Guía de Seguridad de las TIC
CCN-STIC 889K

Guía de Configuración Segura de Oracle Roving Edge Infrastructure

Enero 2026

Edita:

centro criptológico nacional

Fecha de Edición: noviembre de 2025

LIMITACIÓN DE RESPONSABILIDAD

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

AVISO LEGAL

ÍNDICE

1. GUIA DE CONFIGURACIÓN SEGURA DE ORACLE ROVING EDGE INFRASTRUCTURE

1.1 DESCRIPCIÓN DEL USO DE ESTA GUÍA

Esta **Guía de Configuración segura para la Infraestructura Roving Edge** proporciona directrices y **buenas prácticas** para proteger los servicios de Oracle Cloud desplegados en dispositivos Roving Edge, que extienden la infraestructura de Oracle Cloud en ubicaciones con conectividad limitada e incluso sin conectividad a Internet. Esta Guía también incluye recomendaciones para la realización de sincronizaciones seguras entre el dispositivo Roving Edge y la región Cloud de Oracle, una vez se haya establecido la conectividad. El contenido de esta guía se ajusta a los principios y controles definidos por el **Centro Criptológico Nacional** y en cumplimiento con las medidas establecidas por el **Esquema Nacional de Seguridad (ENS).**

La **computación en el borde (*Edge Computing*)**, se ha convertido en un recurso clave para las organizaciones que necesitan tomar decisiones basadas en datos en tiempo real, ya que procesa la información en el lugar en que se origina. Esta capacidad reduce significativamente la latencia, mejora la eficiencia operativa y permite mantener el funcionamiento de sistemas críticos incluso en entornos con conectividad limitada, intermitente o sin conectividad. Al minimizar la dependencia de centros de datos remotos o conexiones a la nube, *Edge Computing* resulta especialmente interesante en escenarios donde la baja latencia, la resiliencia y la soberanía del dato son fundamentales.

La **infraestructura Roving Edge de Oracle (*OCI Roving Edge Infrastructure*)** introduce un **modelo de despliegue único** para la computación en el borde, que permite extender los servicios de Oracle Cloud a entornos remotos con conectividad a internet limitada o inexistente. A diferencia de los modelos tradicionales de nube, que dependen de una conectividad continua, este enfoque acerca la infraestructura en la nube al punto donde se genera el dato, lo que posibilita el procesamiento y análisis en tiempo real en ubicaciones donde la infraestructura convencional en la nube no puede operar.

Mediante el uso de tecnología OCI Roving Edge Infrastructure, permite a las organizaciones cubrir **requisitos operativos asociados a la computación en borde**, tales como baja latencia, autonomía local y resiliencia en escenarios con conectividad limitada o inexistente. Los dispositivos Roving Edge son **unidades portátiles** diseñadas para proporcionar capacidades locales de computación, almacenamiento y red, extendiendo los servicios de Oracle Cloud Infrastructure a entornos remotos sin conectividad directa o permanente con la nube pública.

Esta tecnología fuer originalmente diseñada para cumplir con los requerimientos del **sector de Defensa**, facilitando el despliegue local de capacidades críticas de manera autónoma y segura. Es especialmente relevante además en escenarios como emergencias, control ambiental o seguridad operativa, donde la capacidad de actuar con rapidez y baja latencia es esencial.

La presente guía recoge las instrucciones necesarias para la **configuración segura** tanto de los servicios desplegados en dispositivos Roving Edge, como de los propios nodos físicos, en conformidad con los principios y controles definidos por el **Esquema Nacional de Seguridad (ENS)**.

Además de configurar de forma segura tanto servicios como dispositivos Roving Edge, resulta esencial establecer un enfoque de monitorización continua, que permita detectar actividades o comportamientos anómalos y garantizar una respuesta oportuna.

La terminología empleada para describir los servicios, incluidos los acrónimos utilizados, se encuentra recogida en el glosario anexo a esta guía. Asimismo, se han incluido **referencias a la documentación oficial** del proveedor con el fin de facilitar su consulta y comprensión.

Finalmente, se proporciona un resumen en formato lista de verificación (*checklist*) con las medidas y recomendaciones descritas a lo largo del documento, útil para el control de configuración.

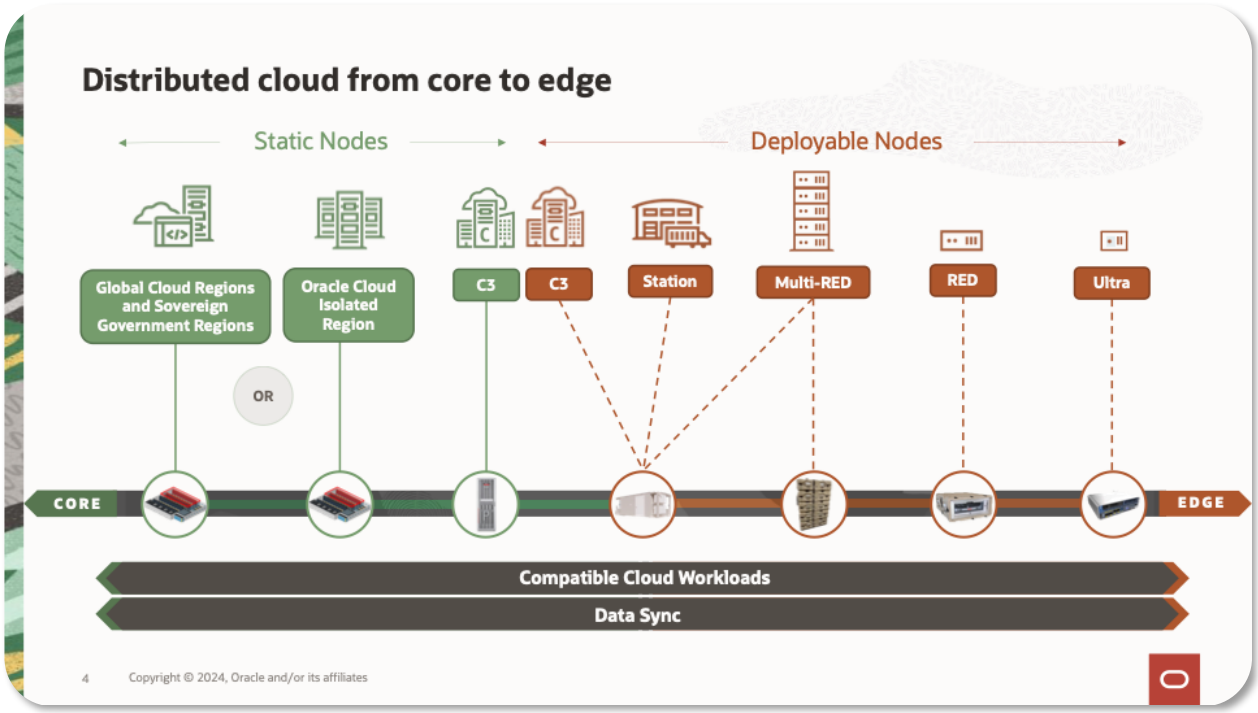
1.2 INTRODUCCIÓN AL SERVICIO *ROVING EDGE INFRASTRUCTURE*

1.2.1 DESCRIPCIÓN DEL SERVICIO

Oracle Cloud Infrastructure (OCI) es la solución *cloud* de Oracle que permite desplegar aplicaciones sobre una infraestructura segura y de alto rendimiento. Combina capacidades avanzadas de computación, almacenamiento y redes, junto con herramientas de inteligencia artificial, gestión y análisis de datos e integración, proporcionando un entorno completo alineado con los estándares de seguridad y conformidad normativa.

OCI está diseñada para responder a los requisitos de soluciones complejas y entornos de misión crítica, ofreciendo capacidades que permiten maximizar la **eficiencia operativa** y garantizar la **seguridad de la información**.

Tal y como se describe en esta guía, **Oracle Roving Edge Infrastructure** es un servicio de Oracle Cloud Infrastructure (OCI) diseñado para proporcionar capacidades de procesamiento, almacenamiento y red en ubicaciones remotas con conectividad limitada o incluso sin conectividad. Esta solución permite desplegar **entornos *cloud* seguros y robustos en el *edge***, facilitando el procesamiento local de datos y reduciendo la latencia en escenarios donde la conectividad con la nube pública es intermitente o inexistente.



Dispositivos Roving Edge en el contexto de modelos de despliegue de nube de Oracle

Esta extensión de la *tenancy* en Oracle Cloud Infrastructure (OCI) permite desplegar imágenes de máquinas virtuales, almacenamiento y sincronización de datos desde la *home region* de OCI a los dispositivos Roving Edge. Los **nodos de Roving Edg**e se crean y configuran directamente desde la consola

de Oracle Cloud Infrastructure (OCI), permitiendo especificar de forma centralizada los recursos y elementos que deben ser precargados o aprovisionados localmente en los dispositivos antes de su entrega. Este proceso garantiza que las imágenes de máquina virtual, los datos y las configuraciones necesarias para las operaciones en el perímetro se definan y gestionen bajo las políticas de seguridad establecidas en la tenencia de OCI, facilitando así el cumplimiento de los requisitos del Esquema Nacional de Seguridad (ENS) y asegurando la integridad y confidencialidad de la información desplegada.

Una vez que el nodo de Roving Edge establece conexión con la región de origen de OCI, es posible sincronizar la información entre los dispositivos desplegados en el perímetro y la *tenancy* principal. Esta sincronización permite tanto la descarga de actualizaciones desde la nube al dispositivo como la subida de nuevos datos generados en el perímetro hacia el almacenamiento centralizado en OCI.

Escenarios de Aplicación Comunes de la infraestructura Roving Edge:

- Ejecución de **cargas de trabajo críticas**, como bases de datos transaccionales (incluyendo Oracle Database), análisis de datos en tiempo real y modelos de *Machine Learning* previamente entrenados. Aunque la solución ofrece integración optimizada con aplicaciones y servicios Oracle, su arquitectura abierta permite también el despliegue de *stacks* tecnológicos personalizados basados en soluciones de código abierto.
- Ejecución de **Aplicaciones** que requieren **altas capacidades de procesamiento local** y un acceso rápido a datos (Input/Output) en situaciones donde la baja latencia resulta crítica. Este tipo de escenarios incluye, entre otros, operaciones de reconocimiento táctico, análisis en tiempo real de vídeo, o la gestión de infraestructura de comunicaciones avanzada como redes 5G desplegadas en el terreno.
- **Almacenamiento y procesamiento de grandes volúmenes de datos** (imágenes, vídeos, audio, datos de sensores IoT, etc…) generados en entornos operativos donde las comunicaciones WAN presentan alta latencia, ancho de banda limitado o ausencia de conectividad. Los nodos Roving Edge permiten realizar un preprocesamiento local seguro de dicha información, incluyendo operaciones de filtrado, compresión, clasificación inicial y filtrado, con el objetivo de optimizar el uso de recursos y preservar la confidencialidad desde el origen.
- Escenarios de computación en remoto que requieren **niveles elevados de seguridad**, **confidencialidad y contención de la información**. Los nodos de Roving Edge permiten ejecutar cargas de trabajo en ubicaciones físicamente aisladas, garantizando que los datos generados o tratados permanecen confinados dentro del dispositivo hasta que se establezcan canales seguros para su transferencia o sincronización con OCI.

