Guía de Seguridad de las TIC
CCN-STIC 889E

Guía de Configuración segura para Oracle OCI Compute - Instancias VM y Bare Metal

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

CCN 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
2022.04.28 15:50:44 +02'00'

Pº de la Castellana 109, 28046 Madrid

NIPO: 083-22-139-5

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

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

AVISO LEGAL

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 PARA ORACLE OCI COMPUTE - INSTANCIAS VM Y BARE METAL 5
1.1 DESCRIPCIÓN DEL USO DE ESTA GUÍA 5
1.2 DEFINICIÓN DEL SERVICIO 5
1.3 SERVICIOS DE OCI COMPUTE 6
2. CONFIGURACIÓN SEGURA PARA ORACLE OCI COMPUTE - INSTANCIAS VM Y BARE METAL 10
2.1 MARCO OPERACIONAL 10
2.1.1 CONTROL DE ACCESO 11
2.1.1.1 IDENTIFICACIÓN 11
2.1.1.2 REQUISITOS DE ACCESO 12
2.1.1.3 SEGREGACIÓN DE FUNCIONES Y TAREAS 14
2.1.1.4 PROCESO DE GESTIÓN DE DERECHOS DE ACCESO 15
2.1.2 EXPLOTACIÓN 15
2.1.2.1 INVENTARIO DE ACTIVOS 15
2.1.2.2 MANTENIMIENTO 16
2.1.2.3 PROTECCIÓN FRENTE A CÓDIGO DAÑINO 19
2.1.2.4 GESTIÓN DE INCIDENTES 28
2.1.2.5 REGISTRO DE LA ACTIVIDAD DE LOS USUARIOS 29
2.1.2.6 REGISTRO DE LA GESTIÓN DE INCIDENTES 29
2.1.2.7 PROTECCIÓN DE CLAVES CRIPTOGRÁFICAS 30
2.1.3 MONITORIZACIÓN DEL SISTEMA 31
2.1.3.1 DETECCIÓN DE INTRUSIÓN 32
2.1.3.2 SISTEMA DE MÉTRICAS 33
2.2 MEDIDAS DE PROTECCIÓN 35
2.2.1 PROTECCIÓN DE LAS COMUNICACIONES 35
2.2.1.1 PERÍMETRO SEGURO 35
2.2.1.2 PROTECCIÓN DE LA CONFIDENCIALIDAD 36
2.2.1.3 SEGREGACIÓN DE REDES 37
2.2.2 PROTECCIÓN DE LA INFORMACIÓN 38
2.2.2.1 CIFRADO 38
2.2.2.2 COPIAS DE SEGURIDAD (BACKUP) 39
3. GLOSARIO 43
4. RESUMEN Y APLICACIÓN DE MEDIDAS 45

1. GUÍA DE CONFIGURACIÓN SEGURA PARA ORACLE OCI COMPUTE - INSTANCIAS VM Y BARE METAL

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 cómputo para las Instancias de máquina virtual (VM) y bare metal, 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 los 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 OCI Compute - Instancias VM y bare metal, 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 incorpora 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 OCI Compute para Instancias de VM y bare metal de las que trata este documento, disponiendo para ello de varios servicios que se detallan a continuación.

1.3 SERVICIOS DE OCI COMPUTE

Dentro de los servicios que ofrece OCI, esta guía abarca, de manera generalizada, los servicios de OCI Compute (recursos informáticos) basados en los distintos tipos de configuración de instancias que ofrecen las siguientes soluciones:

a) **Instancias flexibles de máquina virtual (VM):** Para seleccionar el número de núcleos y memoria que necesitan las aplicaciones.

b) **Instancias de hardware dedicado (bare metal):** Para ejecutar cargas de trabajo de alto rendimiento.

c) **Funciones sin servidor:** Para simplificar el desarrollo de aplicaciones con los recursos informáticos sin servidor.

d) **Contenedores y Kubernetes:** Para crear aplicaciones nativas en las nubes modernas.

e) **Instancias de GPU NVDIA:** Para el aprendizaje automático, visualización científica y otros procesos gráficos.

f) **Instancias de HPC:** Para obtener capacidades de alto rendimiento y aislamiento de tráfico de red.

Para obtener más información relacionada con los servicios de OCI Compute, consulte el siguiente enlace de Oracle:

https://www.oracle.com/es/cloud/compute/

OCI Compute permite aprovisionar y gestionar hosts de recursos informáticos, conocidos como instancias. Una instancia de máquina virtual o bare metal usa una imagen o shape que determina el sistema operativo u otro software, y son totalmente configurables en cuanto a la tecnología de hardware habilitada en OCI para su adecuación a las cargas de trabajo existentes. La unidad especificada o shape durante el proceso de creación de una instancia determina si la instancia es configurada como máquina virtual flexible, GPU o HPC, dependiendo del número de OCPU, memoria, ancho de banda de red (Gbps) y procesador asignado.

Después de crear una instancia, puede acceder a ella de forma segura desde su equipo, reiniciarla, asociar o desconectar volúmenes o terminarla cuando haya finalizado. Es importante conocer que, cuando una instancia se finaliza, cualquier cambio realizado en las unidades locales de la misma se pierde. No obstante, cualquier cambio guardado en los volúmenes asociados a la instancia, se puede conservar si se decide mantener los boot y block volumes.

El servicio de máquina virtual brinda capacidad de cómputo segura y elástica en la nube para cargas de trabajo que van desde pequeños proyectos hasta aplicaciones globales a gran escala, como plataformas de comunicación en tiempo real. Los atributos que definen las instancias de máquina virtual como la flexibilidad y la optimización para una gran variedad de cargas de trabajo resultan ser rentables, debido a un alto rendimiento y costes más bajos.

Por otro lado, los servidores bare metal de Oracle brindan a los clientes aislamiento, visibilidad y control mediante el uso de instancias de cómputo dedicadas. Admiten aplicaciones que requieren una gran cantidad de núcleos, grandes cantidades memoria y un gran ancho de banda, escalando hasta 160 núcleos, 2 TB de RAM y hasta 1 PB de almacenamiento en bloque.

A continuación, se describe los tipos de instancias que puede seleccionar para sus aplicaciones en función de las características como en el número de CPU, cantidad de memoria, recursos de red o la tecnología del procesador:

a) **Funciones de la instancia:** OCI ofrece funciones que permiten personalizar las instancias para cargas de trabajo especializadas y requisitos de seguridad.

   i. **Instancias ejecutables:** Instancias de máquina virtual que proporcionan un nivel base de rendimiento de CPU con capacidad de repartir en un nivel superior para soportar picos ocasionales en el uso.

      Para obtener información detallada de la función de una instancia ejecutable, consulte el siguiente enlace de Oracle:

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

   ii. **Instancias blindadas:** Refuerzan la seguridad del firmware para las instancias de máquina virtual con el fin de defenderse contra el software malicioso. Para obtener más información relacionada con las instancias blindadas, consulte el siguiente enlace de Oracle:

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

b) **Tipos de unidades Shapes:** Una unidad es una plantilla que determina el número de CPU, la cantidad de memoria y otros recursos que están asignados a una instancia informática de máquina virtual o bare metal. OCI ofrece una variedad de unidades que están diseñadas para cumplir con un rango de requisitos de recursos informáticos y aplicaciones.

   i. **Unidades estándar:** Diseñadas para cargas de trabajo de uso general, proporcionando un equilibrio entre recursos de núcleos, memoria y red. Las unidades estándar están disponibles con procesadores basados en Intel, AMD y ARM.

ii. **Unidades de DenseIO:** Diseñadas para grandes bases de datos, cargas de trabajo de big data y aplicaciones que requieren almacenamiento local de alto rendimiento. Las unidades de DenseIO incluyen SSD basados en NVMe asociados localmente.

iii. **Unidades de GPU:** Diseñadas para cargas de trabajo aceleradas por hardware. Se incluye CPU de Intel o AMD y procesadores gráficos de NVDIA para las instancias de VM y bare metal.

Para obtener más información relacionada con las unidades (shapes) basadas en GPU, consultar el siguiente enlace de Oracle:

https://www.oracle.com/cloud/compute/gpu/

iv. **Unidades de cómputo (recursos informáticos) de alto rendimiento (HPC):** Diseñadas para cargas de trabajo de recursos informáticos de alto rendimiento que requieren núcleos de procesador de alta frecuencia y redes de clúster para cargas de trabajo en masa de HPC paralelas.

v. **Unidades optimizadas:** Diseñadas para cargas de trabajo de cómputo que requieren núcleos de procesador de alta frecuencia y latencia baja.

Para obtener más información sobre las unidades de VM disponible en OCI, consulte el siguiente enlace de Oracle en inglés:

https://www.oracle.com/cloud/compute/virtual-machines/

c) **Unidades flexibles:** Permiten personalizar el número de OCPU y la cantidad de memoria asignados a una instancia. El ancho de banda de red y el número de VNIC se ajustan en proporción con el número de OCPU, permitiendo optimizar el rendimiento y minimizar el costo.

Para obtener más información relacionada con las unidades flexibles, consulte el siguiente enlace de Oracle:

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

d) **Tipos de capacidad:** La capacidad bajo demanda es el valor por defecto, pero puede utilizar los siguientes tipos de capacidad que se describen a continuación:

i. **Capacidad bajo demanda:** El coste se basa en la capacidad de cómputo que usa por segundo.

ii. **Capacidad preferente:** Permite ahorrar dinero mediante el uso de instancias preferentes que ejecutan cargas de trabajo durante períodos breves o que se pueden interrumpir cuando se reclama la capacidad.

iii. **Capacidad reservada:** Capacidad de reserva para uso futuro y garantía de disponibilidad para crear instancias de cómputo cuando se necesite. Cuando las instancias se terminan, la capacidad se devuelve a la reserva.

iv. **Capacidad dedicada:** Permite la ejecución de instancias de máquina virtual en servidores dedicados que son un tenant único y no se comparten con otros clientes. Esta función permite cumplir los requisitos de conformidad y normativos para el aislamiento y también, para cumplir con los requisitos de licencia basados en nodos o en hosts que necesitan licencia de todo el servidor.

Para obtener más información relacionada con los hosts dedicados de máquinas virtuales (VHD), consulte el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/Content/Compute/Concepts/dedicatedvmhosts.htm

Los límites de servicio y las cuotas de compartimento se aplican a todos los tipos de capacidad de host. Para obtener más información relacionada con los límites de servicio, consulte el siguiente enlace de Oracle:

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

Por otro lado, se debe tener en cuenta los requisitos previos y los componentes para iniciar las instancias. En primer lugar, se debe conocer el dominio de disponibilidad o el centro de datos de OCI de su región geográfica que aloja recursos en la nube, incluido las instancias para el cumplimiento de los requisitos de redundancia.

En segundo lugar, es necesario disponer al menos de una red virtual en la nube en la que se ejecutan las instancias, mediante la configuración de subredes, tablas de rutas y gateways. Para obtener una visión general de los elementos de la red, consulte el siguiente enlace de Oracle:

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

En tercer lugar, se debe disponer de un mecanismo de seguridad necesario para el acceso a las instancias:

a) En el caso de las instancias de Linux, el acceso se realizará a través de Shell seguro (SSH) y necesitará un par de claves para ello. Puede obtener más información relacionada con la gestión de pares de claves en instancias de Linux, en el siguiente enlace de Oracle:

   https://docs.oracle.com/es-ww/iaas/Content/Compute/Tasks/managingkeypairs.htm

b) En el caso de acceso para instancias de Windows, se realizará mediante una conexión RDP al puerto 3389 y se debe disponer de una cuenta de usuario y contraseña del sistema.

Puede obtener más información acerca de cómo conectarse a las instancias en el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/Content/Compute/Tasks/accessinginstance.htm

Para finalizar, existe en OCI una amplia gama de servicios de almacenamiento para las instancias de cómputo. Puede ampliar el almacenamiento local disponible a través de los siguientes servicios:

a) **Volumen en bloque:** Permite aprovisionar y gestionar dinámicamente volúmenes en bloque que pueden asociarse a una o más instancias. Para obtener más información o una visión general del volumen de bloque, consulte el siguiente enlace de Oracle:

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

b) **Almacenamiento de archivos:** Proporciona un sistema de archivos de red duradero, escalable y seguro al que se puede conectar desde cualquier instancia informática de la red virtual en la nube (VCN). Para obtener más información relacionada con el sistema de archivos, consulte el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/Content/File/Concepts/filestorageoverview.htm

c) **Almacenamiento de objetos y de archivo:** Es una plataforma de almacenamiento en internet de alto rendimiento que permite almacenar una cantidad ilimitada de datos no estructurados de cualquier tipo de contenido. Este almacenamiento es regional y no está ligado a ninguna instancia informática específica, sino que está ligado a un bucket. Para obtener una visión general del servicio, consulte los siguientes enlaces de Oracle para el almacenamiento de objetos y de archivos:

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

https://docs.oracle.com/es-ww/iaas/Content/Archive/Concepts/archivestorageoverview.htm

El presente documento recoge las medidas de aplicación técnica que establece el ENS en la categoría alta, según las medidas de seguridad que deben aplicarse al entorno cloud de Oracle y en concreto a los servicios de OCI Compute.

2. CONFIGURACIÓN SEGURA PARA ORACLE OCI COMPUTE - INSTANCIAS VM Y BARE METAL

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.

2.1 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.

2.1.1 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).

