centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 889A

Guía de Configuración segura para IAM y servicios de seguridad

MARZO 2022

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
2022.03.29 17:48:17 +02'00'

Pº de la Castellana 109, 28046 Madrid

NIPO: 083-22-114-4

Fecha de Edición: marzo de 2022
Sidertia Solutions S.L. ha participado en la realización y modificación del presente documento y sus anexos.

PRÓLOGO

En un mundo cada vez más complejo y globalizado, en el que las tecnologías de la información y la comunicación (TIC) desempeñan un papel de suma importancia, hemos de ser conscientes de que la gestión adecuada de la ciberseguridad constituye un reto colectivo al que necesariamente hemos de enfrentar. Resulta necesario garantizar la protección de la capacidad económica, tecnológica y política de nuestro país, máxime cuando la proliferación de ataques dirigidos y el robo de información sensible representan una realidad incontestable.

Por ello, resulta imprescindible estar al día de las amenazas y vulnerabilidades asociadas al uso de las nuevas tecnologías. El conocimiento de los riesgos que se ciernen sobre el ciberespacio ha de servir para implementar con garantías las medidas, tanto procedimentales como técnicas y organizativas, que permitan un entorno seguro y confiable.

La Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia (CNI), encomienda al Centro Nacional de Inteligencia el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información y de protección de la información clasificada, a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional (CCN)

Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través del Centro Criptológico Nacional, regulado por el Real Decreto 421/2004, de 12 de marzo, diversas actividades directamente relacionadas con la seguridad de las TIC, orientadas a la formación de personal experto, al empleo de tecnologías de seguridad adecuadas y a la aplicación de políticas y procedimientos de seguridad.

Precisamente, esta serie de documentos CCN-STIC es un claro reflejo de la labor que este organismo lleva a cabo en materia de implementación de seguridad, permitiendo la aplicación de políticas y procedimientos, pues las guías han sido elaboradas con un claro objetivo: mejorar el grado de ciberseguridad de las organizaciones, conscientes de la importancia que tiene el establecimiento de un marco de referencia en esta materia que sirva de apoyo para que el personal de la Administración lleve a cabo la difícil tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

Con esta serie de documentos, el Centro Criptológico Nacional, en cumplimiento de sus cometidos y de lo reflejado en el Real Decreto 3/2010 por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración electrónica, contribuye a mejorar la ciberseguridad española y mantener las infraestructuras y los sistemas de información de todas las administraciones públicas con unos niveles óptimos de seguridad. Todo ello, con el fin de generar confianza y garantías en el uso de estas tecnologías, protegiendo la confidencialidad de los datos y garantizando su autenticidad, integridad y disponibilidad.

Marzo de 2022

Paz Esteban López
Secretaria de Estado
Directora del Centro Criptológico Nacional

ÍNDICE

1. GUÍA DE CONFIGURACIÓN SEGURA DE OCI IAM Y SERVICIOS DE SEGURIDAD

1.1 DESCRIPCIÓN DEL USO DE ESTA GUÍA

Esta guía muestra el despliegue y configuración de los servicios de Oracle Cloud Infrastructure (OCI) para cargas de trabajo en la nube pública de Oracle siguiendo las exigencias del Esquema Nacional de Seguridad (ENS).

La principal utilidad de esta guía es identificar los servicios de Identidad y Seguridad que deben configurarse, cumpliendo con las distintas medidas de seguridad que establece el Esquema Nacional de Seguridad. 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.

La nomenclatura de algunos servicios o tecnologías descritos se documenta en el glosario de abreviaturas, incluido como anexo al documento.

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

1.2 DEFINICIÓN DEL SERVICIO

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

El marco de adopción de OCI ayuda a las organizaciones a facilitar su transición a la nube y proporciona a los clientes una metodología para utilizar eficiencias incorporadas de Oracle Cloud, como los servicios de Identidad y Seguridad 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 Infraestructura como Servicio (IaaS) y en el modelo de Plataforma como Servicio (PaaS).

a) **IaaS**: Es un tipo de modelo de servicio de Cloud Computing en el que los recursos de computación se alojan en la nube. Las empresas pueden usar el modelo IaaS para trasladar parte o la totalidad de su uso de la infraestructura de centro de datos in situ o localizada a la nube, donde será propiedad de un proveedor de nube y estará administrada por este. Entre estos elementos de infraestructura se pueden incluir hardware de computación, red y almacenamiento, así como otros componentes y software.

b) **PaaS**: Es un conjunto de servicios que permite crear y gestionar aplicaciones modernas en la era digital, on-premises o en la nube. Proporciona la infraestructura y los componentes que permiten a los desarrolladores, administradores de TI y usuarios crear, integrar, migrar, implementar, proteger y administrar sistemas y aplicaciones. Para ayudar a mejorar la productividad, PaaS ofrece componentes de programación listos para usar que permiten a los desarrolladores integrar nuevas características en sus aplicaciones, incluidas tecnologías innovadoras como inteligencia artificial (IA), chatbots, blockchain y el Internet of Things (IoT). Esto también incluye suites de herramientas de desarrollo de aplicaciones, lo que incluye servicios nativos en la nube, Kubernetes, Docker, motores de contenedor y mucho más.

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 tareas de Identidad y Seguridad de las que trata este documento, disponiendo para ello de varios servicios que se detallan a continuación.

1.3 SERVICIOS DE IDENTIDAD Y SEGURIDAD

1.3.1 REGIONES Y DOMINIOS DE DISPONIBILIDAD

Regiones

Una región de OCI es el componente de nivel superior de la infraestructura. Cada región es un área geográfica independiente con varias ubicaciones, denominadas dominios de disponibilidad (AD), con aislamiento para fallos. Un dominio de disponibilidad es un subcomponente de una región que es independiente y muy fiable. Cada dominio de disponibilidad se crea con una infraestructura totalmente independiente: edificios, generadores de corriente, equipos de refrigeración y conectividad de red. Con la separación física, se proporciona protección contra desastres naturales y de otro tipo.

Dominios de disponibilidad

Los dominios de disponibilidad de la misma región están conectados por una red segura, de alta velocidad y baja latencia, que permite crear y ejecutar aplicaciones y cargas de trabajo muy fiables con un impacto mínimo en la latencia y el rendimiento de las aplicaciones. Todos los enlaces entre dominios de disponibilidad están cifrados.

Dominios de errores

Un dominio de errores es una agrupación de hardware e infraestructura dentro de un dominio de disponibilidad. Cada dominio de disponibilidad contiene tres dominios de errores. Los dominios de errores proporcionan antiafinidad: permiten distribuir las instancias de forma que no estén en el mismo hardware físico dentro de un único dominio de disponibilidad. Un evento de mantenimiento de hardware informático o error de hardware que afecta a un dominio de errores no afecta a las instancias de otros dominios de errores. Además, el hardware físico en un dominio de errores tiene fuentes de alimentación independientes y redundantes, lo que evita que un error en el hardware de la fuente de alimentación dentro de un dominio de errores afecte a otros dominios de errores.

Para controlar la ubicación de las instancias informáticas, las instancias del sistema de base de datos con hardware dedicado o las instancias del sistema de base de datos de máquina virtual, puede especificar de forma opcional el dominio de errores para una nueva instancia o pool de instancias en el momento del lanzamiento. Si no especifica el dominio de errores, el sistema selecciona uno para usted. OCI realiza la mejor colocación posible de antiafinidad en diferentes dominios de errores y optimiza la capacidad disponible en el dominio de disponibilidad. Para cambiar el dominio de errores de una instancia informática, edite el dominio de errores. Para cambiar el dominio de errores de una instancia de sistema de base de datos de máquina virtual o con hardware dedicado, finalícelo e inicie una nueva instancia en el dominio de errores preferido.

Los dominios de errores realizan las siguientes acciones:

a) Proteger contra fallos de hardware inesperados o fallos de fuente de alimentación.

b) Proteger contra interrupciones planificadas debido al mantenimiento del hardware informático.

Con este diseño de infraestructura, Oracle cumple con la norma que establece los medios alternativos dentro del conjunto de medidas para los servicios externos, así como para la continuidad del servicio, obteniendo el Certificado de Conformidad con el Esquema Nacional de Seguridad, en su Categoría Alta, conforme a las exigencias del Real Decreto 3/2010, de 8 de enero, por el que se regula el ENS en el ámbito de la Administración electrónica, según se indica en el correspondiente Informe de Auditoría del ENS de fecha 13 de diciembre de 2021 para:

- Los sistemas de información que soportan los servicios de Oracle Cloud Infrastructure (OCI) enumerados en la página del Anexo del Certificado y ubicados en CPDs externalizados en las siguientes regiones de Europa: Alemania, Italia, Francia y Holanda.

1.3.2 GESTIÓN DE IDENTIDAD Y ACCESO (IDENTITY AND ACCESS MANAGEMENT)

El servicio Oracle Cloud Infrastructure Identity and Access Management (OCI IAM) proporciona autenticación y autorización para todos los recursos y servicios de OCI. Puede utilizar un único tenant compartido por varias unidades de negocio, equipos y personas a la vez que se mantiene la seguridad, el aislamiento y la gobernanza.

Al unirse a OCI, se crea un tenant. Un tenant es una construcción virtual que contiene todos los recursos de OCI que pertenecen al cliente. El administrador del tenant puede crear usuarios y grupos, así como asignarles acceso con menos privilegios a recursos particionados en compartimentos. Un compartimento es un grupo de recursos que se puede gestionar como una sola unidad lógica y ofrece una forma optimizada de gestionar una infraestructura grande.

OCI soporta la federación con Oracle Identity Cloud Service, Microsoft Active Directory y Microsoft Azure Active Directory, así como con otros proveedores de identidad que soportan el lenguaje de marcas de afirmación de seguridad (SAML) 2.0. Los grupos federados se asignan a grupos nativos de IAM, que determinan los permisos de un usuario federado.

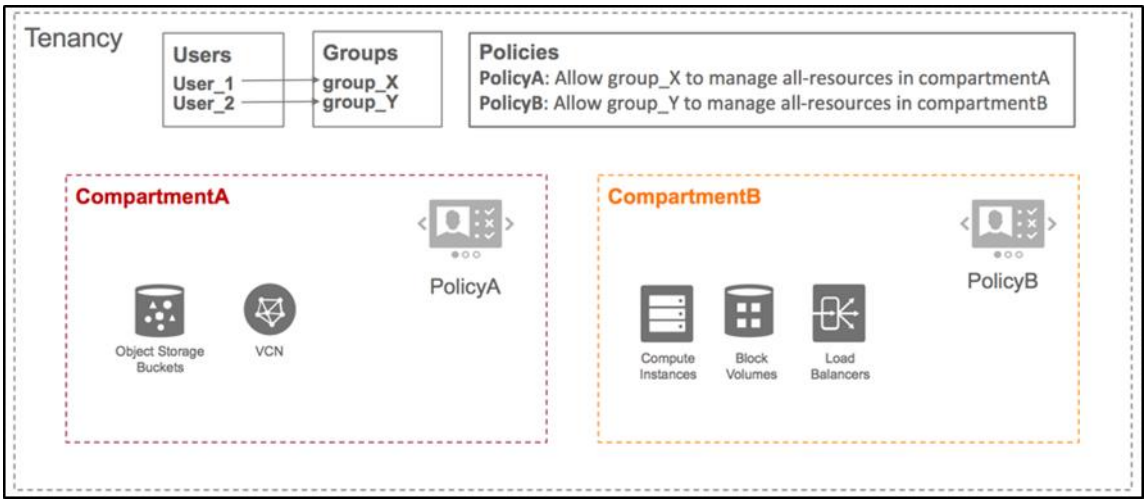


Imagen con la relación de los componentes que conforman OCI IAM para la gestión de derechos de acceso.

1.3.3 CLOUD GUARD

El Servicio de Cloud Guard examina las deficiencias de seguridad de los recursos de OCI relacionadas con la configuración y para examinar los operadores y los usuarios en busca de actividades de riesgo. Tras la detección, Cloud Guard sugiere acciones correctivas y se puede configurar para que realice automáticamente determinadas acciones como, por ejemplo:

a) Detectar una instancia accesible al público (con una dirección IP pública o en una subred pública) y parar la instancia.

b) Detectar un bucket de Object Storage al que se pueda acceder públicamente y desactivarlo.

c) Detectar un inicio de sesión de usuario de una dirección IP sospechosa y restringir el tráfico de esta dirección.

Oracle recomienda activar Cloud Guard en su tenant para examinar todo el contenido del compartimento raíz y todos los subcompartimentos, o bien configurar destinos para comprobar sólo compartimentos específicos. Cada destino está asociado a una receta de detector y cada receta no es más que una agrupación de reglas que definen acciones de usuario o configuraciones de recursos específicas que hacen que Cloud Guard informe un problema. Oracle proporciona varias recetas de detector por defecto de Cloud Guard, que puede utilizar tal cual o personalizar según sea necesario. Por ejemplo, es posible que desee cambiar el nivel de riesgo o la configuración asociada con determinadas reglas de detector. A medida que Cloud Guard agrega nuevas reglas de detector, se activan automáticamente en recetas gestionadas por Oracle y se desactivan en recetas personalizadas.

Una receta de responsable de respuesta de Cloud Guard define la acción o el juego de acciones que se deben realizar en respuesta a un problema identificado por un detector. También puede utilizar los servicios Eventos y Notificaciones para enviar notificaciones cuando Cloud Guard detecte un tipo de problema para el que desee recibir una notificación.

1.3.4 ANÁLISIS DE VULNERABILIDADES

El servicio de Análisis de Vulnerabilidades de Oracle ayuda a mejorar su nivel de seguridad mediante la comprobación rutinaria de los hosts para detectar posibles vulnerabilidades. El servicio genera informes con métricas y detalles sobre estas vulnerabilidades y asigna a cada uno un nivel de riesgo como, por ejemplo:

a) Puertos que se dejan sin intención abiertos que podrían ser un vector de ataque potencial para los recursos en la nube o permitir a los hackers explotar otras vulnerabilidades.

b) Paquetes del sistema operativo que requieran actualizaciones y parches para abordar las vulnerabilidades.

c) Configuraciones del sistema operativo que los hackers puedan aprovechar.

d) Referencias estándar del sector publicadas por el Centro de Seguridad en Internet (CIS) para el sistema operativo de destino.

También puede supervisar estas vulnerabilidades en Cloud Guard, donde se ha indicado que, tras la detección de una vulnerabilidad, sugiere acciones correctivas y estas se pueden configurar para que realice automáticamente determinadas acciones.

1.3.5 SERVICIO ALMACÉN (VAULT)

Puede utilizar el servicio Vault (Almacén) para crear y gestionar recursos del tipo Almacenes, Claves y Secretos.

Un almacén incluye las claves de cifrado y las credenciales secretas que utiliza para proteger sus datos y conectarse a recursos protegidos. Como recursos gestionados por el cliente, tiene control completo sobre quién tiene acceso a sus almacenes, claves y secretos. También controla lo que los usuarios y servicios autorizados pueden hacer con los recursos de almacén. Los niveles de acceso pueden ir desde algo tan granular como si un servicio concreto puede utilizar una clave individual, hasta actividades de gestión del ciclo de vida más impactantes, como si un usuario puede suprimir una clave de un almacén para evitar su uso por completo.

Las claves se almacenan en módulos de seguridad de hardware altamente disponibles y duraderos (HSM) que cumplen con la certificación de seguridad de nivel 3 de seguridad del sistema Federal Information Processing Standards (FIPS) 140-2. Los secretos y las versiones secretas están codificados en base64 y cifrados con claves de cifrado maestras, pero no residen en el HSM.

Los algoritmos de cifrado de claves que admite el Servicio Vault incluyen el estándar de cifrado avanzado (AES), el algoritmo Rivest-Shamir-Adleman (RSA) y el algoritmo de firma digital de curva elíptica (ECDSA). Puede crear y utilizar claves simétricas AES y claves asimétricas RSA para cifrado y descifrado. También puede utilizar claves asimétricas RSA o ECDSA para firmar mensajes digitales.

1.3.6 FIREWALL DE APLICACIÓN WEB (WAF)

OCI Web Application Firewall (WAF) es un servicio de seguridad basado en la nube y conforme con los requisitos de la industria de tarjetas de pago (PCI) que protege las aplicaciones frente al tráfico de Internet no deseado y malicioso. WAF puede proteger cualquier punto final orientado a Internet, lo que proporciona un cumplimiento de reglas consistente en todas sus aplicaciones.

Puede utilizar WAF para crear y gestionar reglas de protección para amenazas de Internet, incluidos los scripts de sitios (XSS), la inyección SQL y otras vulnerabilidades definidas por OWASP. Los bots no deseados se pueden mitigar, mientras que se permite la introducción de los bots beneficiosos. También puede definir y aplicar reglas de protección personalizadas a las configuraciones de WAF mediante el lenguaje de reglas ModSecurity.

También puede utilizar WAF para crear reglas de acceso que definan acciones explícitas para solicitudes que cumplan varias condiciones. Por ejemplo, las reglas de acceso pueden limitar las solicitudes según la geografía o la firma de la solicitud. Se puede definir una acción de regla para que registre y permita, detecte, bloquee, redirija, omita o muestre CAPTCHA para todas las solicitudes que coincidan con las condiciones.

1.3.7 AUDITORÍA (AUDIT)

El Servicio Audit registra todas las llamadas de API a recursos en el tenant de un cliente y una actividad de conexión desde la consola. Puede lograr sus objetivos de seguridad y conformidad mediante el servicio Auditoría para supervisar toda la actividad de usuario en el tenant. Dado que todas las llamadas a la consola, SDK y la línea de comandos (CLI) pasan por las API, se incluye toda la actividad de esos orígenes. Los registros de auditoría están disponibles mediante una API de consulta autenticable o que se pueden recuperar como archivos por lotes de OCI Object Storage. El contenido del log de auditoría incluye la actividad que se produjo, el usuario que la inició, la fecha y la hora de la solicitud, así como la IP de origen, el agente de usuario y las cabeceras HTTP de la solicitud.

1.4 MODELO DE SEGURIDAD COMPARTIDO

OCI ofrece la mejor tecnología de seguridad y procesos operativos para proteger los servicios en la nube empresarial. Sin embargo, para ejecutar de forma segura las cargas de trabajo en OCI, el cliente debe conocer las responsabilidades de seguridad y conformidad. Oracle proporciona de forma inherente seguridad para la infraestructura y las operaciones en la nube (controles de acceso de operadores de nube, aplicación de parches de seguridad de infraestructura, etc.) y el cliente es responsable de configurar de forma segura los recursos en la nube. La seguridad en la nube es una responsabilidad compartida entre el cliente y Oracle.

En un entorno informático compartido de múltiples tenant, Oracle es responsable de la seguridad de la infraestructura en la nube subyacente (como las instalaciones del centro de datos y los sistemas de hardware y software) y el cliente es responsable de proteger las cargas de trabajo y configurar los servicios (como recursos informáticos, red, almacenamiento y base de datos) de manera segura.

En un servidor con hardware dedicado totalmente aislado, de un único tenant y sin software de Oracle, la responsabilidad del cliente aumenta al traer toda la pila de software (sistemas operativos y superiores) en la que despliega las aplicaciones. En este entorno, es responsable de proteger las cargas de trabajo y configurar sus servicios (recursos informáticos, red, almacenamiento, base de datos) de manera segura, así como de garantizar que los componentes de software que se ejecutan en los servidores con hardware dedicado se configuran, se despliegan y se gestionan de forma segura.

Más concretamente, las responsabilidades del cliente y las responsabilidades de Oracle se pueden dividir en las siguientes áreas:

a) **Gestión de identidad y acceso**: Al igual que con todos los servicios en la nube de Oracle, el cliente debe proteger sus credenciales de acceso a la nube y configurar cuentas de usuario individuales. Es responsable de gestionar y revisar el acceso de sus propias cuentas de empleado y de todas las actividades que tienen lugar en su tenant. Oracle es responsable de proporcionar servicios eficaces como, gestión de identidad, autenticación, autorización y auditoría.

b) **Seguridad de la carga de trabajo**: El cliente es responsable de proteger las capas del sistema operativo y de la aplicación de las instancias informáticas contra ataques y riesgos. Esta protección incluye la aplicación de parches en aplicaciones y sistemas operativos, la configuración de sistemas operativos y la protección contra ataques de red y programas maliciosos (malware). Oracle es responsable de proporcionar imágenes seguras que estén reforzadas y tengan los parches más recientes. Además, Oracle facilita la introducción de las mismas soluciones de seguridad de terceros que usa actualmente.

c) **Clasificación de datos y conformidad**: El cliente es responsable de clasificar y etiquetar correctamente los datos, así como cumplir las obligaciones de conformidad. Además, es responsable de auditar las soluciones para asegurarse de que cumplen con las obligaciones de conformidad.

d) **Seguridad de infraestructura de host**: El cliente es responsable de configurar y gestionar de forma segura los servicios de recursos informáticos (hosts virtuales, contenedores), almacenamiento (objetos, almacenamiento local, volúmenes en bloque) y plataforma (configuración de base de datos). Oracle tiene una responsabilidad compartida con el cliente para garantizar que el servicio está configurado y protegido de forma óptima. Esta responsabilidad incluye la seguridad del hipervisor y la configuración de los permisos y los controles de acceso de red. El cliente debe asegurarse de que los hosts se puedan comunicar correctamente y de que los dispositivos puedan conectar o montar los dispositivos de almacenamiento correctos.

e) **Seguridad de la red**: El cliente es responsable de configurar de forma segura elementos de red, como redes virtuales, balanceadores de carga, DNS y gateways. Oracle es responsable de proporcionar una infraestructura de red segura.

f) **Protección de cliente y punto final**: El cliente utiliza varios sistemas de hardware y software, como dispositivos móviles y exploradores, para acceder a sus recursos en la nube. Es responsable de la protección de todos los clientes y puntos finales que permite acceder a los servicios de Oracle.

g) **Seguridad física**: Oracle es responsable de proteger la infraestructura global que ejecutan los servicios ofrecidos en OCI. Esta infraestructura consta del hardware, el software, la red y las instalaciones que ejecutan servicios de OCI.

Puede ampliar los detalles de las responsabilidades de OCI en el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/Content/Security/Concepts/security_overview.htm#Shared_Security_Model

2. DESPLIEGUE SEGURO PARA OCI

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. Para ello, se puede conseguir de 2 formas:

a) **Creando un tenant gratuito**, al que previamente se debe facilitar la información personal y de empresa para la cuenta cloud, disponiendo de 30 días de prueba y un crédito gratuito de inicio para probar los servicios de OCI. Este tenant puede actualizarse posteriormente a uno de los planes de pago, conservando las configuraciones realizadas durante el periodo de pruebas.

b) **Formalizando un contrato con Oracle**, el cual facilitará la cuenta cloud a usar para la posterior activación del tenant asociado al contrato.

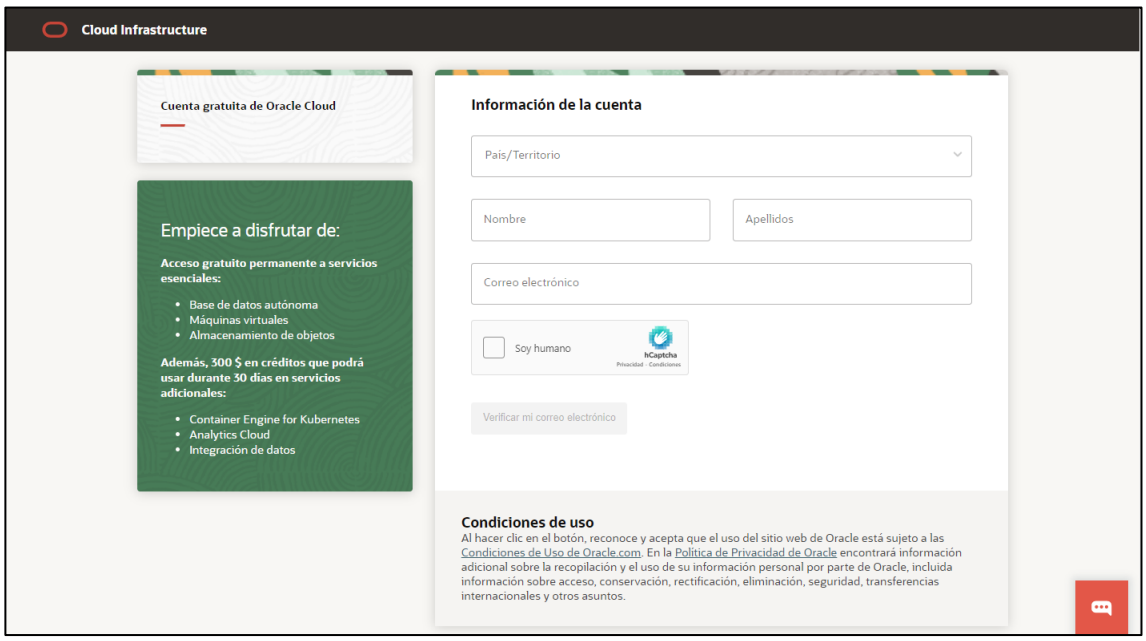
Una vez en disposición de la cuenta y el tenant, ya sea gratuito o mediante contrato directo con Oracle, se hará necesaria la aplicación de las medidas de seguridad que establece el ENS para asegurar el entorno, según la categoría que corresponda a la organización.

2.1 CREAR UN TENANT GRATUITO

Para crear un tenant en OCI será preciso tener en cuenta una serie de aspectos que garanticen la continuidad y la confidencialidad de los servicios consumidos.

Lo primero, es la creación de una cuenta cloud que quedará asociada al tenant y que se realiza desde el siguiente enlace directo de Oracle.

https://signup.cloud.oracle.com

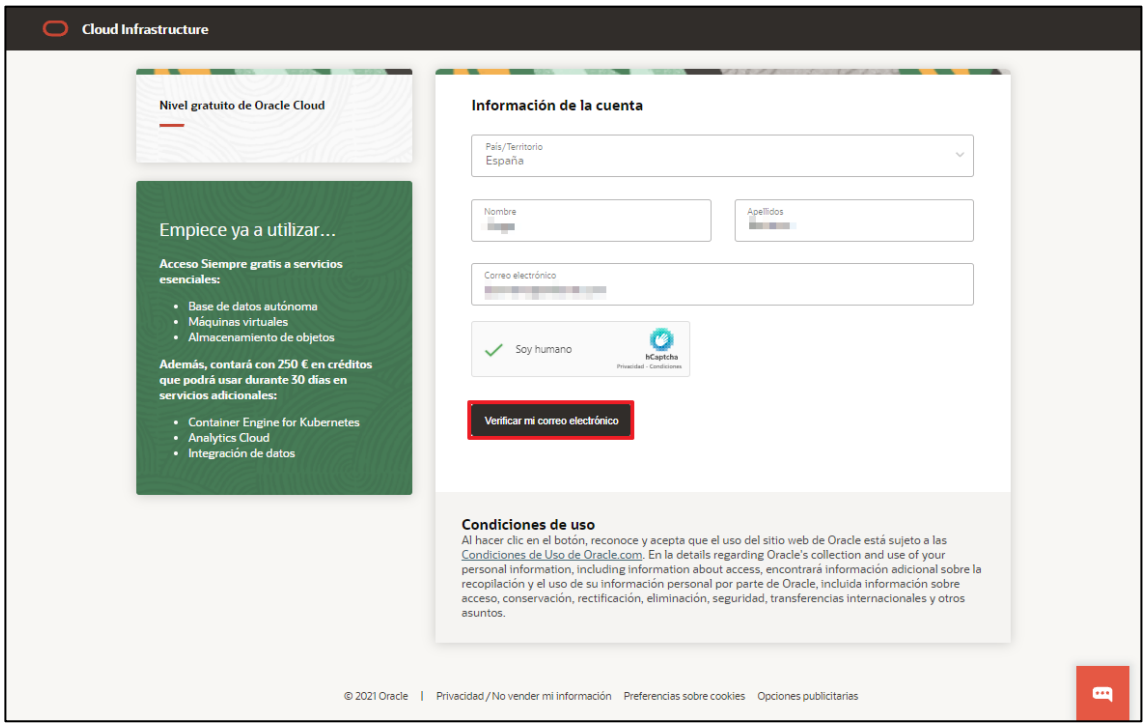


Desde aquí se le informa al usuario de las condiciones que tendrá el tenant gratuito, en cuanto a la duración, 30 días, como al crédito gratuito disponible para la prueba de los servicios.