Para ampliar esta información, se recomienda revisar la documentación oficial accesible en el siguiente enlace:

Visión general de Oracle Roving Edge Infrastructure

1.2.2 CONCEPTOS BÁSICOS

Antes de profundizar en las funcionalidades y opciones de configuración segura de *Oracle Roving Edge Infrastructure*, es fundamental comprender previamente los conceptos clave asociados a capacidades y características principales.

Este conocimiento preliminar constituye la base necesaria para una puesta en marcha segura y eficaz del servicio y dispositivos Roving Edge, garantizando que el despliegue se realice conforme a las mejores prácticas y alineado con los principios de seguridad establecidos por el Esquema Nacional de Seguridad (ENS).

1.2.2.1 GENERAL

- **Consola Oracle Cloud Infrastructure**: Interfaz web para interactuar con los servicios de OCI de forma centralizada y segura.
- **Com*mand Line Interface* (CLI)**: Herramienta que permite gestionar y operar los servicios de OCI mediante líneas de comando, proporcionando acceso directo a las funcionalidades de la plataforma.
- **API**: La Interfaz de Programación de Aplicaciones permite acceder y gestionar de forma programática las funcionalidades de la plataforma, mediante el envío de solicitudes a los servicios de OCI a través de protocolos estándar (principalmente HTTPS y REST).
- **Consola del Dispositivo Roving Edge**: Interfaz web gráfica que permite interactuar localmente con el nodo de Roving Edge, sin necesidad de conectividad directa con Oracle Cloud Infrastructure (OCI).

1.2.2.2 ROVING EDGE INFRASTRUCTURE

- **Roving Edge Infrastructure**: Servicio de Oracle Cloud Infrastructure que permite ejecutar cargas de trabajo basadas en la nube fuera del centro de datos, en ubicaciones remotas o con conectividad limitada.
- **Roving Edge *Device* (RED):** Dispositivo portátil de alto rendimiento diseñado para ejecutar servicios fundamentales de Infraestructura como Servicio (IaaS), optimizados específicamente para entornos remotos o con conectividad limitada.

Opciones del dispositivo de Roving Edge Infrastructure

- **Roving Edge Ultra (Ultra):** Dispositivo compacto y ligero, diseñado para ser transportado por una sola persona en una mochila. A diferencia de otros dispositivos de infraestructura Edge más grandes, Roving Edge Ultra no requiere de una fuente de alimentación externa adicional, lo que permite su operación inmediata en entornos remotos, aislados o de difícil acceso.

Opciones del dispositivo de Roving Edge Infrastructure (Ultra)

- **Aprovisionamiento:** Proceso mediante el cual los datos y aplicaciones necesarios son cargados en el dispositivo Roving Edge desde los *compartments* y espacios de almacenamiento (*buckets*) previamente especificados en Oracle Cloud Infrastructure.
- **Nodo:** Recurso del servicio Roving Edge Infrastructure en OCI que representa un único dispositivo físico, ya sea un Roving Edge Device (RED) o un dispositivo Ultra.
- **Cargas de Trabajo *(Workloads)***: Recursos en OCI que pueden consistir en un bucket de almacenamiento de objetos o una imagen de máquina virtual personalizada. Estas cargas son aprovisionadas en los nodos de Roving Edge para su ejecución local.
- **Sincronización de Datos (*Data Sync*):** Proceso mediante el cual se transfieren datos de almacenamiento de objetos entre la *tenancy* de OCI y los dispositivos Roving Edge. También permite distribuir actualizaciones de software y mantener alineadas cargas de trabajo locales con el entorno cloud.
- **Gestión de versiones de software del dispositivo:** A través del proceso de gestión de versiones, el sistema operativo del dispositivo puede ser actualizado a versiones más recientes de forma controlada. Incluye también la capacidad de revertir a versiones anteriores previamente instaladas, si así se requiere por motivos técnicos u operativos.

1.2.2.3 IDENTIDAD Y ACCESOS

- **Usuario:** Cuenta con privilegios administrativos que permite interactuar con la interfaz y los servicios ofrecidos por el dispositivo Roving Edge Infrastructure. Todos los usuarios disponen de privilegios de administrador, disponiendo de acceso total a la configuración y operación del sistema.
- **Grupo:** Los grupos representan conjuntos de cuentas de usuario, sobre los cuales se aplican de manera colectiva las funciones y políticas configuradas. En los nodos de Roving Edge sólo se utiliza un grupo predeterminado, aunque se permite la creación de nuevos grupos según los requisitos operativos.
- **Políticas:** El acceso a los recursos del entorno se gestiona mediante políticas, las cuales especifican qué grupos pueden realizar qué acciones sobre qué *compartments* o sobre la *tenancy* global. Estas políticas definen el marco de autorización dentro del modelo de seguridad de OCI.

1.2.2.4 SERVICIO DE MÁQUINAS VIRTUALES

- **Instancia:** Máquina Virtual (VM) desplegada sobre un nodo Roving Edge, empleada para ejecutar tareas computacionales o aplicaciones configuradas por el usuario.
- **Imagen:** Una imagen es una plantilla que define el contenido del disco de una máquina virtual, incluyendo el sistema operativo y el software necesario para el funcionamiento de una instancia.
- ***Shape***: El término shape hace referencia a una configuración preestablecida que define los recursos de hardware virtual (como CPU, memoria RAM y otros parámetros) que serán asignados a una instancia durante su aprovisionamiento.
- ***Boot Volume*:** Recurso de almacenamiento desacoplado que aloja el sistema operativo de la instancia y permite el arranque inicial de una instancia virtual.

- **Captura del Historial de Consola:** Mecanismo que permite conservar el contenido mostrado en la consola serie de una instancia, especialmente útil para el análisis de errores en entornos desconectados o remotos.

1.2.2.5 ALMACENTAMIENTO DE OBJETOS (*OBJECT STORAGE*)

- **Bucket:** Recurso de almacenamiento que agrupa objetos bajo un mismo espacio lógico. Cada *bucket* reside dentro de un compartimento y pertenece a un *namespace*.
- **Objeto:** Archivo o conjunto de datos no estructurados cargado en un *bucket* dentro del servicio de almacenamiento de objetos.

1.2.2.6 ALMACENAMIENTO EN BLOQUES (*BLOCK STORAGE*)

- **Volumen de almacenamiento en bloque (*Block Volume*):** Recurso de almacenamiento persistente que puede conectarse a instancias como si fuera un disco físico para proporcionar capacidad adicional.

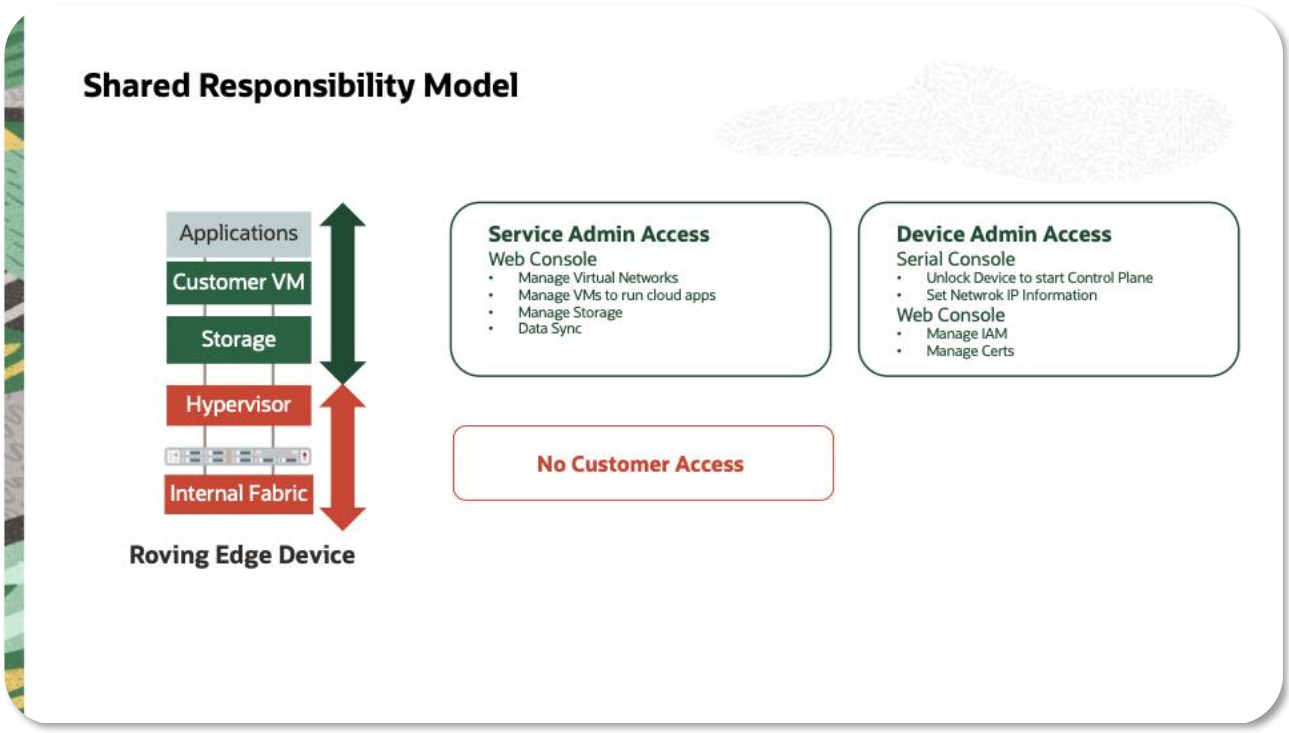
1.2.2.7 REDES VIRTUALES

- **Virtual Cloud Network (VCN):** Entorno de red virtual y aislado lógicamente, desplegado en los centros de datos Oracle, incluidos los nodos Roving Edge, que permite establecer comunicaciones seguras entre recursos y controlar su exposición a redes externas.
- **Subred:** Segmento de red definido dentro de una VCN, por ejemplo 10.0.0.0/24 and 10.0.1.0/24. Las subredes contienen interfaces de red virtuales (VNIC) que permiten la conectividad entre las instancias desplegadas.