2.1.1.1 IDENTIFICACIÓN

El objetivo de la medida de seguridad relacionada con la identificación no es otro que saber quién recibe qué derechos sobre los recursos y quién ha hecho el qué sobre dichos recursos. Las entidades que acceden a los recursos del sistema deben quedar singularmente identificadas, mediante la existencia de mecanismos que garanticen y aseguren la trazabilidad del uso de los recursos. Además, las cuentas de usuario deben ser únicas e inequívocas para cada usuario y servicio de OCI, y deben ser gestionadas de tal forma que queden inhabilitadas cuando las condiciones lo requieran.

La aplicación de esta medida se encuentra definida por OCI a través del identificador OCID. La mayoría de los tipos de recursos, como instancias, volúmenes, redes VCN, usuarios y grupos disponen de un ID único asignado por Oracle. Mediante este identificador, es posible la trazabilidad del uso de los recursos y distinguir unívocamente las cuentas de usuario, grupos, recursos y servicios disponibles en OCI.

Para obtener más información relacionada con los identificadores de recursos de OCI, consulte el siguiente enlace de Oracle:

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

Para garantizar o controlar quién tiene acceso a qué recursos de la nube de Oracle, es necesario la gestión del servicio de OCI IAM para la gestión de identidades y permisos sobre los recursos del sistema y, en concreto, para las instancias de máquina virtual y bare metal.

Un administrador necesitará configurar grupos, compartimentos y políticas que controlen qué usuarios pueden acceder a qué servicios, recursos y qué tipo de acceso queda definido y cómo debe autenticarse una identidad. Además, gracias al servicio de OCI Vault, es posible guardar de manera segura, cifrada y centralizada las credenciales o secretos de los usuarios y claves API que acceden y usan los recursos del tenant, evitando el almacenamiento de las credenciales de usuario en instancias cómputo.

Finalmente, para obtener más información relacionada con el servicio OCI IAM y la configuración de cuentas de usuario, puede consultar la guía de seguridad “CCN-STIC-889A Guía de Configuración segura de IAM y servicios de seguridad”.

2.1.1.2 REQUISITOS DE ACCESO

La medida de seguridad establecida por el ENS y relacionada con los requisitos mínimos de acceso a los recursos del sistema, indica la necesidad de proteger dichos recursos mediante algún mecanismo que impida su utilización, salvo para aquellas entidades que disfruten de los derechos de acceso suficientes.

Se debe, a su vez, controlar el acceso a los recursos del tenant. Los derechos de acceso a los recursos deben establecerse según las decisiones de la persona responsable del recurso, siguiendo la normativa de seguridad del sistema.

La aplicación técnica de esta medida para la presente guía de seguridad debe abarcar todos los recursos implicados con el servicio de OCI Compute. Es decir, se debe controlar el acceso, tanto para las identidades relacionadas con los usuarios o grupos de usuarios de la organización, como para los servicios o grupos dinámicos de OCI, en los siguientes recursos fundamentales que definen la infraestructura que aloja una instancia o grupo de instancias:

a) **Acceso y gestión de compartimentos:** Se debe controlar el acceso a la familia de recursos all-resources.

b) **Acceso y gestión de instancias:** Se debe controlar el acceso al recurso agregado instance-family o los recursos individuales que lo componen para un control más granular. Para la gestión de los recursos relacionados con clústeres para Kubernetes, se debe controlar el acceso a la familia de recursos cluster-family. Por último, para la gestión del acceso al servicio de Oracle Functions (funciones), se debe controlar el acceso a la familia de recursos functions-family.

c) **Acceso y gestión del almacenamiento:** Se debe controlar el acceso al recurso agregado de los siguientes servicios que componen el almacenamiento en OCI:

   i. Volumen de bloque: volumen-family.

   ii. Almacenamiento de archivos: file-family.

   iii. Almacenamiento de objetos y de archivo: object-family.

d) **Acceso y gestión de la configuración de los recursos de red:** Se debe controlar el acceso al recurso agregado virtual-network-family o los recursos individuales que lo componen.

e) **Acceso y gestión de los recursos de monitorización:** Se debe controlar el acceso a los siguientes recursos agregados de los distintos servicios que componen la monitorización y gestión para realizar la supervisión de las instancias de cómputo:

   i. Supervisión: metrics y alarms.

   ii. Aplication Perfomance Monitoring: apm-domains.

   iii. Registro: log-group y log-content.

   iv. Logging Analytics: loganalytics-features-family.

   v. Notificaciones: ons-family.

   vi. Eventos: cloudevents-family, tag-namespace, streams y function-family.

f) **Acceso y gestión de los recursos de seguridad:** Se debe controlar el acceso a las siguientes familias de recursos o los recursos individuales que lo componen de los distintos servicios de seguridad de OCI:

i. Cloud Guard: cloud-guard-family.

ii. Zonas de seguridad: security-zone.

iii. Firewall de aplicaciones web: waas-family.

iv. Certificados: leaf-certificate-family.

v. Servicio de análisis de vulnerabilidades: vss-family.

vi. Vault: secret-family.

vii. Bastion: bastion-family.

viii. Auditoría: audit-events.

Para gestionar una instancia, es necesario la asignación de los permisos correspondientes en las cuentas de usuario, grupos de usuario o grupos dinámicos en los recursos fundamentales descritos. Para obtener más información relacionada con los tipos de recursos agregados y tipos de recursos individuales que forman cada familia, consulte el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/Content/Identity/policyreference/policyreference_topic-ResourceTypes.htm

Se recomienda mantener y gestionar un control estricto del acceso mediante la limitación de los permisos otorgados para la gestión de las instancias y los recursos y servicios relacionados para su funcionamiento:

a) Gestión de instancias y credenciales:

i. Evite conceder el permiso delete a varios grupos de usuarios para evitar la finalización accidental o maliciosa de las instancias.

ii. Gestione grupos dinámicos y accesos a las API de servicio para las instancias mediante claves de corta duración. Para obtener más información, consulte el siguiente enlace de Oracle:

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

b) Control de acceso a metadatos de instancia:

i. Limite el acceso a los metadatos de instancia a usuarios con privilegios en la instancia, debido a que los metadatos proporcionan información como el OCID de la instancia, nombre y campos personalizados o credenciales de corta como las credenciales de grupo dinámico.

ii. Se recomienda un control estricto sobre la creación y modificación de las reglas de firewall del sistema operativo de las instancias. Las instancias usan direcciones locales de enlace para acceder al servicio de metadatos de instancia, DNS, NTP, actualizaciones de núcleo y conexiones iSCSI a volúmenes de inicio. Es necesario usar un firewall basado en host, como iptables que garanticen que solo el usuario raíz esté autorizado para acceder a estas IP.

c) Control de acceso a la red de instancia:

i. Refuerce el Shell seguro (SSH) en todas las instancias.

ii. Use claves privadas SSH seguras para acceder a las instancias y evite las divulgaciones involuntarias.

iii. Limite los permisos de acceso para la gestión de los grupos de seguridad de red de VCN y las listas de seguridad a un reducido número de usuarios que sean administradores de red.

d) Control de acceso a los volúmenes de bloque.

i. Controle el acceso a los volúmenes de bloque a un reducido número de usuarios para prevenir la eliminación de volúmenes de arranque, volúmenes anexos o volúmenes de backup.

ii. Evite la pérdida de datos involuntaria o supresiones maliciosas limitando el permiso delete sobre los recursos de volúmenes de bloque.

2.1.1.3 SEGREGACIÓN DE FUNCIONES Y TAREAS

Esta medida de seguridad establece un control de acceso de forma que se exija la concurrencia de dos o más personas para realizar las tareas críticas, evitando la posibilidad de que un solo individuo autorizado pueda abusar de sus derechos para cometer alguna acción ilícita.

Volviendo a los recursos fundamentales descritos en la medida de seguridad relacionada con los requisitos de acceso, se debe establecer cuentas de administradores o grupos de administradores distintos que gestionen los recursos. Es decir, se debe evitar que un mismo grupo de administradores pueda gestionar los recursos de seguridad a la vez que gestionan los recursos de la red o las herramientas de supervisión.

Por otro lado, el ENS establece que debe separarse como mínimo las funciones de desarrollo de operaciones, configuración y mantenimiento del sistema de operación y la auditoría o supervisión de cualquier otra función.

Oracle dispone del servicio para el control de acceso basado en roles (RBAC) que puede gestionarse mediante el servicio de OCI IAM, proporcionando a los administradores el control necesario sobre el acceso de los usuarios a los recursos de OCI Compute.

2.1.1.4 PROCESO DE GESTIÓN DE DERECHOS DE ACCESO

El proceso de gestión de derechos de acceso es una medida de seguridad establecida por el ENS que indica una serie de principios a aplicar a la hora de realizar el control de acceso adecuado.

Tal y como se ha mencionado en la medida de seguridad relacionada con los requisitos de acceso, la aplicación técnica de la medida debe abarcar todos los ámbitos relacionados con la instancia y su interacción con otros recursos del sistema.

Para ello, se debe tener en cuenta el principio de mínimo privilegio que indica la reducción mínima necesaria de los privilegios, concedidos a los usuarios mediante políticas, con el fin de limitar los daños que puedan causar sus acciones de forma accidental o intencionada en cualquier ámbito relacionado con la instancia. A su vez, los privilegios deben limitarse a la necesidad de conocer para el cumplimiento de sus obligaciones y, además, debe haber una autoridad capaz de conceder, alterar o anular la autorización de acceso a los recursos en cada momento.

En consecuencia, se debe asignar privilegios de rol que restrinja el acceso de los usuarios de cada grupo solamente a los compartimentos que necesitan acceder, escribiendo políticas a nivel de compartimento. Las políticas deben ser lo más detalladamente posible, referenciando a los recursos de destino y los privilegios de acceso requeridos. Además, se debe crear los grupos de usuarios o grupos dinámicos con permisos para realizar aquellas tareas que son comunes a todas sus cargas de trabajo implementadas.

Finalmente, la aplicación técnica de esta medida de seguridad se realiza a través del servicio de OCI IAM, donde se puede gestionar, mediante políticas asignadas a los recursos o familias de recursos, usuarios, grupos de usuarios o grupos dinámicos, los permisos o privilegios de derechos de acceso. Además, puede usar como herramientas las etiquetas y los compartimentos para organizar y aislar los recursos facilitando la gestión de los derechos de acceso.

Para obtener más información sobre la herramienta de etiquetado de OCI, revise la medida de seguridad 2.1.2.1 INVENTARIO DE ACTIVOS de este documento.

2.1.2 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.

2.1.2.1 INVENTARIO DE ACTIVOS

Los soportes de información deben ser etiquetados de tal forma que, sin revelar su contenido, se indique el nivel de seguridad de la información contenida de mayor calificación.

El etiquetado es un servicio de OCI que agrega metadatos a los recursos, lo que permite definir claves y valores asociados a los mismos a través de etiquetas definidas o etiquetas de formato libre, destinadas para especificar atributos de identificación de recursos significativos y relevantes para los usuarios.

Para obtener más información relacionada con el servicio de etiquetado y su funcionamiento, consulte la guía de seguridad "CCN-STIC-889A Guía de Configuración segura para IAM y servicios de seguridad".

No obstante, para los servicios que componen los recursos informáticos de OCI (Compute), además del uso del etiquetado que puede configurarse para la organización de los recursos de un tenant, es posible, también, disponer de un control de acceso basado en etiquetas para las instancias de cómputo de máquina virtual o bare metal, buckets, VCN, etc., o para otorgar, explícitamente, acceso a pods y redes que utilizan recursos de NetworkPolicy en Kubernetes.

Además, el motor de contenedor para Kubernetes utiliza varias etiquetas diferentes al crear y gestionar clústeres que puede consultar en el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/Content/ContEng/Reference/contengsupportedlabelsusecases.htm

Finalmente, se recomienda controlar la creación y gestión de las etiquetas mediante políticas OCI IAM para los administradores, y para el resto de los usuarios del tenant permitirles aplicar las etiquetas. En consecuencia, se evita los errores tipográficos que afectan negativamente a la automatización basada en etiquetas y se mejora la generación de informes basados en etiquetas.

2.1.2.2 MANTENIMIENTO

La medida de seguridad establecida por el ENS se aplica de igual forma para todas las categorías y para la presente guía, la medida dice que se debe disponer de un procedimiento que analice y determine cuándo aplicar las actualizaciones de seguridad, parches, mejoras y nuevas versiones.

La aplicación técnica de esta medida se realiza mediante el servicio de gestión del sistema operativo de OCI para las instancias cómputo. El servicio de gestión del sistema operativo permite gestionar y supervisar las actualizaciones y parches para los entornos del sistema operativo de las instancias de Oracle Cloud. Para ello, gestión del sistema operativo utiliza el plugin del agente de servicio de gestión del sistema operativo para gestionar y aplicar actualizaciones, el cual gestiona el complemento del agente del servicio de gestión del sistema operativo.

Por un lado, entre los componentes y funciones de gestión del sistema operativo, como el complemento del agente del servicio de gestión del sistema operativo, proporciona los permisos necesarios para aplicar actualizaciones en instancias de máquina virtual o bare metal gestionadas, de la siguiente forma:

a) **Instancias de Oracle Linux:** Utiliza los permisos estándar de Linux para una cuenta administrativa sudo para aplicar actualizaciones.

b) **Instancias de Windows:** El plugin del servicio gestión del sistema operativo crea una cuenta de servicio virtual que aplica las actualizaciones en la instancia.