A continuación, se detallan los aspectos necesarios para la correcta configuración de la cuenta.

2.1.1 INFORMACIÓN DE LA CUENTA

En la pantalla de creación de la cuenta para un tenant de OCI, es preciso identificar el país, y los datos personales en cuanto al nombre y los apellidos, para luego proceder a la identificación humana mediante un captcha, tras lo cual se habilita el botón para la verificación del correo electrónico introducido que el cliente deberá validar.



Una vez verificado, llegará un correo electrónico para validar la cuenta de correo. Una vez validado, se abrirá una nueva ventana en el navegador para continuar el proceso de creación, solicitando la contraseña, nombre de la empresa, un nombre para el tenant y, por último, la región donde se creará el tenant que tiene una gran importancia en cuanto a los servicios ofertados y las comunicaciones que serán más agiles a la hora de seleccionar una ubicación más próxima a la del cliente.

Tras completar todos los campos de forma satisfactoria, se habilitará el botón “Continuar” para seguir con el proceso.

Se abrirá una nueva ventana donde se deberán rellenar los datos de la empresa en cuanto a los datos de la dirección física de la misma.

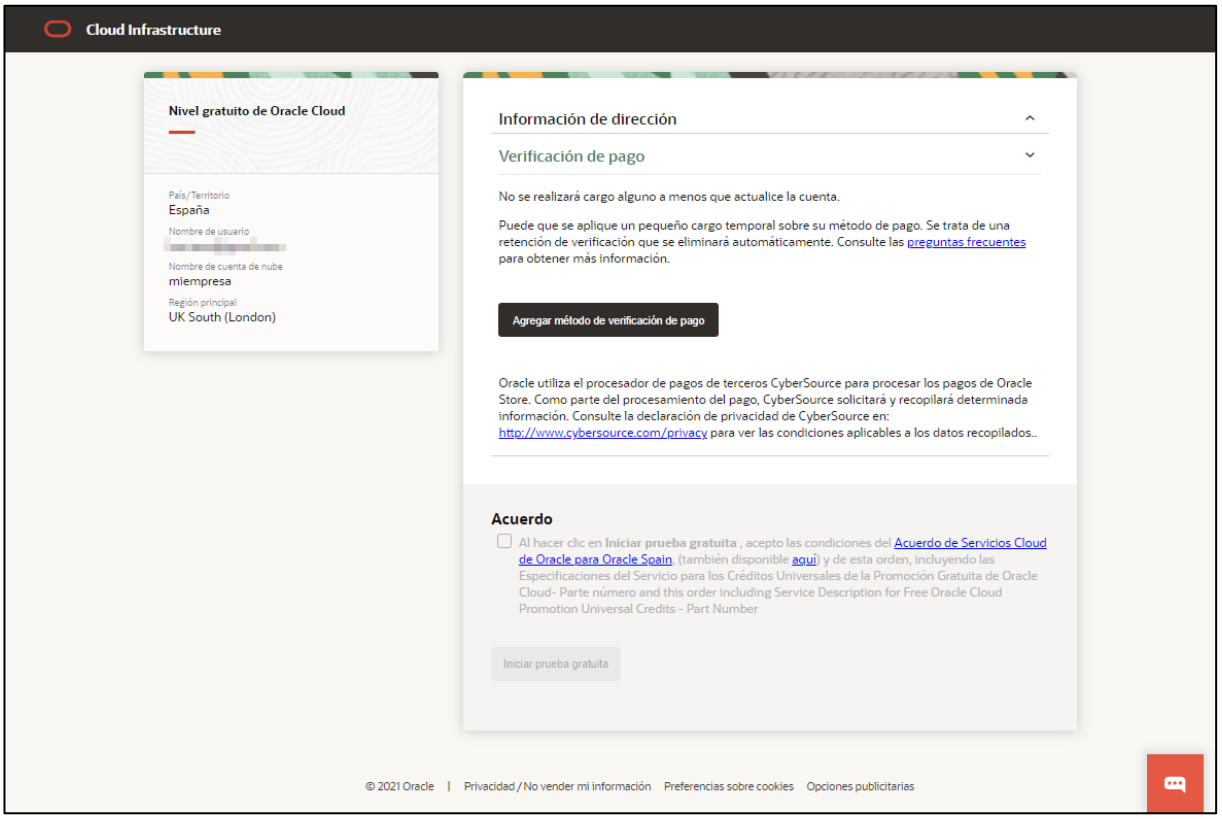
Completados los datos, se habilitará el botón “Continuar” para proseguir con la verificación de un método de pago que, por su obligatoriedad en el proceso de alta, se detalla a continuación.

2.1.2 MÉTODO DE PAGO

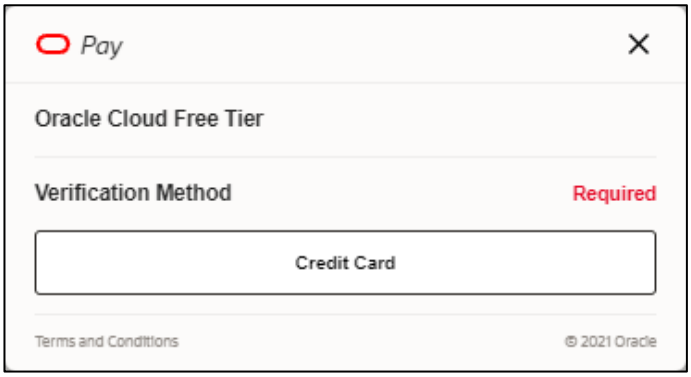
Se detallarán los medios de pago a utilizar para la gestión económica de los servicios utilizados.

El método de pago es un requisito obligatorio para el alta de una cuenta, para asociarlo a un tenant, aunque este sea gratuito y con un crédito inicial para pruebas, como se ha visto en el punto 2.1 CREAR UN TENANT GRATUITO, de este documento.

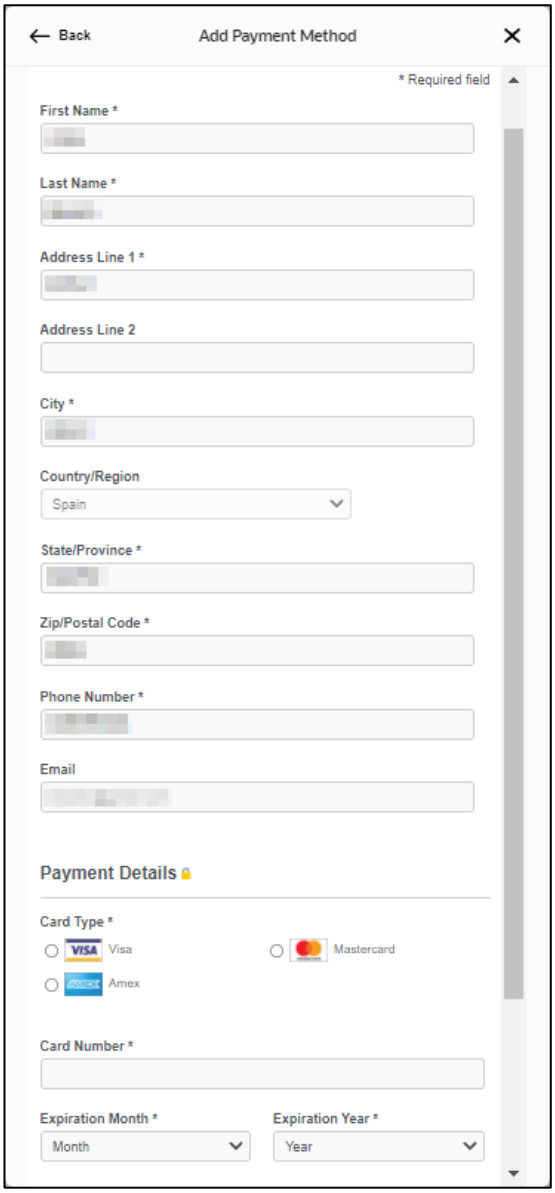
Para ello, llegado el momento de solicitar un método de pago, se abrirá la siguiente ventana en el navegador.



Una vez que pulse el botón “Agregar método de verificación de pago”, mostrará la siguiente ventana emergente donde se aprecia que el método es requerido para continuar.



Pulsando en el botón “Credit Card” mostrará una nueva ventana emergente, con los datos personales y dirección agregados en los pasos anteriores y los nuevos campos para añadir una tarjeta de crédito que será asociada a la cuenta del tenant para los costes de los servicios que se vayan creando.



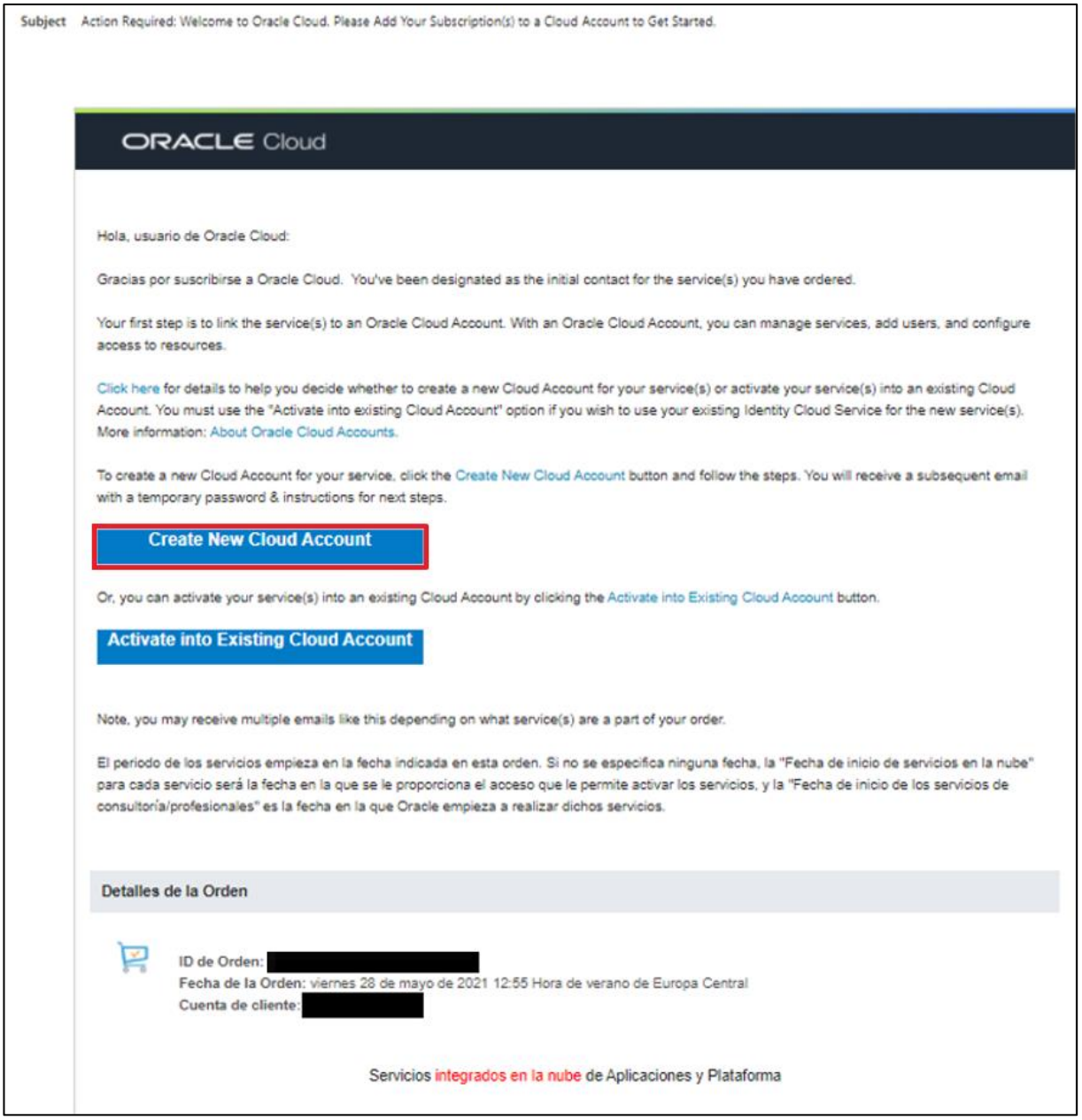
Nota: Los cargos en la tarjeta de crédito para un tenant gratuito no se realizarán mientras no se sobrepase la cantidad asignada de forma gratuita. En el ejemplo mostrado anterior se observa que son 250€.

Con los datos introducidos y validados, se finaliza el asistente para la creación de una cuenta en el tenant y se accede al panel de control.

2.2 FORMALIZAR UN TENANT CON ORACLE

Otra opción para desplegar un tenant es formalizar un contrato directo con Oracle, el cual proveerá a la organización de la cuenta cloud para acceder al tenant y los servicios de OCI.

Oracle, aprovisionará la cuenta con créditos universales y la organización recibirá un correo electrónico de activación que deberá revisar para activar los servicios, proporcionando los datos solicitados para terminar la configuración de la cuenta.



Subject Action Required: Welcome to Oracle Cloud. Please Add Your Subscription(s) to a Cloud Account to Get Started.

ORACLE Cloud

Hola, usuario de Oracle Cloud:

Gracias por suscribirse a Oracle Cloud. You've been designated as the initial contact for the service(s) you have ordered.

Your first step is to link the service(s) to an Oracle Cloud Account. With an Oracle Cloud Account, you can manage services, add users, and configure access to resources.

Click here for details to help you decide whether to create a new Cloud Account for your service(s) or activate your service(s) into an existing Cloud Account. You must use the "Activate into existing Cloud Account" option if you wish to use your existing Identity Cloud Service for the new service(s). More information: About Oracle Cloud Accounts.

To create a new Cloud Account for your service, click the Create New Cloud Account button and follow the steps. You will receive a subsequent email with a temporary password & instructions for next steps.

Create New Cloud Account

Or, you can activate your service(s) into an existing Cloud Account by clicking the Activate into Existing Cloud Account button.

Activate into Existing Cloud Account

Note, you may receive multiple emails like this depending on what service(s) are a part of your order.

El periodo de los servicios empieza en la fecha indicada en esta orden. Si no se especifica ninguna fecha, la "Fecha de inicio de servicios en la nube" para cada servicio será la fecha en la que se le proporciona el acceso que le permite activar los servicios, y la "Fecha de inicio de los servicios de consultoría/profesionales" es la fecha en la que Oracle empieza a realizar dichos servicios.

Detalles de la Orden

ID de Orden: [redacted]
Fecha de la Orden: viernes 28 de mayo de 2021 12:55 Hora de verano de Europa Central
Cuenta de cliente: [redacted]

Servicios integrados en la nube de Aplicaciones y Plataforma

Se le solicitará la siguiente información:

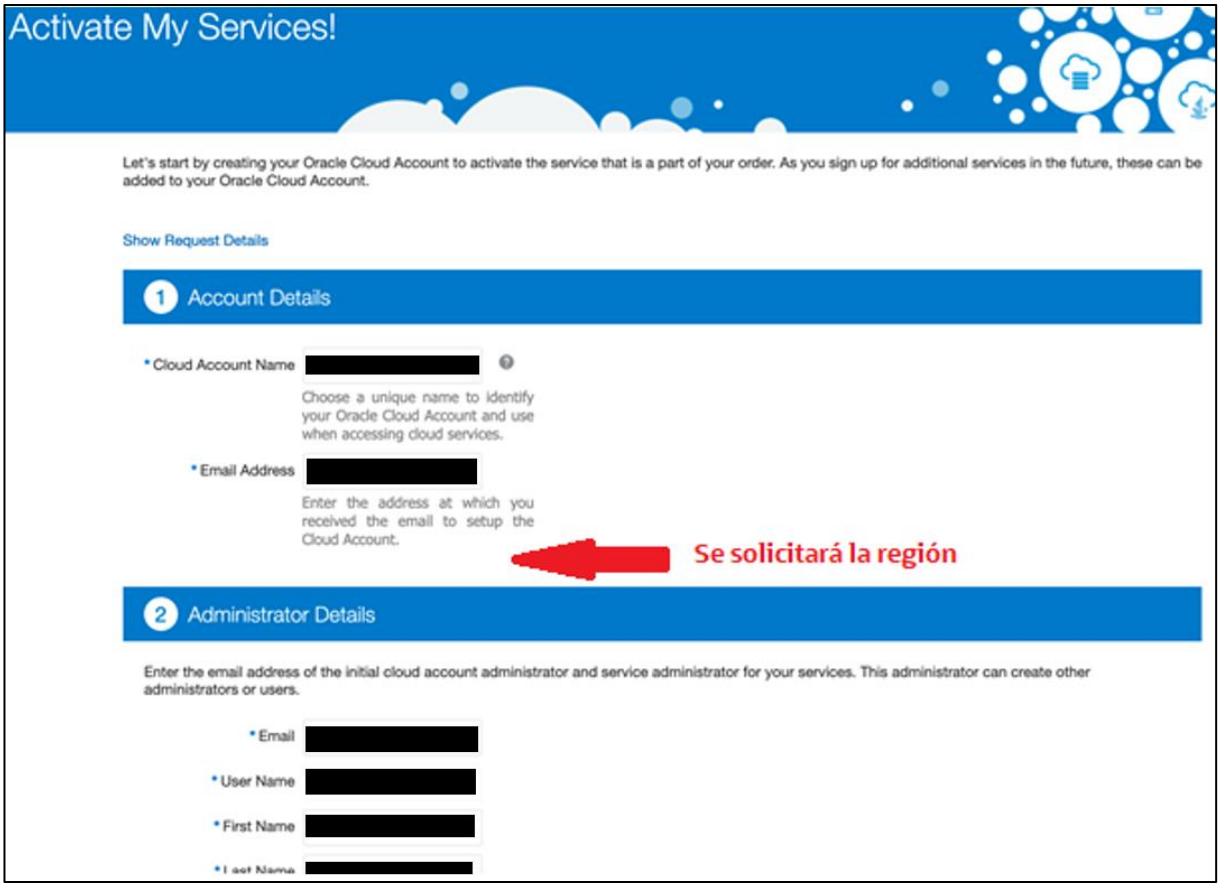
a) Crear un nuevo nombre de cuenta, que se utilizará para identificar su cuenta en la Nube.

b) En caso de pedir la dirección debe proporcionar la misma dirección de correo electrónico en la que recibió el correo de bienvenida. A esta dirección se le enviarán las instrucciones para acceder a su nueva Cuenta Cloud. Se le pedirá la dirección de correo electrónico sólo si no tiene ya una cuenta en la nube.

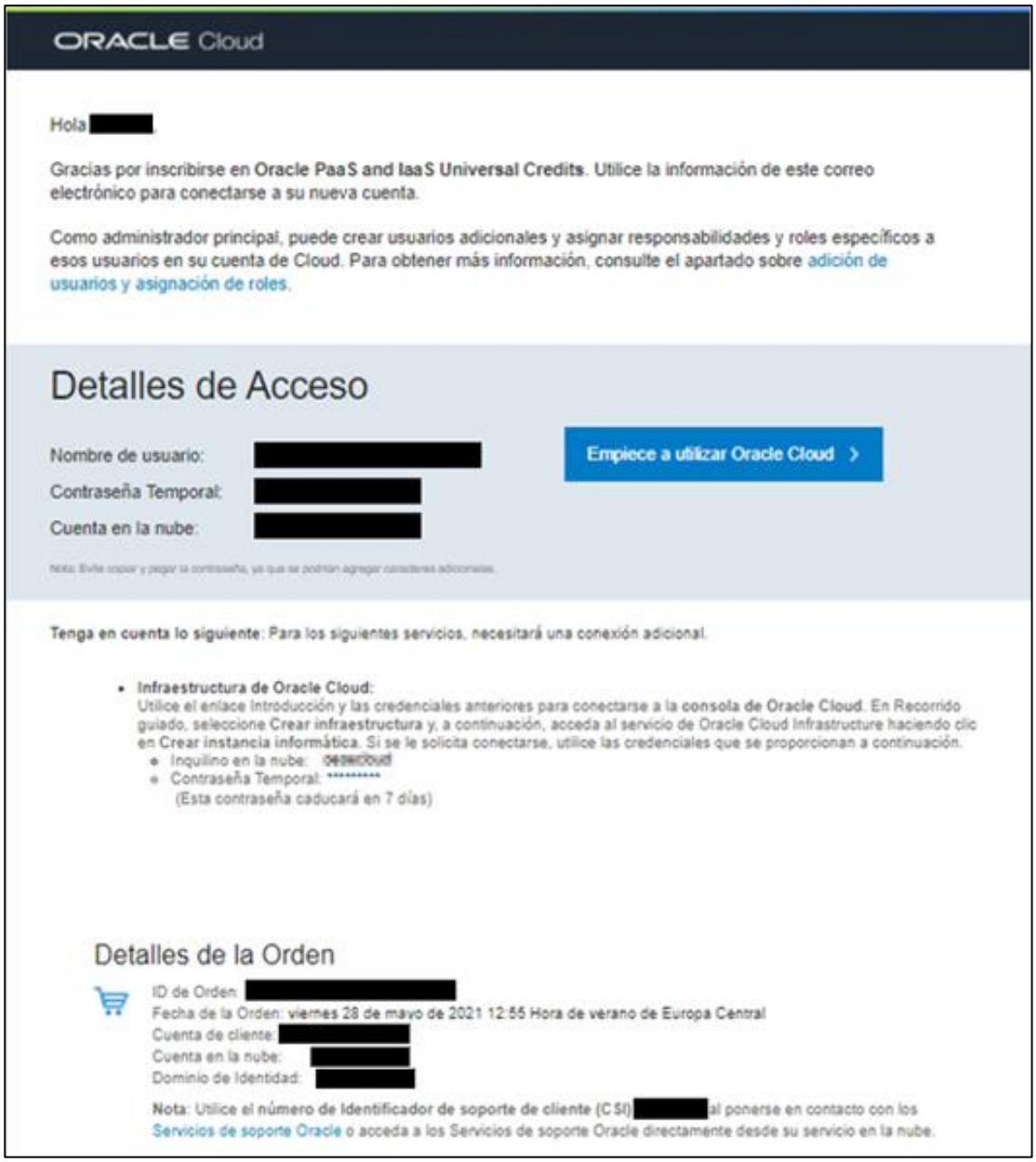
c) Seleccionar una región de datos por defecto para crear el tenant.

d) Indicar los datos del administrador de la cuenta de la nube (cloud Account Administrator). La persona que especifique aquí será tanto un administrador de la cuenta en la nube como un administrador de servicios y podrá crear otros usuarios según sea necesario. Esta persona gestionará y supervisará los servicios de la cuenta en la nube especificada.

e) Cuando haya introducido toda la información necesaria, debe hacer clic en “Crear cuenta” para enviar la solicitud de una Cuenta en la nube de Oracle.



f) Una vez activada con éxito recibirá otro correo electrónico, como el que puede verse a continuación, donde recibirá las credenciales de acceso. Debe utilizar esta información para acceder a la cuenta y cambiar la contraseña proporcionada, al iniciar la sesión.



ORACLE Cloud

Hola [redacted]

Gracias por inscribirse en **Oracle PaaS and IaaS Universal Credits**. Utilice la información de este correo electrónico para conectarse a su nueva cuenta.

Como administrador principal, puede crear usuarios adicionales y asignar responsabilidades y roles específicos a esos usuarios en su cuenta de Cloud. Para obtener más información, consulte el apartado sobre adición de usuarios y asignación de roles.

Detalles de Acceso

Nombre de usuario: [redacted]
Contraseña Temporal: [redacted]
Cuenta en la nube: [redacted]

Empiece a utilizar Oracle Cloud >

Nota: Evite copiar y pegar la contraseña, ya que se podrían agregar caracteres adicionales.

Tenga en cuenta lo siguiente: Para los siguientes servicios, necesitará una conexión adicional.

- **Infraestructura de Oracle Cloud**:
  Utilice el enlace Introducción y las credenciales anteriores para conectarse a la consola de Oracle Cloud. En Recorrido guiado, seleccione Crear infraestructura y, a continuación, acceda al servicio de Oracle Cloud Infrastructure haciendo clic en Crear instancia informática. Si se le solicita conectarse, utilice las credenciales que se proporcionan a continuación.
  - Inquilino en la nube: [redacted]
  - Contraseña Temporal: [redacted]
    (Esta contraseña caducará en 7 días)

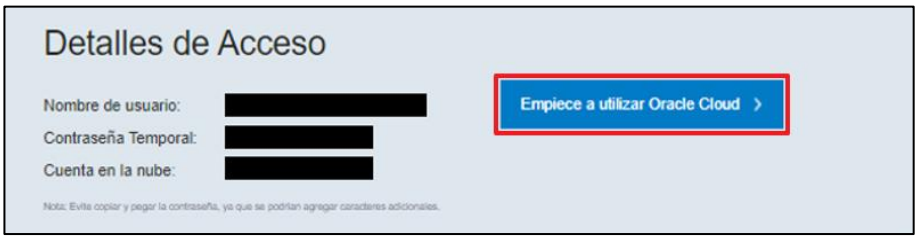
Detalles de la Orden

ID de Orden: [redacted]
Fecha de la Orden: viernes 28 de mayo de 2021 12:55 Hora de verano de Europa Central
Cuenta de cliente: [redacted]
Cuenta en la nube: [redacted]
Dominio de Identidad: [redacted]

Nota: Utilice el número de Identificador de soporte de cliente (CSI) [redacted] al ponerse en contacto con los Servicios de soporte Oracle o acceda a los Servicios de soporte Oracle directamente desde su servicio en la nube.

2.2.1 ACCESO A LA CUENTA EN LA NUBE POR PRIMERA VEZ

Para acceder a la nube, debe abrir el correo electrónico de bienvenida, anotar el nombre de usuario y la contraseña temporal y, a continuación, hacer clic en el botón "Empiece a utilizar Oracle Cloud >". Cuando todos los servicios estén aprovisionados en la cuenta, recibirá una notificación en el panel de "Mis Servicios".