1.2.3 MODELO DE RESPONSABILIDAD COMPARTIDA

La infraestructura Roving Edge extiende la *tenancy* de Oracle Cloud hasta el perímetro, aplicando el mismo modelo de responsabilidad compartida, esto es, estableciendo una distribución clara de responsabilidades operativas y de seguridad entre el proveedor (Oracle) y el cliente, siendo clave para una adecuada gestión del riesgo y la protección de la información.

Para facilitar su implementación y garantizar una asignación clara de tareas, el modelo establece una división estructurada de responsabilidades que distingue dos ámbitos de actuación diferenciados: **la gestión operativa,** responsabilidad del cliente y la **gestión de la infraestructura subyacente**, responsabilidad de Oracle:



Modelo de Responsabilidad Compartida para la Infraestructura Roving Edge

a) **Ámbito de responsabilidad del cliente: Gestión de servicios y dispositivos.** El cliente es responsable de las tareas de administración de los servicios desplegados y del control de los propios dispositivos físicos. Estas funciones abarcan tanto tareas operativas como configuraciones de seguridad, necesarias para garantizar la integridad, responsabilidad y confidencialidad del entorno.

   a. Administración de servicios:

      i. Gestión de redes virtuales (VCN). Definición de la arquitectura de red, subredes, listas de control de acceso, rutas y otros componentes relacionados.

      ii. Gestión de máquinas virtuales, creación y supervisión de instancias para el despliegue de aplicaciones.

      iii. Gestión de almacenamiento.

      iv. Sincronización de datos, coordinación y validación de procesos de replicación y sincronización de datos con la nube.

   b. Administración del dispositivo:

      i. Consola Serie (*Serial Console*): Acceso para el desbloqueo del dispositivo, configuración inicial y parametrización de red.

      ii. Consola Web (*Web Console*): Administración de identidades, políticas de acceso y certificados.

El cliente deberá aplicar medidas de seguridad adecuadas en todas estas áreas, conforme a las recomendaciones del Esquema Nacional de Seguridad (ENS) y buenas prácticas del Centro Criptológico Nacional (CCN).

b) **Ámbito de responsabilidad de Oracle: Gestión de la infraestructura subyacente.** Oracle es responsable del mantenimiento y securización de los componentes físicos y lógicos que soportan la solución Roving Edge. Implica garantizar la seguridad, disponibilidad y mantenimiento de los componentes base:

   a. Nodo físico *(bare metal)*: Hardware físico que conforma la base del entorno Roving Edge. Incluye tareas de mantenimiento físico, gestión de fallos y protección contra manipulaciones.

   b. Plano de control, *runtime* y sistema operativo: Subsistemas software que permiten la gestión del ciclo de vida de los servicios, comunicación entre componentes, arranque seguro y administración general del entorno.

En resumen, la supervisión y el control de acceso a los servicios, máquinas virtuales y recursos desplegados en Roving Edge recaen exclusivamente en el cliente, quien debe establecer las políticas de autenticación, acceso remoto y gestión de identidades, mientras que Oracle administra únicamente los componentes de infraestructura, sin acceso autorizado a los servicios ni a la información del cliente, respetando así el principio de segregación de funciones y confidencialidad.

Las **recomendaciones de esta guía de configuración segura** se estructuran conforme a este modelo de responsabilidad compartida, dotando al cliente del conocimiento y herramientas necesarias para la gestión y configuración de los recursos de su ámbito.

2. DESPLIEGUE SEGURO DE LA INFRAESTRUCTURA ROVING EDGE: CONFIGURACIÓN DE NODOS Y RECURSOS

El despliegue de la **Infraestructura Roving Edge** permite implementar un entorno seguro y distribuido en el perímetro, integrado con Oracle Cloud. Como se menciona anteriormente en la introducción al servicio, está diseñada para operar de forma confiable en sitios remotos o con conectividad limitada, asegurando la continuidad y protección de los servicios incluso cuando la conexión con la nube pública es intermitente o inexistente.

En este contexto, el proceso de despliegue se desarrolla en varias fases clave:

- **Asignación y preparación de dispositivos (*Node provisioning*)**, asignación, reserva y registro de los nodos que formarán parte de la Infraestructura Roving Edge para un uso específico.
- **Preconfiguración de cargas de trabajo** para garantizar que el entorno esté listo para procesar y gestionar datos locales de manera eficiente (opcional)
- **Entrega segura de dispositivos,** asegurando su correcta configuración y protección.
- **Configuración básica de recursos esenciales,** incluyendo máquinas virtuales, almacenamiento y redes.

Este proceso asegura tanto la conformidad con los requisitos de seguridad, como la eficiencia operativa, garantizando un infraestructura resiliente y segura. Alineado con las mejores prácticas de protección de datos e integridad, permite un desempeño estable en escenarios con conectividad limitada o inexistente.

2.1 SOLICITUD DE NODOS ROVING EDGE. RECOMENDACIONES DE SEGURIDAD

Tal y como se menciona en la descripción general del servicio, la Infraestructura Roving Edge se basa en dispositivos especialmente diseñados para transportar y desplegar entornos de **Oracle Cloud Infrastructure (OCI)** en ubicaciones remotas o de difícil acceso.

Antes de iniciar la provisión de nodos Roving Edge, es fundamental evaluar los modelos de dispositivos disponibles. La correcta selección del dispositivo es calve para optimizar la infraestructura en el Edge, alineando los recursos escogidos con los requisitos específicos de procesamiento y almacenamiento en el entorno de despliegue.

Modelos de dispositivos Roving Edge disponibles:

- **Dispositivo Roving Edge:** Dispositivo portátil de alto rendimiento, reforzado para operar de forma segura en entornos remotos, hostiles o con conectividad limitada. Su estructura resistente y su portabilidad permiten una operación confiable en entornos operativos exigentes. El dispositivo RED se comercializa en distintas configuraciones técnicas, denominadas *shapes*, que permiten adaptarse a los requerimientos específicos de procesamiento, almacenamiento de cada caso de uso.

Dispositivo Roving Edge (RED)

- **Roving Edge Ultra (Ultra):** Variante altamente portátil del dispositivo Roving Edge, que por sus dimensiones puede ser transportada por una sola persona en medio de transporte tipo mochila. Está concebida para escenarios en los que el despliegue de dispositivos RED no resulta viable por limitaciones logísticas, de acceso o infraestructura. El dispositivo puede operar sin necesidad de una fuente de alimentación externa durante un tiempo limitado, lo que facilita sus uso en entornos remotos o de difícil acceso.

Roving Edge Ultra (Ultra)

Cada modelo de Roving Edge presenta características específicas orientadas a maximizar el rendimiento y la eficiencia en distintos entornos operativos. Una comprensión precisa de sus capacidades

y usos previstos permite realizar una selección informada en el momento de la solicitud, asegurando que los recursos desplegados en el borde se alineen con los objetivos operativos y de seguridad.

El detalle de las especificaciones técnicas de cada dispositivo puede consultarse en el siguiente enlace:

Especificaciones Técnicas de los dispositivos

La solicitud de un dispositivo Roving Edge requiere la **creación previa de un nodo** en el entorno de Oracle Cloud Infrastructure, utilizando los servicios de nube híbrida (Hybrid Cloud Services). La creación del nodo se realiza en el entorno de Oracle Cloud Infrastructure en coherencia con el diseño de Roving Edge, como una extensión y gestionada de la nube de Oracle. Esta aproximación facilita una gestión centralizada de los dispositivos, asegura la aplicación consistente de políticas de seguridad y permite una integración supervisada con servicios cloud. La definición del nodo en esta fase previa permite:

- Preconfigurar las cargas de trabajo que serán ejecutadas localmente
- Aplicar controles de acceso y políticas de seguridad
- Estandarizar el despliegue, reduciendo los tiempos de configuración en el escenario de operaciones
- Asegurar que el dispositivo esté preparado para operar de forma segura y eficiente desde el momento de su entrega.

Para realizar una solicitud de dispositivo Roving Edge es imprescindible contar con una cuenta activa en Oracle Cloud Infrastructure (OCI). Para obtener **información detallada sobre los requisitos y procedimientos** para solicitar un dispositivo, consulte el siguiente enlace:

Solicitud de dispositivos

2.1.1 CREACIÓN DE UN NODO DE INFRAESTRUCTURA ROVING EDGE

El primer paso para solicitar un dispositivo Roving Edge es la creación del nodo desde la consola de Oracle Cloud Infrastructure. Este nodo actúa como una representación lógica del dispositivo físico dentro del entorno cloud, permitiendo su configuración, gestión y posterior sincronización con los servicios de OCI.

Durante el proceso de creación del nodo, es necesario seleccionar la **región de OCI** en la que se registrará y gestionará dicho nodo. Esta elección es importante, ya que determina el ámbito geográfico y lógico desde el cual se administrará el dispositivo, por lo que han de tenerse en cuenta las siguientes consideraciones.

- **Gestión y Configuración**: Los dispositivos Roving Edge se configuran y administran exclusivamente desde la región seleccionada. Esta región actuará como punto central de control, supervisión y actualización.
- **Sincronización de datos:** Los dispositivos sincronizan datos e imágenes desde la región de OCI asignada. Todo contenido que deba ser preinstalado en el dispositivo deberá cargarse desde esta región.

En entornos cloud, los recursos suelen desplegarse y gestionarse mediante tres métodos principales: la **consola web de OCI**, la **interfaz de línea de comandos (CLI)** y la **interfaz de programación de aplicaciones (API)**. Estos mecanismos, ampliamente soportados en OCI, también están disponibles para la provisión de nodos Roving Edge, facilitando la selección del método que mejor se adapte a las necesidades de automatización y operación de cada usuario.