Además, las instancias pueden ser gestionadas de manera individual o mediante grupos de instancias que reciben las actualizaciones.

Para obtener más información sobre la administración de grupos de instancias gestionadas, consulte el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/os-management/osms/osms-instance-groups.htm

Por otro lado, el servicio de gestión del sistema operativo utiliza orígenes de software que proporcionan paquetes a las instancias de Linux, realizando un seguimiento de las actualizaciones disponibles para esos paquetes. También proporciona la gestión de paquetes para Linux y gestión de actualizaciones para Windows mediante acciones de instalación y búsqueda.

Entre otras funciones del servicio de gestión del sistema operativo, cabe destacar la búsqueda de exposiciones y vulnerabilidades comunes (CVE) para las instancias Linux. Esta utilidad proporciona y determina el nivel de exposición del tenant buscando los CVE concretos desde la web de Oracle en inglés:

https://linux.oracle.com/security/

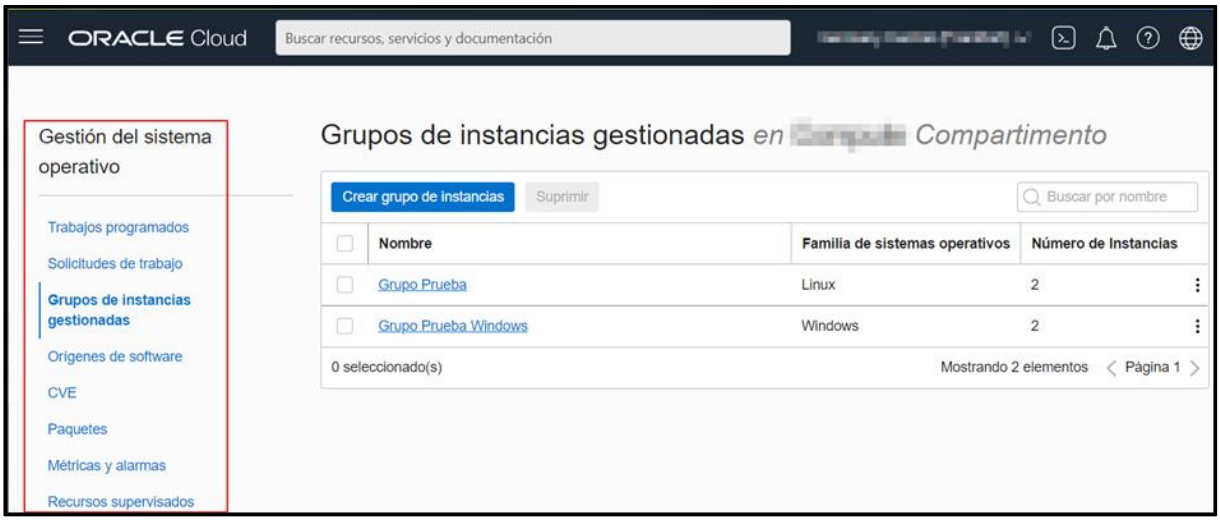
Además, mediante la supervisión y detección de recursos es posible la detección automática y el control básico sobre los recursos que se ejecutan en instancias de Oracle Linux gestionadas por el servicio de gestión del sistema operativo.

Al mismo tiempo, el servicio de gestión del sistema operativo permite la programación de trabajos y las solicitudes de trabajo para la gestión de las actualizaciones, a través de acciones y fechas concretas.

Para obtener más información relacionada con los trabajos programados y las solicitudes de trabajo, consulte el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/os-management/osms/osms-work-requests-jobs.htm

Para acceder al servicio de gestión del sistema operativo debe navegar por el menú de OCI → Recursos informáticos → Gestión del sistema operativo.



Menú de navegación del servicio de gestión del sistema operativo.

Dentro del panel de gestión del sistema operativo se pueden realizar las siguientes acciones que definen el servicio de gestión y supervisión de las actualizaciones y parches del sistema:

a) **Trabajos programados:** Las actualizaciones se pueden gestionar de manera inmediata o programada en una fecha y hora definida o de manera periódica. Cuando se alcanza la fecha y hora programada, se crea una o varias solicitudes de trabajo para realizar la acción y disponer de un control total sobre los trabajos programados.

b) **Solicitudes de trabajo:** Las acciones como la instalación o eliminación de actualizaciones son asíncronas e inician solicitudes de trabajo. Puede utilizar la solicitud de trabajo para realizar un seguimiento del estado de las operaciones, incluido aquellas que hayan fallado. El servicio de gestión del sistema operativo mantiene un historial completo de las solicitudes de trabajo de las instancias gestionadas o los grupos de instancias gestionadas.

c) **Grupos de instancias gestionadas:** Permiten agrupar instancias para programar actualizaciones.

d) **Orígenes de software:** Permite la configuración y control de los repositorios en las instancias. Se distinguen entre orígenes principales o de base y los orígenes secundarios. Una instancia solamente puede tener un origen de software principal y varios orígenes secundarios. También es posible crear un origen personalizado de software con una lista de paquetes adaptada a las imágenes (BYOI).

e) **CVE:** Permite la gestión de los CVEs en las instancias. A través del cuadro de búsqueda, puede introducir un CVE concreto y verificar si está instalado en una instancia determinada, además de comprobar la información del paquete y sus dependencias.

f) **Paquetes:** Permite la gestión de paquetes para instancias Linux y Windows. Entre las acciones que se pueden realizar se distingue la búsqueda de paquetes, la instalación y actualización de los paquetes o la eliminación de paquetes. Para obtener más información sobre la gestión de paquetes Linux, las categorías aplicadas o cómo buscar y encontrar paquetes concretos, consulte el siguiente enlace de Oracle:

   https://docs.oracle.com/es-ww/iaas/os-management/osms/osms-package-management.htm

   Asimismo, para obtener más información acerca de las actualizaciones de Windows y cómo instalar los KB por instancia o grupos de instancias, consulte el siguiente enlace de Oracle:

   https://docs.oracle.com/es-ww/iaas/os-management/osms/osms-windows-updates.htm

g) **Métricas y alarmas:** Permiten la monitorización de las instancias gestionadas por el servicio de gestión del sistema operativo para la supervisión del estado, la capacidad, rendimiento y las actualizaciones de seguridad disponibles mediante la visualización de gráficas.

h) **Recursos supervisados:** Proporciona funciones como la detección automática basada en procesos y supervisión del estado, uso de CPU y memoria de recursos como Oracle Database, Listener, WebLogic Server, Oracle HTTP Server, Servidor Apache o Tomcat. Además, dispone de un historial de métricas, alarmas y notificaciones mediante la plataforma de supervisión de OCI. Para obtener más información del servicio de supervisión de OCI, consulte la guía de seguridad “CCN-STIC-889B Guía de Configuración segura para Monitorización y gestión”.

Para obtener más información relacionada con el servicio de gestión del sistema operativo, consulte el siguiente enlace de Oracle, donde se podrá ver los flujos de trabajo, las imágenes soportadas, requisitos y necesidades de configuración de políticas de IAM:

https://docs.oracle.com/es-ww/iaas/os-management/osms/osms-getstarted.htm

Para finalizar, es necesario actualizar los clústeres de Kubernetes usando el motor de contenedor para Kubernetes. Una vez publicada una nueva versión de Kubernetes y cuando el motor de contenedor soporte dicha versión, se puede actualizar la versión de Kubernetes que se ejecuta en los nodos de plano de control y los nodos de trabajador de un clúster.

No obstante, los nodos de plano de control y los nodos de trabajador que componen el clúster pueden ejecutar diferentes versiones de Kubernetes, siempre y cuando cumpla con la política de soporte de sesgo de versión de Kubernetes descrita en la documentación oficial de Kubernetes, que puede consultar a través del siguiente enlace en inglés:

https://kubernetes.io/releases/version-skew-policy/

Para obtener más información relacionada con la actualización de clústeres de Kubernetes, revise el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/Content/ContEng/Tasks/contengupgradingclusters_topic.htm

2.1.2.3 PROTECCIÓN FRENTE A CÓDIGO DAÑINO

La medida de seguridad referente a la protección frente a código dañino establecido por el ENS, indica que se debe disponer de mecanismos de prevención y reacción frente a código dañino como virus, gusanos, troyanos, programas espías y en general todo lo conocido como malware o software malicioso.

Para ello, OCI dispone de varios servicios de seguridad que se van a categorizar según el objetivo a proteger. Además de la protección de las instancias, es necesario proteger también el dato guardado a través de los diferentes servicios de almacenamiento de OCI y la infraestructura de red que permite la comunicación de una instancia. Asimismo, las herramientas de control de acceso como las herramientas de detección y reacción o el servicio de auditoría son fundamentales para la protección de la infraestructura frente a ataques inesperados.

No obstante, para la presente medida de seguridad, centrada en la instancia como recurso informático de máquina virtual y bare metal, OCI dispone de los servicios Cloud Guard, zonas de seguridad, análisis de vulnerabilidades y Security Advisor (Asesor de seguridad) para su aplicación técnica.

La aplicación técnica de los demás servicios de seguridad disponibles en OCI como IAM, gestión del sistema operativo, WAF, bastión o Vault entre otros, se describen en las distintas medidas de protección contempladas en la presente guía de seguridad.

Para empezar, Cloud Guard es un servicio en la nube que ayuda a los clientes a supervisar, identificar, lograr y mantener una estrategia sólida en Oracle Cloud. Cloud Guard examina los recursos de OCI para detectar actividades de riesgo.

Tras su detección, Cloud Guard presenta sugerencias de actuación a través del servicio de Security Advisor (Asesor de seguridad), prestando asistencia o tomando automáticamente medidas correctivas en función de la configuración del servicio. Para obtener más información relacionada con el servicio de Cloud Guard, consulte la guía de seguridad "CCN-STIC-889A Guía de Configuración segura para IAM y servicios de Seguridad".

Para continuar, el servicio de zonas de seguridad permite que los recursos en OCI, incluido los recursos de computación, redes y almacenamiento de objetos cumplen con los mecanismos de prevención descritos en esta medida.

Una zona de seguridad está asociada a un compartimento y una receta de zona de seguridad. Una receta de zona de seguridad es una colección de políticas que se aplican en la zona de seguridad. Cuando se crea o se actualiza recursos en una zona de seguridad, OCI valida estas operaciones con la lista de políticas definidas en la receta de la zona de seguridad. Si se infringe alguna política de zona de seguridad, se deniega la operación.

Asimismo, en el tenant se dispone de una receta predefinida denominada Receta de máxima seguridad, que incluye todas las políticas de zona de seguridad disponibles gestionadas por Oracle y sin posibilidad de modificación.

En general, las políticas de la zona de seguridad restringen las siguientes acciones que podrían vulnerar la seguridad de la infraestructura:

a) Los recursos no se pueden mover de una zona de seguridad a un compartimento estándar.

b) Los datos de una zona de seguridad no se pueden copiar en un compartimento estándar.

c) Todos los componentes necesarios para un recurso en una zona de seguridad también deben estar ubicados en una zona de seguridad. Los recursos que no se encuentran en una zona de seguridad pueden ser vulnerables.

d) Los recursos en una zona de seguridad no deben ser accesibles desde internet.

e) Los recursos de una zona de seguridad deben cifrarse mediante claves administradas por el cliente.

f) Los recursos en una zona de seguridad deben respaldarse de forma regular y automática.

g) Los recursos en una zona de seguridad deben usar solo configuraciones y plantillas aprobadas por Oracle.

Para obtener más información relacionada con las políticas de Zona de seguridad, consulte el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/security-zone/using/security-zone-policies.htm

Para la creación de una zona de seguridad, debe navegar por el menú de navegación de OCI → Identidad y seguridad → Zonas de seguridad → Visión general, y realizar las siguientes acciones:

a) Haga clic en el botón “Crear zona de seguridad” desde el panel de visión general.

b) Introduzca un nombre y una descripción evitando compartir información confidencial. Oracle Cloud creará un compartimento con el mismo nombre y lo asignará a la zona de seguridad creada.