También puede acceder desde la siguiente dirección de Oracle:

https://cloud.oracle.com

Introduzca las credenciales e inicie sesión. El sistema le pedirá que cambie la contraseña inicial por una nueva y tras realizarlo le dirigirá a un viaje guiado (*Guide Journey*). A continuación, puede:

a) Utilizar el Guided Journey para conocer los servicios, tutoriales y otra documentación disponible para ayudarle a empezar a utilizar Oracle Cloud. Puede ver un video desde el siguiente enlace: https://videohub.oracle.com/media/Customer+Guided+Journey+-+Welcome+to+Oracle+Cloud/0_yr2a8o9g/123762302

b) Hacer clic en "Dashboard" para ir al panel de control de "Mis Servicios", donde podrá explorar las características de la cuenta de Cloud.

Nota: Cuando se registre, Oracle establecerá la cuenta de la persona que activó el tenant cloud, como Administrador Principal, agregándola al grupo por defecto "Administradores" de "tenant Policy". Se recomienda añadir algún administrador adicional, al inicialmente creado al activar la cuenta, y no utilizar esta para las labores de administración del tenant como buena práctica.

3. CONFIGURACIÓN SEGURA PARA OCI IAM Y SERVICIOS DE SEGURIDAD

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).

3.1.1.1 IDENTIFICACIÓN

Esta medida especifica los mecanismos para garantizar la autenticidad y trazabilidad de las diferentes entidades. Esto se transforma y genera una identificación singular para cada organización, usuario, proceso o servicio. De esta manera, siempre se podrá conocer quién recibe qué derechos y se podrá saber qué acciones ha realizado.

La identificación de usuario se traduce en la necesidad de crear cuentas únicas e inequívocas para cada usuario y servicio de OCI. 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.

Estas cuentas únicas, deben garantizar que cuando el usuario tenga diferentes roles frente al sistema (por ejemplo, como ciudadano, como trabajador interno del organismo y como administrador de los sistemas) recibirá identificadores singulares para cada uno de los casos de forma que siempre queden delimitados privilegios y registros de actividad.

Para ello, Oracle dispone del Servicio OCI Identity and Access Management (OCI IAM) para la gestión de las cuentas de usuario, así como para la asignación de permisos mediante la pertenencia de esas cuentas a grupos, a través de políticas que establecen los permisos específicos de cada grupo o cuentas de usuario, a los compartimentos o recursos de un tenant.

La creación de usuarios para la identificación del acceso a los recursos a los cuales tenga derecho de uso; podrá ser de 2 tipos:

a) Usuarios Federados.

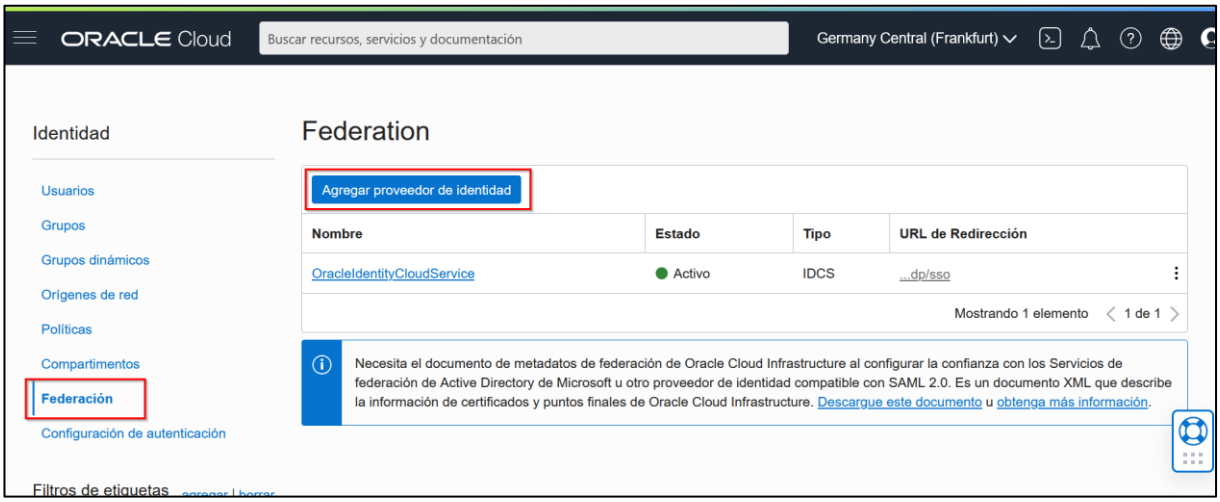
b) Usuarios Locales.

Nota: Debido al continuo proceso de mejora continua y evolución tecnológica, y en particular a lo que afecta al servicio OCI IAM, el cual se encuentra en pleno cambio durante el desarrollo de esta guía, es posible que alguna información detallada en el documento difiera de la que se encuentre en el momento de aplicar estas medidas.
Por favor, siga los enlaces del fabricante donde le mostrará la información más actualizada acerca de sus servicios. En dicha documentación, el administrador deberá escoger entre IAM con dominios (https://docs.oracle.com/es-ww/iaas/Content/Identity/home.htm) o IAM sin dominios (https://docs.oracle.com/es-ww/iaas/Content/Identity/home1.htm), según aplique en su tenant.

Gestión de Usuarios Federados

Si se desea utilizar los usuarios ya existentes en la organización del cliente, se deberá crear previamente la configuración de un proveedor de identidad que pueda conectar con el conjunto de usuarios federados que hayan sido definidos en el directorio de la organización, para poder acceder a los recursos de la nube de OCI.

Esta consola es accesible a través del menú principal de OCI → Identidad y seguridad → Federación.



Acceso a la Consola de FEDERACION para añadir otros proveedores de Identidad.

Selección del proveedor de identidad.

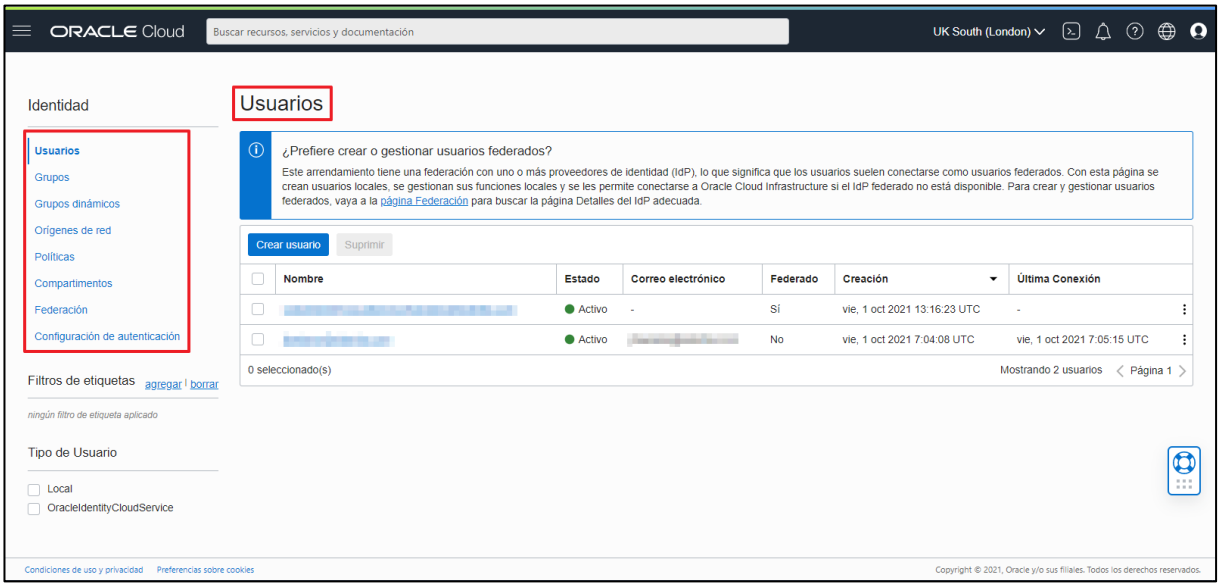
La mejor práctica de Seguridad; que coincide con las buenas prácticas de Oracle al respecto de las cuentas de usuario, es la utilización de cuentas federadas ya que las cuentas locales tienen un uso más enfocado a emergencias, como si de un usuario administrador "root" se tratara.

Puede ampliar la información actualizada acerca de la gestión de proveedores de identidad de OCI mediante el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/Content/Identity/identityproviders/manage-identity-providers.htm

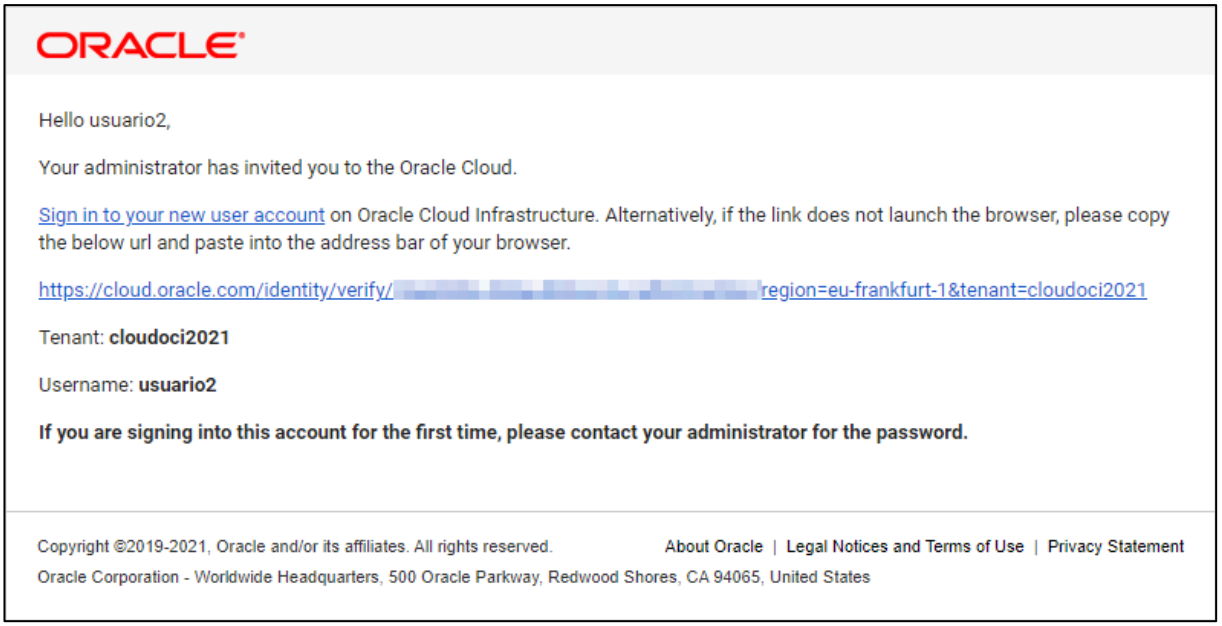
Gestión de Usuarios Locales

Para la gestión de usuarios locales en un tenant de Oracle se accede al menú principal de OCI → Identidad y seguridad → Usuarios.



Durante el proceso de creación de un usuario, no se establece ninguna contraseña, por lo que es necesario que el administrador, entre en la cuenta del usuario recién creado, y establezca una provisional de un solo uso, que el usuario deberá cambiar en el primer acceso.

Cuando el usuario reciba el aviso de alta de su nueva cuenta, deberá pulsar el correspondiente enlace del correo electrónico para verificar.



ORACLE

Hello usuario2,

Your administrator has invited you to the Oracle Cloud.

Sign in to your new user account on Oracle Cloud Infrastructure. Alternatively, if the link does not launch the browser, please copy the below url and paste into the address bar of your browser.

https://cloud.oracle.com/identity/verify/[redacted]region=eu-frankfurt-1&tenant=cloudoci2021

Tenant: **cloudoci2021**

Username: **usuario2**

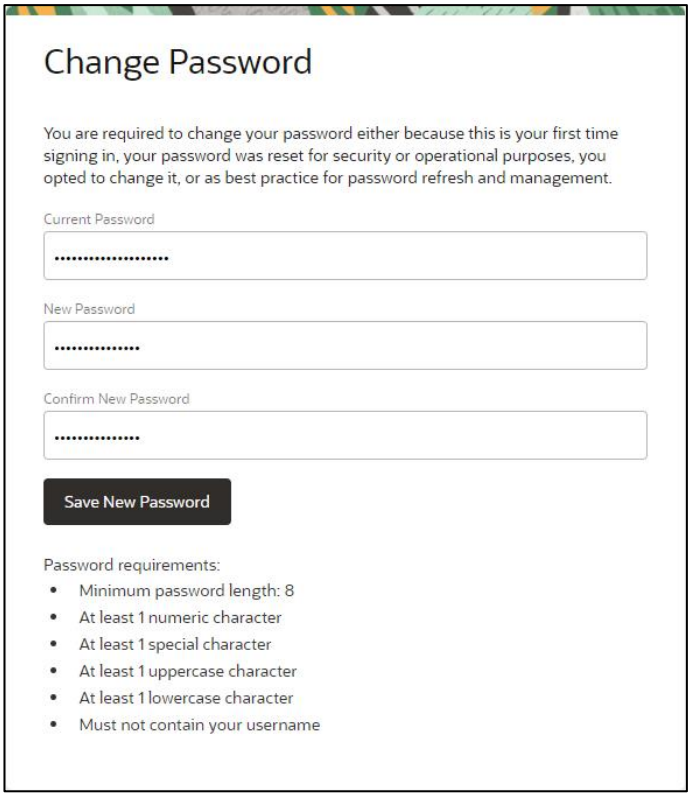
If you are signing into this account for the first time, please contact your administrator for the password.

Copyright ©2019-2021, Oracle and/or its affiliates. All rights reserved. About Oracle | Legal Notices and Terms of Use | Privacy Statement

Oracle Corporation - Worldwide Headquarters, 500 Oracle Parkway, Redwood Shores, CA 94065, United States

Imagen del correo electrónico que recibirá el nuevo usuario creado para verificar su acceso.

Una vez inicie la sesión con la contraseña proporcionada de un solo uso se le pedirá el cambio por una de su elección, manteniendo la complejidad establecida en el tenant.



Change Password

You are required to change your password either because this is your first time signing in, your password was reset for security or operational purposes, you opted to change it, or as best practice for password refresh and management.

Current Password

New Password

Confirm New Password

Save New Password

Password requirements:

- Minimum password length: 8
- At least 1 numeric character
- At least 1 special character
- At least 1 uppercase character
- At least 1 lowercase character
- Must not contain your username

Ventana del cambio de contraseña tras el primer inicio de sesión del nuevo usuario.

En el siguiente enlace puede ampliar la información del servicio OCI IAM de Oracle sobre la gestión de usuarios:

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

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.

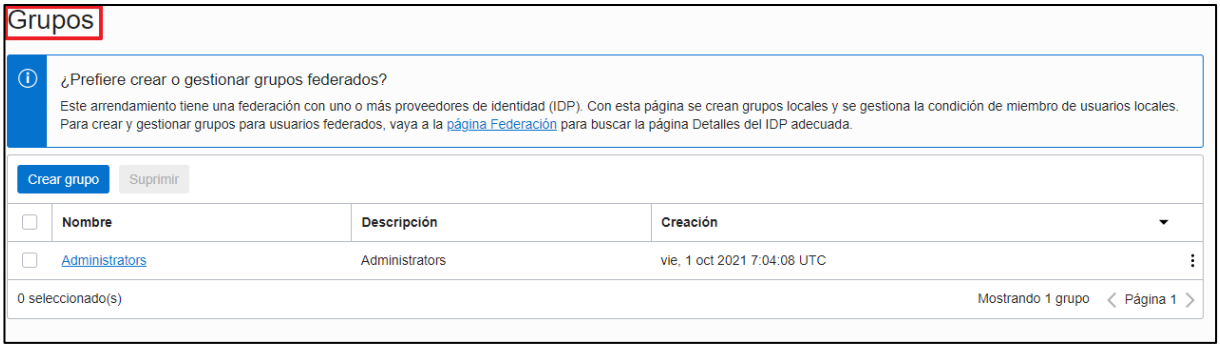
Estos derechos se controlarán y asignarán atendiendo a la política y normativa de seguridad de la organización, a través de la persona responsable de dicha determinación y haciendo uso de mínimo privilegio.

Principalmente se controlará el acceso a los componentes del sistema y sus ficheros o registros de configuración.

Mediante el Servicio OCI IAM, Oracle implementa el control acerca de quién tiene acceso a los recursos en la nube; dicho control está definido por la pertenencia a grupos y durante la creación de un usuario, OCI mantiene ese privilegio mínimo, no asignando por defecto ninguna pertenencia a ningún grupo.

Nota: Debido al continuo proceso de mejora continua y evolución tecnológica, y en particular a lo que afecta al servicio OCI IAM, el cual se encuentra en pleno cambio durante el desarrollo de esta guía, es posible que alguna información detallada en el documento difiera de la que se encuentre en el momento de aplicar estas medidas.
Por favor, siga los enlaces del fabricante donde le mostrará la información más actualizada acerca de sus servicios. En dicha documentación, el administrador deberá escoger entre IAM con dominios (https://docs.oracle.com/es-ww/iaas/Content/Identity/home.htm) o IAM sin dominios (https://docs.oracle.com/es-ww/iaas/Content/Identity/home1.htm), según aplique en su tenant.

Esta consola está accesible a través del menú principal de OCI → Identidad y seguridad → Grupos.



Detalle de la Consola para la creación de Grupos.

Puede ampliar la información acerca de la gestión de grupos en OCI IAM a través del siguiente enlace de Oracle:

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

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.

Oracle cuenta con el control de acceso basado en roles (RBAC) que se gestiona mediante OCI IAM, proporcionando a los administradores un control granular sobre el acceso de los usuarios a los recursos de OCI y las acciones que los usuarios pueden realizar en estos recursos.

Puede ampliar la información acerca de los roles administrativos en el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/Content/Identity/roles/understand-administrator-roles.htm

OCI IAM le permite controlar quién tiene acceso a sus recursos en la nube. Puede controlar qué tipo de acceso tiene un grupo de usuarios y a qué recursos específicos. OCI IAM utiliza componentes para la asignación de permisos, ejemplos de estos componentes son, los recursos, usuarios, grupos, compartimentos, políticas, etc.

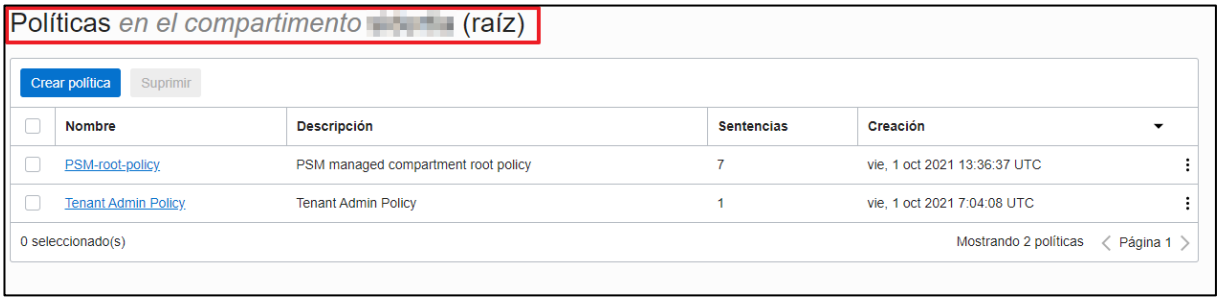
Nota: Debido al continuo proceso de mejora continua y evolución tecnológica, y en particular a lo que afecta al servicio OCI IAM, el cual se encuentra en pleno cambio durante el desarrollo de esta guía, es posible que alguna información detallada en el documento difiera de la que se encuentre en el momento de aplicar estas medidas.
Por favor, siga los enlaces del fabricante donde le mostrará la información más actualizada acerca de sus servicios. En dicha documentación, el administrador deberá escoger entre IAM con dominios (https://docs.oracle.com/es-ww/iaas/Content/Identity/home.htm) o IAM sin dominios (https://docs.oracle.com/es-ww/iaas/Content/Identity/home1.htm), según aplique en su tenant.

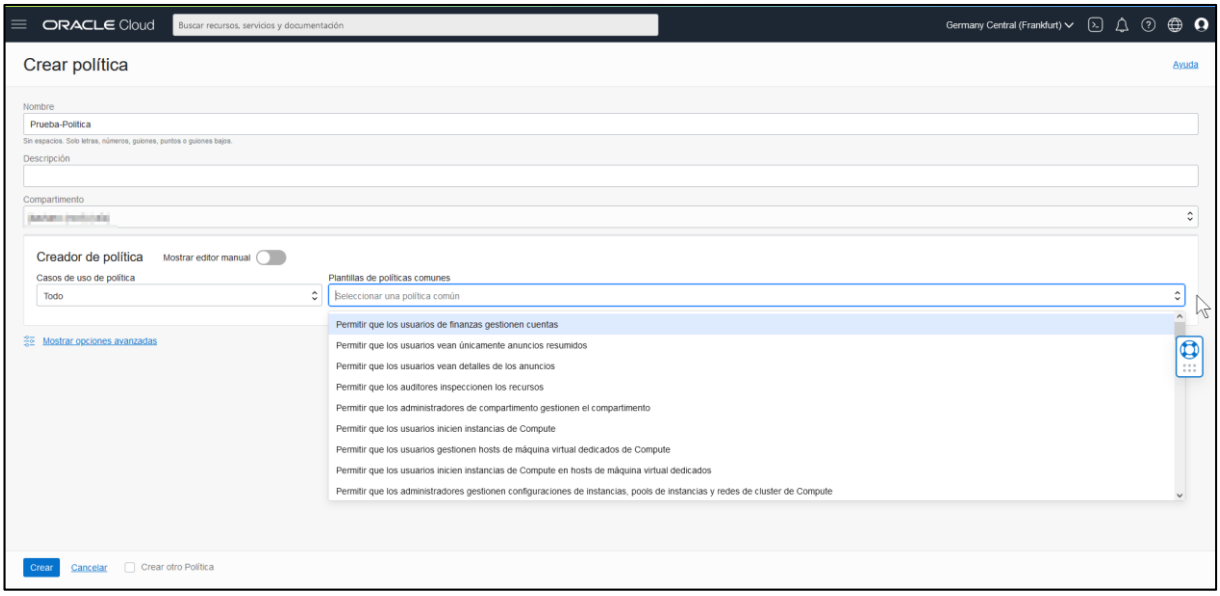
El Servicio OCI IAM implementa el control acerca de quién (usuarios o grupos) tiene acceso a los recursos en la nube. Dicho control está definido por la configuración de Grupos y Políticas:

a) **Definición de Grupos** por roles que se aplican al acceso y gestión de los recursos. Esto se ha explicado en el punto anterior 3.1.1.2 REQUISITOS DE ACCESO.

b) **Definición de Políticas** para la gestión de los permisos por grupos de roles.

   Una vez definidos los Grupos con los permisos según los roles, asigne a través de Políticas, qué acciones podrá realizar cada grupo para gestionar los distintos recursos. Debe utilizar la consola de políticas a través del menú principal de OCI → Identidad y seguridad → Políticas.





Detalle de la creación/gestión de Políticas.

Puede ampliar la información acerca de las Políticas en OCI y su implementación, en el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/Content/Identity/policiesgs/get-started-with-policies.htm

Puede ampliar la información de las funcionas avanzadas de políticas del servicio OCI IAM en el siguiente enlace de Oracle:

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

Puede ampliar la implementación de Políticas comunes en OCI en el siguiente enlace de Oracle:

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

3.1.1.4 PROCESO DE GESTIÓN DE DERECHOS DE ACCESO

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

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

Esta gestión se realiza desde el Servicio OCI IAM, atendiendo a los principios mencionados anteriormente para la asignación de derechos de acceso mínimos. Por defecto, al crear un nuevo usuario no se asigna ningún permiso, hasta asignarle posteriormente la pertenencia a grupos.

Nota: Debido al continuo proceso de mejora continua y evolución tecnológica, y en particular a lo que afecta al servicio OCI IAM, el cual se encuentra en pleno cambio durante el desarrollo de esta guía, es posible que alguna información detallada en el documento difiera de la que se encuentre en el momento de aplicar estas medidas.
Por favor, siga los enlaces del fabricante donde le mostrará la información más actualizada acerca de sus servicios. En dicha documentación, el administrador deberá escoger entre IAM con dominios (https://docs.oracle.com/es-ww/iaas/Content/Identity/home.htm) o IAM sin dominios (https://docs.oracle.com/es-ww/iaas/Content/Identity/home1.htm), según aplique en su tenant.

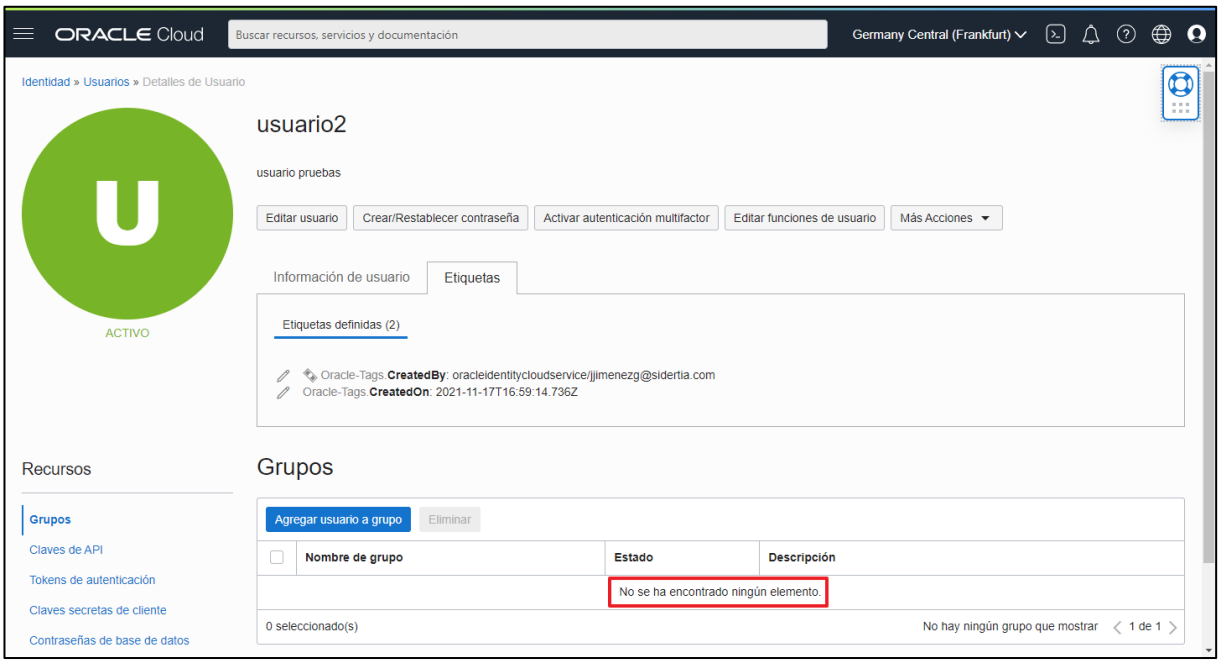


Imagen mostrando la ausencia de permisos por defecto a grupos tras la creación de un nuevo usuario.