El proceso de provisión puede presentar ligeras variaciones según el modelo de dispositivo. Para instrucciones detalladas sobre la provisión de los modelos Roving Edge Device (RED) y Roving Edge Ultra, consulte los enlaces proporcionados a continuación:

Creación de un nodo de dispositivo GEN1 de Roving Edge Infrastructure

Creación de un nodo de dispositivo GEN2 de Roving Edge Infrastructure (Compute, GPU y Almacenamiento)

Creación de un nodo de dispositivo Roving Edge Ultra

2.1.2 CONSIDERACIONES DE SEGURIDAD DURANTE EL APROVISIONAMIENTO DEL NODO

Durante el proceso de aprovisionamiento de los nodos Roving Edge, resulta fundamental aplicar una serie de medidas de seguridad orientadas a garantizar la integridad y confidencialidad de la infraestructura. Aplicar estas medidas desde la etapa inicial ayuda a garantizar un despliegue seguro y confiable, reduciendo la posibilidad de accesos no autorizados o configuraciones erróneas.

2.1.2.1 SEGURIDAD DEL DISPOSITIVO

Durante el aprovisionamiento inicial de los nodos de Roving Edge, es fundamental seguir una serie de pasos destinados a garantizar la **seguridad del dispositivo**. Estas medidas contribuyen de forma directa a reforzar la postura general de seguridad del sistema, como se detalla a continuación:

- Definición de la **contraseña de Super Usuario**. Esta contraseña protege la cuenta administrativa del nodo, que permite realizar operaciones críticas sobre el dispositivo. Es fundamental, por tanto, establecer una contraseña robusta para evitar accesos no autorizados.
- Definición de la **Frase de Desbloqueo (Unlock Passphrase)**. La frase de desbloque es requerida para acceder a los datos cifrados localmente en el dispositivo. Su configuración adecuada es esencial para preservar la confidencialidad de la información, ya que constituye una medida de protección frente a accesos no autorizados a información sensible.

2.1.2.2 ETIQUETADO (*TAGGING*)

Durante el proceso de aprovisionamiento del nodo, se ofrece la posibilidad de aplicar etiquetas (tags) para asociar metadatos que faciliten la identificación, clasificación y gestión de los recursos. Aunque su

uso es opcional y puede hacerse con posterioridad, se recomienda definir las etiquetas desde esta etapa inicial para mejorar la organización y permitir una administración más eficiente del entorno desplegado.

En caso de habilitar el etiquetado, deberán definirse los siguientes elementos:

- **Espacio de Nombres (Tag Namespace)**, contenedor lógico que agrupa etiquetas relacionadas bajo un mismo contexto organizativo o funcional.
- **Clave de Etiqueta (Tag Key)** Representa el atributo o categoría que se desea identificar en el recurso (por ejemplo, entorno, nivel de confidencialidad). Actúa como el nombre de la propiedad que se va a describir mediante metadatos.
- **Valor de Etiqueta (Tag Value)** Es el dato específico asociado a la clave. La clave y el valor juntos conforman una pareja identificadora que facilita la trazabilidad, clasificación y control de recursos desplegados.

El uso adecuado del etiquetado contribuye significativamente a control y seguimiento de los recursos desplegados. Para más información sobre esta funcionalidad, consulte el siguiente enlace.

Visión general del servicio Etiquetado

2.1.2.3 CERTIFICADOS

Durante el aprovisionamiento, existe la posibilidad de configurar certificados digitales con el fin de garantizar una autenticación segura y fortalecer la protección del nodo Roving Edge. Esta configuración contribuye a mantener la integridad y disponibilidad del sistema.

Opciones para la gestión de certificados:

- **Servicio propio de certificados**. Será imprescindible proporcionar la información de la autoridad certificadora.
- **Servicio OCI *Certificate***. Igualmente, será imprescindible ingresar los datos de la autoridad certificadora creada previamente.
- **Certificados auto firmados predeterminados**. Es posible usar los certificados que ya vienen configurados en el dispositivo. En este caso, esta sección ha de dejarse en blanco. Estos certificados se activan después de recibir el dispositivo.

En los casos en los que sea necesario proporcionar información para la correcta emisión y gestión del certificado digital, los parámetros principales que completarse durante este proceso son:

- **Nombre Común (*Common Name*)**, es el nombre que identifica al certificado.
- **Autoridad Certificadora Emisora** (***Issuer Certificate Authority***) in <compartment>: Selección de la Autoridad Certificadora que emite y renueva el certificado.
- Fecha límite de **Validez del Certificado** (*Certificate Validity End Date*)
- **Algoritmo de Firma** *(Signature Algorithm)***:** Algoritmo utilizado para firmar digitalmente el certificado.
- **Key Algorithm:** Algoritmo utilizado para la generación de la clave criptográfica.
- ***Compartment* del Certificado**

Oracle recomienda utilizar Autoridades Certificadoras (CAs) distintas para cada solicitud de dispositivo. Aunque técnicamente es posible emplear la misma CA raíz, se aconseja definir CA subordinadas diferentes por cada despliegue. Esta medida reduce el riesgo de compromiso, evitando la dependencia de una única CA que, si se viera comprometida, podría afectar al conjunto de los dispositivos.

La configuración de la **Autoridad Certificadora (CA)** para los dispositivos Roving Edge puede definirse una vez completada la solicitud del dispositivo:

Gestión de Certificados

Una gestión adecuada de los certificados y una configuración cuidadosa de sus parámetros permite reforzar la seguridad de la infraestructura en tres áreas fundamentales:

- **Autenticación Segura**: Asegurando que sólo entidades legítimas puedan establecer comunicación con los dispositivos.
- **Integridad de los datos:** Protege contra manipulaciones no autorizadas en las comunicaciones.
- **Resiliencia frente a amenazas basadas en certificados:** Minimiza el riesgo derivado del uso fraudulento o la suplantación de certificados digitales.

2.2. ASOCIACIÓN DE UNA CARGA DE TRABAJO A UN NODO ROVING EDGE

La asociación de una carga de trabajo consiste en asignar a un nodo Roving Edge un conjunto de recursos y contenidos desde Oracle Cloud Infrastructure, como aplicaciones y datos, necesarios para su operación. Esta vinculación se puede realizar en el momento de crear el nodo, garantizando que el dispositivo cuente con todo lo requerido desde su despliegue, o bien después de su aprovisionamiento.

En el siguiente enlace se encuentra la guía detallada sobre cómo vincular una carga de trabajo a un nodo Roving Edge en el entorno Oracle Cloud Infrastructure:

Asociación de una carga de trabajo a un nodo de Roving Edge Infrastructure

2.3. PROCESO APROVISIONAMIENTO SEGURO DEL NODO DE ROVING EDGE

Una vez que la solicitud del nodo ha sido aprobada, se inicia el **proceso de aprovisionamiento** del nodo. Durante esta fase, los dispositivos de la Infraestructura Roving Edge se preparan conforme a las especificaciones solicitadas, garantizando un despliegue seguro y conforme a las mejores prácticas.

Las acciones principales que se llevan a cabo durante el aprovisionamiento son:

- Instalación del **sistema operativo** y del software base necesario en cada dispositivo.
- Configuración de **mecanismos de cifrado** para proteger el almacenamiento local del dispositivo.
- Carga de la imagen del sistema y los datos correspondiente a las **cargas de trabajo** asociadas a la solicitud del nodo.

Antes de comenzar el aprovisionamiento, cada dispositivo Roving Edge es sometido a un proceso de borrado seguro de datos, siguiendo el estándar NIST 800-88, garantizando la completa sanitización de los datos almacenados.

Una vez completado, el dispositivo se entrega listo para su integración y operación segura.

2.4. PROCESO DE *SETUP* SEGURO DEL NODO DE ROVING EDGE

Una vez que el dispositivo Roving Edge ha sido aprovisionado y entregado por Oracle, es necesario llevar a cabo un proceso de configuración inicial que garantice su operación segura y eficiente dentro del entorno Oracle Cloud.

Consulte la documentación oficial de Oracle para información actualizada sobre modelos soportados y configuraciones específicas:

Configuración de un dispositivo Oracle Roving Edge Device

Este proceso de configuración segura de un dispositivo Roving Edge incluye las etapas esenciales para establecer un entorno seguro y confiable, que garantice la seguridad operativa desde el inicio.

1. **Comprobación de la Integridad del HARDWARE,** verificando que el dispositivo no presenta modificaciones o alteraciones indebidas que puedan comprometer su seguridad, asegurando su autenticidad y fiabilidad.

   Recibir e inspeccionar el envío

2. **Protección de las CONEXIONES DE RED,** estableciendo controles y configuraciones orientados a proteger las comunicaciones.

   Conexión de cables del dispositivo Roving Edge

   Configuración de la emulación de terminal

   Configurar parámetros de red

3. **Establecimiento de mecanismos robustos de AUTENTICACIÓN y CIFRADO**, descargando e instalando los certificados de la Autoridad Certificadora Raíz (*Root CA*), garantizando una conexión de confianza entre el dispositivo y la consola de gestión.

   Descargue el certificado de CA raíz

Adoptar estas recomendaciones desde la fase inicial contribuye a consolidar una infraestructura segura, favoreciendo el funcionamiento estable y protegido del dispositivo en su entorno operativo.

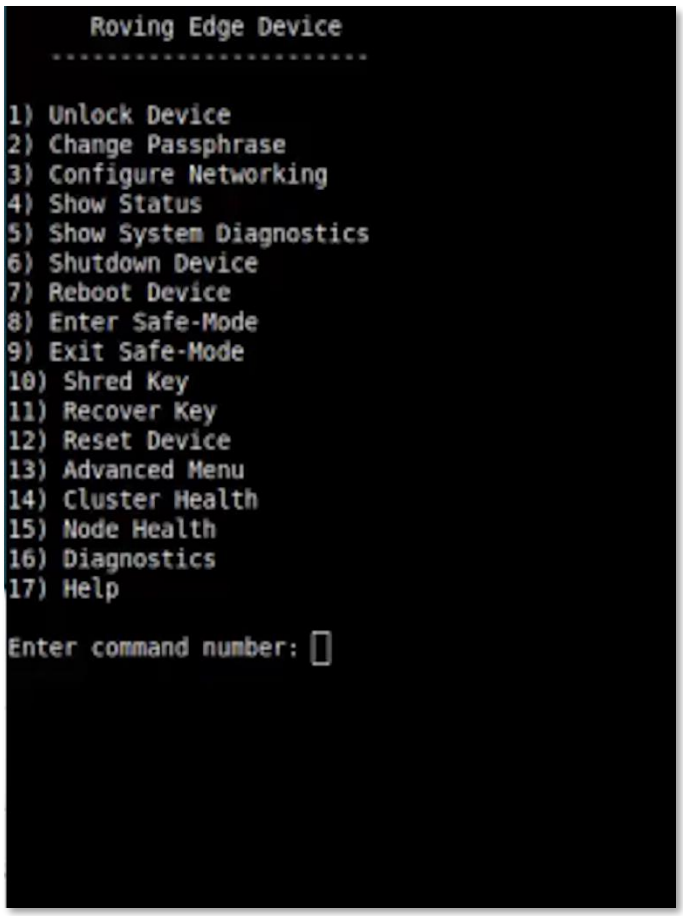
2.5. USO DE LA CONSOLA PUERTO SERIE

En despliegues de Roving Edge, donde los dispositivos se configuran y operan localmente con conectividad a la nube limitada o intermitente, disponer de un método fiable de acceso local resulta fundamental para una administración segura y eficiente.