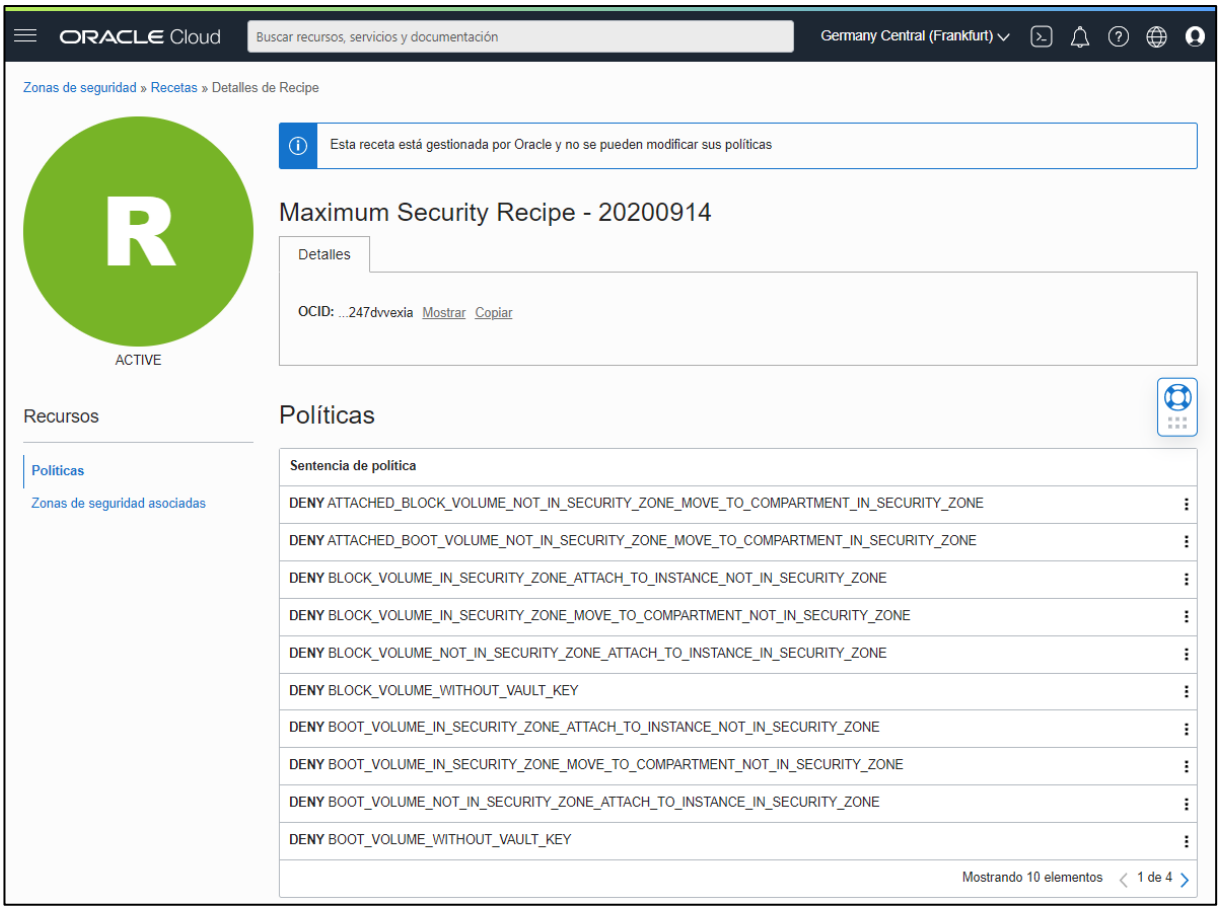
Ventana para crear una zona de seguridad.

c) También puede seleccionar el compartimento en el que desea que Oracle Cloud cree una nueva Zona. Para finalizar, haga clic en el botón “Crear zona de seguridad”.

d) Haga clic en el nombre de la nueva Zona de seguridad creada para obtener más datos.

Detalles de la Zona de seguridad.

e) Haga clic en el menú “Recetas” para obtener más información.



Políticas predefinidas por Oracle Cloud de la Zona de seguridad configurada.

Asimismo, existe en OCI el servicio llamado Security Advisor (Asesor de seguridad) que unifica los servicios de Cloud Guard y zonas de seguridad y otros servicios en un panel homogéneo. OCI Security Advisor (Asesor de seguridad) combina los flujos de trabajo existentes para crear de manera eficiente recursos que cumplan con los requisitos básicos de seguridad desde el principio, reforzando las mejores prácticas de seguridad incluido los requisitos de configuración para los recursos en las zonas de seguridad.

Mediante el servicio de OCI Security Advisor (Asesor de seguridad), es posible crear un bucket o sistema de ficheros, una instancia de máquina virtual o un volumen de bloque de manera segura. Para obtener más información relacionada con el servicio, consulte el siguiente enlace de Oracle:

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

Cabe destacar el servicio de análisis de vulnerabilidades de OCI para la detección de vulnerabilidades mediante análisis rutinarios en los hosts. El servicio genera informes con métricas y detalles sobre estas vulnerabilidades. El servicio de análisis de vulnerabilidades puede identificar varios tipos de problemas de seguridad en las instancias de cómputo de máquina virtual y bare metal:

a) Puertos abiertos que pueden ser un vector de ataque potencial para los recursos en la nube.

b) Paquetes del sistema operativo que requieren actualizaciones y parches que aborden las vulnerabilidades.

c) Configuraciones del sistema operativo que pueden dejar expuestas a las instancias a posibles ataques.

d) Comprobación de las referencias estándar del sector publicadas por el CIS.

Nota: El servicio de análisis de vulnerabilidades está disponible únicamente para las imágenes de Linux.

Para utilizar el servicio de análisis y comprobar las vulnerabilidades de seguridad en las instancias cómputo, se debe configurar una receta de exploración, un destino, los permisos de acceso para la configuración del servicio y los permisos otorgados al propio servicio, para la activación del agente de exploración en las instancias de destino.

Para obtener más información relacionada con las políticas necesarias para la exploración de hosts, consulte el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/scanning/using/managing-host-targets.htm

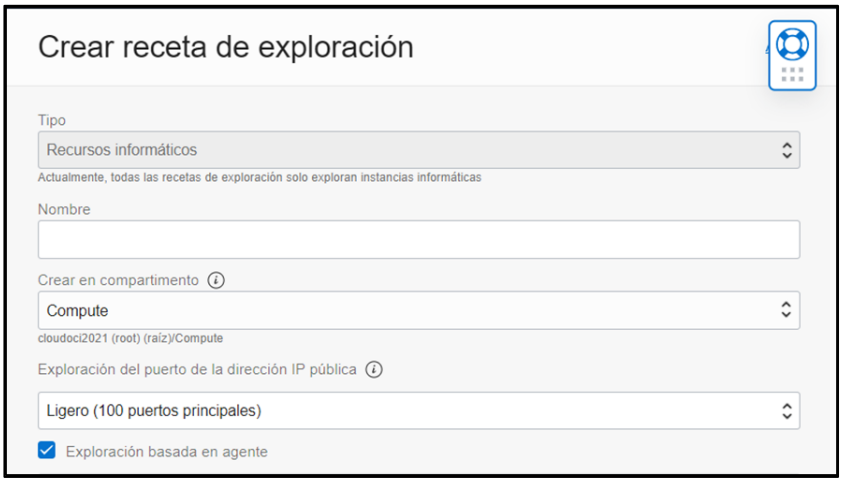
Para crear una receta de explotación, debe navegar por el menú de OCI → Identidad y seguridad → Explorando → Recetas de exploración.

Debe crear una Receta de exploración y seleccionar los siguientes elementos del cuadro:

a) Tipo de recurso a explorar.

b) Nombre de la receta.

c) El compartimento donde se ejecutará la receta.

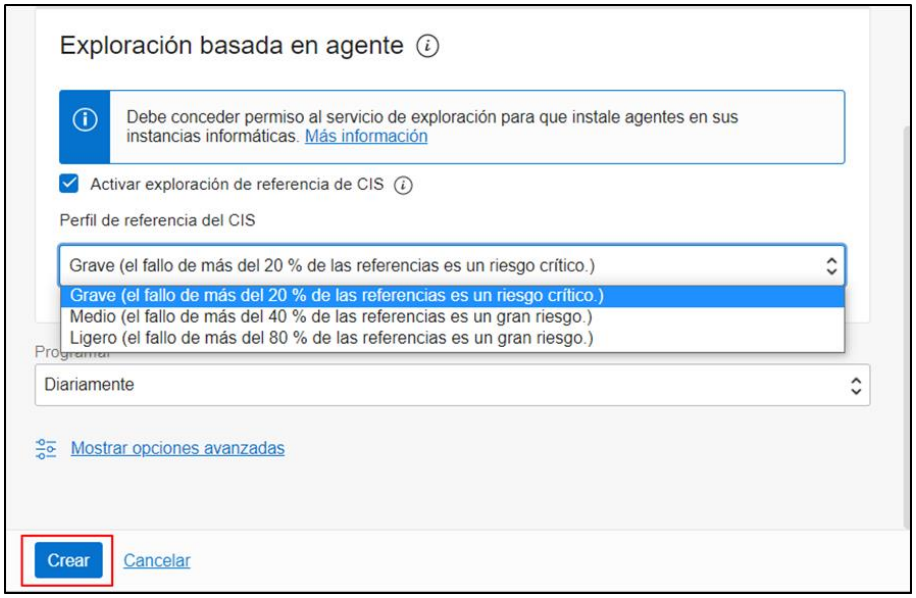


Ventana para la creación de una receta (Parte superior).

d) Exploración de puertos abiertos.

e) Exploración basada en agente para las instancias de cómputo.

f) Seleccione activar exploración de referencia de CIS para las instancias Linux y elegir un porcentaje de gravedad de las referencias.



Ventana para la creación de una receta (Parte inferior).

g) Por último, seleccione la programación para la exploración de vulnerabilidades.

Para crear un destino, debe navegar por el menú de OCI → Identidad y seguridad → Explorando → Destinos.

Debe crear un Destino y seleccionar los siguientes elementos del cuadro:

a) Seleccione el tipo de recurso a explorar.

b) Identifique el destino con un nombre.

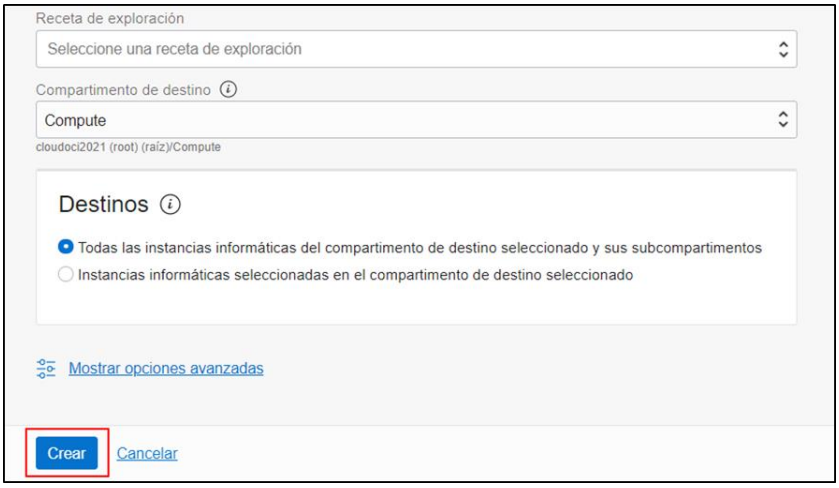
c) Seleccione el compartimento para crear este recurso.

Ventana para la creación de un Destino.

d) Opcionalmente, puede añadir una descripción para el destino.

e) Elija la receta de exploración creada con anterioridad.

f) Seleccione el compartimento que contiene las instancias de cómputo que desea explorar.

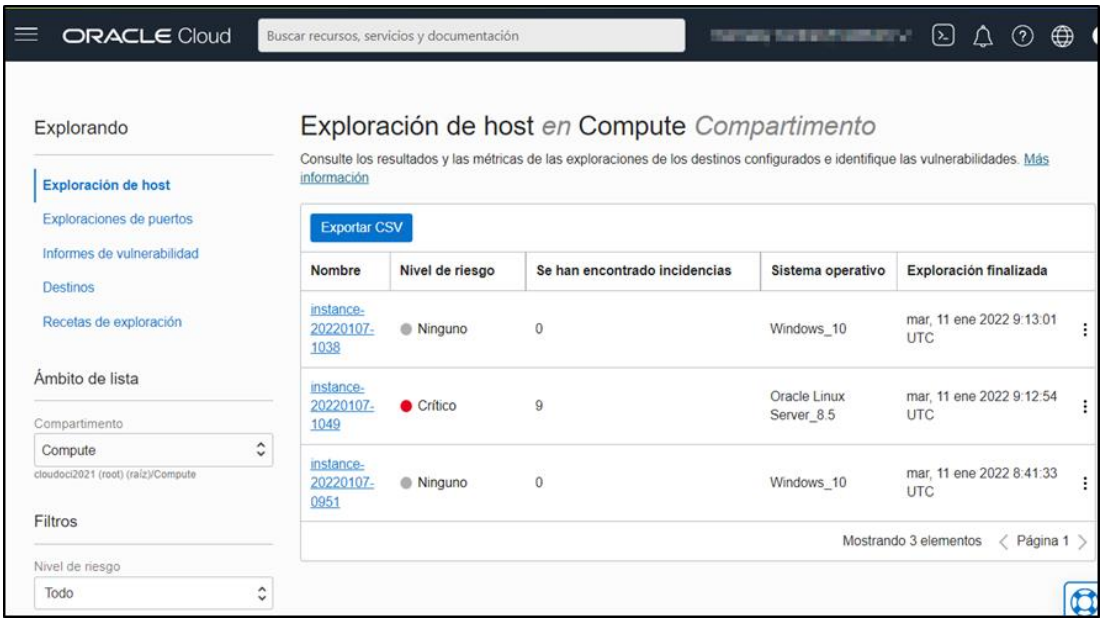


g) Puede elegir en destinos explorar todas las instancias de cómputo del compartimento de destino seleccionado y sus subcompartimentos o bien explorar las instancias cómputo seleccionadas en el compartimento de destino seleccionado.

h) Por último, haga clic en Crear para disponer de un destino de exploración.