Desde la consola de "Identidad y Seguridad" de OCI, los administradores pueden gestionar los diferentes permisos a los usuarios mediante la asignación a:

a) **Compartimentos**: Recopilación heterogénea de recursos con fines de aislamiento de seguridad y control de acceso.

b) **Grupos**: Recopilación de usuarios que comparten un conjunto similar de privilegios de acceso. Los administradores pueden otorgar políticas de acceso que autorizan a un grupo a usar o gestionar recursos en un tenant. Todos los usuarios de un grupo heredan el mismo conjunto de privilegios.

c) **Políticas**: Conjunto de reglas de autorización que definen el acceso a los recursos de un tenant.

A continuación, se muestra una imagen donde se aprecia la relación entre todos los componentes de Oracle necesarios para la asignación de permisos, mediante la construcción de Políticas.

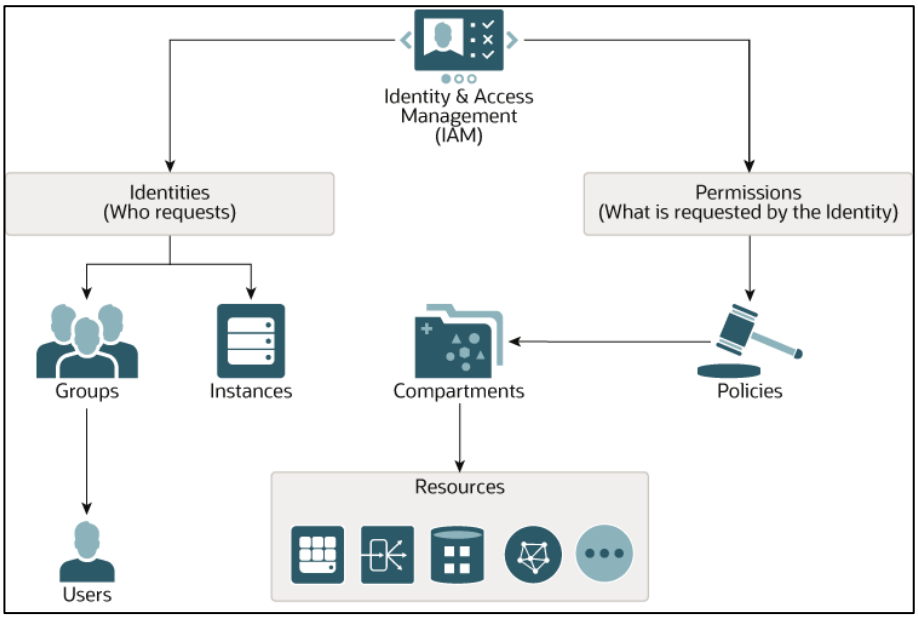
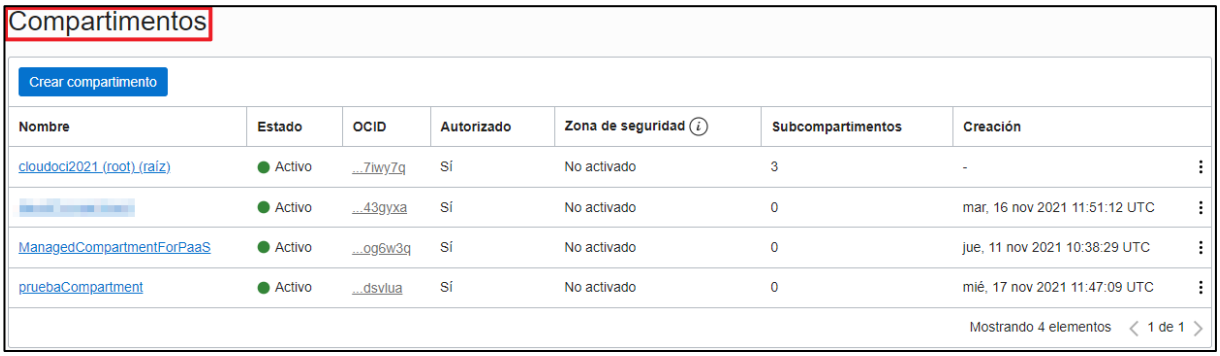
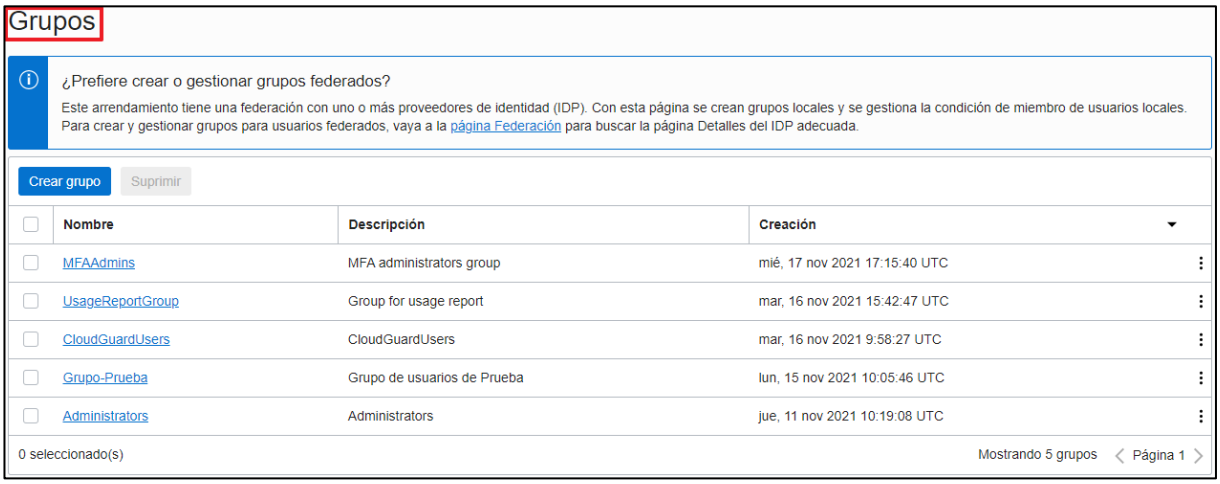


Imagen sobre la relación entre los tres componentes para la asignación de permisos a los usuarios.

Para la configuración de estos objetos, previos a la asignación de derechos a los usuarios, debe acceder a la consola a través del menú principal de OCI → Identidad y seguridad → Identidad.

Desde esta consola, puede acceder al resto de configuraciones necesarias para la correcta asignación de permisos a los usuarios, creando previamente los correspondientes compartimentos, grupos y políticas.





Puede ampliar las recomendaciones de seguridad para OCI IAM en el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/Content/Security/Reference/iam_security.htm

En los siguientes enlaces, puede acceder a la información sobre la gestión de Compartimentos, Grupos y Políticas en el servicio OCI IAM de Oracle:

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

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

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

3.1.1.5 MECANISMO DE AUTENTICACIÓN

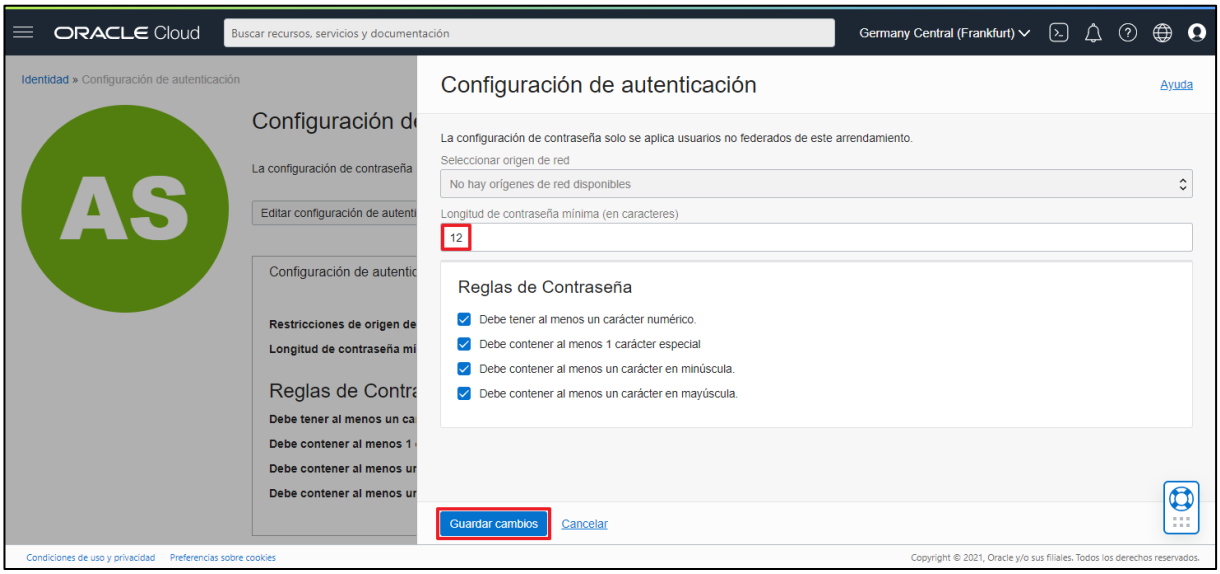
Dentro de los procesos habituales en el manejo de los sistemas de la información, el relativo a la autenticación corresponde al primero a llevar a efecto. Antes de acceder a datos, gestionar recursos o tratar servicios es necesario indicar al sistema "quién eres".

El sistema de autenticación se puede traducir tecnológicamente mediante múltiples mecanismos, siendo el del empleo de una contraseña el más habitual pero no por ello el más seguro, sino todo lo contrario. Los mecanismos de autenticación se deberán adecuar en función del nivel de criticidad de la información o el servicio atendiendo lógicamente a diferentes criterios.

Según establece el propio Esquema Nacional de Seguridad, en el nivel alto, se prohíbe el uso de autenticadores basados en el empleo de claves concertadas y se exige para ello el uso de dispositivos físicos o biometría. Para ello deberán emplearse algoritmos acreditados por el Centro Criptológico Nacional y que Oracle cumple, disponiendo del Certificado de cumplimiento con el ENS en su Categoría Alta.

En cuanto al uso de contraseñas Oracle dispone en el Servicio OCI IAM, a través de la consola accesible del menú principal de OCI → Identidad y seguridad → Configuración de autenticación, para definir la complejidad del uso de contraseñas para los usuarios, así como la longitud de esta.

Para la Categoría Alta, se recomienda una longitud de al menos 12 caracteres y con la máxima complejidad que se pueda establecer, configurándolo desde el botón "Editar configuración de autenticación" y estableciendo el valor del parámetro, como se aprecia en la siguiente imagen. De igual modo se recomienda mantener marcadas todas las "Reglas de Contraseña" para garantizar la robustez de éstas.



Configuración de la longitud de la contraseña modificada para la Categoría Alta del ENS.

La autenticación multifactor (MFA) es un método de autenticación que requiere el uso de más de un factor para verificar la identidad de un usuario y actualmente, Oracle dispone de dos configuraciones según el tipo de usuario.

Nota: Debido al continuo proceso de mejora continua y evolución tecnológica, y en particular a lo que afecta al servicio OCI IAM, el cual se encuentra en pleno cambio durante el desarrollo de esta guía, es posible que alguna información detallada en el documento difiera de la que se encuentre en el momento de aplicar estas medidas.
Por favor, siga los enlaces del fabricante donde le mostrará la información más actualizada acerca de sus servicios. En dicha documentación, el administrador deberá escoger entre IAM con dominios (https://docs.oracle.com/es-ww/iaas/Content/Identity/home.htm) o IAM sin dominios (https://docs.oracle.com/es-ww/iaas/Content/Identity/home1.htm), según aplique en su tenant.

MFA para Usuarios Federados

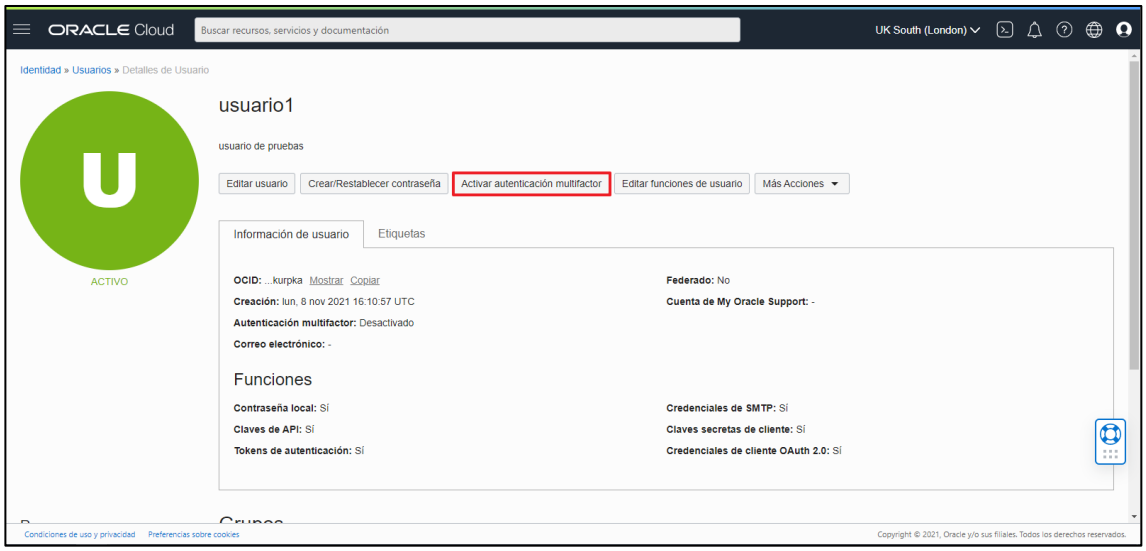
Con la MFA activada en un dominio de identidad, cuando un usuario se conecta a una aplicación, se le solicita su nombre de usuario y contraseña, que es el primer factor, algo que conoce. A continuación, el usuario debe proporcionar un segundo tipo de verificación. Esto se denomina verificación en dos pasos. Los dos factores funcionan conjuntamente para agregar una capa adicional de seguridad mediante el uso de información adicional o un segundo dispositivo para verificar la identidad del usuario y completar el proceso de conexión.

En el siguiente enlace puede ampliar información acerca de la gestión MFA de Oracle para usuarios Federados:

https://docs.oracle.com/es-ww/iaas/Content/Identity/mfa/understand-multi-factor-authentication.htm

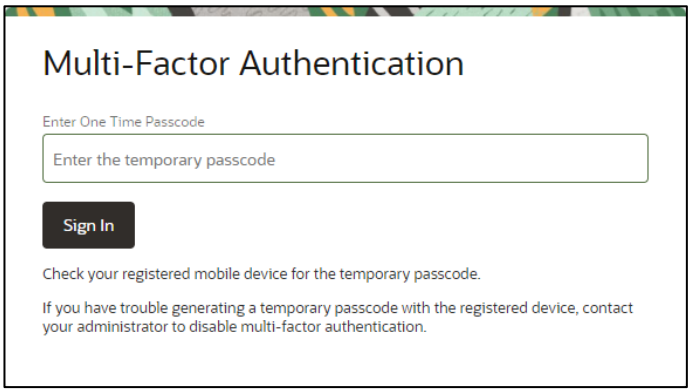
MFA para Usuarios Locales

El servicio OCI IAM, también proporciona acceso utilizando el doble factor de autenticación a los usuarios locales para garantizar la medida del ENS en la Categoría Alta. Esta consola es accesible a través del menú principal de OCI → Identidad y seguridad → Usuarios.



Acceso a la configuración del doble factor desde el perfil de un usuario.

Es necesario instalar una aplicación de autenticación, escanear el código e introducir el código que devuelve la aplicación.



Mensaje de solicitud del código de autenticación proporcionado por la aplicación del dispositivo móvil.

Las aplicaciones de autenticación compatibles con Oracle para el uso del doble factor son, Oracle Mobile Authenticator y Google Authenticator.

Nota: Un administrador no puede activar MFA para otro usuario. Cada usuario debe activar MFA para sí mismo mediante un dispositivo al que tendrá acceso cada vez que se conecte.

Puede comprobar los usuarios que tienen el doble factor configurado mediante el siguiente comando, desde Oracle Shell:

```
oci iam user list --all --output table --query "data [*].{user:\"name\", OCID:id, MFA:\"is-mfa-activated\"}" | grep True
```

Nota: Si desea ver los que no lo tienen activado, cambie el valor final “True” por “False”.

Puede restringir el acceso a los recursos exclusivamente a los usuarios autenticados a través de la autenticación de contraseña de un solo uso basada en tiempo del servicio OCI IAM. Esta restricción se configura en la política que permite el acceso a los recursos.

Para restringir el acceso otorgado a través de una política a los usuarios verificados con MFA, agregue el siguiente comando a la política a la que desee implementar el acceso solo a usuarios con MFA activado:

```
where request.user.mfaTotpVerified='true'
```

Por ejemplo, si su organización tiene una política para permitir al grupo GroupA gestionar instancias y desea agregarle acceso únicamente a los usuarios que utilicen el doble factor de autenticación (MFA), el código quedaría así:

```
allow group GroupA to manage instance-family in tenancy where
request.user.mfaTotpVerified='true'
```

Puede ampliar información acerca de la gestión MFA para usuarios Locales en el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/Content/Identity/Tasks/usingmfa.htm#Managing_MultiFactor_Authentication

3.1.1.6 ACCESO LOCAL Y REMOTO (LOCAL & REMOTE LOGON)

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

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

El Esquema Nacional de Seguridad tiene en cuenta la aplicación de medidas diferentes atendiendo a la criticidad de servicios y sistemas.

Ya desde el nivel más bajo es necesaria la prevención de los ataques para evitar intentos reiterados contra los sistemas de autenticación, limitando el número de intentos y que estos queden registrados, tanto los intentos satisfactorios como los erróneos,

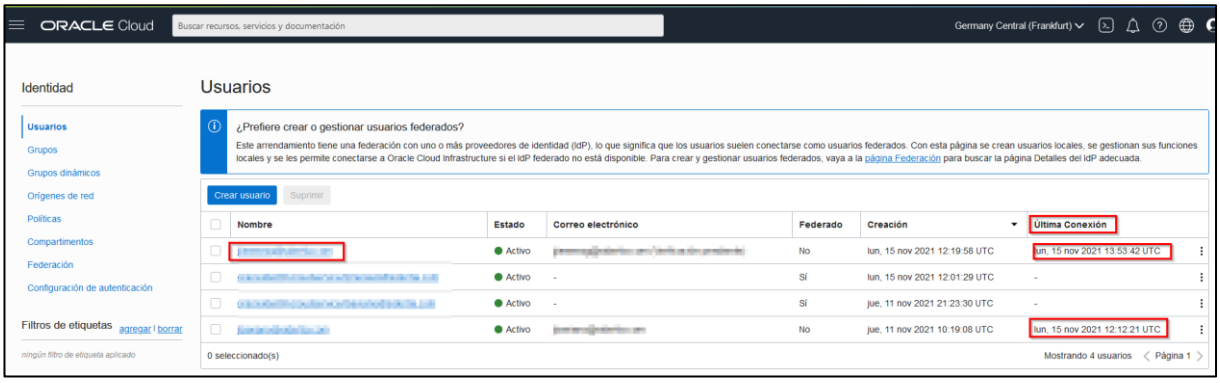
Oracle establece una limitación de 10 intentos de conexión antes de proceder al bloqueo de la cuenta del usuario, que necesitará de un administrador para su desbloqueo.

https://docs.oracle.com/es-ww/iaas/Content/Identity/Tasks/usingmfa.htm#Unblocking_a_User_After_Unsuccessful_Signin_Attempts

Para el nivel alto, se exige la utilización del doble factor de autenticación (MFA) para el acceso a la consola de administración, debiendo informar a los usuarios de sus obligaciones después de obtener el acceso, proporcionándoles el detalle de la última vez que se ha autenticado.

Para poder verificar los inicios de sesión de los usuarios, como indica la norma, OCI IAM proporciona esta información a través de los siguientes menús:

a) Desde la consola de usuarios a través del menú principal de OCI → Identidad y seguridad → Usuarios.



Consola de gestión de usuarios de OCI IAM.

b) Desde el servicio de Auditoría se recogen las acciones de los usuarios con mayor detalle, a través del menú principal de OCI → Observación y gestión → Registro → Auditoría.

Acceso a la Consola de Auditoría, donde realizar búsquedas de los registros.


```
{
  "datetime": 1637168649230
  "logContent": {
    "data": {
      "additionalDetails": {...}
      "availabilityDomain": "AD3"
      "compartmentId": "ocid1.tenancy.oc1..aaaaaaaat64tid7bxdwf72ip6xxqzckfd4xxvmgwy6zsnxgzvn7xtb7iwy7q"
      "compartmentName": "cloudoci2021"
      "definedTags": NULL
      "eventGroupingId": NULL
      "eventName": "ChangePassword"
      "freeformTags": NULL
      "identity": {
        "authType": NULL
        "callerId": NULL
        "callerName": NULL
        "consoleSessionId": NULL
        "credentials": NULL
        "ipAddress": "81.33.31.245"
        "principalId": "ocid1.user.oc1..aaaaaaaayaxp4bbsb33xrl4klx3tqio2sljfhqoas5ct4ayoxn4j2navmkwq"
        "principalName": "usuario2"
        "tenantId": "ocid1.tenancy.oc1..aaaaaaaat64tid7bxdwf72ip6xxqzckfd4xxvmgwy6zsnxgzvn7xtb7iwy7q"
        "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95
      }
      "message": "ChangePassword succeeded"
      "request": {...}
      "resourceId": NULL
      "response": {...}
```


Logs que evidencian la trazabilidad de las acciones realizadas por los usuarios Cambio de clave.


```
{
  "datetime": 1637168593872
  "logContent": {
    "data": {
      "additionalDetails": {...}
      "availabilityDomain": "AD3"
      "compartmentId": "ocid1.tenancy.oc1..aaaaaaaat64tid7bxdwf72ip6xxqzckfd4xxvmgwy6zsnxgzvn7xtb7iwy7q"
      "compartmentName": "cloudoci2021"
      "definedTags": NULL
      "eventGroupingId": NULL
      "eventName": "InteractiveLogin"
      "freeformTags": NULL
      "identity": {
        "authType": NULL
        "callerId": NULL
        "callerName": NULL
        "consoleSessionId": NULL
        "credentials": NULL
        "ipAddress": "81.33.31.245"
        "principalId": "ocid1.user.oc1..aaaaaaaayaxp4bbsb33xrl4klx3tqio2sljfhqoas5ct4ayoxn4j2navmkwq"
        "principalName": "usuario2"
        "tenantId": "ocid1.tenancy.oc1..aaaaaaaat64tid7bxdwf72ip6xxqzckfd4xxvmgwy6zsnxgzvn7xtb7iwy7q"
        "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95
      }
      "message": "InteractiveLogin succeeded"
      "request": {...}
      "resourceId": NULL
      "response": {...}
```


Logs que evidencian la trazabilidad de las acciones realizadas por los usuarios; Acceso de usuario.

Logs que evidencian la trazabilidad de las acciones realizadas por los usuarios; Bloqueo de cuenta de usuario.

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.

OCI dispone del Servicio Tagging (Etiquetado), que permite agregar metadatos a los recursos, lo que brinda la posibilidad de definir claves y valores y asociarlos a recursos, para dar cobertura a la medida y poder gestionar un inventario con el uso de estas etiquetas, pudiendo ser utilizadas para organizar y visualizar los recursos según las necesidades de una organización.

El Servicio Tagging proporciona dos métodos para agregar etiquetas a los recursos. Cada uno de ellos ofrece un tipo de etiqueta diferente con el que trabajar:

a) **Etiquetas definidas**: Los administradores de etiquetas gestionan los metadatos de los recursos.

b) **Etiquetas de formato libre**: Los usuarios aplican metadatos no gestionados a los recursos.

Puede aplicar etiquetas a los recursos para facilitar la organización según las necesidades de negocio. Puede aplicar las etiquetas al crear un recurso o puede actualizar el recurso más tarde con las etiquetas que desee.

En el método de etiquetas definidas, un administrador de etiquetas crea y gestiona todas las etiquetas que los usuarios aplican a los recursos. Utilice la política de OCI IAM para seleccionar los administradores de etiquetas que puedan crear etiquetas. La ventaja de este método es que puede crear y gestionar las claves y los valores que se utilizan para etiquetar recursos. De esta forma, se evitan los errores tipográficos que afectan negativamente a la automatización basada en etiquetas, además de obtenerse una generación de informes mejorada basada en las etiquetas.

En el método de formato libre, los usuarios pueden agregar etiquetas a los recursos. El usuario que crea o modifica un recurso edita o aplica cada una de las etiquetas al recurso.

Puede ampliar la información al respecto de estas etiquetas de recursos a través del siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/Content/General/Concepts/resourcetags.htm

La mayoría de las funciones de Tagging requieren etiquetas definidas. Con "etiqueta" se hace referencia genérica a las etiquetas definidas por la organización y creadas por los administradores de etiquetas. Si desea crear metadatos en los que pueda confiar para gestionar recursos y recopilar datos, utilice las etiquetas definidas.

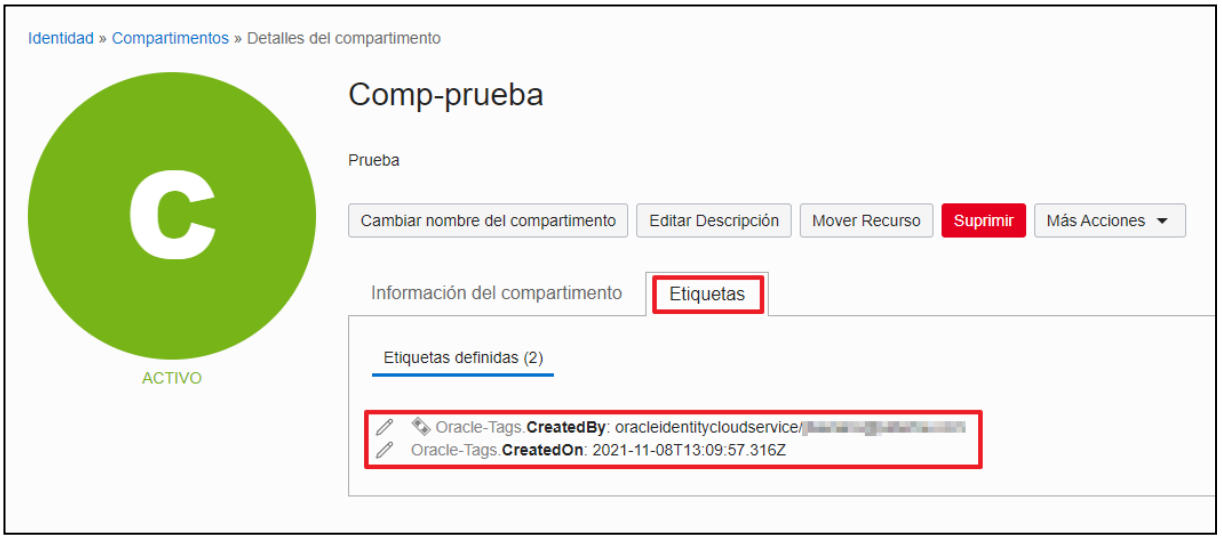


Imagen sobre las etiquetas automáticas establecidas en un recurso ejemplo de tipo Compartimento.