La **Consola Serie** proporciona una interfaz directa sobre el dispositivo que facilita la gestión y resolución de incidencias, garantizando el control operativo incluso en entornos con conectividad restringida o desconectados. Entre sus funciones clave destacan:

- **Configuración inicial**: Permite el acceso seguro para ajustar parámetros esenciales, como la configuración de red y otros ajustes básicos.
- **Seguridad y control de acceso**: Funciona como medio para desbloquear el dispositivo mediante "frase de desbloqueo/acceso", asegurando que únicamente el personal autorizado pueda operarlo.
- **Diagnóstico y Recuperación:** Proporciona herramientas para la detección de fallos y opciones de recuperación ante incidencias.
- **Opciones críticas de seguridad:** Facilita cambios seguros de la "frase de desbloqueo/acceso", reinicios controlados y procedimientos de emergencia, como la destrucción segura de claves criptográficas.

El acceso mediante consola serie incluye las siguientes opciones disponibles para el usuario:



Para más información sobre comandos y configuraciones disponibles, se recomienda revisar la documentación de Oracle relativa a las operaciones con la consola serie:

Funcionamiento de la consola serie

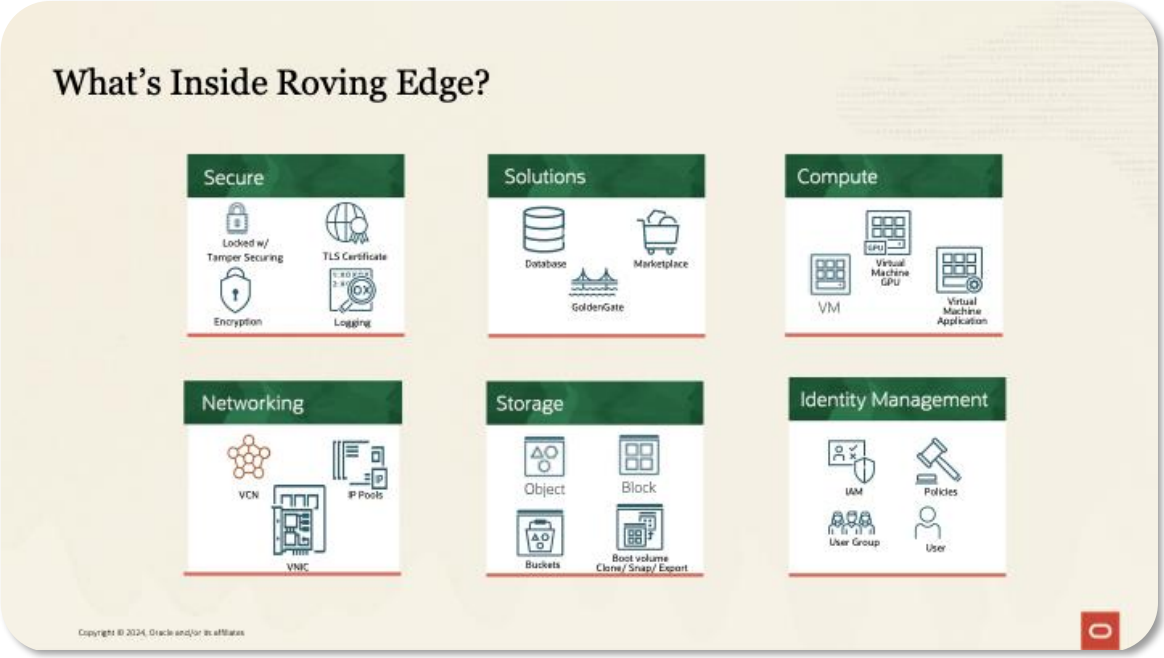
2.6. GESTIÓN SEGURA DE LOS SERVICIOS A DESPLEGAR EN EL DISPOSITIVO

Como se menciona en secciones previas de la presente guía, ***Roving Edge Infrastructure*** proporciona un **conjunto integral de servicios** diseñados para ofrecer capacidades de computación seguras, autónomas y de alto rendimiento en entornos desconectados, remotos o tácticos. Aunque la infraestructura de Roving Edge ofrece un entorno robusto para la computación en el borde, los servicios disponibles presentan una funcionalidad simplificada en comparación con Oracle Cloud Infrastructure (OCI), debido a las limitaciones inherentes de operar en entornos aislados.

Esta sección describe brevemente los servicios disponibles en los nodos desplegados y, cuando sea aplicable, incluye referencias a la correspondiente *Guía CCN-STIC* correspondiente a estos servicios, las cuales están específicamente adaptadas a cada servicio, ofreciendo recomendaciones detalladas de seguridad y buenas prácticas. Dada su naturaleza especializada, se recomienda consultar dichas guías directamente para obtener una comprensión más completa y precisa de las medidas de seguridad requeridas para cada servicio.

En la sección *Marco Operacional y Medidas de Protección* se ampliarán los detalles sobre las prácticas de gestión segura aplicables a los servicios desplegados en el dispositivo. Esta sección se ajusta a los controles de seguridad definidos en el Esquema Nacional de Seguridad (ENS).

Los servicios que pueden desplegarse en el dispositivo incluyen: GESTIÓN DE IDENTIDAD, REDES, CÓMPUTO, ALMACENAMIENTO y SINCRONIZACIÓN DE DATOS.



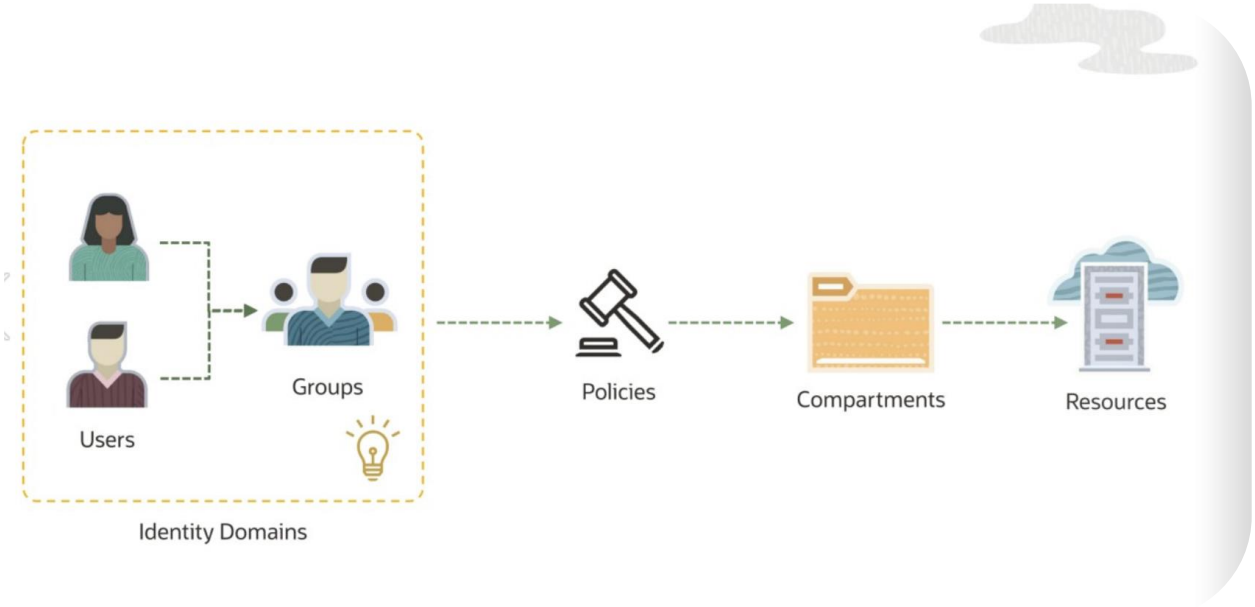
Visión General de los servicios disponibles en Infraestructura Roving Edge

2.6.1 GESTIÓN DE IDENTIDADES

La gestión de Identidades y Accesos (IAM por sus siglas en inglés) constituye un pilar fundamental en la protección de los entornos desplegados en dispositivos RED. De acuerdo con el ENS, el control de accesos es un principio clave para asegurar que únicamente los usuarios autorizados puedan interactuar con los sistemas de información, minimizando así el riesgo de accesos no autorizados, fugas de información o escaladas de privilegios indebidas.

El ENS establece que los mecanismos de control de acceso deben diseñarse conforme a los principios de **mínimo privilegio**, **necesidad de saber** y **segregación de funciones**, criterios plenamente alineados con los enfoques de **Arquitectura *Zero Trust***.

En este contexto, Oracle aplica los principios de Zero Trust mediante el uso de mecanismos de control de acceso fundamentados en la verificación continua de identidad, la evaluación de políticas dinámicas y el análisis de atributos contextuales. El modelo de gestión de OCI IAM permite una administración segura y granular de los accesos mediante el uso estructurado de **usuarios**, **grupos**, **políticas**, **compartimentos** y **recursos**, elementos fundamentales para aplicar los principios ya mencionados de mínimo privilegio, necesidad de saber y segregación de funciones.



Principales componentes del servicio de Gestión de Identidades y Accesos

Aunque IAM en RED proporciona las funciones esenciales para la gestión de accesos, éstas son **limitadas en comparación con las características más avanzadas de OCI**, que incluye la gestión federada de identidades y una mayor integración con el resto de los servicios. En RED, algunos componentes están restringidos a configuraciones predeterminadas, como un único **compartimento** o una sola ***tenancy***.

Para asegurar la implementación segura de OCI IAM en conformidad con el Esquema Nacional de Seguridad, es importante consultar la "***CCN-STIC 889A Guía de Configuración Segura para IAM y servicios de seguridad***". Las consideraciones operativas y las configuraciones adicionales en RED.