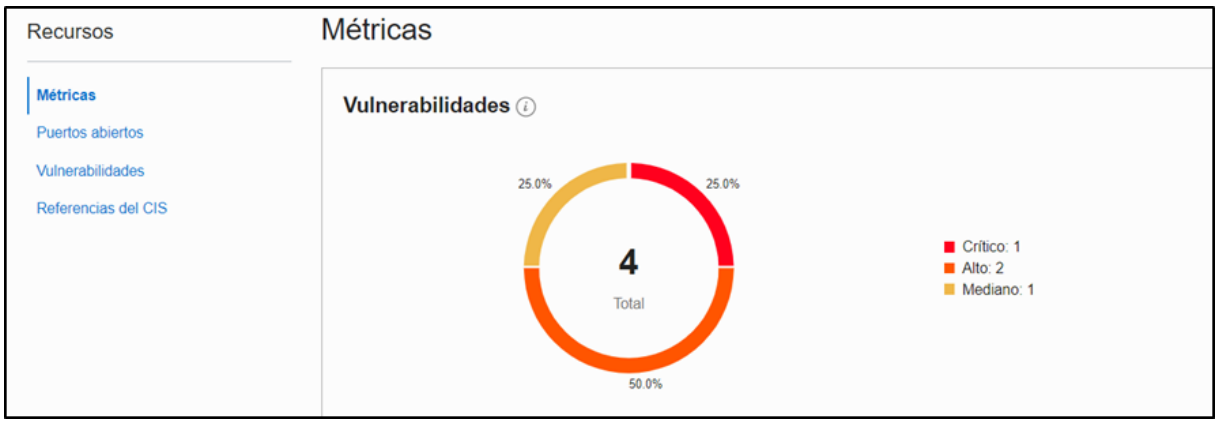
Para finalizar, en el panel de exploración se pueden ver los siguientes elementos que aportan información sobre las instancias de cómputo:

a) El apartado de exploración de host, indica los resultados y las métricas de las exploraciones de los destinos configurados que identifican las vulnerabilidades de seguridad en las instancias de cómputo de manera individualizada.

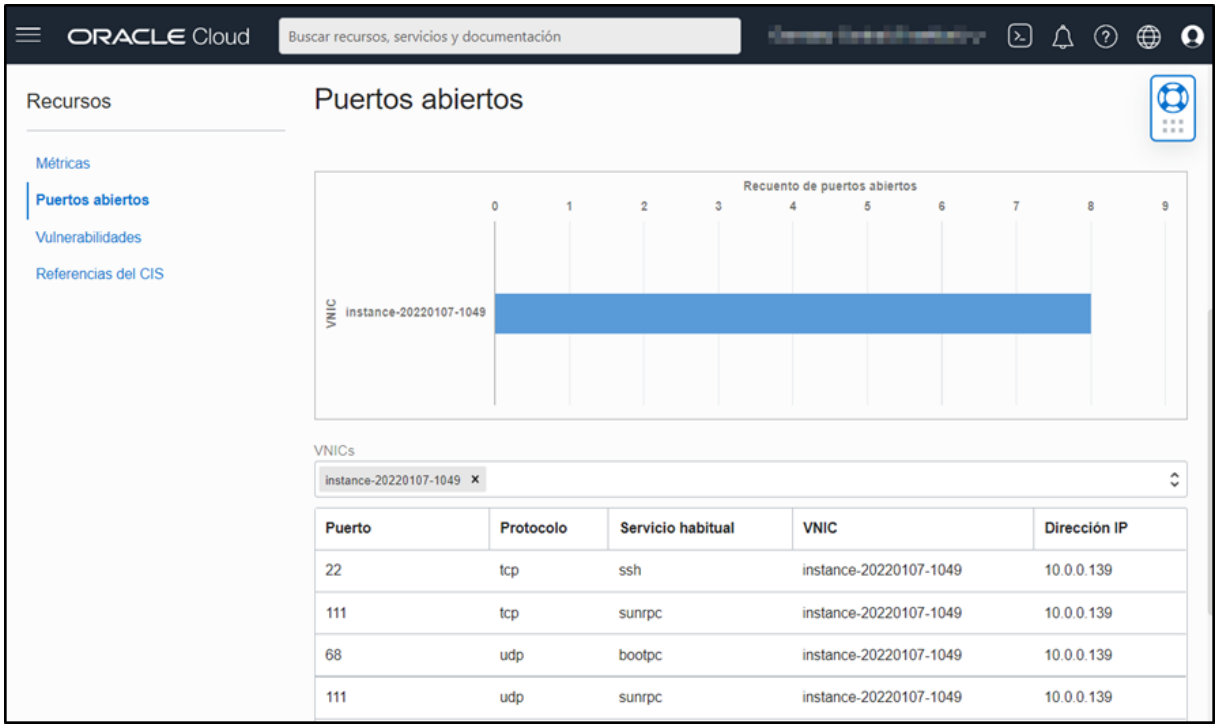


b) Dentro del apartado de exploraciones de host, accediendo a los recursos de cada instancia de manera individual, se puede ver una serie de recursos del servicio de análisis de vulnerabilidades que proporcionan la información necesaria, para establecer una estrategia de seguridad que minimice la superficie de ataque y cumpla con la medida de seguridad establecida por el ENS:

i. **Métricas:** proporciona información gráfica de las vulnerabilidades existentes de la instancia informática.

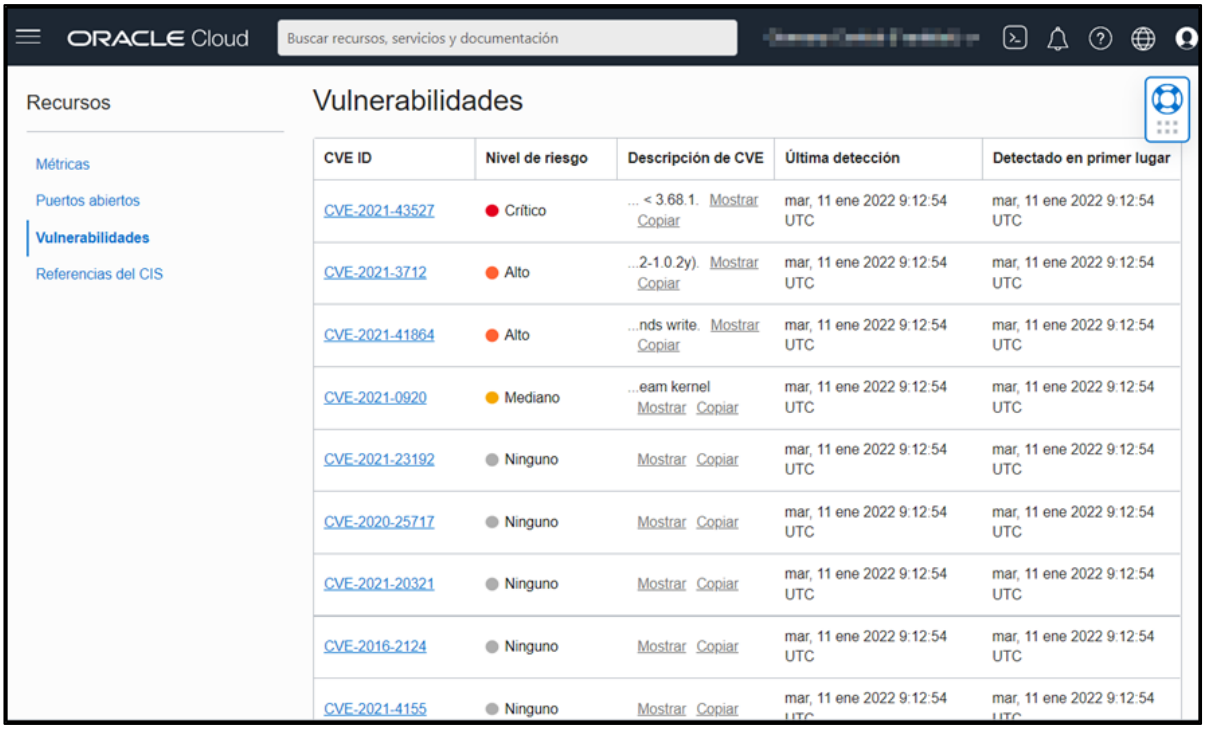


ii. **Puertos abiertos**: proporciona información de los puertos abiertos actualmente por cada instancia. Para ello, se debe seleccionar en el cuadro de VNICs, la instancia concreta que se desee examinar.



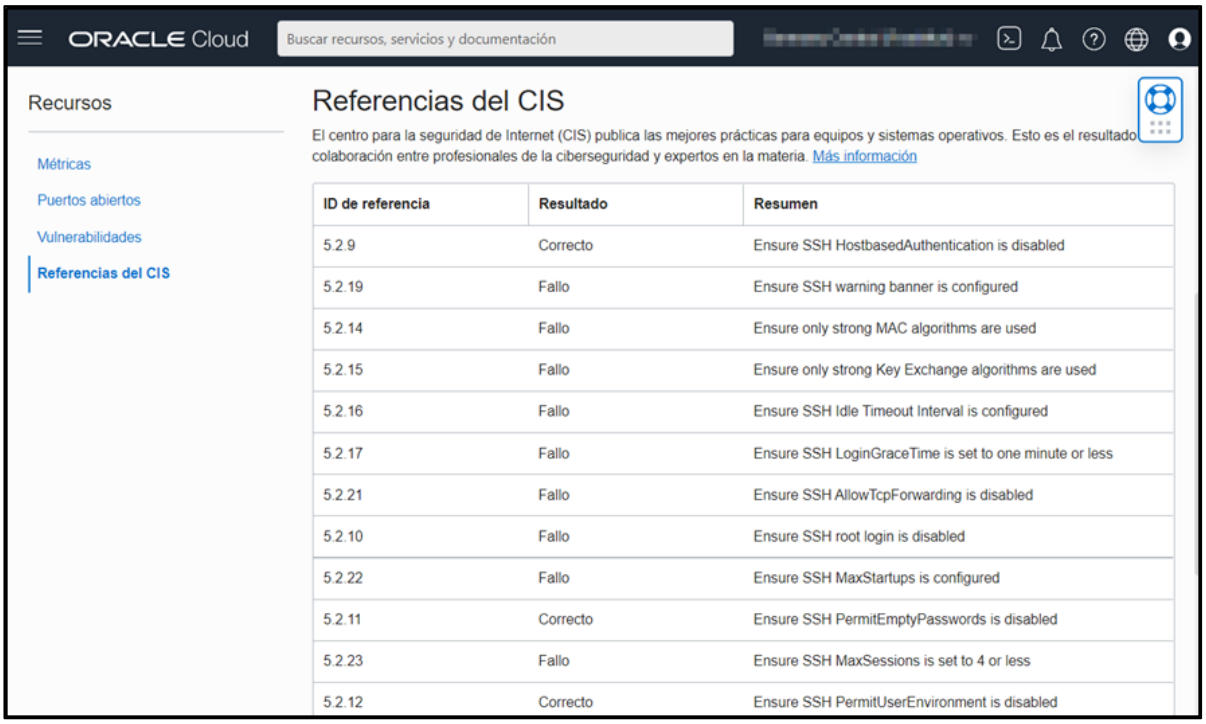
Panel de puertos abiertos.

c) **Informes de vulnerabilidad:** proporciona información de las vulnerabilidades y exposiciones comunes conocidas e identificadas en MITRE CVE List.



Panel de vulnerabilidades detectadas en las instancias de cómputo.

d) **Referencias del CIS:** proporciona información relacionada con las mejores prácticas para las instancias de cómputo y los sistemas operativos.



Panel de referencias del CIS.

2.1.2.4 GESTIÓN DE INCIDENTES

Para la presente medida de seguridad, el ENS establece que debe disponerse de un proceso integral para hacer frente a los incidentes que puedan tener un impacto en la seguridad del sistema, incluyendo los siguientes elementos:

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 la protección de los registros.

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

d) Procedimiento para informar a las partes interesadas, tanto internas como externas.

e) Procedimientos para prevenir que se repita el incidente, incluir la identificación del usuario y la forma de tratar el incidente y actualizar, mejorar u optimizar la resolución de incidentes.

La gestión de incidentes que afecten a datos de carácter personal tendrá en cuenta lo dispuesto en las diferentes leyes nacionales y de la Unión Europea.

Para esta medida procedimental, OCI dispone de herramientas de reporte como Cloud Guard que apoyan y previenen incidentes, minimizando los riesgos posibles para los recursos del tenant. El servicio en la nube ayuda en la supervisión, identificación y mantenimiento de una estrategia de seguridad, examinando los recursos y detectando deficiencias de seguridad relacionadas con la configuración. Tras la detección de un incidente, OCI Cloud Guard puede ofrecer sugerencias, prestar asistencia o tomar medidas correctivas en función de la configuración previa dada al servicio.

No obstante, antes de poder activar el servicio de Cloud Guard para la gestión de la presente media de seguridad, es necesario cumplir con los siguientes requisitos que puede consultar a través del siguiente enlace de Oracle:

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

Además, Oracle dispone de una serie de recomendaciones a realizar antes de activar el servicio de Cloud Guard, que puede consultar a través del siguiente enlace de la documentación oficial:

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

Para finalizar, puede obtener más información del servicio a través de la guía de seguridad “CCN-STIC-889A Guía de Configuración segura para IAM y servicios de seguridad”.

2.1.2.5 REGISTRO DE LA ACTIVIDAD DE LOS USUARIOS

La medida de seguridad indica que deben registrarse todas las actividades de los usuarios en el sistema, de manera que exista un registro que indique quién realizó una actividad, cuándo se realizó y sobre qué recurso se hizo. También se debe recoger la actividad de los usuarios y administradores en cuanto puedan acceder a la configuración y actuar en el mantenimiento del sistema.