A la hora de crear etiquetas definidas, puede utilizar estas para asignar permisos ya que se pueden añadir como “condiciones” a las políticas definidas para añadir una segregación aun mayor a dichos permisos, identificando en la condición que se cumpla con el contenido definido en las etiquetas.

Puede ampliar el uso de etiquetas para el control de acceso en el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/Content/Tagging/Tasks/managingaccesswithtags.htm

También encontrará la información del Servicio Tagging en el siguiente enlace de Oracle:

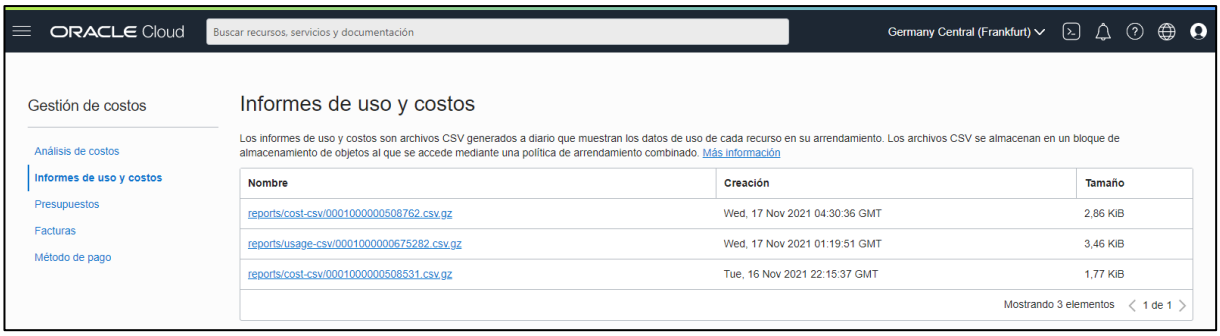
https://docs.oracle.com/es-ww/iaas/Content/Tagging/Concepts/taggingoverview.htm

Si el servicio Tagging (Etiquetado) no fuera suficiente, OCI proporciona una herramienta de terceros para su gestión, denominada "Ansible". La recopilación Ansible de OCI está preinstalada en una imagen de la plataforma Oracle Linux Cloud Developer y es responsabilidad de la organización el despliegue y utilización de esta herramienta para dar cumplimiento de las medidas que establece el ENS.

Puede consultar los requisitos para utilizar Ansible, así como la instalación de la imagen en un sistema operativo Oracle Linux, versión 7 u 8, en el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/Content/API/SDKDocs/ansiblegetstarted.htm#installing_with_yum

Otra forma de gestionar el inventario que ofrece Oracle es a través de los recursos y su consumo. Dentro del menú "Gestión de costos" se puede llevar un control de los recursos del tenant que además son exportables a ficheros CSV para su manipulación posterior, y permiten gestionar dicho inventario.



Ventana de la Gestión de costos para llevar un control del inventario de recursos del tenant.

3.1.2.2 CONFIGURACIÓN DE SEGURIDAD

En cuanto a la configuración de seguridad, el ENS establece que los equipos deben cumplir unos parámetros mínimos para su entrada en operación.

Los equipos, antes de su entrada en producción, deberán configurarse de tal forma que:

a) Se retiren cuentas y contraseñas estándar.

b) Se aplique la regla de mínima funcionalidad.

Se considera indispensable que el sistema no proporcione funcionalidades gratuitas, solamente las estrictamente necesarias. Esto permitirá adaptarse al principio de mínima exposición. Para ello se eliminarán o desactivarán aquellas funciones que no sean de interés, que no sean necesarias e incluso aquellas que sean inadecuadas al fin que se persigue.

Adicionalmente se deshabilitarán, como parte de los mecanismos de mínima funcionalidad y exposición de la información manejada, todos aquellos procesos que pudieran implicar el envío de información al fabricante o todos aquellos servicios automatizados susceptibles de reportar datos o funcionalidad de los servidores.

Esta medida se aplica de forma automática desde OCI, al contemplar la funcionalidad mínima de los recursos cuando se crean como, por ejemplo, a la hora de crear una red donde por defecto solo se abre el puerto 22 para acceso SSH y no se conceden permisos a las cuentas o grupos de seguridad, salvo a la cuenta que creó el recurso. El resto de las funcionalidades y permisos se deben gestionar tras la creación de los recursos.

En el siguiente enlace, Oracle proporciona orientación y recomendaciones útiles para configurar de forma segura Servicios específicos en OCI:

https://docs.oracle.com/es-ww/iaas/Content/Security/Reference/configuration_security.htm

3.1.2.3 GESTIÓN DE LA CONFIGURACIÓN

Esta medida se encarga de gestionar la configuración de todos los componentes del sistema para mantener una mínima funcionalidad, una seguridad por defecto, una adaptabilidad para nuevas necesidades, así como reaccionar ante vulnerabilidades e incidentes y su posterior gestión de cambios.

A este respecto, OCI dispone del Servicio Cloud Guard para su gestión, siendo responsabilidad de la organización la configuración del servicio según sus políticas internas de seguridad.

Para ello, debe dirigirse al menú de OCI → Identidad y seguridad → Cloud Guard y activarlo.

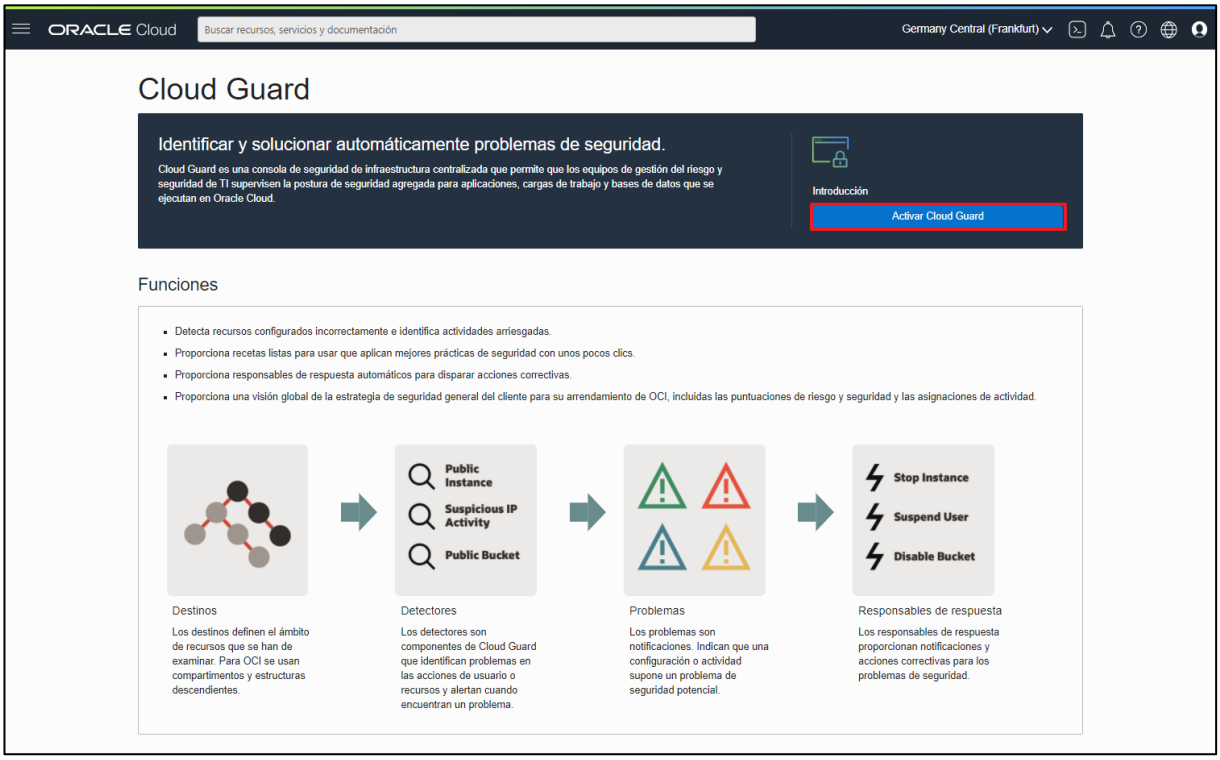
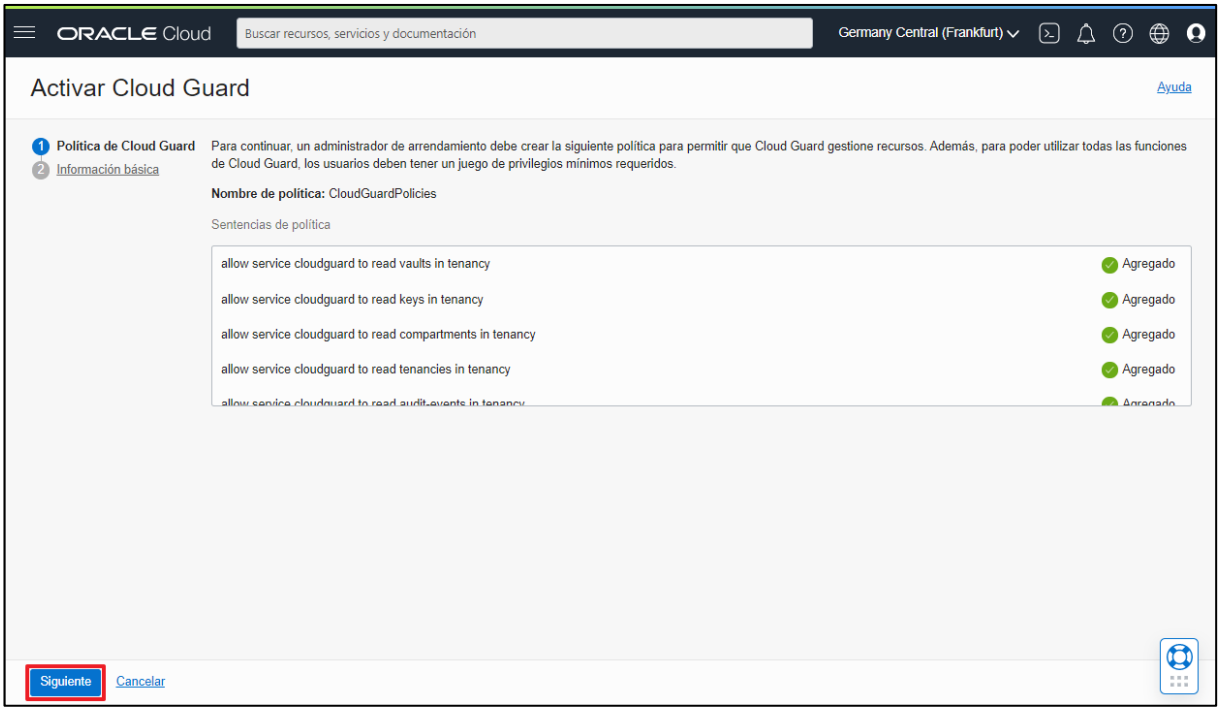


Imagen del servicio Cloud Guard para su activación y configuración.



Asistente para la activación del servicio Cloud Guard.

Tras activar el servicio, el asistente informa que se debe crear una política para permitir la gestión de los recursos desde Cloud Guard con las siguientes sentencias:

```
allow service cloudguard to read vaults in tenancy
allow service cloudguard to read keys in tenancy
allow service cloudguard to read compartments in tenancy
allow service cloudguard to read tenancies in tenancy
allow service cloudguard to read audit-events in tenancy
allow service cloudguard to read compute-management-family in tenancy
allow service cloudguard to read instance-family in tenancy
allow service cloudguard to read virtual-network-family in tenancy
allow service cloudguard to read volume-family in tenancy
allow service cloudguard to read database-family in tenancy
allow service cloudguard to read object-family in tenancy
allow service cloudguard to read load-balancers in tenancy
allow service cloudguard to read users in tenancy
allow service cloudguard to read groups in tenancy
allow service cloudguard to read policies in tenancy
allow service cloudguard to read dynamic-groups in tenancy
allow service cloudguard to read authentication-policies in tenancy
allow service cloudguard to use network-security-groups in tenancy
allow service cloudguard to read data-safe-family in tenancy
```

En el siguiente paso, en Información básica, se seleccionará la región de informe y las recetas por defecto que establece Oracle.

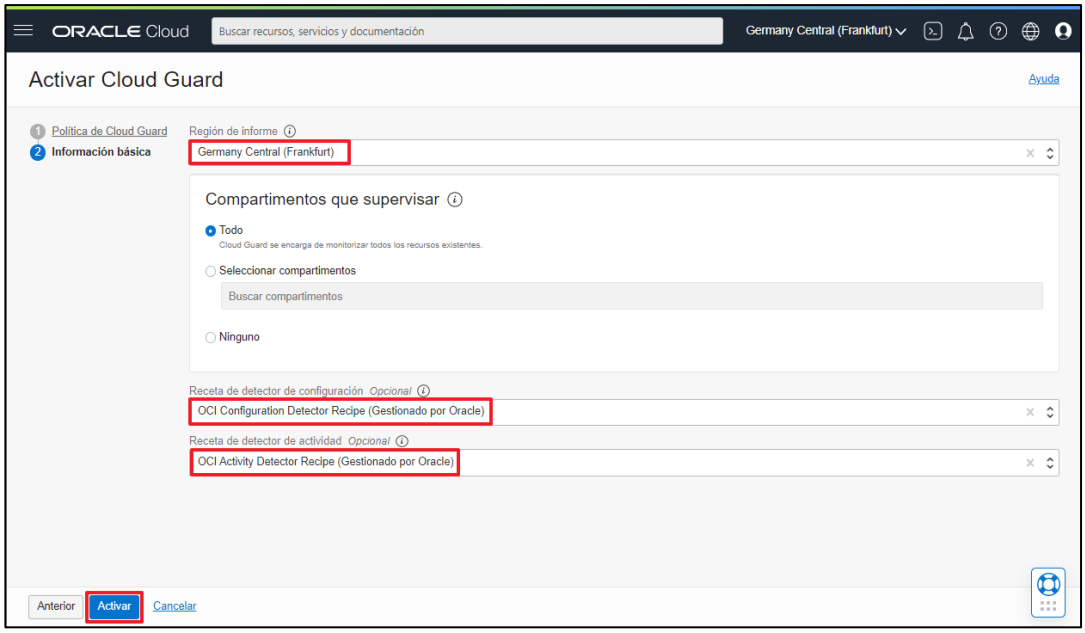


Imagen con los campos necesarios a cumplimentar para activar el Servicio Cloud Guard en el tenant.

Una vez activado el servicio, ya puede acceder al mismo desde el siguiente botón de la ventana de finalización o desde el menú OCI → Identidad y seguridad → Cloud Guard.

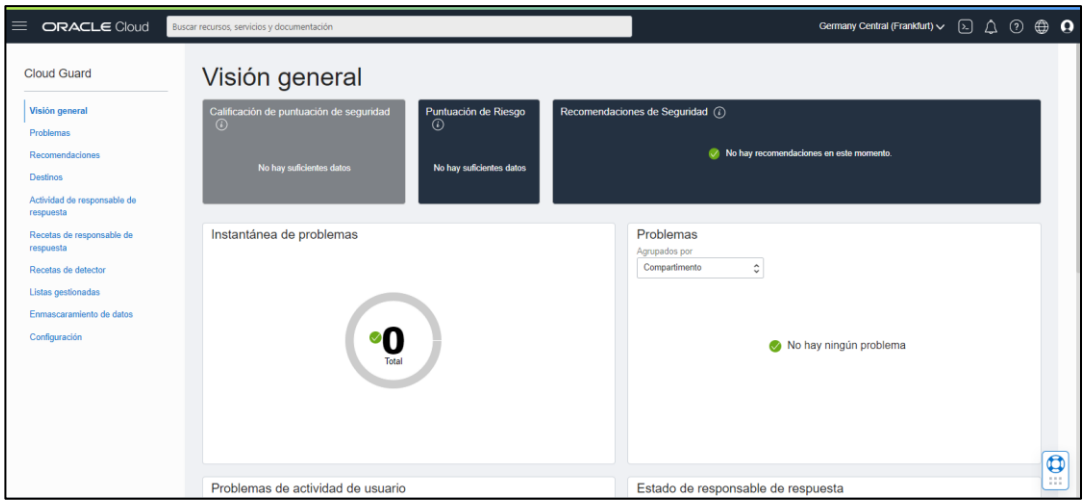


Imagen de la visión general del estado del tenant.

Puede ampliar la información acerca del Servicio Cloud Guard, la gestión de vulnerabilidades y de incidentes en los siguientes enlaces:

https://docs.oracle.com/es-ww/iaas/cloud-guard/using/cg-concepts.htm

https://docs.oracle.com/es-ww/iaas/Content/Security/Reference/responses_to_vulnerabilities.htm

https://docs.oracle.com/es-ww/iaas/scanning/using/overview.htm

3.1.2.4 MANTENIMIENTO

La medida establece una seguridad mínima que se aplica de igual forma en las 3 categorías del ENS, y que puede ser configurada desde el Servicio OS Management para Windows en OCI.

Para mantener el equipamiento 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.

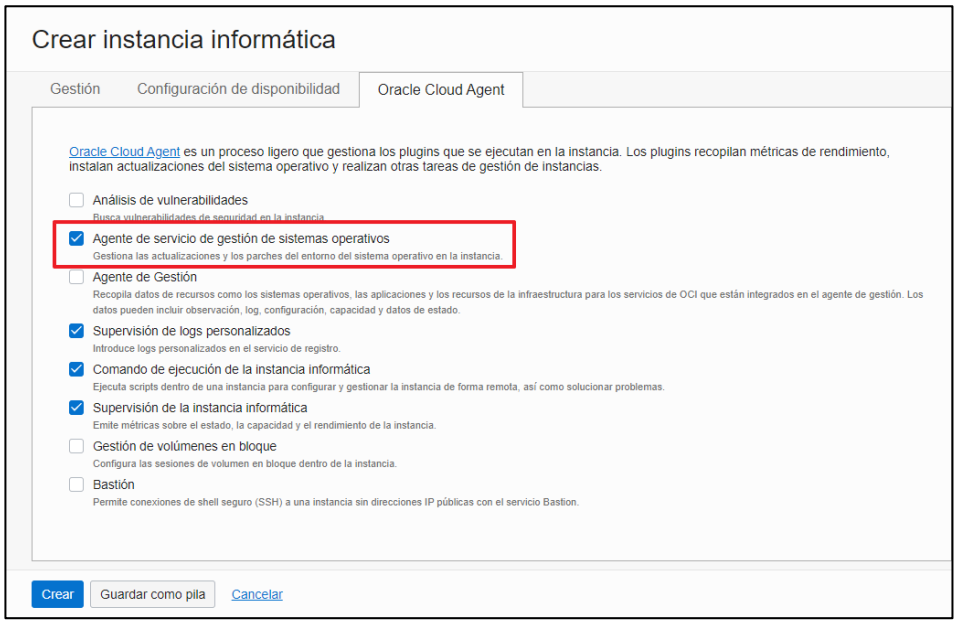
b) Se efectuará un seguimiento continuo de los anuncios de defectos.

c) 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 aplicación o no de la actualización.

No es objeto de esta guía especificar los mecanismos a emplear para mantener actualizados los sistemas ni la prioridad de los mismos, que caen del lado de la organización y sus políticas de seguridad.

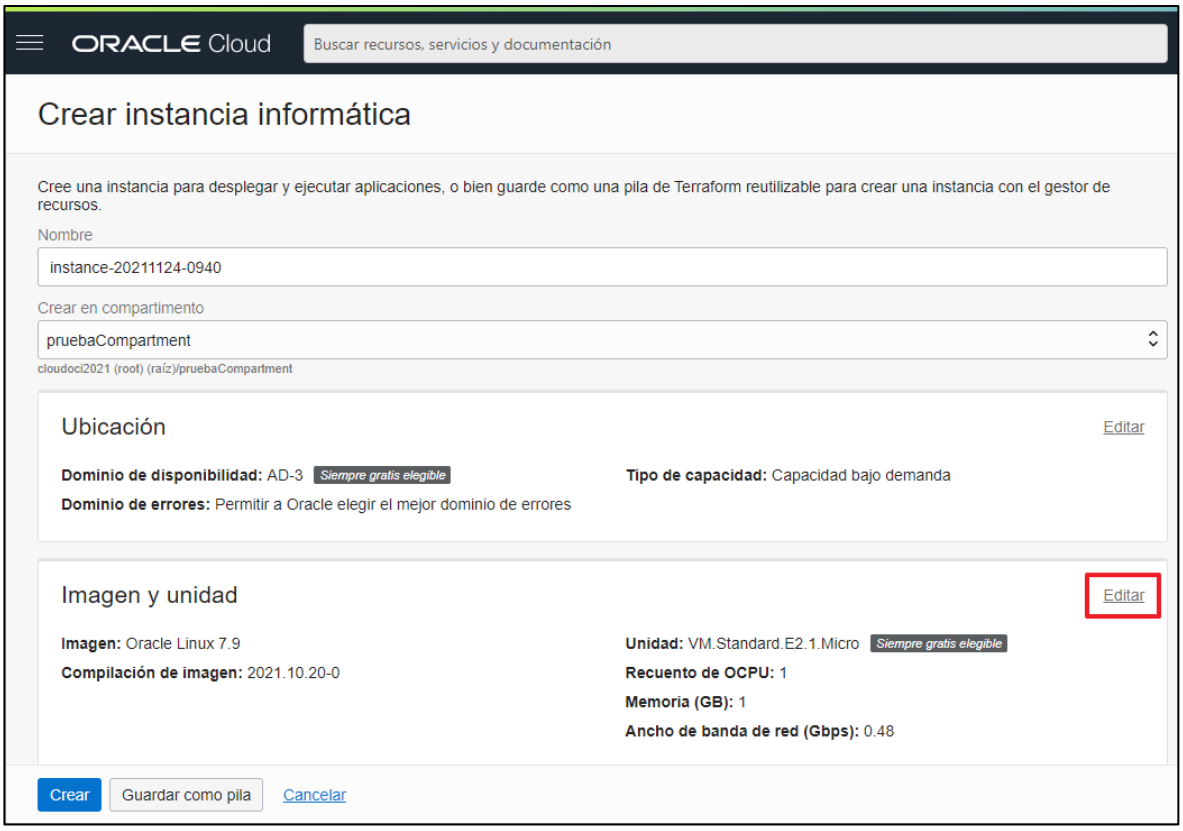
Para esta medida, OCI dispone de varios servicios y herramientas que se encargarán de mantener los sistemas, por ejemplo:

a) Servicio OS Management para Windows:

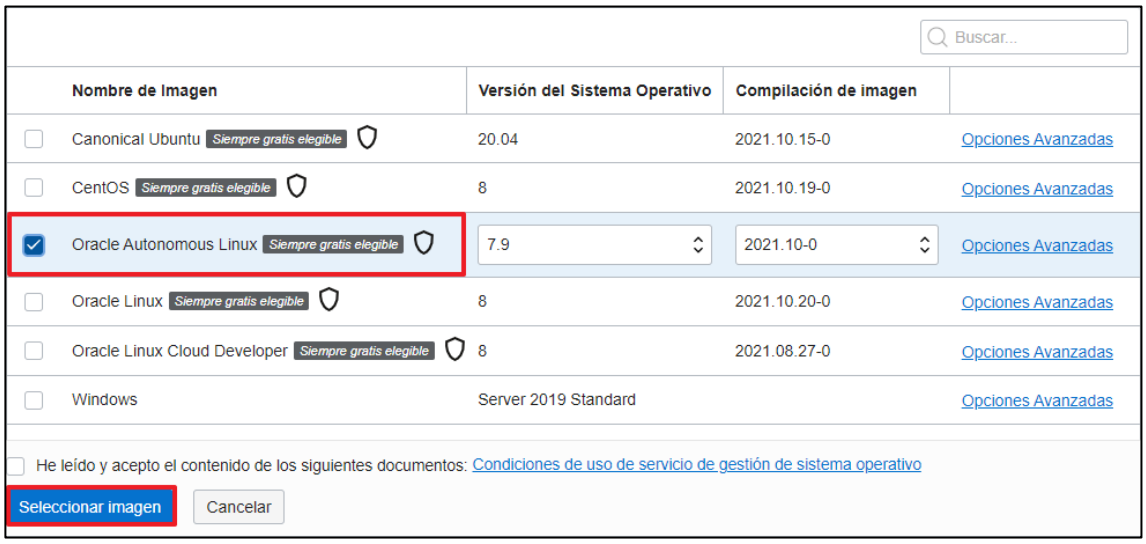


Instalación del agente de servicio de gestión de sistemas operativos para las actualizaciones y parches.

b) Autonomous Linux:



Una vez editada la imagen, Enel botón “Cambiar la imagen”, podrá seleccionar las imágenes “Autonomous” autogestionadas por Oracle para su mantenimiento.



3.1.2.5 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”.

Oracle implementa software antivirus/malware en los sistemas utilizados por los servicios OCI, sin embargo, los clientes son responsables de implementar las soluciones anti-malware en su propio entorno. OCI pone a disposición un servicio de escaneo de vulnerabilidades que es nativo de Oracle.

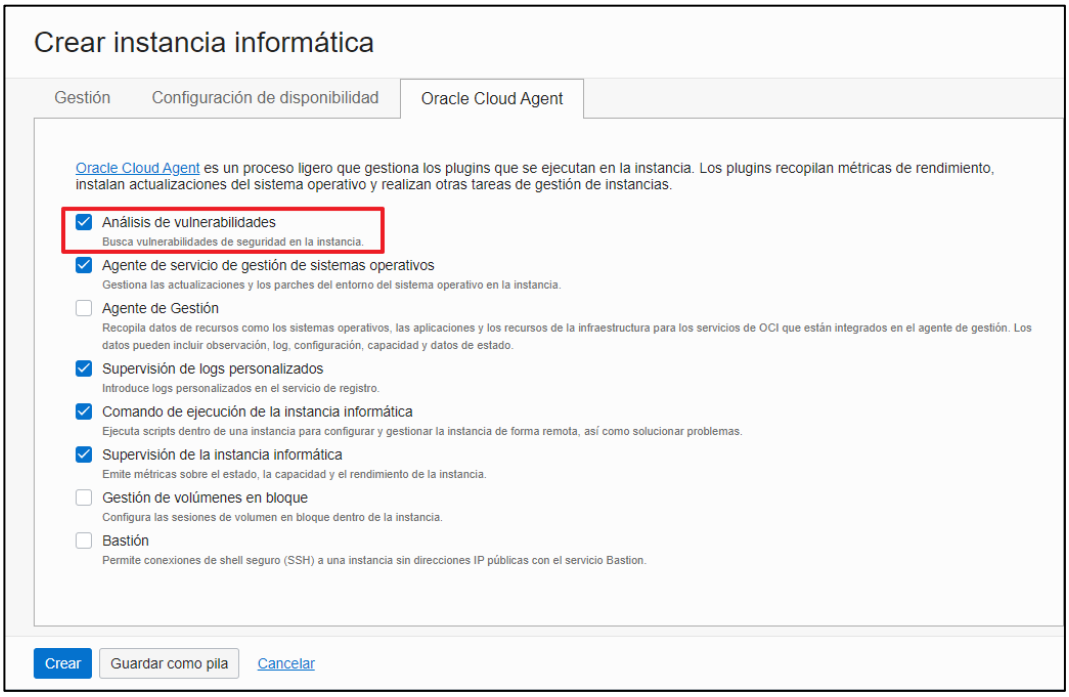


Imagen de la creación de una instancia, habilitando el escaneo de vulnerabilidades desde OCI.