Guía de Configuración segura para IAM y servicios de seguridad — Guía de Seguridad de las TIC CCN-STIC 889A

2.6.2 REDES VIRTUALES

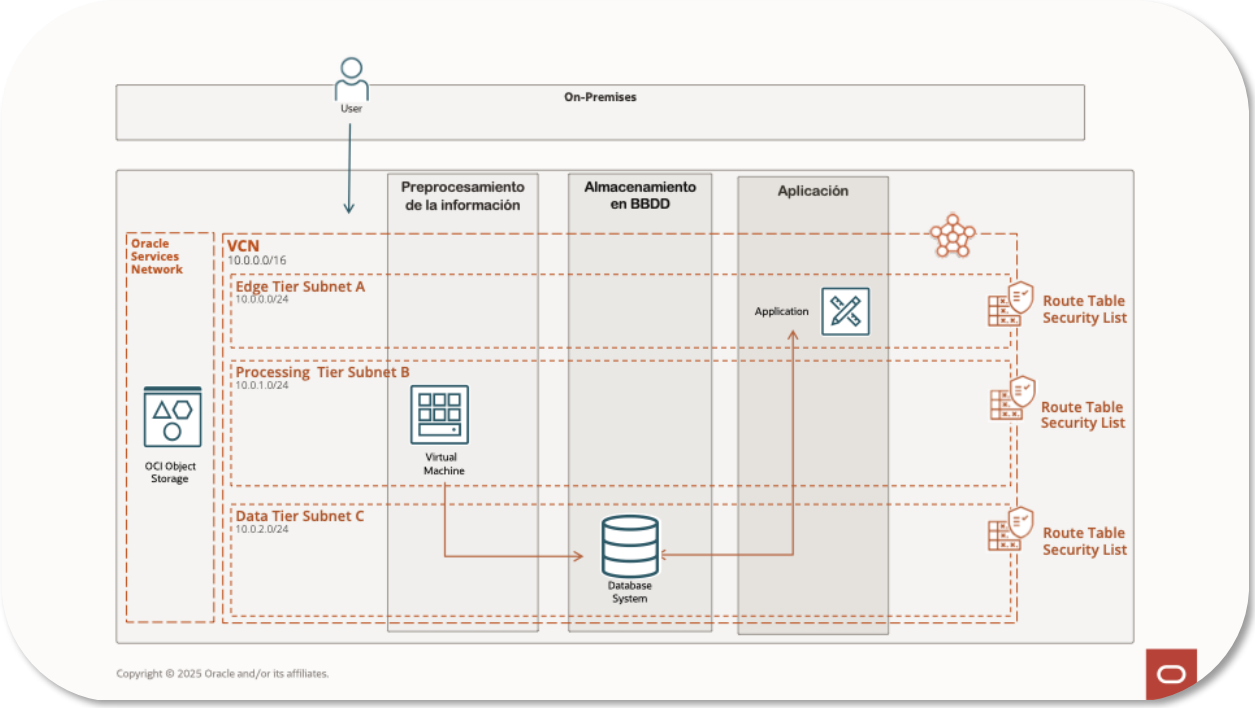
La infraestructura de red en dispositivos Roving Edge permite una gestión robusta y escalable de las configuraciones de red, incluso en entornos desconectados o desplegados en ubicaciones remotas. Como se menciona con anterioridad en la Guía, el dispositivo RED actúa como una extensión del entorno *cloud* dentro de una *tenancy* de OCI, manteniendo una arquitectura coherente en cuanto a segmentación, aislamiento y seguridad de red.

Los dispositivos RED incorporan un servicio de red avanzado basado en el uso de **Virtual Cloud Network (VCN) y *subnets* (subredes),** componentes clave para estructurar y proteger el flujo de tráfico dentro del entorno RED, y garantizar la comunicación segura entre las cargas de trabajo desplegadas localmente.

De acuerdo con las recomendaciones del **Esquema Nacional de Seguridad (ENS)**, la red y el entorno operativo desplegado en los dispositivos Roving Edge (RED) deben estar debidamente **segmentados**, **aislados** y **controlados**, aplicando **políticas restrictivas de acceso** que permitan mitigar riesgos y garantizar un nivel elevado de protección frente a amenazas.

Una configuración adecuada de la Virtual Cloud Network y sus subredes asociadas permite implementar estas buenas prácticas, proporcionando la flexibilidad necesaria para definir límites de red claros, aplicar políticas de acceso precisas. Este enfoque garantiza la protección de la información crítica y el enrutado seguro del tráfico, reduciendo la superficie de exposición a posibles amenazas.

Además, esta segmentación se alinea con los principios de **Arquitectura *Zero Trust***, que exige la verificación constante de identidad y contexto antes de autorizar cualquier acceso, y validación igualmente constante del tráfico según las políticas de seguridad establecidas.



Arquitectura simplificada que muestra la red virtual desplegada en la infraestructura Roving y las subredes, con aislamiento por capas

Los aspectos técnicos necesarios para implementar de forma segura la **segmentación de red**, el **control de perímetros de acceso** y la **protección de la confidencialidad** de las comunicaciones serán tratados con mayor detalle en la sección correspondiente a *Medidas de Protección*.

2.6.3 CÓMPUTO

El servicio de **Cómputo** disponible en la infraestructura Roving Edge (RED) permite el despliegue y gestión de **instancias virtuales (VMs)** en entornos remotos o desconectados, garantizando la capacidad de ejecutar cargas de trabajo con flexibilidad y escalabilidad, incluso en ubicaciones con recursos limitados o sin conectividad permanente con el entorno de cloud.

Este servicio facilita la creación, configuración y operación de máquinas virtuales sobre el dispositivo RED, permitiendo ajustar el uso de **recursos computacionales** a los requerimientos específicos de cada misión o carga de trabajo. Su diseño permite mantener la ejecución de servicios y aplicaciones en entornos edge garantizando la operación autónoma y segura en ubicaciones remotas.

Si bien las capacidades del servicio de cómputo permiten un alto grado de personalización, especialmente en la configuración de máquinas virtuales y tareas operativas, es fundamental aplicar **prácticas de configuración segura** para garantizar la protección del entorno. Por ello se recomienda consultar la guía "***CCN-STIC-889E: CS Oracle OCI Compute Instancias VM y Bare Metal***", que incluye un conjunto detallado de recomendaciones y buenas prácticas sobre:

- Configuración segura de máquinas virtuales.
- Implementar mecanismos de protección mediante el cifrado de la información y activación de arranque seguro (*Secure Boot*).
- Establecer controles de acceso basados en identidad para gestionar usuarios y permisos en las instancias virtuales.

Guía de Seguridad de las TIC
CCN-STIC 889E

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

La infraestructura Roving Edge ofrece funcionalidades específicas para la gestión y operación de máquinas virtuales (VMs), orientadas a garantizar flexibilidad, autonomía y seguridad en entornos remotos con conectividad limitada. Entre las principales capacidades se incluyen:

- **PERSISTENCIA DE CONFIGURACIONES PERSONALIZADAS EN EL ARCHIVO DE *HOSTS***

  Se habilita la persistencia de los cambios realizado en el archivo *hosts* de los dispositivos RED, asegurando que las configuraciones de red personalizadas se mantengan activas tras reinicios o actualizaciones del sistema. Esta capacidad es esencial en entornos *Edge*, donde la gestión remota puede ser limitada, permitiendo la operación autónoma de configuraciones de red críticas y reduciendo la necesidad de intervenciones manuales.

  La configuración detallada está descrita en la siguiente referencia técnica:

  Conservación de ediciones de archivos de hosts para Roving Edge Infrastructure

- **ACTUALIZACIÓN SEGURA DE DNS**

  Las modificaciones no controladas en la configuración DNS pueden afectar negativamente en la resolución de nombres y la funcionalidad del sistema. Para garantizar la continuidad operativa y evitar cambios no autorizados, es necesario aplicar medidas de protección específicas.

  A continuación, se detallan los procedimientos para configurar de forma segura los ajustes DNS y protegerlos frente a modificaciones no autorizadas:

  Actualización de DNS en instancias de Roving Edge Infrastructure

- **USO DE *cloud-init* PARA LA PERSONALIZACIÓN DE INSTANCIAS**

  Cloud-init es una herramienta que permite automatizar la inicialización y configuración de instancias de cómputo en la infraestructura Roving Edge. Su uso facilita la implantación de entornos preconfigurados, garantizando consistencia en los despliegues y reduciendo la necesidad de intervención manual.

  La infraestructura Roving Edge permite el uso de scripts de personalización basados en ***cloud-init***, lo que facilita un aprovisionamiento seguro y eficiente de las instancias de cómputo. Estas personalizaciones se conservan tras reinicios del sistema, garantizando la continuidad de los ajustes de seguridad y configuración, especialmente en entornos donde la intervención manual es limitada.

  Para obtener información detallada sobre su implementación, consulte la documentación técnica oficial.

  Adición de información de cloud-init para Roving Edge Infrastructure

- **USO DE REPOSITORIOS ORACLE EN INSTANCIAS LINUX**

  Para garantizar la actualización segura y efectiva de instancias Oracle Linux en entornos RED, es necesario establecer correctamente los ajustes del repositorio. Se puede optar por:

  - El uso de un servidor proxy, o,
  - La configuración de un repositorio privado.

  Además, se incluye el acceso al servicio *Unbreakable Linux Network (ULN*), que proporciona herramientas como *Ksplice* para mantener la integridad del sistema.

  La guía completa para configurar esta funcionalidad se encuentra disponible en:

  Uso de repositorios de Oracle en instancias de Oracle Linux para Roving Edge Infrastructure

- **EJECUCIÓN DE UTILIDADES DE LÍNEA DE COMANDOS**

  La ejecución de comandos CLI sobre instancias de cómputo alojadas en dispositivos RED permite una gestión directa y local, sin depender de conectividad externa. Esta capacidad es especialmente útil en entornos aislados o con comunicaciones restringidas.

  Para una configuración adecuada de la instancia, incluyendo la asignación de IP local, referencia del dispositivo y control de acceso mediante IP Tables puede consultarse el enlace que se proporciona a continuación:

  
  Configuración del host para ejecutar comandos de la CLI en instancias alojadas en dispositivos

- **CONFIGURACIÓN DEL SISTEMA OPERATIVO PARA SOPORTAR VNICs SECUNDARIAS**

  En escenarios donde una instancia de cómputo tiene asociadas múltiples interfaces de red virtual (**VNICs**), es necesario ajustar la configuración del sistema operativo para garantizar una **conectividad adecuada y segura**.