Por otro lado, se deben registrar todas aquellas actividades realizadas con éxito y también los intentos fracasados. Para la categoría alta, el ENS establece que deben activarse los registros de actividad en los servicios de compute (recursos informáticos). Además, se dispondrá de un sistema automático de recolección de registros y correlación de eventos mediante una consola centralizada.

La aplicación técnica de la presente medida de seguridad puede ser realizada mediante el servicio de auditoría de OCI. El servicio de auditoría registra automáticamente todas las acciones de los usuarios y las llamadas a todos los puntos finales de la interfaz pública de programación de aplicaciones (API) mediante eventos de log.

Para obtener más información relacionada con la visión general del servicio de auditoría, consulte la guía de seguridad “CCN-STIC-889A Guía de Configuración segura para IAM y servicios de seguridad”.

Para obtener más información relacionada con los logs de auditoría, consulte la guía de seguridad “CCN-STIC-889B Guía de Configuración segura para Monitorización y gestión”.

Para finalizar, es importante revisar periódicamente las políticas para asegurarse de que se cumplen las buenas prácticas de seguridad. El auditor de políticas puede revisar las políticas de IAM manualmente desde la consola de OCI, o bien desde el servicio de Cloud Guard de OCI, ya que dispone de dos recetas de detector de configuración y una receta de detector de actividad específica para las políticas de IAM.

Además, se debe revisar la actividad de los usuarios en el servicio de OCI Vault para controlar qué o quién ha accedido y ha realizado qué acciones sobre qué claves y secretos guardados en los almacenes de la organización.

2.1.2.6 REGISTRO DE LA GESTIÓN DE INCIDENTES

El registro de la gestión de incidentes indica el deber de registrar todas las actuaciones relacionadas con la gestión de incidentes, de manera que se registre el reporte inicial, las actuaciones de emergencia y las modificaciones del sistema derivadas del incidente. Además, se debe registrar las evidencias que puedan sostener una demanda judicial o hacer frente a ella, cuando el incidente pueda llevar a actuaciones disciplinarias sobre el personal interno, proveedores externos o la persecución de delitos. Por último, y a consecuencia del análisis de los incidentes, debe revisarse la determinación de los eventos auditables.

La aplicación técnica de la presente medida de seguridad involucra los servicios de OCI Cloud Guard y OCI Eventos. OCI conserva los registros de auditoría por 365 días sin borrar ninguna acción realizada en la gestión de los problemas desde el servicio de Cloud Guard, garantizando la existencia de evidencias frente a los posibles problemas detectados.

Por otro lado, el servicio de OCI eventos, recoge eventos de los servicios definidos en OCI Compute, como las instancias de cómputo, el motor de contenedor para Kubernetes o los servicios de almacenamiento y servicios de red.

Para obtener más información relacionada con los servicios que generan eventos, consulte el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/Content/Events/Reference/eventsproducers.htm

Además, el servicio de eventos permite habilitar la automatización basada en los cambios de estado de los recursos del tenant, enviando notificaciones a través del servicio de OCI notificaciones.

Para obtener más información relacionada con el servicio de notificaciones, consulte la guía de seguridad "CCN-STIC-889B Guía de Configuración segura para Monitorización y gestión".

Por otro lado, es posible la configuración de los servicios de eventos y notificaciones para enviar notificaciones, siempre que Cloud Guard detecte un problema para el que se desea notificar, a través de los siguientes tipos de eventos:

a) **Problema solucionado:** Cuando un responsable de respuesta configurado para solucionar automáticamente cualquier problema detectado emprende la solución.

b) **Umbral de problema alcanzado:** Cuando Cloud Guard descubre que se han alcanzado determinados umbrales debido a señales de auditoría excesivas de servicios como VCN o IAM.

Para hacerlo, se debe configurar los servicios de eventos y notificaciones desde la región de informe de Cloud Guard, que combina los problemas de las regiones supervisadas y envía el evento en la nube desde la región de informe.

Finalmente, para obtener más información relacionada con la configuración de notificaciones para la detección de incidentes por parte de Cloud Guard, consulte el siguiente enlace de Oracle:

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

2.1.2.7 PROTECCIÓN DE CLAVES CRIPTOGRÁFICAS

Según el ENS, las claves criptográficas deben protegerse durante todo su ciclo de vida, desde su generación, transporte al punto de explotación, custodia durante la explotación, archivo posterior a su retirada de explotación activa hasta su destrucción final.

La protección de claves criptográficas para la categoría alta, el ENS establece que debe aislarse los medios de generación de las claves de los medios de explotación, y aquellas claves que sean retiradas de operación y deban ser archivadas, también debe realizarse en medios aislados de los medios de explotación. Además, deben usarse programas evaluados o dispositivos criptográficos certificados, así como el empleo de algoritmos acreditados por el CCN.

Para ello, OCI dispone del servicio Vault que permite gestionar de forma centralizada, tanto las claves de cifrado como los secretos o credenciales usados para el acceso seguro a los recursos de la nube. Además, mediante el servicio de OCI Vault es posible cumplir todos los requisitos establecidos por el ENS en la presente medida de seguridad en un medio de explotación.

El servicio de Vault se compone de tres recursos fundamentales para poder gestionar: almacenes, claves y secretos. Y dichos recursos se conectan con los servicios de almacenamiento o los servicios de compute (recursos informáticos) o bases de datos. También se integra con el servicio de OCI IAM, para controlar quién y qué servicios pueden acceder a qué claves y secretos y el servicio OCI Audit, para proporcionar una forma de supervisar quién o el qué ha hecho uso de las claves y secretos almacenados.

Por otro lado, OCI Vault dispone de dos modos de almacenamiento para la custodia durante la generación, explotación, archivado y destrucción final de los almacenes, claves y secretos. Una vez creado el almacén, éste no puede ser modificado:

a) **Almacén de tipo público por defecto:** La partición HSM donde se aloja el almacén creado es compartida con otros almacenes.

b) **Almacén de tipo privado:** Un almacén privado virtual reside en una partición aislada de HSM.

Todos los tipos de almacenes garantizan la seguridad e integridad de los secretos y claves de cifrado almacenados en los módulos HSM, que cumplen con la certificación de seguridad de nivel 3 de los estándares de procesamiento de información federal (FIPS) 140-2.

Además, 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).

Para finalizar, el servicio de OCI Vault permite la generación y gestión de versiones para las claves y los secretos dentro de un almacén. Solamente estará disponible en los medios de explotación una versión de la clave o secreto, pudiendo poner en reserva una versión nueva o archivar una versión antigua, cumpliendo con la exigencia establecida por parte del ENS para el archivado de las claves criptográficas.

Además, en lo que concierne a la presente guía de configuración segura para OCI Compute, se debe utilizar el servicio Vault para generar, importar o guardar claves y secretos para su uso en los servicios de almacenamiento necesarios para el funcionamiento de las instancias, y para generar, importar o guardar las credenciales de los usuarios o API para el acceso y uso de los recursos del tenant.

Para obtener más información relacionada con el servicio OCI Vault y la generación de almacenes, claves y secretos, consulte la guía de seguridad “CCN-STIC-889A Guía de Configuración segura para IAM y servicios de seguridad”.

2.1.3 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.

2.1.3.1 DETECCIÓN DE INTRUSIÓN

La medida de seguridad establecida por el ENS indica que se debe disponer de las herramientas necesarias para la detección o prevención de intrusión en el sistema. Para ello, OCI dispone varias herramientas de seguridad nativas, como el servicio de Cloud Guard para los recursos del tenant, el servicio de análisis de vulnerabilidades para las instancias de cómputo o las herramientas de terceros que puede encontrar en el Marketplace.

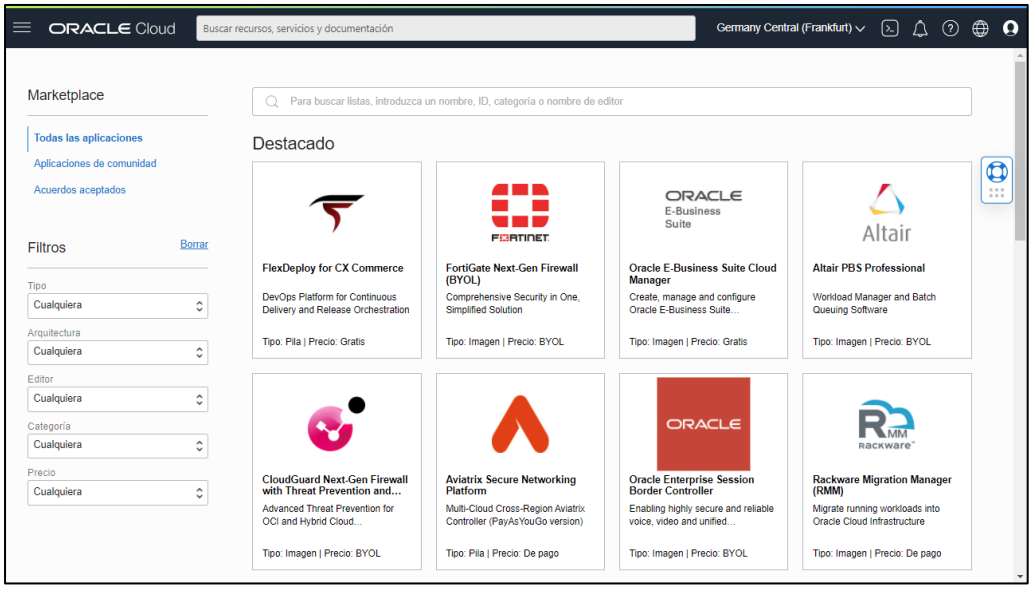
Así pues, para obtener más información relacionada con el servicio de Cloud Guard, puede consultar la guía de seguridad "CCN-STIC-889A Guía de Configuración segura para IAM y servicios de seguridad". Por otro lado, en la medida de seguridad indicada en el punto 2.1.2.3 PROTECCIÓN FRENTE A CÓDIGO DAÑINO, puede encontrar más información relacionada con el servicio de análisis de vulnerabilidades.

Para finalizar, OCI Marketplace es una tienda en línea que ofrece soluciones específicamente a clientes de OCI. En su catálogo, puede encontrar listas para dos tipos de soluciones de Oracle y partners de confianza: imágenes y pilas. Estos tipos de listas incluyen diferentes categorías de aplicaciones gratuitas y otras de pago.

Las imágenes son plantillas de unidades de disco duro virtuales que determinan el sistema operativo y el software que se va a ejecutar en una instancia. Las pilas representan definiciones de grupos de recursos de OCI en las que puede trabajar como si se tratara de un grupo. Cada pila tiene una configuración que consta de uno o más archivos de configuración declarativos. La imagen o la pila ofrece una forma más optimizada y personalizada de comenzar a utilizar el software de un publicador.

Para acceder al Marketplace de OCI y buscar software para la detección de intrusión, debe navegar por el menú de OCI → Marketplace → Todas las aplicaciones.

a) En la sección de filtros de la página de todas las aplicaciones del Marketplace, puede filtrar la búsqueda de aplicaciones de seguridad por tipo, arquitectura, editor, categoría y precio.



Menú de Marketplace con todas las aplicaciones disponibles.

2.1.3.2 SISTEMA DE MÉTRICAS

La medida de seguridad establecida por el ENS para el sistema de métricas en la categoría alta dice, que deben recopilarse los datos necesarios atendiendo a la categoría del sistema, para conocer el grado de implantación de las medidas de seguridad aplicadas y proveer el informe anual requerido. Además, se deben recopilar datos para valorar el sistema de gestión de incidentes, permitiendo conocer el número de incidentes de seguridad tratados, el tiempo empleado para cerrar el 50% de los incidentes y el tiempo empleado para cerrar el 90% de los incidentes.

Por último, se deben recopilar datos para conocer la eficiencia del sistema de seguridad TIC como la cantidad de recursos consumidos, horas invertidas y presupuesto final.

Una métrica es una medida relacionada con el estado, la capacidad o el rendimiento de un recurso determinado. Los principales recursos que deben supervisarse son aquellos que conciernen a los servicios de OCI Compute y los servicios y recursos relacionados que posibilitan el funcionamiento de los servicios de OCI Compute. Puede mencionarse como recursos importantes de los servicios relacionados aquellos concernientes al almacenamiento, la infraestructura de red o la seguridad.

Las métricas son un conjunto de referencias y otra información proporcionada por un espacio de nombres de métrica, para una métrica determinada. Un espacio de nombres es un contenedor abstracto en el que un grupo de uno o más identificadores únicos pueden existir. Asimismo, una métrica definida en un espacio de nombres está asociada con ese espacio de nombres en particular.

Por otro lado, el servicio de supervisión permite supervisar de forma activa y pasiva los recursos en la nube mediante las funciones de métricas y alarmas, a fin de notificar en caso de que dichas métricas alcancen los disparadores especificados por las alarmas. Asimismo, las métricas se emiten al servicio de supervisión en forma de puntos de datos no procesados o pares de marca de tiempo-valor junto con las dimensiones y los metadatos.

Para obtener más información relacionada con el servicio de supervisión y otros servicios de monitorización y gestión, consulte la guía de seguridad “CCN-STIC-889B Guía de Configuración segura para Monitorización y gestión”.