Los sistemas de detección de seguridad, incluidos NIDS y Anti-malware, están configurados para actualizarse automáticamente al menos cada 24 horas. Los clientes son responsables de configurar los ajustes de actualización para sus sistemas.

No es objeto de esta guía indicar cómo se deben configurar estos productos, pero si mostrarlos para que la organización haga uso de ellos para cumplir las medidas que establece el ENS al respecto.

Para controlar cómo se exploran los recursos es necesario crear una “receta de exploración” a través del menú de OCI → Identidad y seguridad → Explorando → Recetas de exploración.

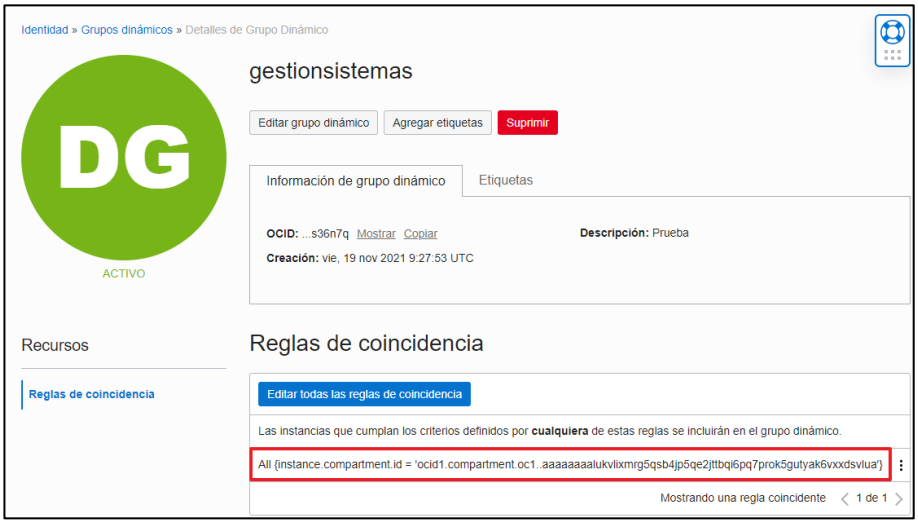
Imagen de los parámetros de una receta de exploración de ejemplo.

Para que la receta actúe, es necesario crear un grupo dinámico concediendo permisos a las instancias de un compartimento. Puede ampliar la información sobre los Grupos dinámicos en OCI IAM mediante el siguiente enlace de Oracle:

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

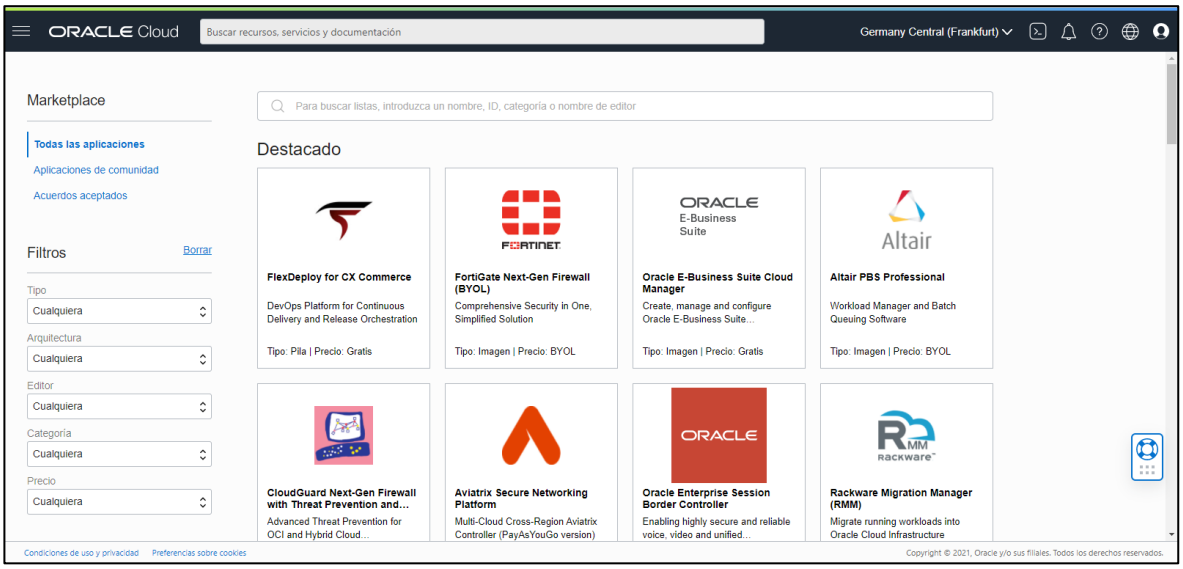
Por ejemplo, cree un grupo dinámico denominado “gestionsistemas”, y agregue la regla de coincidencia siguiente:

All {instance.compartment.id = '[OCI ID del compartimento de las instancias a explorar]'}



Ejemplo de Grupo dinámico con la regla definida para todas las instancias de un compartimento del tenant.

Adicionalmente en OCI se pueden desplegar herramientas de seguridad de terceros disponibles en el Marketplace de OCI, para un despliegue más rápido. La consola está accesible a través del menú principal de OCI → Marketplace.



Sitio del Marketplace desde donde poder desplegar herramientas de seguridad de terceros.

Para ampliar la información acerca del Servicio Marketplace y la disponibilidad de las herramientas de terceros, puede seguir el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/Content/Marketplace/Concepts/marketoverview.htm

3.1.2.6 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) Procedimiento de reporte de incidentes reales o sospechosos, detallando el escalado de la notificación.

b) Procedimiento de toma de medidas urgentes, incluyendo la detención de servicios, el aislamiento del sistema afectado, la recogida de evidencias y protección de los registros, según convenga al caso.

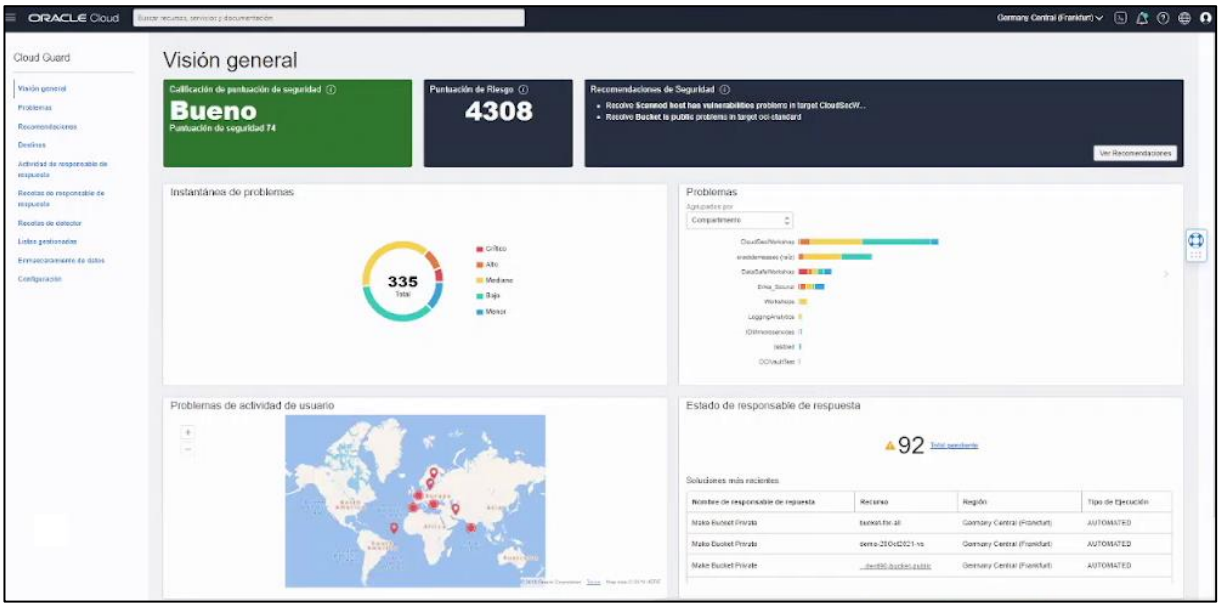
c) Procedimiento de asignación de recursos para investigar las causas, analizar las consecuencias y resolver el incidente.

d) Procedimientos para informar a las partes interesadas, internas y externas.

e) Procedimientos para prevenir la repetición de un incidente, así como incluir en los procedimientos de usuario la identificación y forma de tratar el incidente y actualizar, extender, mejorar u optimizar los procedimientos de resolución de incidentes.

Aunque es una medida más procedimental que técnica, OCI tiene disponibles servicios que apoyan, reportan y previenen estos incidentes para minimizar los riesgos, como el Servicio Cloud Guard y el Servicio OCI IAM.

Cloud Guard ofrece un panel de control con una visión general del estado de seguridad a través de una calificación de puntuación de seguridad y de riesgos, por los que realiza posteriormente recomendaciones al respecto.



Ejemplo de dashboard del servicio de Cloud Guard con el estado y puntuación del nivel de seguridad del tenant.

Puede ampliar la información acerca de la gestión de problemas desde el servicio de Cloud Guard a través del siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/cloud-guard/using/part-problems.htm

3.1.2.7 REGISTRO DE LA ACTIVIDAD DE LOS USUARIOS

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

a) Quién realiza la actividad, cuándo la realiza y sobre qué.

b) La actividad de los usuarios y especialmente la de los operadores y administradores del sistema en el momento en que pueden acceder a la configuración y actuar en el mantenimiento del mismo.

c) Las actividades realizadas con éxito, así como los intentos fallidos.

d) La determinación de las actividades y el nivel de detalle se determinarán en base al análisis de riesgos que se haya realizado sobre el sistema.

El ENS establece la activación de los registros de actividad en los sistemas para recoger las actividades mencionadas con anterioridad, indicando que se deben revisar los registros activados para buscar patrones anormales y añade para esta Categoría Alta que se debe disponer de un sistema automático de recolección de eventos, o sea, una consola de seguridad centralizada. OCI dispone del servicio OCI Audit, el cual recolecta y centraliza los eventos relacionados con las actividades de los usuarios.

El Servicio Audit de OCI registra automáticamente llamadas a todos los puntos finales soportados de la interfaz pública de programación de aplicaciones (API) de OCI como eventos de log. Actualmente, todos los servicios soportan el registro mediante Audit. El Servicio Almacenamiento de Objetos admite el registro de eventos relacionados con los buckets (cubos), pero no de eventos relacionados con objetos concretos. Los eventos de log registrados por el Servicio Audit incluyen llamadas a la API realizadas por la consola de OCI, la interfaz de línea de comandos (CLI), Software Development Kits (SDK), sus propios clientes personalizados u otros servicios de OCI. La información que se incluye en los logs incluye lo siguiente:

a) Hora a la que se ha producido la actividad de API.

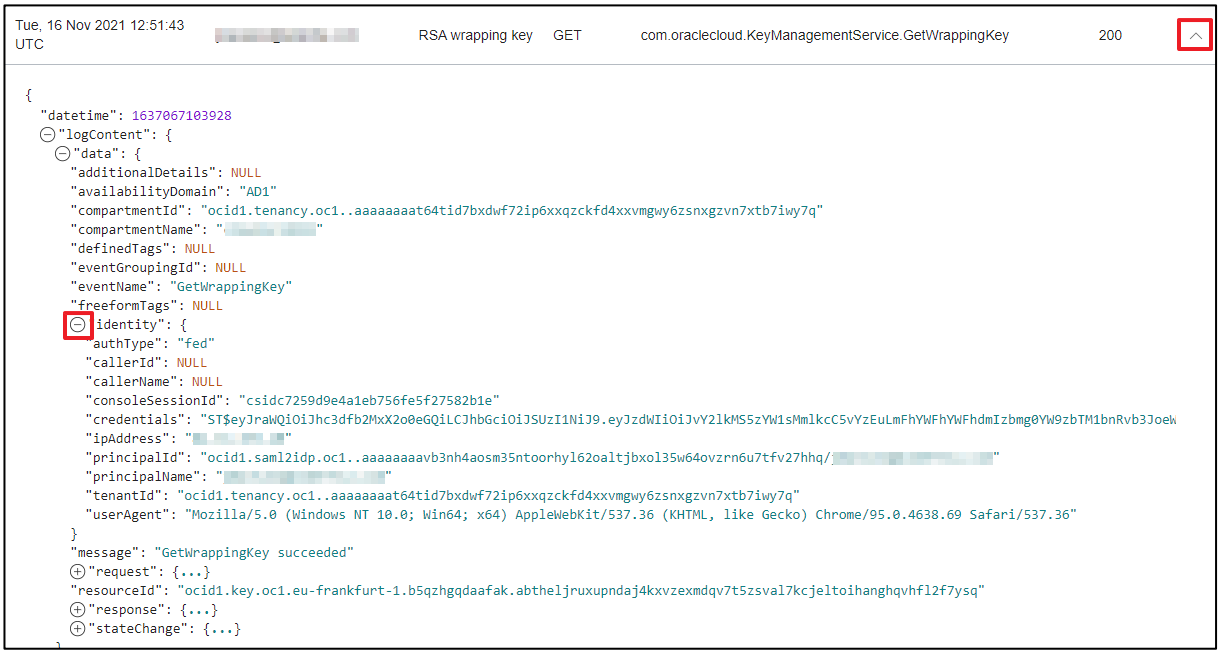
b) Origen de la actividad.

c) Destino de la actividad.

d) Tipo de acción.

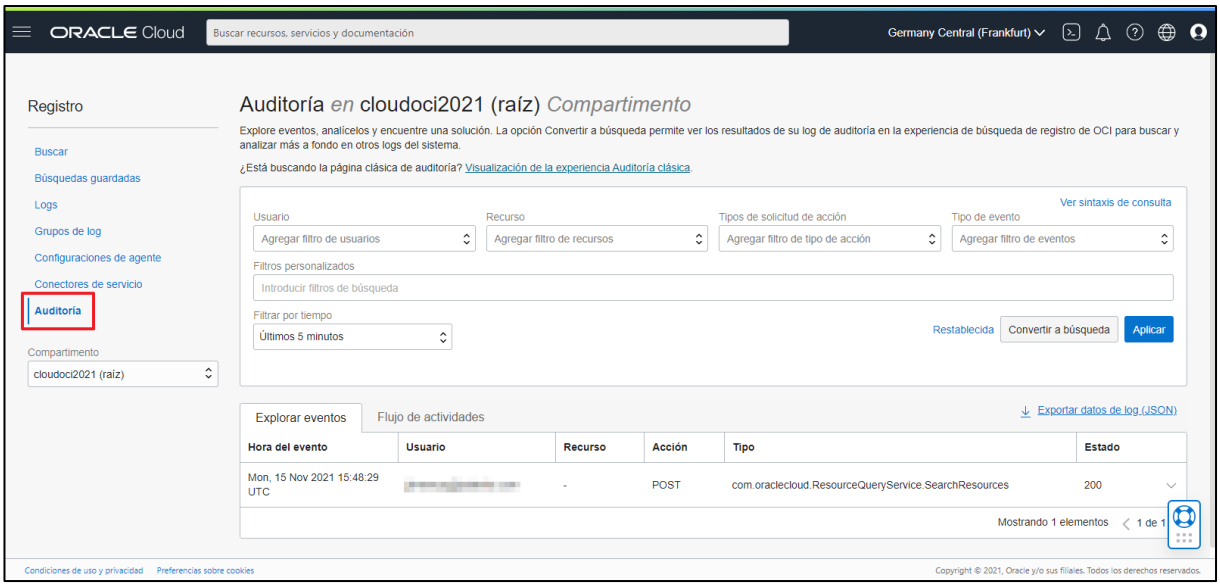
e) Tipo de respuesta.

Cada evento de log incluye un ID de cabecera, recursos de destino, registro de hora del evento registrado, parámetros de solicitud y de respuesta. Puede ver los eventos registrados por el servicio Audit mediante la consola, la API o el SDK para Java. Los datos de eventos se pueden utilizar para realizar diagnósticos, realizar un seguimiento del uso de recursos, supervisar la conformidad y recopilar eventos relacionados con la seguridad.

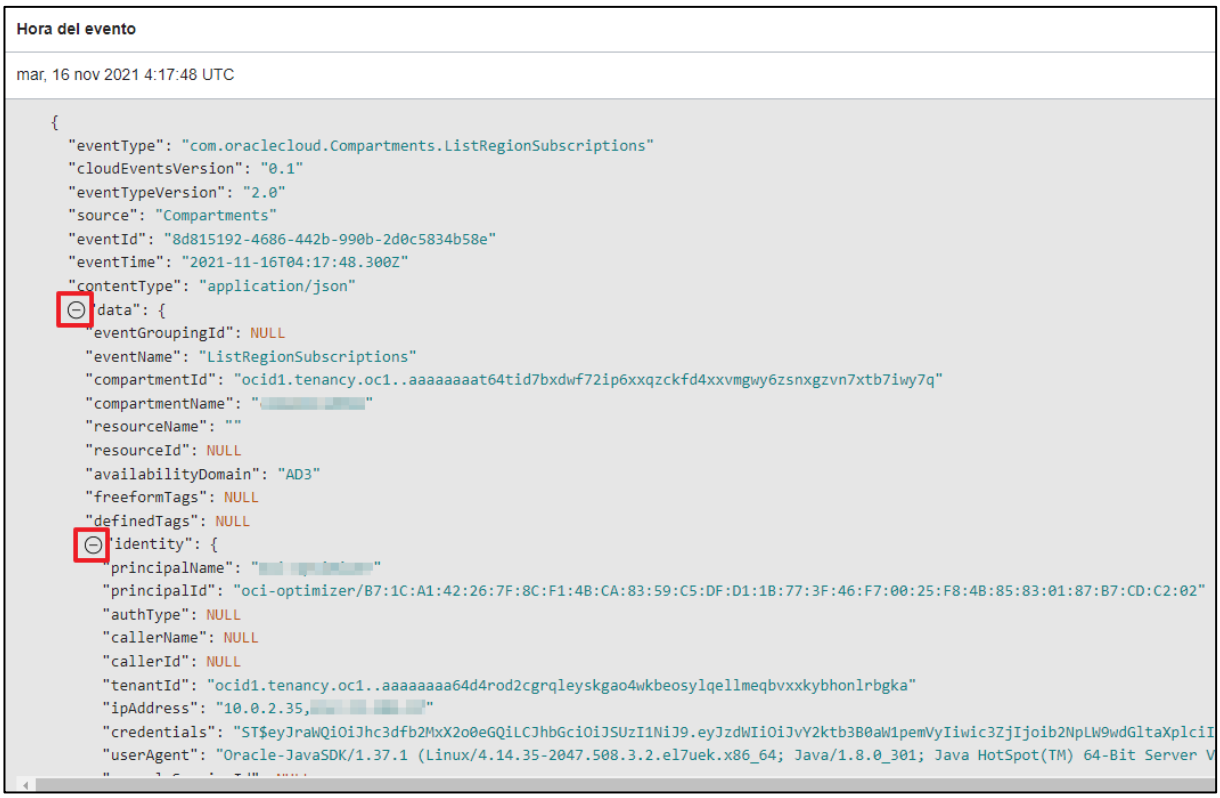


Detalle extendido de la información de un Registro de Auditoría.

Al servicio Audit se accede desde OCI → Observación y gestión → Registro → Auditoría.



Visualización del Servicio de Auditoría de registros en OCI.



Detalle extendido de los componentes de un registro de auditoría donde se muestra más información.

3.1.2.8 REGISTRO DE LA GESTIÓN DE INCIDENTES

Esta medida indica la necesidad de registrar todas las actuaciones relacionadas con la gestión de incidentes, de forma que:

a) Se registrará el reporte inicial, las actuaciones de emergencia y las modificaciones del sistema derivadas del incidente.

Se registrará aquella evidencia que pueda, posteriormente, sustentar una demanda judicial, o hacer frente a ella, cuando el incidente pueda llevar a actuaciones disciplinarias sobre el personal interno, sobre proveedores externos o a la persecución de delitos. En la determinación de la composición y detalle de estas evidencias, se recurrirá a asesoramiento legal especializado.

Como consecuencia del análisis de los incidentes, se revisará la determinación de los eventos auditables.

Oracle ofrece la gestión de los registros de los incidentes de seguridad a través del Servicio Cloud Guard para cliente y también mediante la aplicación PagerDuty que puede implementar desde el Servicio de Marketplace.

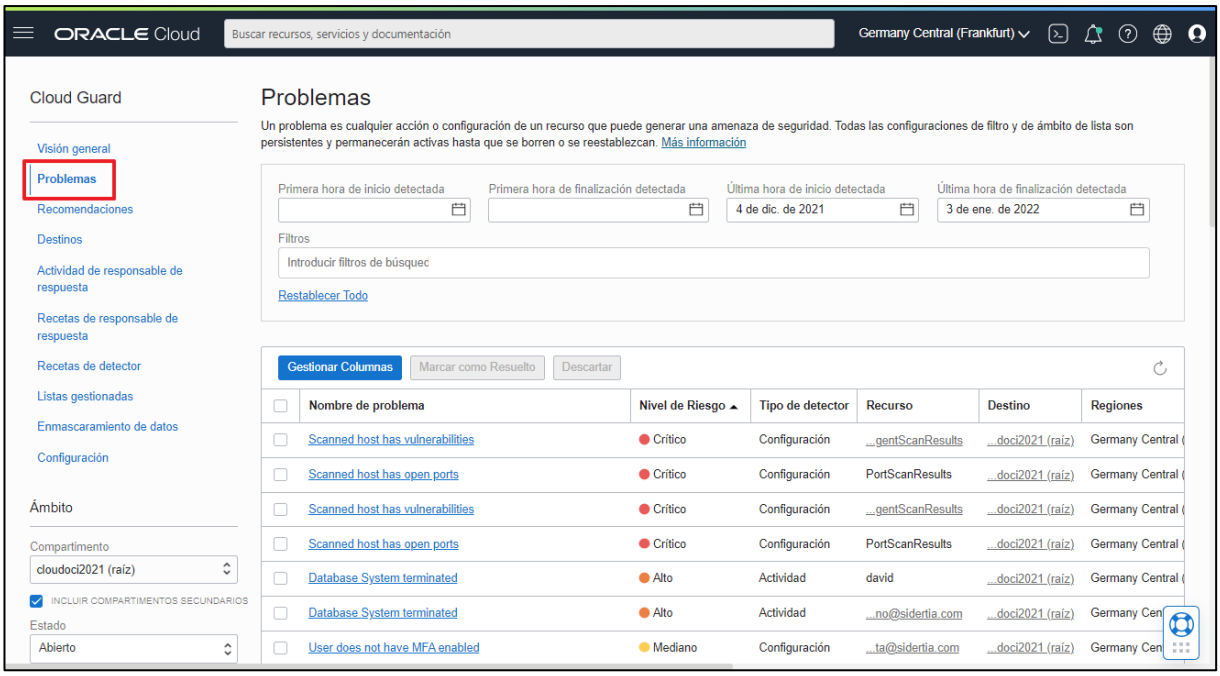


Imagen de los incidentes de seguridad detectados como problemas en Cloud Guard.

Puede ampliar la información sobre la gestión de incidentes mediante el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/cloud-guard/using/export-notifs-config.htm

Puede consultar más información acerca de la herramienta PagerDuty a través del siguiente enlace de Oracle:

https://cloudmarketplace.oracle.com/marketplace/es_ES/listing/97287453/

3.1.2.9 PROTECCIÓN DE CLAVES CRIPTOGRÁFICAS

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

Para cumplir con la correcta protección de las claves criptográficas OCI cuenta con el Servicio Vault, que permite gestionar de forma central las claves de cifrado que protegen los datos y las credenciales secretas que se utilizan para acceder de forma segura a los recursos. Los almacenes guardan de manera segura secretos y claves de cifrado maestras que puede almacenar en los archivos de configuración o en el código. Específicamente, según el modo de protección, las claves se almacenan en el servidor o se almacenan en módulos de seguridad de hardware altamente disponibles y duraderos (HSM) que cumplen con la certificación de seguridad de nivel 3 de seguridad de los estándares de procesamiento de información federal (FIPS) 140-2.

Puede utilizar el servicio Vault para crear y gestionar almacenes, claves y secretos o delegar en OCI la gestión de las claves en Oracle y que estas sean transparentes para el cliente.

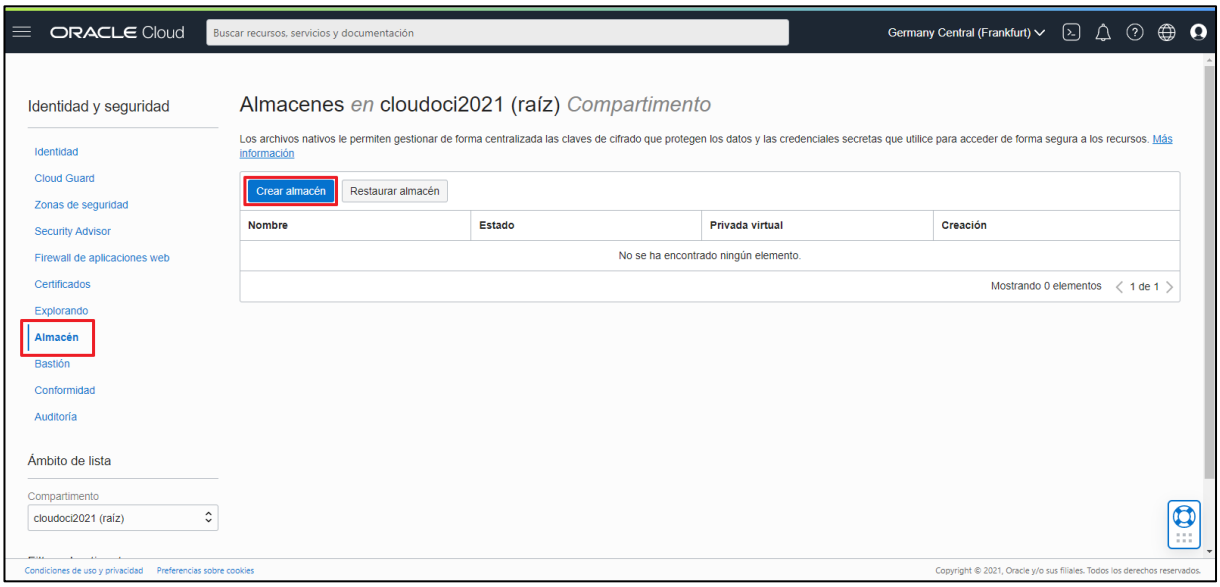
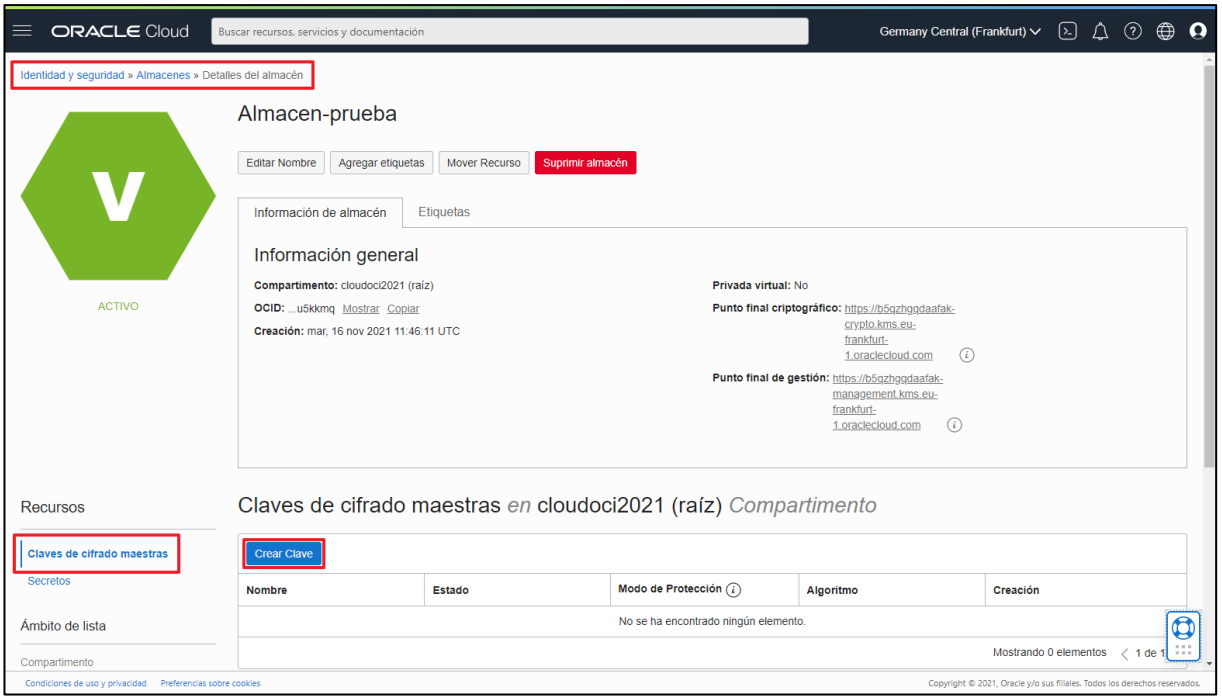


Imagen del Servicio Vault de OCI para el Almacén de claves y credenciales secretas de datos y recursos.