  Esta configuración permite que las direcciones IP públicas asociadas a VNICs secundarias puedan establecer comunicación con la instancia. Para ello, deben aplicarse los parámetros adecuados de filtrado de rutas inversas (*Reverse Path Filtering*), que permiten gestionar correctamente el tráfico entrante.

  Para instrucciones detalladas sobre esta configuración, consulte la documentación técnica disponible en este enlace:

  
  Configuración del sistema operativo de la instancia para las VNIC secundarias

2.6.4 ALMACENAMIENTO

Los dispositivos Roving Edge proporcionan servicios de almacenamiento local que reproducen las capacidades ofrecidas en una región Cloud de OCI, operando directamente sobre el dispositivo, sin necesidad de conexión activa a la nube.

Estos servicios permiten gestionar datos de forma segura y eficiente en entornos donde se requiere operar de manera autónoma. Dentro de este entorno, se distinguen dos tipos de almacenamiento principales:

- **Object Storage**: almacenamiento basado en objetos, ideal para grandes volúmenes de datos no estructurados mediante una arquitectura de objetos.
- **Block Volume**: almacenamiento de bloques persistente, utilizado principalmente como discos virtuales para instancias de cómputo

2.6.4.1 OBJECT STORAGE

El servicio de **Object Storage** disponible en la infraestructura Roving Edge, diseñado para almacenar datos no estructurados, es especialmente útil para cargas de trabajo que requieren almacenamiento masivo de información, como información multimedia, archivos de respaldo, registro de eventos (logs) o datos generados por sensores, elementos clave en entornos *Edge* con procesamiento local.

Este servicio permite la creación y gestión de **contenedores (*buckets*) y objetos**, proporcionando una solución segura y escalable para el almacenamiento de grandes volúmenes de datos en entornos perimetrales.

El servicio garantiza que únicamente los usuarios y sistemas autorizados puedan acceder a los datos, mediante la aplicación de políticas de control de acceso granulares. Asimismo, se integran mecanismos avanzados de cifrado como **Cifrado Siempre Activo** (*Always-On Encryption*), ***SEE-C (Server-Side Encryption with Customer-Provided Keys)***, que permite aportar claves de cifrado propias para el cifrado de la información. Adicionalmente, el servicio incorpora medidas de protección avanzadas como claves de **cifrado únicas por bucket y objeto**, la posibilidad de aplicar políticas de **control de acceso a nivel de objeto** (*Object-Level IAM*) y el uso de **Private Endpoints**, que permiten restringir el tráfico a entornos de red previamente autorizados.

Para una descripción completa del servicio de Object Storage, puede acceder al documento técnico a través del siguiente enlace:

Almacenamiento de objetos para Roving Edge Infrastructure

2.6.4.2 BLOCK VOLUME

El **Servicio de Volúmenes en Bloque** (*Block Volume*) en la infraestructura Roving Edge permite el aprovisionamiento de almacenamiento persistente para máquinas virtuales (VMs) desplegadas localmente en el dispositivo RED. Este tipo de almacenamiento se utiliza tanto para discos de arranque como para volúmenes de datos adicionales, y es fundamental en escenarios perimetrales con recursos principales y sin conexión permanente.

El servicio permite al operador gestionar de forma local el ciclo de vida completo de los volúmenes: creación, visualización, edición, eliminación y vinculación con instancias de cómputo, garantizando una administración eficiente del almacenamiento persistente en entornos perimetrales.

Para obtener más información o una visión general del volumen de bloque en Roving Edge Infrastructure, consulte la documentación técnica en el siguiente enlace:

Volúmenes en bloque para Roving Edge Infrastructure

2.6.5 SINCRONIZACIÓN DE DATOS

Aunque los dispositivos Roving Edge están diseñados para operar en escenarios conectados, semi-conectados o completamente desconectados de la nube, la sincronización de datos entre los dispositivos RED y la región de OCI, es una tarea altamente recomendable para garantizar la **coherencia operativa, la continuidad del servicio y la actualización de seguridad**.

El servicio de sincronización de datos permite la transmisión de información entre los contenedores de *Object Storage (buckets)* ubicados en el RED y su equivalente en la nube de OCI. Esta capacidad facilita la transferencia eficiente de datos, y contribuye tanto al respaldo seguro como a la distribución de actualizaciones. A continuación, se describen las principales características disponibles:

- **Sincronización Bidireccional:** Permite sincronizar datos en ambos sentidos, desde la nube al dispositivo RED y viceversa, garantizando que los datos actualizados localmente se almacenan a largo plazo en OCI, y que los cambios realizados en la nube se reflejen en el entorno local.

- **Distribución de actualizaciones de software:** La sincronización no se limita a datos operativos, también permite distribuir actualizaciones de software y parches de seguridad de OCI hacia los dispositivos RED, reduciendo la necesidad de intervención manual y asegurando que el dispositivo opere con las versiones más recientes y seguras.

Para una guía detallada sobre la configuración y gestión del servicio de sincronización de datos, consulte la documentación técnica disponible:

Sincronización de datos de Roving Edge Infrastructure

3. CONFIGURACIÓN SEGURA DE ROVING EDGE INFRASTRUCTURE

El **Esquema Nacional de Seguridad (ENS)** establece un conjunto de medidas de seguridad orientadas a la protección de sistemas de información. Aunque está dirigido principalmente a entidades del sector público que manejan información crítica y sensible, también constituye un marco de referencia aplicable para organizaciones privadas.

Estas medidas se estructuran en tres grandes grupos:

- **MARCO ORGANIZATIVO:** Incluye políticas, procedimientos y gobernanza que garantizan la seguridad a nivel organizativo, definiendo roles, responsabilidades y protocolos.
- **MARCO OPERACIONAL:** Se centra en las acciones y procedimientos diarios para mantener la seguridad en los sistemas, tales como la respuesta a incidentes, monitorización y evaluaciones periódicas de seguridad.
- **MEDIDAS DE PROTECCIÓN:** Comprende controles técnicos específicos para salvaguardar la información, los sistemas y las redes, tales como el cifrado, la autenticación y mecanismos de control de acceso.

Si bien el Marco Organizativo aborda la gobernanza interna, políticas y procedimientos que cada identidad debe implementar, esta guía se focaliza en el **Marco Operacional** y en las **Medidas de Protección** relacionadas con el despliegue, gestión y operación segura de la Infraestructura Roving Edge.

3.1 MARCO OPERACIONAL

Este grupo comprende el conjunto de medidas de seguridad necesarias para proteger el correcto funcionamiento del sistema como un conjunto integrado de componentes con un propósito específico. Para alcanzar el cumplimiento de los principios fundamentales y los requisitos mínimos de seguridad, deben implementarse las medidas de seguridad detalladas en esta sección. La aplicación de dichas medidas será proporcional a las necesidades de seguridad del sistema y a la clasificación de la información que este debe proteger.

3.1.1 CONTROL DE ACCESOS

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. Un control de acceso efectivo implica la gestión adecuada de privilegios, el seguimiento de las acciones de los usuarios y el mantenimiento de un registro claro y detallado de los eventos de acceso.

En el contexto de Roving Edge Infrastructure, estos principios se materializan mediante el uso de *Oracle Cloud Infrastructure Identity and Access Management* (OCI IAM). OCI IAM ofrece mecanismo de verificación de identidad, gestión de accesos basado en políticas, segregación de funciones mediante roles y autenticación robusta, asegurando un control de acceso alineado con los requisitos de seguridad del sistema.

Las siguientes secciones describen las medidas de protección del Control de Accesos aplicado a OCI Roving Edge Infrastructure, estructurado en los siguientes apartados:

- Identificación
- Requisitos de Acceso
- Segregación de Roles y Funciones
- Mecanismos de Autenticación.

Adicionalmente, el sistema debe registrar todas las actividades de acceso y uso para posibilitar la detección de incidentes y la respuesta adecuada en caso de brechas de seguridad o fallos del sistema.

3.1.1.1 IDENTIFICACIÓN

La identificación constituye la base fundamental del control de accesos, estableciendo la necesidad de contar con mecanismos que garanticen la **autenticidad y trazabilidad** de todas las entidades que interactúan con el sistema. Estas entidades incluyen organizaciones, usuarios, procesos y servicios. El objetivo de esta medida es asegurar que cada entidad posea una identidad única e inequívoca, lo cual es crucial para gestionar los derechos de acceso otorgados y rastrear las acciones realizadas sobre los recursos del sistema. Dichas cuentas deberán ser gestionadas de tal forma que deban ser inhabilitadas cuando se den una serie de condicionantes:

a) El usuario deje la organización.

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

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

El servicio OCI IAM, integrado en Roving Edge Infrastructure, da respuesta a esta necesidad estableciendo una arquitectura segura de identificación y gestión de identidades. A través de este servicio, se habilita la creación de cuentas, la definición de grupos, la asignación de permisos mediante políticas, y el control granular de acceso en función del perfil de cada entidad.

- **Cuentas de usuario y grupos:** Cada **cuenta de usuario** y cada grupo del entorno de Roving Edge están identificados de forma única mediante un **OCID**, permanente e inmutable asignado en el momento de su creación. Esta codificación garantiza que la identidad de cada entidad no puede ser alterada o duplicada, lo que facilita la trazabilidad completa de las acciones realizadas sobre los recursos del sistema. Las cuentas se agrupan en estructuras lógicas denominadas **grupos**, a las que se asignan **políticas de acceso** que definen los permisos y privilegios efectivos.
- De igual manera, los **recursos desplegados** en la infraestructura **OCI** (como instancias de cómputo, almacenamiento y redes virtuales) reciben su propio OCID. Este identificador también es único e inmutable, lo que permite gestionar de forma segura cada recurso dentro del entorno, sin ambigüedad.

En este marco, los OCIDs constituyen el mecanismo base para identificar de manera unívoca cada elemento. Su sintaxis sigue una estructura estandarizada definida por Oracle, que incluye información sobre el tipo de recurso, la región, el dominio de identidad y un identificador único, con el siguiente formato:

```
ocid1.<RESOURCE TYPE>.<REALM>.[REGION][.FUTURE USE(currently in blank)].<UNIQUE ID>
```

Algunos ejemplos ilustrativos:

Tenancy

```
ocid1.tenancy.oc1..aaaaaaaaba3pv6wkcr4jqae5f44n2b2m2yt2j6rx32uzr4h25vqstifsfdsq
```

Instancia de cómputo:

```
ocid1.instance.oc1.phx.abuw4ljrlsfiqw6vzzxb43vyypt4pkodawglp3wqxjqofakrwvou52gb6s5
```

La utilización de identificadores OCID constituye un elemento clave para la gestión segura del sistema, al permitir la trazabilidad individualizada de cada usuario, grupo y recurso. Esta capacidad de identificación está integrada de forma nativa tanto en la consola de gestión como en las interfaces de programación (API), lo que facilita la administración centralizada y auditable del sistema. Este enfoque refuerza el cumplimiento de los principios establecidos por el ENS en lo relativo a la autenticación, el control de acceso y la supervisión de actividades.