A continuación, se describen varios espacios de nombres de métricas de los servicios de OCI Compute y los servicios de la infraestructura donde se ejecutan los recursos informáticos. Cada espacio de nombres incluye métricas particulares y únicas de cada recurso y servicio que debe ser monitorizado:

Servicio	Espacio de nombres de métrica	Descripción
Instancias de cómputo.	oci_computeagent	Métricas relacionadas con el nivel de actividad y el rendimiento de las instancias de cómputo.
	oci_instancespools	Métricas relacionadas con el estado del ciclo de vida de las instancias en los pools de instancias.

Servicio	Espacio de nombres de métrica	Descripción
	oci_compute_infrastructure_health	Métricas relacionadas con el estado activo/inactivo y el estado de mantenimiento de las instancias de cómputo.
	oci_compute	Métricas relacionadas con el servicio de metadatos de instancia (IMDS) que proporciona información sobre la ejecución de instancias de cómputo.
Functions (funciones).	oci_faas	Métricas que miden la capacidad, rendimiento y el estado de las funciones desplegadas.
Kubernetes	oci_oke	Métricas para supervisar los clústeres de Kubernetes y pools de nodos y nodos de trabajadores individuales.
Volumen de bloque.	oci_blockstore	Métricas relacionadas con el servicio de volumen de bloque. Las métricas son para un volumen individual, ya sea de inicio o de bloque.
Almacenamiento de archivos.	oci_filestorage	Métricas para supervisar el estado, la capacidad y el rendimiento de los sistemas de archivos y los destinos de montaje.
Almacenamiento de objetos.	oci_objectstorage	Métricas para supervisar el estado, la capacidad y el rendimiento de los buckets y objetos.
Networking.	oci_vcn	Métricas emitidas por las tarjetas de interfaz de red virtual (VNIC)
Bastión.	oci_bastion	Métricas que supervisan el estado, capacidad y rendimiento del servicio OCI Bastión.
Vault.	oci_kms_keys oci_secrets	Métricas para la supervisión del uso de los secretos y claves de cifrado maestras.
Análisis de vulnerabilidades.	oci_vss	Métricas para la supervisión de las vulnerabilidades detectadas por el servicio en los recursos en la nube.
Gestión del Sistema operativo.	oci_osms	Las métricas del servicio de gestión del sistema operativo ayudan a medir el número de instancias gestionadas activas e inactivas, el número de instancias gestionadas con actualizaciones de seguridad disponibles y el número de instancias gestionadas con actualizaciones disponibles.
Firewall de aplicaciones web (WAF).	oci_waf	Las métricas de servicio de WAF ayudan a medir los diferentes niveles de tráfico que encuentran las políticas de WAF, incluido el tráfico no malicioso.

Servicio	Espacio de nombres de métrica	Descripción
Eventos.	oci_cloudevents	Las métricas ayudan a medir el éxito de las reglas que se crean (en términos de coincidencia con un patrón y entrega), así como la calidad y el ámbito de los eventos emitidos en el tenant.

Para finalizar y obtener más información relacionada con las métricas emitidas por los servicios soportados por supervisión, consulte el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/Content/Monitoring/Concepts/monitoringoverview.htm#SupportedServices

2.2 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.

2.2.1 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.

2.2.1.1 PERÍMETRO SEGURO

Para la presente medida de seguridad, el ENS establece para la categoría alta, que debe disponerse de un sistema de cortafuegos que separe la red interna del exterior. Todo el tráfico debe atravesar el cortafuegos y solamente dejará transitar los flujos previamente autorizados. Además, el sistema de cortafuegos debe disponer de dos más equipos de diferentes fabricantes y asegurarse de la redundancia del sistema.

Por un lado, debe usarse firewalls basados en host para restringir el acceso a las instancias mediante el control de puertos, protocolos y tipos de paquetes que transitan por las capas 3, 4 y 5 del modelo OSI o las capas de red, transporte y sesión del modelo TCP/IP.

Por defecto, todas las plataformas de imagen o shape incluyen reglas esenciales del firewall que permiten a los administradores de instancias de Windows o root para instancias de Linux, realizar conexiones salientes a los puntos finales de red iSCSI (169.254.0.2:3260, 169.254.2.0/24:3260) que sirven los volúmenes de inicio y en bloque de la instancia. Por ello, no se debe eliminar estas reglas del firewall.

Por otro lado, la solución técnica que ofrece OCI para la protección de las capas superiores de comunicación reside en el servicio WAF, que es un firewall de aplicaciones web basado en regiones y asociado a un punto de aplicación, que se distingue de cualquier firewall basado en host por el nivel de aplicación de la protección.

Un firewall de aplicaciones web protege contra ataques complejos de capa 7 o de capa de aplicación como inyecciones SQL, inyecciones STML, exploits y otras vulnerabilidades definidas por OWASP, filtrando, mediante reglas, el tráfico HTTP o HTTPS. La respuesta de un WAF será permitir que una solicitud transite, sea auditada, registrada o bloqueada, para proteger las aplicaciones web que corren en las instancias y disponen de una comunicación con el exterior.

Nota: Puede revisar las aplicaciones disponibles en el Marketplace de OCI donde puede encontrar diferentes fabricantes y soluciones de firewall para el cumplimiento de la medida de seguridad en la categoría alta.

Finalmente, para obtener más información relacionada con el servicio de OCI WAF, consulte el siguiente enlace de Oracle:

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

2.2.1.2 PROTECCIÓN DE LA CONFIDENCIALIDAD

Para la categoría alta, el ENS establece que deben emplearse redes privadas virtuales cuando la comunicación discurra por redes fuera del propio dominio de seguridad, empleando, a su vez, algoritmos acreditados por el CCN. Además, preferiblemente deben emplearse dispositivos de hardware en el establecimiento y uso de la red privada virtual y productos certificados conforme a lo establecido en el ENS.

La aplicación técnica para la protección de la confidencialidad se realiza mediante el servicio de red de OCI. Los elementos de seguridad que ofrece OCI para las conexiones VCN, VPN y FastConnect son las subredes privadas, las listas de seguridad y los grupos de seguridad de red.

a) **Subredes privadas:** al crear una subred, se considera pública por defecto, lo que significa que las instancias de esa subred pueden tener direcciones IPv4 o IPv6 públicas, permitiendo la comunicación a internet. Puede cambiar y crear la subred solicitando que sea privada, lo que no permite el uso de direcciones IP públicas y la comunicación de internet.

   Por tanto, los administradores de la red pueden asegurarse de que las instancias de la subred no tengan acceso a internet, incluso si la VCN tiene un Gateway de internet en funcionamiento y las reglas de seguridad y las reglas del firewall permiten el tráfico.

Para obtener una visión general de las VCN y las subredes, consulte el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/Content/Network/Tasks/managingVCNs_topic-Overview_of_VCNs_and_Subnets.htm

b) **Listas de seguridad:** el servicio de red de OCI ofrece dos funciones de firewall virtual para controlar el tráfico en el nivel de paquete. La primera función, las listas de seguridad, actúan como cortafuegos virtuales para las instancias de cómputo y otros recursos. 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. Esto es, todas las VNIC de una subred determinada están sujetas al mismo conjunto de listas de seguridad.

   Al crear una subred, debe asociarle al menos una lista de seguridad. Puede ser la lista de seguridad predeterminada de la VCN o una o más listas de seguridad que haya creado. No obstante, para el control de acceso, debe especificar el comportamiento en el que vaya a residir la lista de seguridad, pudiendo mover dichas listas entre compartimentos.

   Para obtener más información relacionada con las reglas de seguridad para controlar el tráfico a nivel de paquete, consulte el siguiente enlace de Oracle:

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

c) **Grupos de seguridad de red (NSG):** al igual que las listas de seguridad, los grupos de seguridad de red actúan como un firewall virtual para las instancias de cómputo y otros tipos de recursos del tenant. Sin embargo, a diferencia de una lista de seguridad que se aplica a las VNIC de una subred concreta, un grupo de seguridad de red se aplica a un conjunto concreto de VNIC. En comparación con las listas de seguridad, los grupos de seguridad de red permiten separar la arquitectura de subred de la VCN de una forma más granular, pero no son excluyentes, pudiendo convivir conjuntamente las Listas de seguridad con los NSG.

   Para obtener más información relacionada con el soporte para grupos de seguridad de red, consulte el siguiente enlace de Oracle:

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

2.2.1.3 SEGREGACIÓN DE REDES

La medida de seguridad establece que debe haber segregación de redes para acotar el acceso a la información. En consecuencia, la propagación de los incidentes de seguridad queda restringidos al entorno donde se producen. Para la categoría alta del ENS, la red se segmentará en segmentos de forma que exista los siguientes elementos de protección basados en el control, mantenimiento y monitorización de la red:

a) Control de entrada de los usuarios que llegan a cada segmento, mediante la disposición de un plan previo que abarque la jerarquía de compartimentos para la organización de los recursos. Por un lado, debe quedar definido los grupos de usuarios que necesitarán acceder a los recursos del tenant a través de la escritura de políticas necesarias y ajustadas, que cumplen con el principio de privilegio mínimo.

Por otro lado, OCI dispone del servicio de zonas de seguridad asociada a los compartimentos, que asegura las cargas de trabajo, la configuración de los servicios y aplicaciones a través de una receta de seguridad.

b) Control de salida de la información disponible en cada segmento. Las redes deben ser segmentadas por subredes, tanto privadas como públicas, diseñando con precisión aquellos recursos que deben ser protegidos de las comunicaciones con el exterior.

   OCI dispone de funciones de control como las listas de seguridad y los grupos de seguridad de red para la elaboración de reglas que controlan el tráfico en el nivel de paquete.

c) Las redes pueden ser segmentadas por dispositivos físicos o lógicos, donde el punto de interconexión debe estar completamente asegurado, mantenido y monitorizado.

Para finalizar, el usuario cuenta con el servicio de OCI WAF que, junto con los compartimentos, zonas de seguridad, subredes, listas de seguridad o grupos de seguridad de red, sirve para la realización de los controles establecidos por el ENS para la presente medida de protección de las comunicaciones.

2.2.2 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.

2.2.2.1 CIFRADO

Según el ENS, la información con un nivel alto de confidencialidad debe ser cifrada durante su almacenamiento, así como durante su transmisión. Solamente estará descifrada mientras se esté haciendo uso de ella. Además, para el uso de la criptografía en las comunicaciones, se estará a lo dispuesto en la medida de protección de la confidencialidad [mp.com.2] descrita anteriormente.

El cifrado de la información puede definirse según el movimiento de los datos en un momento determinado. Esto es, si la información está en tránsito o en reposo.

El cifrado en tránsito proporciona una manera de proteger los datos entre instancias y sistemas de archivos montados mediante el cifrado TLS v1.2 (seguridad de capa de transporte), mientras que, si la información se encuentra en reposo, todos los datos son cifrados por defecto, pero las claves de cifrado pueden ser gestionadas por Oracle o bien por el cliente.

El cifrado en tránsito no requiere ninguna actualización del destino de montaje o la configuración de exportación del sistema de archivos. Para activar el cifrado en tránsito al crear una instancia informática, tan solo se debe marcar la opción de usar cifrado en tránsito en el volumen de inicio.

Para activar el cifrado en tránsito en una instancia ya creada, consulte el siguiente enlace de Oracle:

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

Por otro lado, para cifrar la información en reposo almacenada en un bloque, cuando éste se crea, se cifra por defecto, tanto el volumen creado como sus copias de seguridad mediante el algoritmo basado en el estándar AES-256. También puede cifrar los volúmenes de datos mediante herramientas como dm-crypt, Veracrypt o BitLocker.

Para obtener más información relacionada con la protección de los volúmenes de bloque, consulte el siguiente enlace de Oracle:

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

Finalmente, para los demás servicios de almacenamiento como el almacenamiento de archivos o el almacenamiento de objetos, todos los datos se cifran por defecto cuando están inactivos mediante AES-256. El cifrado no puede desactivarse y las claves de cifrado de la información se cifran también mediante una clave maestra, que puede gestionar a través del servicio de OCI Vault y consulte más información a través del siguiente enlace de la documentación oficial de Oracle:

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

2.2.2.2 COPIAS DE SEGURIDAD (BACKUP)

El ENS establece que deben realizarse copias de seguridad que permitan recuperar datos perdidos de manera accidental o intencionadamente, con una antigüedad determinada. Las copias de seguridad deben poseer el mismo nivel de seguridad que los datos originales en lo que se refiere a la integridad, confidencialidad, autenticidad y trazabilidad. En particular, se considerará que las copias de seguridad estén cifradas garantizando la confidencialidad de la información.

Además, las copias de seguridad deben abarcar toda la información de trabajo de la organización. Aplicaciones en explotación, incluyendo los sistemas operativos.

También los datos de configuración de servicios, aplicaciones, equipos u otros de naturaleza análoga y, por último, las copias de seguridad deben abarcar, también, las claves utilizadas para preservar la confidencialidad de la información.

Por un lado, se deben realizar copias de seguridad de datos en servicios de almacenamiento que identifique los distintos servicios en los que residen los datos en la aplicación.

a) **Dispositivos NVMe conectados localmente en OCI:** Algunas unidades de instancia de OCI incluyen dispositivos NVMe asociados localmente. Estos dispositivos proporcionan una latencia extremadamente baja y un almacenamiento en bloque de alto rendimiento. OCI no protege estos dispositivos ya que son dispositivos individuales instalados localmente en la instancia. Es la responsabilidad de la organización proteger y gestionar la durabilidad de los datos en estos dispositivos.