Tras crear un Almacén para el guardado de las claves y secretos, es necesario crear las claves y/o secretos para un compartimento.



Detalle de un Almacén donde poder crear claves de cifrado y secretos para un compartimento.

Nota: Antes de crear un secreto, necesita al menos una clave de cifrado activada en el almacén.

A continuación, dispone de un enlace de Oracle donde puede ampliar la información acerca del servicio Vault.

https://docs.oracle.com/es-ww/iaas/Content/KeyManagement/Concepts/keyoverview.htm

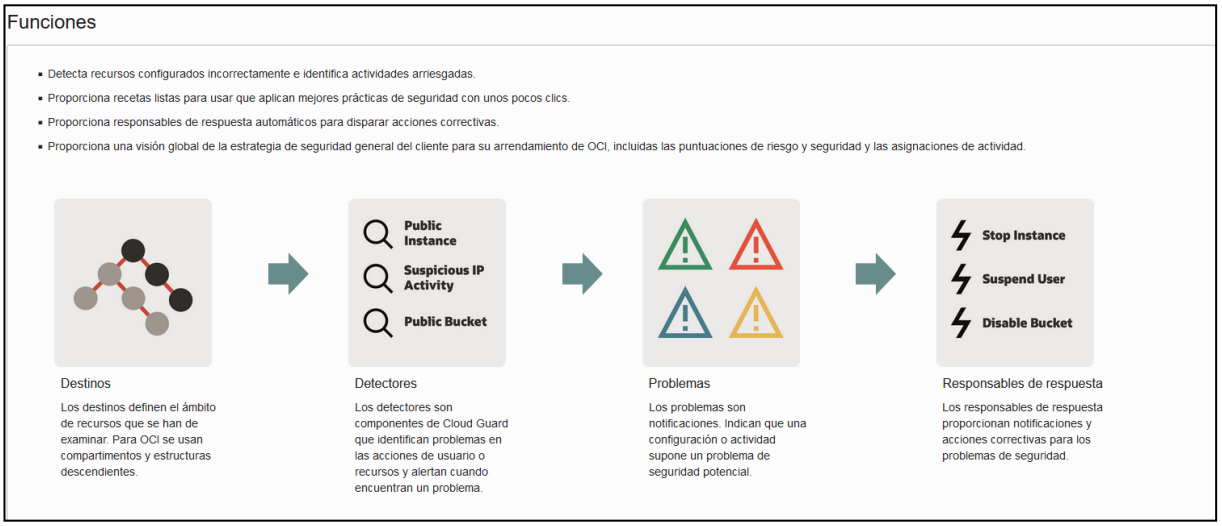
3.1.3 MONITORIZACIÓN DEL SISTEMA

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 35 del RD 3/2010, de 8 de enero, por el que se regula el ENS.

3.1.3.1 DETECCIÓN DE INTRUSIÓN

La medida indica que se debe disponer de herramientas de detección o de prevención de intrusión. Para ello, OCI dispone de varias posibilidades o herramientas:

a) Servicio Cloud Guard.

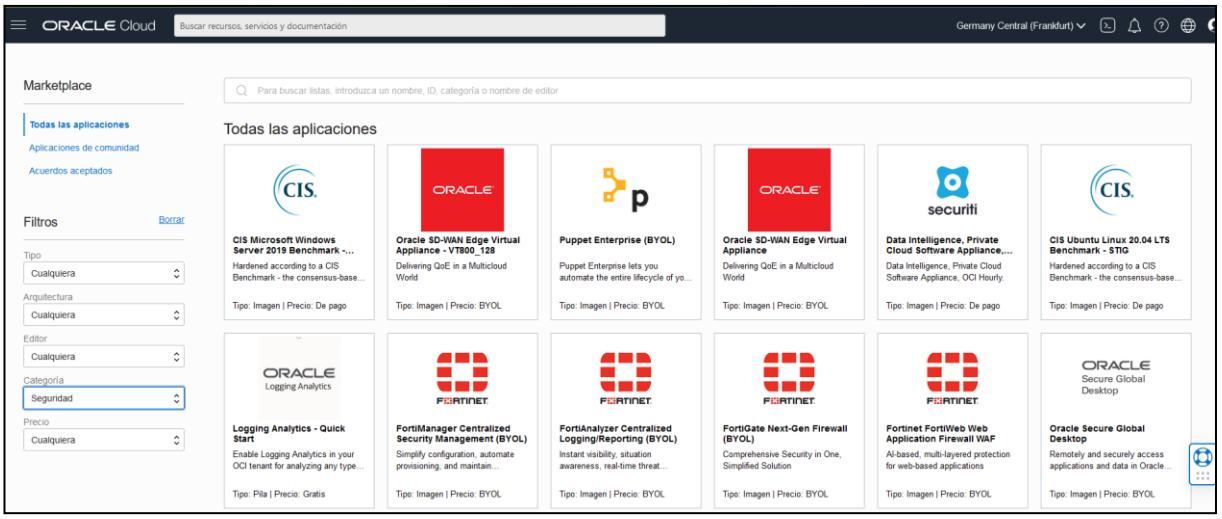


Puede ampliar la información sobre Cloud Guard en el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/cloud-guard/using/cg-concepts.htm

b) Aplicaciones del Servicio MarketPlace.

Este servicio ofrece a los usuarios y clientes una tienda online con soluciones específicas de terceros enlazadas en función de las diferentes categorías.



Detalle de posibilidades de implantación de herramientas de terceros a través de este servicio.

Puede ampliar la información sobre MarketPlace en el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/Content/Marketplace/Concepts/marketoverview.htm

c) Servicio de Informes de vulnerabilidades.

La creación de Informes de vulnerabilidades permite la generación y automatización de procesos rutinarios para poder detectar posibles vulnerabilidades. Existen varias opciones dentro de esta característica, como escaneos de puertos e identificación de parches o actualizaciones para determinados sistemas o servicios.

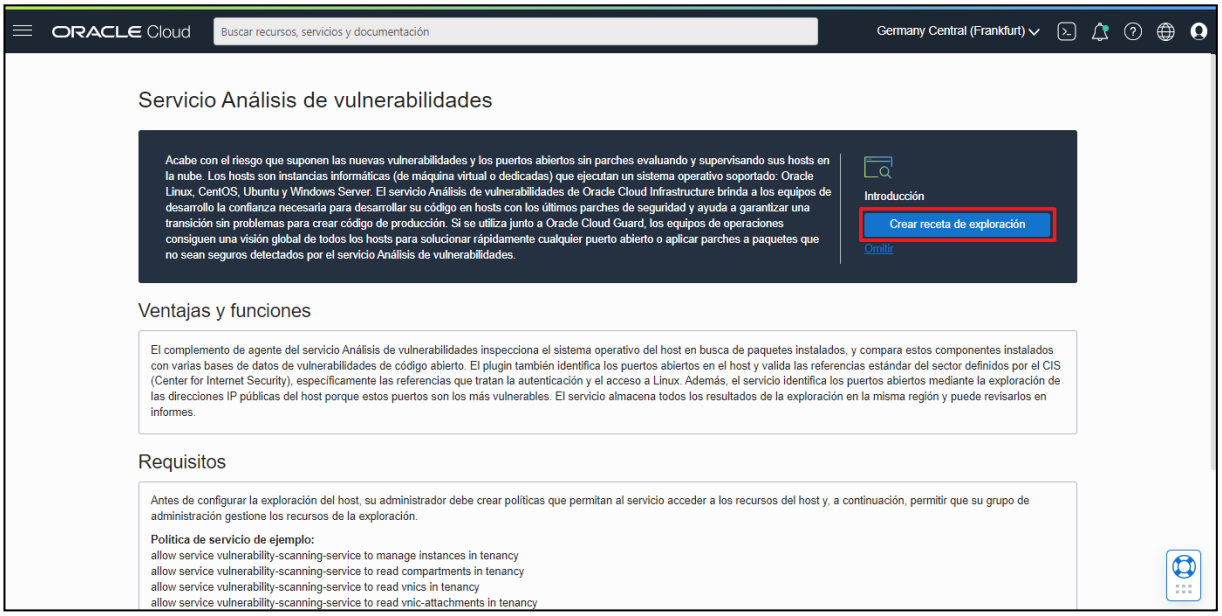
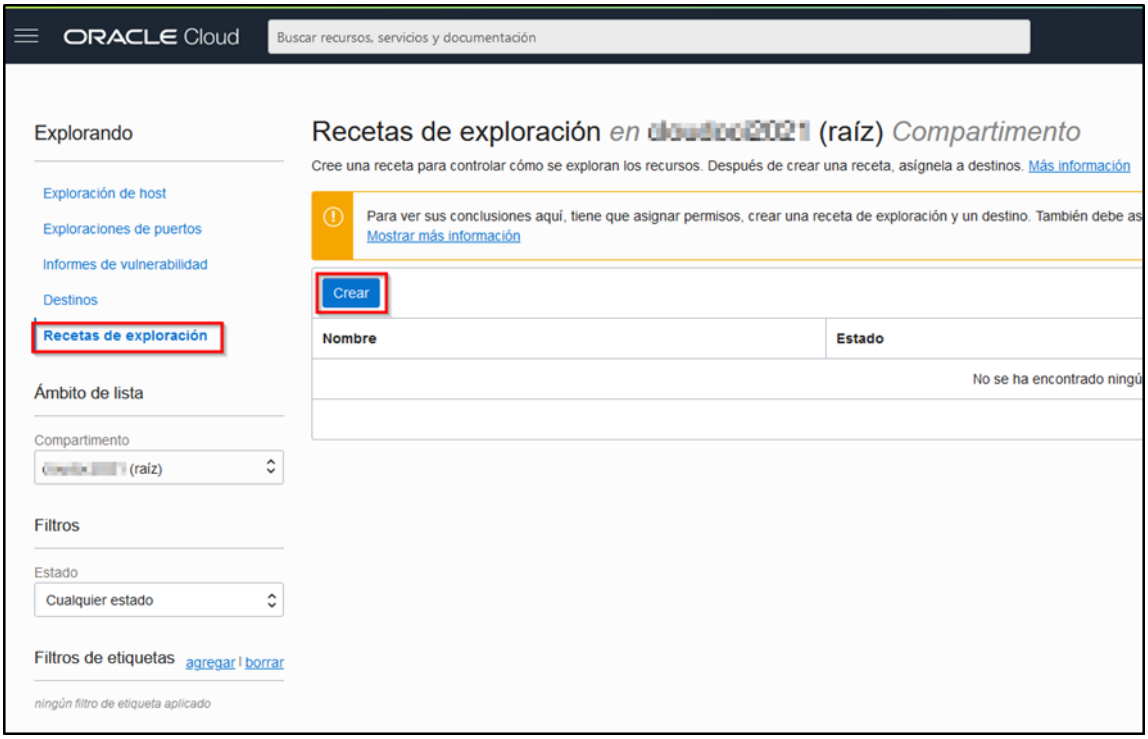


Imagen del servicio de Vulnerabilidades para la creación de recetas de exploración.



Puede ampliar la información sobre los Informes de Vulnerabilidad en el siguiente enlace:

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

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.

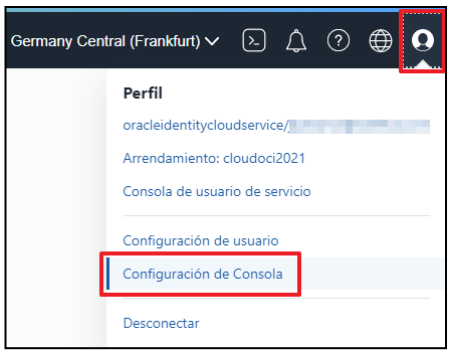
3.2.1.1 BLOQUEO DE PUESTO DE TRABAJO

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.

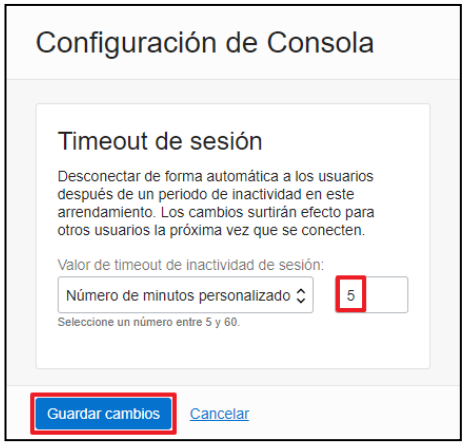
Esta medida contempla la desconexión de la sesión pasado un cierto tiempo de inactividad.

La aplicación técnica de esta medida la recoge el Servicio OCI IAM, donde se establecerá un único valor a la desconexión de la sesión cumplir con la norma.

Esta configuración se puede realizar desde un usuario administrador y aplicará al conjunto de usuarios del tenant que inicien sesión en la consola de gestión OCI.



Menú de configuración del tiempo de expiración de la sesión de usuario.



Configuración de la caducidad de la sesión de usuario establecida a los 5 minutos de inactividad.

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 PERÍMETRO SEGURO

El ENS establece en esta medida la disposición de cortafuegos para la separación de las redes de la organización de manera que, separe la red interna del exterior. Todo el tráfico deberá atravesar dicho cortafuegos y sólo dejará transitar los flujos previamente autorizados.

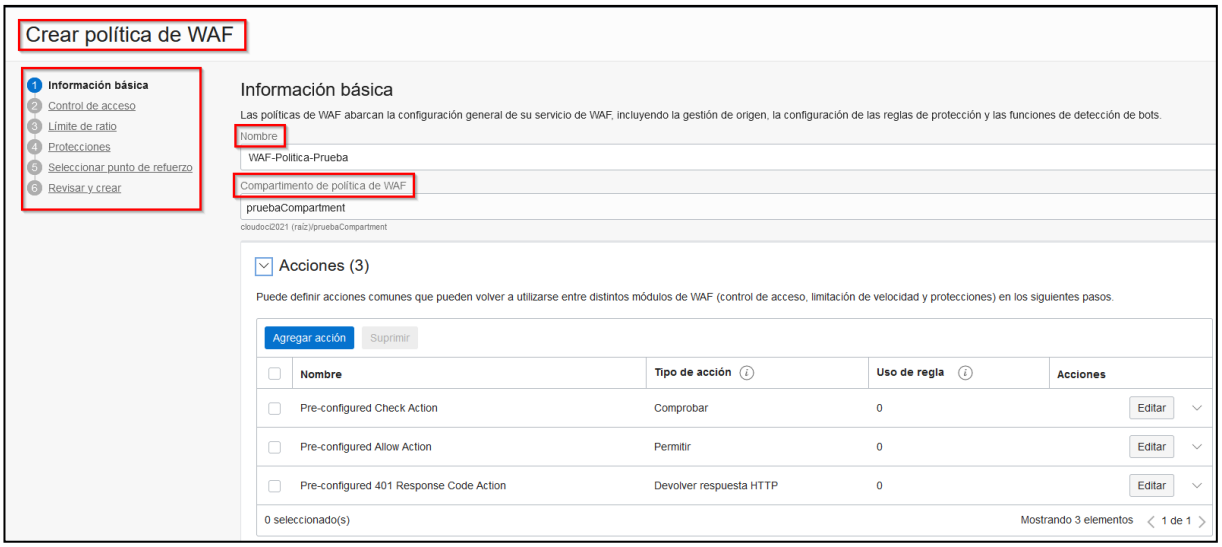
A este respecto, OCI dispone de fabricantes de cortafuegos como Palo Alto, Fortinet en Oracle Cloud Marketplace, además del Servicio WAF para establecer estas medidas. WAF es un servicio de seguridad global basado en la nube y conforme a los requisitos de la industria de tarjetas de pago (PCI) que protege las aplicaciones frente al tráfico de Internet no deseado y malicioso. WAF puede proteger cualquier punto final orientado a Internet, lo que proporciona un cumplimiento de reglas consistente en todas las aplicaciones de clientes. OCI proporciona inherentemente la mitigación de DDoS L3/4", además "Maximum Security Zones", para seguridad perimetral de recursos.

WAF proporciona la capacidad de crear y gestionar reglas para amenazas de Internet, incluidos los scripts de sitios (XSS), la inyección SQL y otras vulnerabilidades definidas por OWASP. Los bots no deseados se bloquean, mientras que se otorga acceso a los bots beneficiosos. Las reglas de acceso pueden establecer límites según la geografía o la firma de la solicitud.

El centro de operaciones de seguridad (SOC) global controla el panorama de amenazas de Internet de manera ininterrumpida y actúa como una extensión de su infraestructura de TI.

El acceso a este servicio se puede iniciar desde la consola OCI → Identidad y seguridad → Firewall de aplicaciones web → Recursos de políticas de perímetro.

Imagen acerca de las Políticas de WAF desde dónde poder crear nuevas políticas.



Asistente de la creación de una nueva política de WAF.

Puede ampliar la información del servicio en el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/Content/WAF/Concepts/overview.htm

En cuanto a la seguridad del perímetro, OCI WAF dispone de políticas de perímetro, las cuales enrutan el tráfico a través de WAF sin reglas activadas. Al crear una política sin reglas activadas, se garantiza que no haya regresiones con un proxy inverso delante de la aplicación.

Para crear una política de perímetro puede visitar el siguiente enlace de Oracle sobre la gestión de políticas de perímetro:

https://docs.oracle.com/es-ww/iaas/Content/WAF/Tasks/managingwaf.htm

3.2.2.2 PROTECCIÓN DE LA CONFIDENCIALIDAD

Esta medida indica que se emplearán redes privadas virtuales cuando la comunicación discurra por redes fuera del propio dominio de seguridad, empleando algoritmos acreditados 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.

OCI dispone, dentro del servicio Networking (Red), para implementar redes privadas virtuales en las comunicaciones para conectar la infraestructura de la nube con la red local de la organización, mediante VPN de sitio a sitio u OCI FastConnect.

a) **VPN de Sitio a Sitio**: Ofrece varios túneles de IPSec entre el borde de la red existente y la VCN, a través de un DRG creado y conectado a una VCN.

b) **OCI FastConnect**: Ofrece una conexión privada entre el perímetro de la red existente y OCI. El tráfico no atraviesa internet. Se admite tanto el intercambio de tráfico privado como público. Esto significa que los hosts locales pueden acceder a direcciones privadas de IPv4 o IPv6 en la VCN, así como a direcciones regionales públicas de IPv4 o IPv6 en OCI.

Estas conexiones se encuentran definidas en la guía de seguridad "CCN STIC 889C Guía de Configuración segura para Arquitecturas Híbridas", y se recomienda su consulta para ampliar los detalles en profundidad de las conexiones externas mediante VPN en la nube de Oracle.

3.2.2.3 SEGREGACIÓN DE REDES

La segregación de redes acota el acceso a la información y, consiguientemente, la propagación de los incidentes de seguridad, que quedan restringidos al entorno donde ocurren. En esta categoría, se segmentará la red de forma que haya:

a) Control de entrada de los usuarios que llegan a cada segmento.

b) Control de salida de la información disponible en cada segmento.

c) Las redes se pueden segmentar por dispositivos lógicos. El punto de interconexión estará particularmente asegurado, mantenido y monitorizado.

Oracle ofrece dentro del Servicio Networking, redes virtuales VCN, como redes virtuales privadas, VPN de sitio a sitio y FastConnect que, mediante la implementación de reglas de seguridad, actúan como cortafuegos virtuales para las instancias informáticas y otros tipos de recursos, dando protección a las comunicaciones a través de dos funciones para controlar el tráfico en el nivel de paquete:

a) **Listas de seguridad**: Tipo por defecto de cortafuego virtual ofrecido por el servicio de Networking y que actúan para las instancias de cómputo y otros tipos de recursos. Una lista de seguridad se compone de un conjunto de reglas de seguridad de entrada y salida que se aplican a todas las VNIC de cualquier subred con la que esté asociada la lista de seguridad.

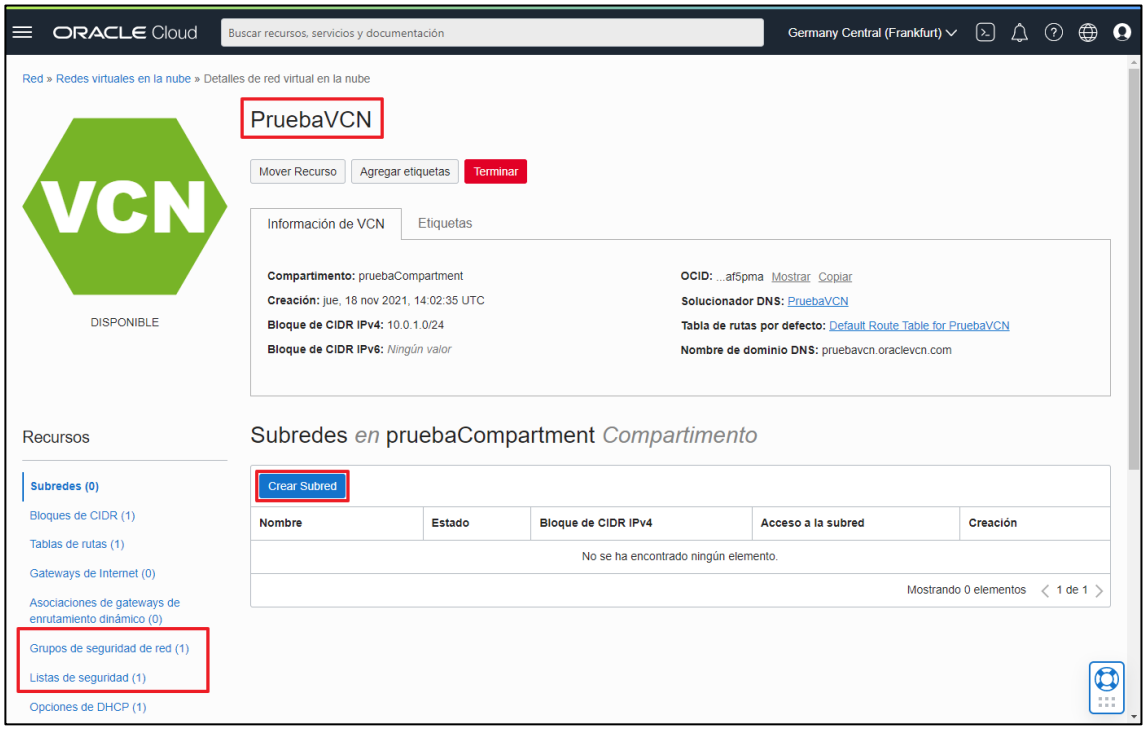
b) **Grupos de seguridad de red (NSG)**: Otro tipo de firewall virtual que Oracle ha diseñado para componentes de aplicaciones que tienen posiciones de seguridad diferentes. Los NSG solo se admiten para servicios específicos.

Estas dos funciones ofrecen diferentes maneras de aplicar reglas de seguridad a un conjunto de tarjetas de interfaz de red virtual (VNIC) en la red virtual en la nube (VCN). Mientras las Listas de seguridad se aplican a todas las VNIC de una subred, los NSG se aplican a un grupo específico de VNIC, permitiendo utilizar una mayor segregación que las Listas de seguridad.

Ambas funciones utilizan reglas de seguridad y para realizar la gestión de estos dos elementos de seguridad, debe acceder a la consola OCI → Red → Redes virtuales en la nube.

Accediendo a través de las propiedades de cada Red Virtual creada, y de forma automática, cada Red Virtual genera una serie de Reglas de Entrada y Salida por defecto. A partir de estas, el nivel de segmentación se realizará en función de las necesidades de comunicación del servicio, abriendo y cerrando puertos.

Imagen de ejemplo de una Red virtual VCN.



Detalle para la creación de Listas y Grupos de seguridad desde una VCN existente.

Puede obtener más información sobre el funcionamiento de las Reglas de seguridad y la comparación general de las Listas de seguridad y los Grupos de seguridad en los siguientes enlaces de Oracle:

https://docs.oracle.com/es-ww/iaas/Content/Network/Concepts/securityrules.htm

https://docs.oracle.com/es-ww/iaas/Content/Network/Concepts/securitylists.htm

https://docs.oracle.com/es-ww/iaas/Content/Network/Concepts/networksecuritygroups.htm

Para realizar los controles de segregación de las redes, Oracle cuenta además con otros componentes de red como el servicio WAF para instancias, el uso de subredes de VCN, y el uso de Compartimentos para la asignación de permisos mediante políticas.

Puede ampliar la información en los siguientes enlaces de Oracle:

https://docs.oracle.com/es-ww/iaas/Content/WAF/Concepts/overview.htm

https://docs.oracle.com/es-ww/iaas/Content/Security/Reference/networking_security.htm

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

Para ampliar la información acerca de la segregación de redes en OCI debe consultar la guía de seguridad “CCN-STIC-889C Guía de Configuración segura para Arquitecturas Híbridas”.

