	Escaneo de vulnerabilidades (Vulnerability Scanning)
GitHub: https://github.com/oracle-quickstart/terraform-oci-cis-landing-zone-security	

Observabilidad y monitoreo	
Módulos	Eventos (Events)
	Alarmas (Alarms)
	Notificaciones (Notifications)
	Corrientes (Streams)
	Conectores de servicio (Service Connectors)
https://github.com/oracle-quickstart/terraform-oci-cis-landing-zone-observability	

Información adicional y en más detalle se puede consultar en los siguientes enlaces:

- https://docs.oracle.com/en-us/iaas/Content/cloud-adoption-framework/technology-implementation.htm
- https://www.cisecurity.org/benchmark/oracle_cloud
- https://docs.oracle.com/en-us/iaas/Content/cloud-adoption-framework/landing-zone-v2.htm
- https://github.com/oracle-quickstart/oci-landing-zones
- https://blogs.oracle.com/cloud-infrastructure/post/oracle-enterprise-landing-zone-v2
- https://www.ateam-oracle.com/post/cis-landing-zone-enhanced-modules

8. GLOSARIO

A continuación se 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.
CCN-CERT	Centro Criptológico Nacional y Centro Nacional de Inteligencia
CDaaS	Content Delivery as a Service.
CIS	Center for Internet Security.
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.
ELSA	Enterprise Linux Security Advisory.
ENS	Esquema Nacional de Seguridad.
EPM	Enterprise Perfomance Management.
ERM	Enterprise Risk Management.
ERP	Enterprise Resource Planning.
EURA	Acceso Restringido a la Unión Europea. European Union Restricted Access
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.

Término	Definición
JWT	JSON Web Token.
KPI	Key Perfomance Indicator.
LDAP	Lightweight Directory Access Protocol.
LLDD	Landing Zones
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.
OELZ	Oracle Enterprise Landing zone
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.
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.

Término	Definición
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.

9. 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
Dimensión(es): • Trazabilidad – T • Autenticidad – A	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
Dimensión(es): • Confidencialidad – C • Integridad – I • Trazabilidad – T • Autenticidad – A	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 Oracle Cloud Fusion y EPM Applications.	☐Si ☐No	☐Si ☐No

Control ENS	Medidas y Configuración	Estado	
		Observaciones:	
op.acc.3	Segregación de funciones y tareas	Aplica	Cumple
Dimensión(es): • Confidencialidad – C • Integridad – I • Trazabilidad – T • Autenticidad – A	Se han asignado los roles necesarios para el acceso a los servicios de Oracle Cloud Fusion y EPM Applications desde la Consola de Seguridad.	☐Si ☐No	☐Si ☐No
		Observaciones:	
op.acc.4	Proceso de gestión de derechos de acceso	Aplica	Cumple
Dimensión(es): • Confidencialidad – C • Integridad – I • Trazabilidad – T • Autenticidad – A	Se han gestionado los derechos de acceso de los usuarios a los servicios de Oracle Cloud Fusion y EPM Applications 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 (usuarios externos)	Aplica	Cumple
Dimensión(es): • Confidencialidad – C • Integridad – I • Trazabilidad – T • Autenticidad – A	Para un escenario de acceso local a los servicios de Oracle Cloud Fusion y EPM Applications, 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

Control ENS	Medidas y Configuración	Estado	
		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:	
	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.acc.6	Mecanismos de autenticación (usuarios de la organización)	Aplica	Cumple
Dimensión(es): • Confidencialidad – C • Integridad – I • Trazabilidad – T • Autenticidad – A	Se cambian las credenciales con la periodicidad marcada por la política de la organización y de aquellos recursos que acceden a los servicios de Oracle Cloud Fusion y EPM Applications.	☐Si ☐No	☐Si ☐No
		Observaciones:	
	Se retiran y deshabilitan las credenciales cuando la entidad (persona, equipo o proceso) que se autentica termina su relación con el sistema de Oracle Cloud Fusion y EPM Applications.	☐Si ☐No	☐Si ☐No
		Observaciones:	

Control ENS	Medidas y Configuración	Estado	
	Se limita el número de intentos permitidos, bloqueando la oportunidad de acceso una vez superado tal número, requiriendo la intervención de los administradores de seguridad para reactivar la cuenta.	☐Si ☐No	☐Si ☐No
		Observaciones:	
	Se han implementado los requisitos de seguridad que resultan de la aplicación de la ITS de Interconexión de sistemas de información, cuando ésta se promulgue, o en su defecto la guía CCN-STIC 811 sobre Interconexión en el ENS	☐Si ☐No	☐Si ☐No
		Observaciones:	
op.nub.	Servicios en la nube		
op.nub.1	Protección de servicios en la nube	Aplica	Cumple
	Se han certificado los servicios Oracle Cloud Fusion y EPM Applications 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.	☐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 y EPM Applications.	☐Si ☐No	☐Si ☐No

Control ENS	Medidas y Configuración	Estado	
		Observaciones:	
op.exp.5	Gestión de cambios	Aplica	Cumple
	Se están 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
Dimensión(es): • Trazabilidad – T	Se ha habilitado la funcionalidad de auditoría para las aplicaciones de Oracle Cloud Fusion y EPM Applications.	☐Si ☐No	☐Si ☐No
		Observaciones:	
	Se ha configurado los objetos comerciales y los atributos de las aplicaciones de Oracle Cloud Fusion y EPM Applications.	☐Si ☐No	☐Si ☐No
		Observaciones:	
	Se está revisando periódicamente la auditoría de suplantación que proporciona Oracle.	☐Si ☐No	☐Si ☐No

Control ENS	Medidas y Configuración	Estado	
		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 y EPM Applications.	☐Si ☐No	☐Si ☐No
		Observaciones:	
op.mon	Monitorización del sistema		
op.mon.2	Sistema de métricas	Aplica	Cumple

Control ENS	Medidas y Configuración	Estado	
	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
Dimensión(es): • Confidencialidad – C	Se dispone de los últimos navegadores validados por Oracle para el uso de las aplicaciones de Oracle Cloud Fusion y EPM Applications.	☐Si ☐No	☐Si ☐No
		Observaciones:	
mp.info	Protección de la información		
mp.info.6	Copias de seguridad	Aplica	Cumple
Dimension(es): • Disponibilidad – D	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