   Hay tres modos de fallo principales que se deben tener en cuenta al proteger los dispositivos NVMe locales:

   i. Fallo de un dispositivo NVMe.

   ii. Pérdida de la instancia o el dominio de disponibilidad.

   iii. Corrupción o pérdida de datos por error de aplicación o usuario.

   Puede mitigar el fallo de un dispositivo NVMe en Linux mediante el uso de Local Volume Manager (LVM) para configurar el nivel RAID adecuado según las necesidades de protección del dispositivo. Los otros dos requieren implementar un método de copia de seguridad.

   Para obtener más información relacionada con la protección de datos en dispositivos NVMe, consulte el siguiente enlace de Oracle:

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

b) **Volúmenes de bloque:** El servicio de volumen en bloque permite aprovisionar y gestionar de forma dinámica volúmenes de almacenamiento en bloque. Todos los volúmenes tienen durabilidad incorporada y se ejecutan en hardware redundante dentro de un único dominio de disponibilidad. Proporciona funciones integradas para realizar copias de seguridad de los datos en el servicio de almacenamiento de objetos de OCI. Puede utilizar las copias de seguridad para la continuidad del negocio y la recuperación ante desastres. Están disponibles las siguientes opciones de copia de seguridad.

   i. Copias de seguridad programadas, automatizadas y basadas en políticas, con la opción de incrementales o completas. Las políticas están predefinidas o definidas por el usuario.

   ii. Copias de seguridad manuales bajo demanda, con una selección de incrementales o completas. Las copias de seguridad manuales no tienen ningún período de retención asociado y se almacenan indefinidamente.

   Para obtener más información relacionada con las copias de seguridad de volumen de bloque, consulte el siguiente enlace de Oracle:

   https://docs.oracle.com/es-ww/iaas/Content/Block/Concepts/blockvolumebackups.htm

c) **Almacenamiento de archivos:** El servicio proporciona un sistema de archivos de red duradero, escalable, seguro y empresarial. Es un sistema de archivos compartidos donde los datos se replican para aumentar la durabilidad en cada dominio de disponibilidad.

Están disponibles las siguientes opciones de copia de seguridad:

i. Utilice instantáneas para la protección de datos del sistema de archivos. Las instantáneas son una vista puntual y consistente donde los datos. están copiados durante la escritura y abarcan todo el sistema de archivos. Las secuencias de comandos y las herramientas están disponibles para copiar manualmente instantáneas en el almacenamiento de objetos en la misma región o en otra diferente. Para mejorar la durabilidad en un dominio de disponibilidad múltiple, el servicio de almacenamiento de objetos replica los datos almacenados en los dominios de disponibilidad. Utilice el conjunto Parallel File Tools para gestionar las instantáneas. El conjunto proporciona versiones paralelas de tar, rm y cp y puede ejecutar solicitudes en sistemas de archivos grandes en paralelo, lo que maximiza el rendimiento de las operaciones de protección de datos.

ii. Utilice los comandos rsync y rclone para transferir datos al servicio de almacenamiento de objetos u otro sistema de archivos.

Para obtener más información relacionada con la gestión de instantáneas del almacenamiento de archivos, consulte el siguiente enlace de Oracle:

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

d) **Almacenamiento de objetos:** este servicio regional es una plataforma de almacenamiento en internet de alto rendimiento que proporciona datos de alta durabilidad y disponibilidad en varios dominios de disponibilidad (AD), en una región de varios dominios de errores y en varios dominios de errores en una sola región de AD. El servicio proporciona almacenamiento en internet y de alto rendimiento para los datos no estructurados.

Los datos se almacenan de forma redundante en varios servidores de almacenamiento. El servicio de almacenamiento de objetos de OCI controla activamente la integridad de los datos y garantiza la redundancia. Además, el servicio detecta y repara automáticamente los datos dañados. Si se detecta una pérdida de redundancia, el servicio crea automáticamente más copias de datos.

Para obtener más información relacionada con la replicación del servicio de almacenamiento de objetos, consulte el siguiente enlace de Oracle:

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

Por otro lado, según establece el ENS para la presente medida de seguridad, se debe realizar copias de seguridad para las claves preservando la confidencialidad de la información. Para ello, el servicio de OCI Vault permite realizar copias de seguridad de almacenes, claves y almacenar dichas copias en buckets o fuera de OCI, en su propia infraestructura.

No obstante, el único tipo de almacén del que se puede realizar una copia de seguridad es un almacén de tipo privado virtual. De manera similar, el único tipo de clave de cifrado que puede realizarse una copia de seguridad es en una clave de cifrada maestra, protegida por un módulo HSM. Tampoco se puede realizar copias de seguridad de secretos o credenciales.

Para finalizar y obtener más información relacionada con las copias de seguridad del servicio de OCI Vault, consulte el siguiente enlace de Oracle:

https://docs.oracle.com/es-ww/iaas/Content/KeyManagement/Tasks/backingupvaultsandkeys.htm

3. GLOSARIO

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

Término	Definición
AES	Advanced Encryption Standard (Estándar de cifrado avanzado).
AMD	Compañía estadounidense Advanced Micro Devices.
API	Application Programming Interface (Interfaz de Programación de Aplicaciones).
ARM	Advanced RISC Machine (Máquina de arquitectura RISC avanzada).
Bare metal	Hardware dedicado.
Bucket	Cubo o almacén de datos ilimitado, de alto rendimiento, duradero y seguro.
BYOI	Bring your own identity (Traiga su propia identidad).
CCN	Centro Criptológico Nacional.
CIS	Center for Internet Security (Centro de Seguridad en Internet).
Compute	Recursos informáticos.
CPU	Central Processing Unit (Unidad Central de Procesamiento).
CVE	Common Vulnerabilities and Exposures (Vulnerabilidades y exposiciones comunes.
Dense I/O	Forma densa para grandes cargas de trabajo.
DNS	Domain Name System (Sistema de nombres de dominio).
ECDSA	Elliptic Curve Digital Signature Algorithm (Algoritmo de firma digital de curva elíptica).
ENS	Esquema Nacional de Seguridad.
Gbps	Gigabit por segundo.
GPU	Graphics Processing Unit (Una unidad de procesamiento gráfico).
HPC	High Perfomance Computing (Unidades de recursos informáticos de alto rendimiento).
HSM	Hardware Secure Module (Módulo de seguridad de hardware).
HTTP	Hypertext Transfer Protocol (Protocolo de Transferencia de Hipertexto).
HTTPS	HyperText Transfer Protocol Secure (Protocolo seguro de transferencia de hipertexto).
IA	Inteligencia artificial.
IMDS	Instance Metadata Service (Servicio de metadatos de la instancia).
iSCSI	Internet SCSI.
LVM	Local Volume Manager (Gestor de volúmenes lógicos).
NSG	Network Security Groups (Grupos de Seguridad de Red).
NTP	Network Time Protocol (Protocolo de tiempo de red).
NVMe	Non-Volatile Memory Express (Memoria exprés no volátil).
OCI	Oracle Cloud Infrastructure (Infraestructura de Nube de Oracle).
OCI IAM	Identity and Access Management (Gestión de identidad y acceso).
OCID	Oracle Cloud Identifier (identificador en la nube de Oracle).

Término	Definición
OCPU	Oracle Central Processing Unit (unidad de procesamiento central de Oracle).
OSI	Open Systems Interconnection (Modelo de interconexión de sistemas abiertos).
OVAL	Open Vulnerability and Assessment Language (Lenguaje abierto de vulnerabilidad y evaluación).
OWASP	Open Web Application Security Project (Proyecto de código abierto de seguridad de aplicaciones web).
RBAC	Role based access control (Control de acceso basado en roles).
RDP	Remote Desktop Protocol (Protocolo de Escritorio Remoto).
SCSI	Small Computer System Interface (Interfaz de sistemas informáticos pequeños).
Shape	Unidad o forma de una plantilla que determina la cantidad de CPU, memoria y otros recursos que se asignan a una instancia.
SQL	Structured Query Language (Lenguaje de Consulta Estructurado).
SSH	Secure Shell.
TCP	Transmission Control Protocol (Protocolo de Control de Transmisión).
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 la capa de transporte).
VCN	Virtual Cloud Network (Redes virtuales en la nube).
VM	Virtual machine (Máquina virtual).
VNIC	Virtual Network Interface Card (Tarjetas de interfaz de red virtual).
VPN	Virtual Private Network (Red privada virtual).
WAF	Web Application Firewall (Firewall de aplicaciones web).

4. 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 de OCI IAM para la administración de instancias de máquina virtual y bare metal.	☐Si ☐No	☐Si ☐No
		Observaciones:	
op.acc.2	Requisitos de acceso	Aplica	Cumple
	Se han creado los grupos de seguridad necesarios en la organización para la gestión de los recursos necesarios para la gestión de los servicios de Compute.	☐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) para los recursos de Compute.	☐Si ☐No	☐Si ☐No
		Observaciones:	

Control ENS	Medidas y Configuración	Estado	
op.acc.4	Proceso de gestión de derechos de acceso	Aplica	Cumple
	Se han gestionado los privilegios de acceso de los usuarios mediante la definición de políticas que cumplen los principios de mínimo privilegio, necesidad de conocer y capacidad para autorizar.	☐Si ☐No	☐Si ☐No
		Observaciones:	
OP.EXP	EXPLOTACIÓN		
op.exp.1	Inventario de activos	Aplica	Cumple
	Se están etiquetando los recursos relacionados con el servicio de Compute como redes, almacenamiento, compartimentos, etc., mediante el servicio de etiquetado de OCI.	☐Si ☐No	☐Si ☐No
		Observaciones:	
op.exp.4	Mantenimiento	Aplica	Cumple
	Se ha gestionado las actualizaciones mediante el servicio de gestión del sistema operativo de OCI.	☐Si ☐No	☐Si ☐No
		Observaciones:	
op.exp.4	Protección frente a código dañino	Aplica	Cumple
	Se está supervisando la estrategia de seguridad mediante el servicio de Cloud Guard y se ha creado una zona de seguridad para las instancias de cómputo.	☐Si ☐No	☐Si ☐No
		Observaciones:	

Control ENS	Medidas y Configuración	Estado	
op.exp.7	Gestión de incidentes	Aplica	Cumple
	Se dispone de un proceso integral para hacer frente a los incidentes de seguridad y se está apoyando en herramientas de reporte como Cloud Guard.	☐Si ☐No	☐Si ☐No
		Observaciones:	
op.exp.8	Registro de la actividad de los usuarios	Aplica	Cumple
	Se ha revisado los registros de actividad en busca de patrones anormales mediante el servicio de auditoría de OCI.	☐Si ☐No	☐Si ☐No
		Observaciones:	
op.exp.9	Registro de la gestión de incidentes	Aplica	Cumple
	Se está usando OCI Cloud Guard y OCI Eventos para el registro de las evidencias.	☐Si ☐No	☐Si ☐No
		Observaciones:	
op.exp.11	Protección de claves criptográficas	Aplica	Cumple
	Se ha configurado el servicio OCI Vault (almacén), limitando el acceso tan sólo al grupo de usuarios administradores de claves.	☐Si ☐No	☐Si ☐No
		Observaciones:	

Control ENS	Medidas y Configuración	Estado	
OP.MON	MONITORIZACIÓN DEL SISTEMA		
op.mon.1	Detección de intrusión	Aplica	Cumple
	se está usando la herramienta Cloud Guard y el servicio de análisis de vulnerabilidades para la detección de intrusión.	☐Si ☐No	☐Si ☐No
		Observaciones:	
op.mon.2	Sistema de métricas	Aplica	Cumple
	Se está gestionando los datos de las métricas de los servicios relacionados con Compute mediante el servicio de Supervisión y Notificaciones.	☐Si ☐No	☐Si ☐No
		Observaciones:	
MP	MEDIDAS DE PROTECCIÓN		
MP.COM	PROTECCIÓN DE LAS COMUNICACIONES		
mp.com.1	Perímetro seguro	Aplica	Cumple
	Se ha configurado el firewall a nivel de host y de aplicación para el control de puertos, protocolos y tipos de paquetes que transitan por las capas 3, 4, 5 y 7 del modelo de OSI.	☐Si ☐No	☐Si ☐No
		Observaciones:	
mp.com.2	Protección de la confidencialidad	Aplica	Cumple
	Se ha configurado subredes privadas, listas de seguridad o grupos de seguridad para las instancias de cómputo.	☐Si ☐No	☐Si ☐No
		Observaciones:	

Control ENS	Medidas y Configuración	Estado	
mp.com.4	Segregación de redes	Aplica	Cumple
	Se han configurado redes virtuales en la nube y subredes para el aislamiento de redes.	☐Si ☐No	☐Si ☐No
		Observaciones:	
MP.INFO	PROTECCIÓN DE LA INFORMACIÓN		
mp.info.3	Cifrado	Aplica	Cumple
	Se ha activado el cifrado en tránsito durante la creación de instancias de cómputo.	☐Si ☐No	☐Si ☐No
		Observaciones:	
mp.info.9	Copias de seguridad (backup)	Aplica	Cumple
	Se han realizado copias de seguridad de datos en los servicios de almacenamiento asociados a las instancias de cómputo.	☐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