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 CIFRADO

Para el cifrado de información, en esta Categoría Alta del ENS se determina su dimensión en cuanto a la confidencialidad, indicando que se debe cifrar la información con un nivel alto en confidencialidad durante su almacenamiento, así como durante su transmisión. Sólo estará en claro mientras se está haciendo uso de ella.

Para el uso de criptografía en las comunicaciones, se estará a lo dispuesto en la norma [mp.com.2] Protección de la confidencialidad que se ha sido tratado en el punto 3.2.2.2 PROTECCIÓN DE LA CONFIDENCIALIDAD de este documento.

El cifrado en tránsito proporciona una manera de proteger los datos entre instancias y sistemas de archivos montados mediante el cifrado TLS v.1.2 (seguridad de capa de transporte). Junto con otros métodos de seguridad como Vault (KMS) y el cifrado estático "at-rest" de File Storage, Object Storage y Block Storage. El cifrado en tránsito proporciona una seguridad completa.

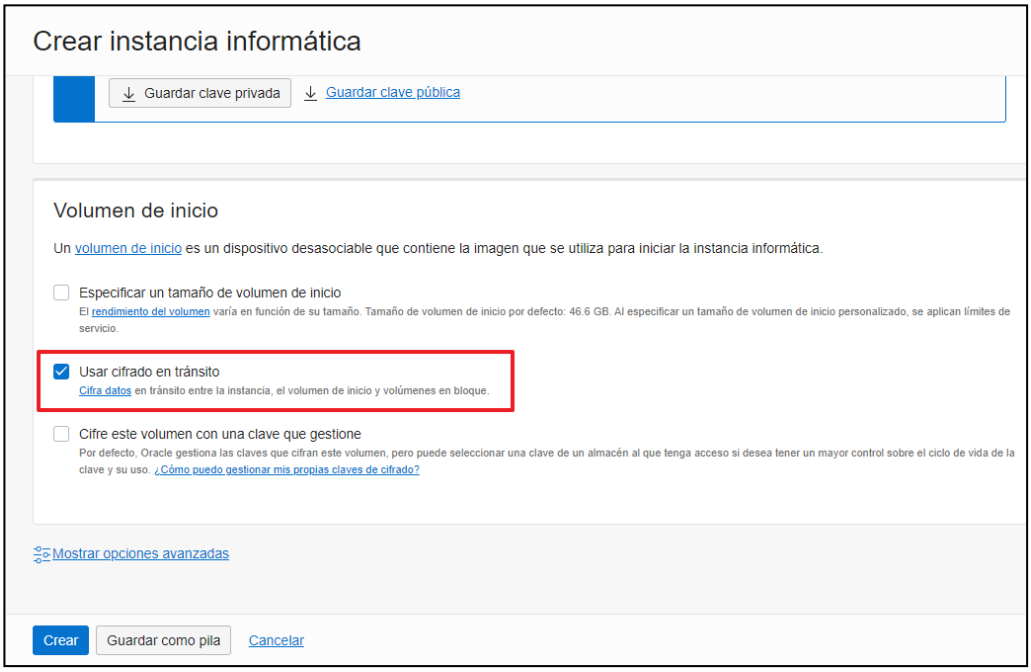


Imagen de la configuración de cifrado en tránsito al crear una instancia de VM.

En cuanto al cifrado estático, proporciona seguridad para los datos de archivos que se guardan en un disco (o de forma estática) mediante el cifrado de dichos datos. Mediante la tecnología de Oracle Transparent Data Encryption (TDE), el cifrado estático, cifra los datos almacenados en bases de datos Oracle para impedir el acceso a ellos por parte de usuarios no autorizados.

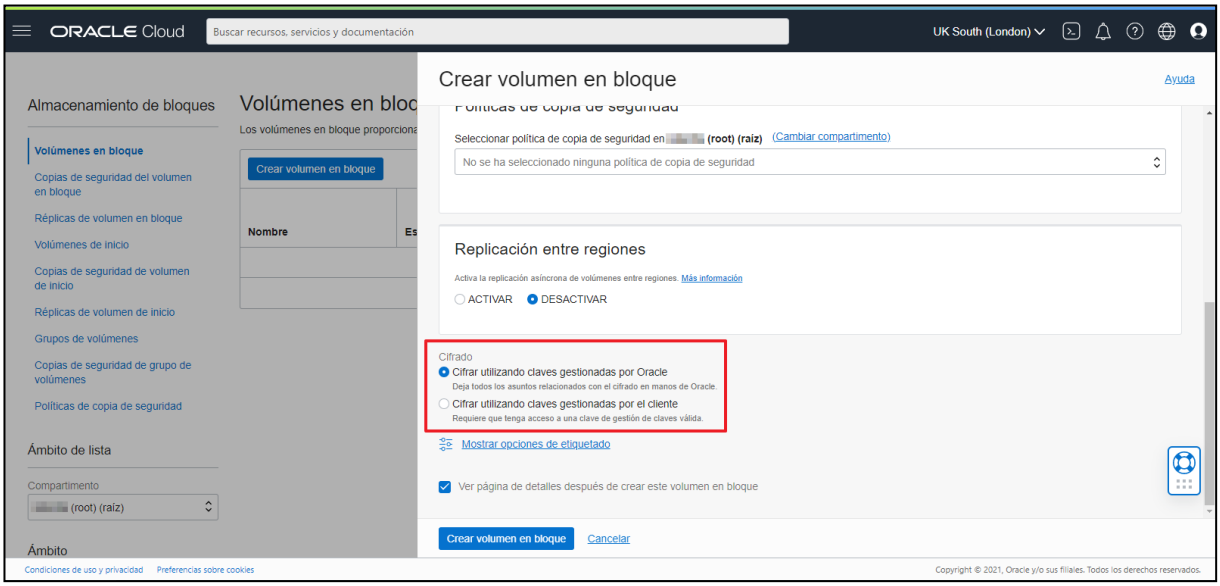


Imagen de la configuración de cifrado al crear un volumen en bloque.

Puede ampliar la información acerca de la activación del cifrado en tránsito en el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/Content/File/Tasks/intransitencryption.htm

Para la activación del cifrado estático puede seguir el siguiente enlace de Oracle:

https://docs.oracle.com/cloud/latest/related-docs/OMCEZ/es_ww/EncryptionAtRest.htm

Para ampliar la información acerca del cifrado estático siga el siguiente enlace de Oracle:

https://docs.oracle.com/es/solutions/oci-best-practices/protect-data-rest1.html

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 DE SERVICIOS Y APLICACIONES WEB

Los sistemas dedicados a la publicación de información no deberán ser publicados sin estar antes protegidos frente a las amenazas propias de los servicios web. OCI facilita una serie de servicios para alcanzar el correcto cumplimiento de esta medida a través de su Servicio WAF y el uso de certificados.

OCI dispone en la actualidad de la emisión de certificados internos de la nube para los recursos. Los certificados de OCI proporcionan a las organizaciones capacidades de emisión, almacenamiento y gestión de certificados, incluida la revocación y la renovación automática. Si la organización dispone de una autoridad de certificación (CA) de terceros que se encuentre en uso, puede importar certificados emitidos por esa CA para su uso en un tenant de OCI.

Para la gestión de estos Certificados debe acceder a la consola desde, OCI → Identidad y seguridad → Certificados.

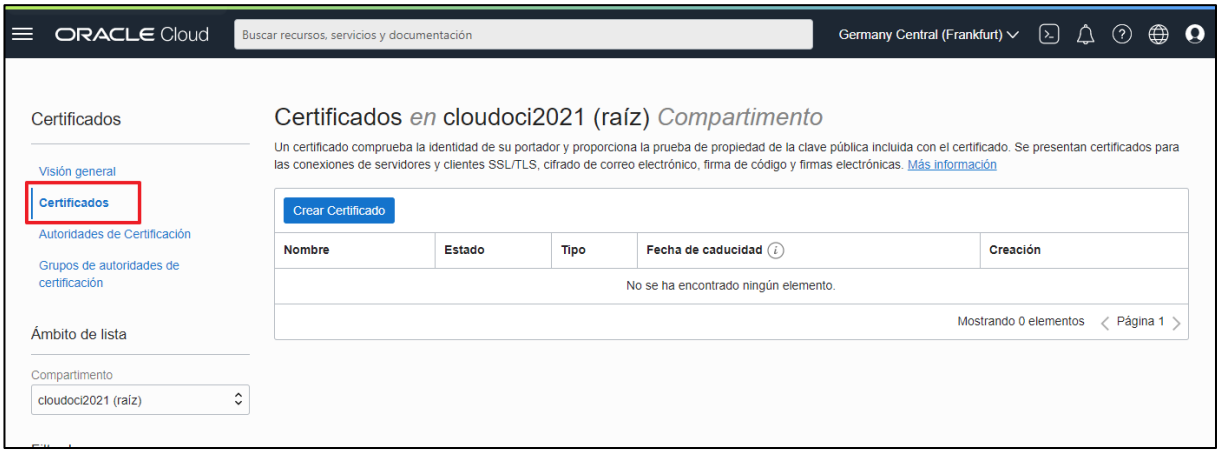


Imagen de la consola de Certificados internos de los recursos.

Puede ampliar la información sobre los Certificados en el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/Content/certificates/overview.htm

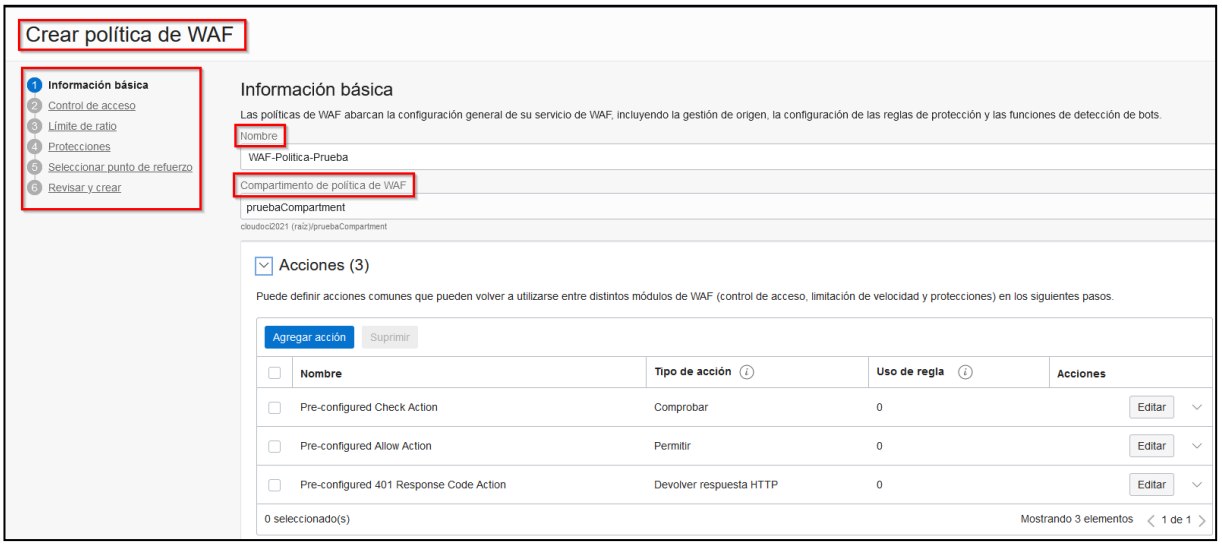
También puede utilizar SSL con la política de WAF, para lo cual debe agregar un grupo de certificados. El paquete de certificados que cargue incluye el certificado público y la clave privada correspondiente. OCI acepta certificados autofirmados de terceros en formato PEM y se pueden utilizar para la comunicación interna dentro de OCI. La integración con OCI Load Balancing permite asociar sin problemas un certificado TLS emitido o gestionado por certificados con recursos que necesitan certificados.

Puede ampliar la información acerca del uso de Certificados en los Balanceadores de Carga en el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/Content/Balance/Tasks/managingcertificates.htm

Para la Gestión de los Certificados desde WAF inicie la consola OCI → Identidad y seguridad → Firewall aplicaciones web.

Imagen acerca de las Políticas de WAF desde dónde poder crear nuevas políticas.



Asistente de la creación de una nueva política de WAF.

Puede ampliar la información del servicio en el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/Content/WAF/Concepts/overview.htm

Para la protección de servicios y aplicaciones, OCI WAF dispone de certificados y reglas de protección personalizadas para ello. Desde el menú OCI → Identidad y seguridad → Firewall aplicaciones web → Recursos de política de perímetro de OCI → Certificados.

Durante la creación de un Certificado, puede seleccionar la opción de hacer un Certificado autofirmado para usarlo en lugar de un certificado emitido por una autoridad de certificación.

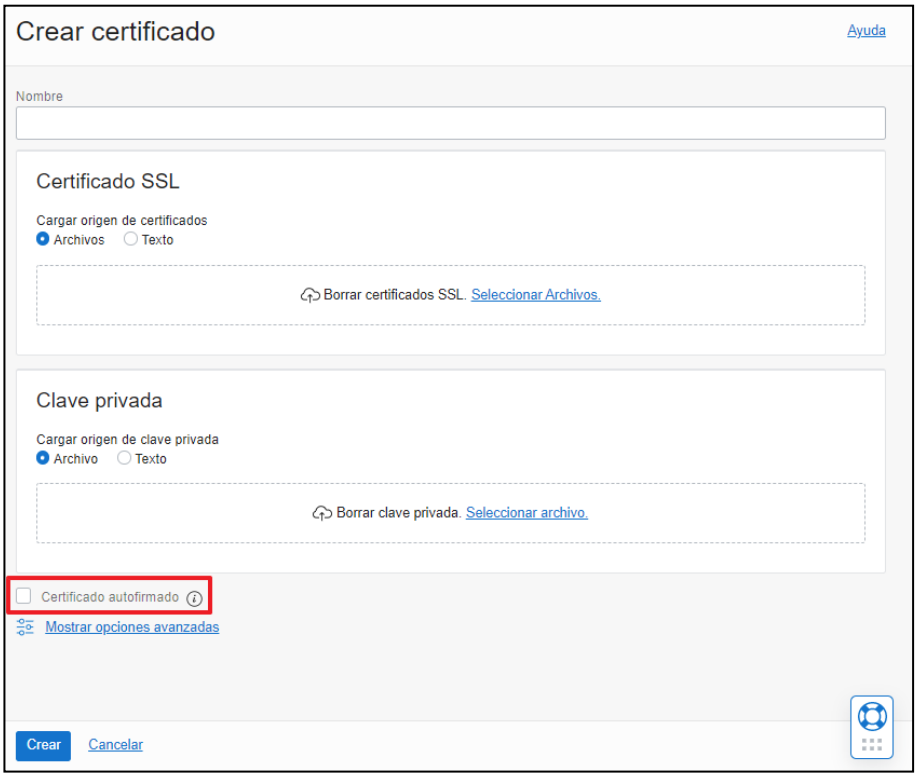


Imagen del detalle de cómo crear un Certificado autofirmado.

Puede ampliar la información de uso y gestión de certificados en WAF a través del siguiente enlace de Oracle a través de la consola o mediante las API:

https://docs.oracle.com/es-ww/iaas/Content/WAF/Tasks/wafsettings.htm

3.2.4.2 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.

Oracle dispone del Servicio WAF para mitigar los ataques DoS y DDoS en capa 7. Un ataque DDoS es un ataque a menudo intencionado que consume los recursos de una organización, normalmente mediante un gran número de orígenes distribuidos. Los ataques DDoS se pueden clasificar en capa 7 o capa 3/4 (L3/4), según lo definido por el modelo de interconexión de sistema abierto (OSI). Los ataques DDoS L3/4 son ataques DDoS que se producen en niveles inferiores de la pila OSI que los de capa 7. Entre los ejemplos de tales ataques se incluyen UDP, CharGen y NTP Flood. OCI proporciona inherentemente la mitigación de DDoS L3/4.

Un ataque DDoS de capa 7 es un ataque DDoS que envía tráfico HTTP/S para consumir recursos y alterar la capacidad de un sitio web para entregar contenido o dañar al propietario del sitio. El servicio WAF puede proteger recursos basados en HTTP de capa 7 desde DDoS de capa 7 y otros vectores de ataque de aplicaciones web.

En el siguiente enlace, podrá ampliar la información sobre este tipo de ataques y cómo implementarlos en Oracle:

https://docs.oracle.com/es-ww/iaas/Content/WAF/Concepts/ddos.htm

Para la Categoría Alta, el ENS también establece la necesidad de un sistema de detección de ataques de denegación de servicio, un procedimiento de reacción e impedir el lanzamiento de ataques desde las propias instalaciones.

Para realizar estas acciones Oracle dispone de la gestión de alarmas desde el Servicio de Monitoring. Su uso e implementación se explica en el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/Content/Monitoring/Tasks/managingalarms.htm

4. GLOSARIO

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

Término	Definición
AD	Availability Domain (Dominios de Disponibilidad).
API	Application Programming Interface (Interfaz de Programación de Aplicaciones).
Bucket	Cubo o almacén de datos ilimitado, de alto rendimiento, duradero y seguro.
CA	Certificate Authority (Autoridad Certificadora).
CIS	Center for Internet Security (Centro de Seguridad en Internet).
CCN	Centro Criptológico Nacional.
CLI	Command Line Interface (Interfaz de Línea de Comandos).
DDoS	Destributed Denial of Service (Denegación de Servicio Distribuido).
DoS	Denial of Service (Denegación de Servicio).
E-C@C	Exadata Cloud at Customer (Nube de Exadata en el Cliente).
ENS	Esquema Nacional de Seguridad.
HSM	Hardware Security Module (Módulos de seguridad por Hardware).
IA	Inteligencia Artificial.
IaaS	Infrastructure as a Service (Infraestructura como Servicio).
IDCS	Identity Cloud Services (Servicios de Identidad de la Nube).
KMS	Key Management Service.
MFA	Multi Factor Authentication (Doble Factor de Autenticación).
MOS	My Oracle Support (Soporte de Oracle a cliente)
NIDS	Network Intrusion Detection System.
NSG	Network Security Group (Grupo de Seguridad de Red).
O-C@C	Oracle Cloud at Customer (Nube de Oracle en el Cliente).
OCI	Oracle Cloud Infrastructure (Infraestructura de Nube de Oracle).
OCI IAM	Identity and Access Management (Gestión de Identidad y Acceso).
On-Premises	Se indica así a la instalación local de la infraestructura de TI en cuanto a su equipamiento, comunicaciones o aplicaciones.
OWASP	Open Web Application Security Project (Proyecto de Seguridad de Aplicaciones WEB).
PaaS	Platform as a Service (Plataforma como Servicio).
RBAC	Role Based Access Control (Control de Acceso Basado en Roles).
SDK	Software Development Kits (Paquetes de Desarrollo de Software).
SOC	Security Office Center (Centro de Operaciones de Seguridad).
SQL	Structured Query Language (Lenguaje de Consulta Estructurado).
TDE	Transparent Data Encryption (Encriptación de Datos Transparente).

Término	Definición
Tenant	Arrendamiento que contrata una organización y en el que Oracle presenta los servicios OCI contratados por el cliente.
TLS	Transport Layer Security (Seguridad de Capa de Transporte)
VCN	Virtual Cloud Network (Red de Nube Virtual).
VNIC	Virtual Network Interface Card (Tarjeta de Interfaz de Red Virtual).
VPN	Virtual Private Network (Red Privada Virtual).
WAF	Web Application Firewall (Firewall de Aplicación Web).
XSS	Cross-site scripting (Secuencias de Comandos en Sitios Cruzados).

5. RESUMEN Y APLICACIÓN DE MEDIDAS

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

Control ENS	Medidas y Configuración	Estado	
OP	MARCO OPERACIONAL		
OP.ACC	CONTROL DE ACCESO		
op.acc.1	Identificación	Aplica	Cumple
	Se ha configurado el uso de cuentas federadas y/o locales de OCI IAM para la administración del tenant.	☐Si ☐No	☐Si ☐No
		Observaciones:	
op.acc.2	Requisitos de acceso	Aplica	Cumple
	Se han gestionado los requisitos de acceso de los usuarios, creando en OCI IAM los grupos de seguridad necesarios en la organización y asignando a ellos las cuentas de usuario.	☐Si ☐No	☐Si ☐No
		Observaciones:	
op.acc.3	Segregación de funciones y tareas	Aplica	Cumple
	Se han creado los grupos de seguridad basados en roles (RBAC) en la consola de OCI IAM.	☐Si ☐No	☐Si ☐No
		Observaciones:	

Control ENS	Medidas y Configuración	Estado	
	Se han creado las políticas de acceso de los grupos RBAC a los recursos que le corresponda a cada uno en la consola de OCI IAM.	☐Si ☐No	☐Si ☐No
		Observaciones:	
op.acc.4	Proceso de gestión de derechos de acceso	Aplica	Cumple
	Se han gestionado los derechos de acceso de los usuarios a los Grupos y Compartimentos mediante la definición de políticas en OCI IAM, manteniendo: • Mínimo privilegio. • Necesidad de conocer. • Capacidad para autorizar.	☐Si ☐No	☐Si ☐No
		Observaciones:	
op.acc.5	Mecanismo de autenticación	Aplica	Cumple
	Se ha establecido el valor de la longitud de las contraseñas a 12 caracteres.	☐Si ☐No	☐Si ☐No
		Observaciones:	
	Se ha habilitado MFA a los usuarios administradores del tenant de OCI.	☐Si ☐No	☐Si ☐No
		Observaciones:	

Control ENS	Medidas y Configuración	Estado	
op.acc.6 y 7	Acceso local y remoto (local & remote logon)	Aplica	Cumple
	Se ha comprobado el acceso a la nube de los usuarios con permisos a través de las auditorias del último acceso realizado.	☐Si ☐No	☐Si ☐No
		Observaciones:	
OP.EXP	EXPLOTACIÓN		
op.exp.1	Inventario de activos	Aplica	Cumple
	Se gestiona el control de los recursos del tenant desde la gestión de costos o alguna herramienta disponible en OCI, como Ansible.	☐Si ☐No	☐Si ☐No
		Observaciones:	
	Se han configurado etiquetas personalizadas para todos los servicios de OCI según la clasificación o calificación de cada recurso o servicio.	☐Si ☐No	☐Si ☐No
		Observaciones:	
op.exp.2	Configuración de seguridad	Aplica	Cumple
	Se verifica en la entrada en producción de los equipos que deben configurarse para que: • Se retiren cuentas y contraseñas estándar. • Se aplique la regla de mínima funcionalidad.	☐Si ☐No	☐Si ☐No
		Observaciones:	

Control ENS	Medidas y Configuración	Estado	
op.exp.3	Gestión de la configuración	Aplica	Cumple
	Se ha activado el Servicio de Cloud Guard en el tenant de OCI.	☐Si ☐No	☐Si ☐No
		Observaciones:	
op.exp.4	Mantenimiento	Aplica	Cumple
	Se ha comprobado que en los equipos en producción se gestiona su mantenimiento desde los Servicios OCI: • OS MANAGEMENT, mediante el "Agente de servicio de gestión del Sistemas Operativos" y este está en funcionamiento y reportando. • Autonomous Linux.	☐Si ☐No	☐Si ☐No
		Observaciones:	
op.exp.6	Protección frente a código dañino	Aplica	Cumple
	Ha verificado la configuración del agente de "Análisis de vulnerabilidades" se encuentra activo en las instancias de VM.	☐Si ☐No	☐Si ☐No
		Observaciones:	
op.exp.7	Gestión de incidentes	Aplica	Cumple
	Una vez activado el Servicio de Cloud Guard, se han verificado las recomendaciones de seguridad que aparecen en la consola.	☐Si ☐No	☐Si ☐No
		Observaciones:	

Control ENS	Medidas y Configuración	Estado	
op.exp.8	Registro de la actividad de los usuarios	Aplica	Cumple
	Ha comprobado que el Servicio de Auditoría de OCI está activado y registrando eventos.	☐Si ☐No	☐Si ☐No
		Observaciones:	
op.exp.9	Registro de la gestión de incidentes	Aplica	Cumple
	Una vez activado el Servicio de Cloud Guard, se han verificado los problemas registrados que aparecen en la consola.	☐Si ☐No	☐Si ☐No
		Observaciones:	
op.exp.11	Protección de claves criptográficas	Aplica	Cumple
	Ha configurado el servicio Vault (almacén), limitando el acceso tan sólo al grupo de usuarios administradores de claves.	☐Si ☐No	☐Si ☐No
		Observaciones:	
OP.MON	MONITORIZACIÓN DEL SISTEMA		
op.mon.1	Detección de intrusión	Aplica	Cumple
	Una vez activado el Servicio de Cloud Guard, se han verificado los problemas para detectar alguna intrusión en el sistema.	☐Si ☐No	☐Si ☐No
		Observaciones:	

Control ENS	Medidas y Configuración	Estado	
	Se ha implementado y configurado alguna herramienta desde Marketplace para la detección de Intrusión.	☐Si ☐No	☐Si ☐No
		Observaciones:	
	Se ha configurado el Servicio de Informes de vulnerabilidad, creando recetas de exploración.	☐Si ☐No	☐Si ☐No
		Observaciones:	
MP	MEDIDAS DE PROTECCIÓN		
MP.EQ	PROTECCIÓN DE LOS EQUIPOS		
mp.eq.2	Bloqueo de puesto de trabajo	Aplica	Cumple
	Se ha configurado en la Consola del tenant el tiempo de expiración de la sesión para caducar a los 5 minutos.	☐Si ☐No	☐Si ☐No
		Observaciones:	
MP.COM	PROTECCIÓN DE LAS COMUNICACIONES		
mp.com.1	Perímetro seguro	Aplica	Cumple
	Se han creado las políticas en el Servicio WAF para separar la red interna del exterior.	☐Si ☐No	☐Si ☐No
		Observaciones:	

Control ENS	Medidas y Configuración	Estado	
mp.com.2	Protección de la confidencialidad	Aplica	Cumple
	Se han implementado, dentro del Servicio de Networking de OCI, “Redes virtuales en la nube” para las conexiones internas	☐Si ☐No	☐Si ☐No
		Observaciones:	
mp.com.4	Segregación de redes	Aplica	Cumple
	Se han configurado VCN para el aislamiento de redes.	☐Si ☐No	☐Si ☐No
		Observaciones:	
MP.INFO	PROTECCIÓN DE LA INFORMACIÓN		
mp.info.3	Cifrado	Aplica	Cumple
	Se ha configurado el cifrado en tránsito en las instancias de OCI.	☐Si ☐No	☐Si ☐No
		Observaciones:	
	Se ha configurado el cifrado estático en el almacenamiento de OCI.	☐Si ☐No	☐Si ☐No
		Observaciones:	

Control ENS	Medidas y Configuración	Estado	
MP.S	PROTECCIÓN DE LOS SERVICIOS		
mp.s.2	Protección de servicios y aplicaciones web	Aplica	Cumple
	Se ha verificado el uso de certificados de autenticación de sitio web mediante una CA interna.	☐Si ☐No	☐Si ☐No
		Observaciones:	
	Se ha verificado el uso de certificados de autenticación de sitio web mediante certificados autofirmados.	☐Si ☐No	☐Si ☐No
		Observaciones:	
mp.s.8	Protección frente a la denegación de servicio	Aplica	Cumple
	Se ha configurado DDOS en aquellas VNET expuestas a potenciales ataques externos.	☐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