GESTION DE USUARIOS

Como se indica al comienzo de esta sección, en la infraestructura Roving Edge, cada usuario representa una entidad individual con un conjunto único de atributos y permisos que definen su acceso y capacidades dentro del sistema. La gestión segura y adecuada de usuarios es fundamental para mantener la integridad y confidencialidad de los recursos. Con esto, al **crear un usuario** en la Infraestructura Roving Edge, deben considerarse los siguientes **atributos**:

- Nombre de usuario único: Cada usuario debe tener un nombre único dentro de la plataforma, que servirá también como identificador para el inicio de sesión de la consola.
- Descripción del usuario: Debe incluirse una descripción clara que permita identificar el rol o función del usuario dentro de la organización.

Un usuario recién creado no tiene **permisos** asignados de forma predeterminada. Para que un usuario pueda operar en la infraestructura Roving Edge, debe ser asignado a uno o más grupos. Estos grupos están vinculados a políticas de acceso que determinan los recursos y operaciones permitidos dentro de la *tenancy*.

Para acceder a la Infraestructura Roving Edge, el usuario debe contar con las **credenciales** necesarias según el tipo de acceso. Para el acceso a la **Consola**, el usuario debe disponer de una contraseña segura que cumpla con las políticas de seguridad definidas. Para el acceso por **API**, el usuario debe contar con la clave API autorizadas para operar mediante interfaces programáticas.

La gestión de usuarios en OCI Roving Edge puede realizarse a través de múltiples interfaces, proporcionando flexibilidad tanto para la administración manual como para la automatización:

i) **OCI Console** – En la consola web de la infraestructura Roving Edge, navegar a

Identity Management → Users,

navegar para realizar operaciones administrativas desde interfaz gráfica

ii) **OCI API** – Permite el acceso programático a las funciones de gestión de usuarios, facilitando la integración con sistemas externos de identidad o herramientas de automatización.

iii) **OCI Command Line Interface (CLI)** – Proporciona comandos específicos para la gestión de usuarios desde línea de comandos.

Las siguientes acciones están disponibles para la gestión de usuarios y grupos en la infraestructura Roving Edge:

USUARIOS

Crear, listar, consultar detalles, editar, actualizar capacidades y eliminar usuarios

GRUPOS

Crear, listar, consultar detalles, editar, añadir usuarios a un grupo, eliminar usuarios de un grupo y eliminar grupos

Para instrucciones detalladas sobre cómo ejecutar estas tareas, se recomienda consultar la documentación oficial:

Identity and Access Management (IAM) para Roving Edge Infrastructure

Adicionalmente, Oracle proporciona una **guía de configuración segura** para todo el servicio OCI IAM, la cual incluye recomendaciones específicas y buenas prácticas para una gestión de identidades y accesos.

Guía de Configuración segura para IAM y servicios de seguridad — Guía de Seguridad de las TIC CCN-STIC 889A

3.1.1.2 REQUISITOS DE ACCESO

De acuerdo con las medidas de seguridad establecidas por el Esquema Nacional de Seguridad, todos los recursos de un sistema deben estar protegidos frente a accesos no autorizados. Esto implica la implementación de **mecanismos de control de acceso** que impidan el uso indebido de los recursos por parte de entidades no autorizadas.

Sólo las organizaciones, usuarios o roles con permisos expresamente otorgados deben tener capacidad para acceder o administrar dichos recursos. Estos permisos deben estar regulados por las políticas de seguridad de la organización, asignados por una autoridad designada y en consonancia con el principio de mínimo privilegio.

Para garantizar el cumplimiento de esta medida de seguridad, el control de acceso se implementa principalmente en dos niveles:

1. **Acceso al Dispositivo Roving Edge mediante Consola Serie**

   El acceso administrativo directo al dispositivo físico Roving Edge debe estar estrictamente restringido. Este tipo de acceso, que proporciona capacidades de administración avanzadas, está protegido mediante una **frase de desbloqueo** (*passphrase*), la cual se configura durante el proceso de aprovisionamiento del nodo (véase sección 2.1: *Consideraciones de seguridad durante el aprovisionamiento del nodo*).

   - Esta contraseña actúa como primera línea de defensa contra accesos físicos no autorizados.
   - La modificación de la *passphrase* puede realizarse directamente a través de la interfaz de la Consola Serie (véase sección *2.5: Operación de la Consola Serie*).
   - Se recomienda definir una política de cambio periódico de esta *passphrase*, así como su custodia segura.

2. **Acceso a Recursos Desplegados dentro de Roving Edge Infrastructure.**

   Este nivel se refiere a la gestión de accesos a todos los recursos virtuales desplegados en el RED, incluyendo máquinas virtuales, almacenamiento, configuraciones de red, herramientas de monitorización y parámetros de seguridad.

   La protección de estos recursos se basa en la aplicación de mecanismos de autenticación y autorización, mediante políticas diseñadas según el perfil de usuario y el tipo de recurso.

   Tal como se indicó previamente, el control de acceso a estos recursos se gestiona a mediante el servicio OCI IAM (*Identity and Access Management*), que permite definir políticas de seguridad granulares, que establecen con precisión qué identidades pueden realizar qué acciones sobre los recursos desplegados.

   En línea con lo establecido por el Esquema Nacional de Seguridad respecto del principio de mínimo privilegio, **ningún acceso es concedido de forma predeterminada**. Todo permiso debe ser otorgado explícitamente por la autoridad competente.

   La descripción operativa del proceso de gestión de derechos y permisos se abordará más adelante en esta guía.

3.1.1.3 SEGREGACIÓN DE FUNCIONES Y TAREAS

El Esquema Nacional de Seguridad (ENS) establece que deben implementarse medidas organizativas y técnicas que garanticen la **segregación de funciones** como parte del control de acceso. Esta medida tiene como finalidad preservar la integridad del sistema y reforzar la trazabilidad de las acciones realizadas, evitando que una única persona pueda ejecutar cambios críticos de manera unilateral, y asegurando que las funciones críticas estén adecuadamente distribuidas entre **distintos perfiles o unidades organizativas**.

En relación con los recursos críticos identificados en las medidas de control de acceso, es necesario establecer **cuentas de administrador diferenciadas** o grupos de administración específicos para su gestión. Esta separación funcional debe aplicarse, en particular, sobre componentes sensibles como los recursos de seguridad, la infraestructura de red y las herramientas de monitorización, garantizando que ningún grupo de administradores concentre simultáneamente el control sobre todos ellos.

Adicionalmente, el ENS establece la necesidad **de separar funciones clave dentro del ciclo de vida de los sistemas**, tales como el desarrollo, la configuración operativa, el mantenimiento del sistema y las tareas de auditoría. La acumulación de funciones críticas en un único rol o unidad organizativa compromete la

capacidad de detección y control, por lo que debe evitarse en todo caso para preservar la integridad del sistema.

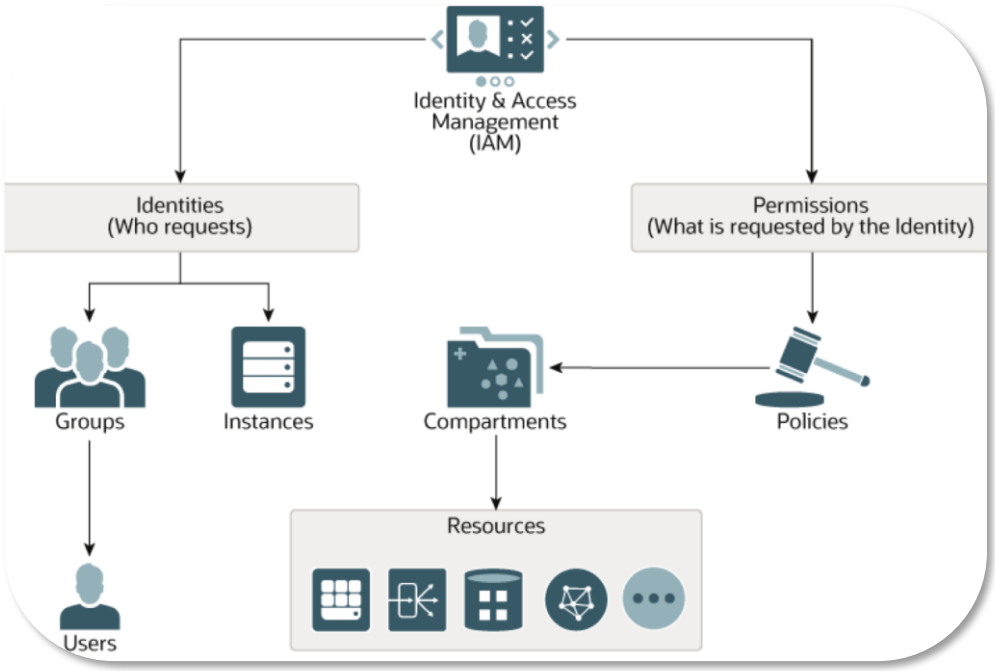
Para facilitar esto, Oracle proporciona el **Control de Acceso Basado en Roles** (RBAC) a través del servicio OCI IAM. RBAC permite a los administradores configurar el acceso de los usuarios a los recursos de OCI Roving Edge alineado con el principio de mínimo privilegio. De esta manera, cada usuario dispone únicamente de los permisos necesarios para el desempeño de sus funciones específicas. Mediante la creación de grupos y asignación de políticas adecuadas en OCI IAM, los administradores pueden garantizar que las funciones de seguridad y operativas se mantengan debidamente segregadas.

3.1.1.4 PROCESO DE GESTIÓN DE DERECHOS DE ACCESO

El proceso de gestión de derechos de acceso se fundamenta en los principios de **mínimo privilegio**, **necesidad de conocimiento** y **capacidad de autorización**, con el objetivo de limitar el acceso a los recursos a aquellos usuarios y sistemas que requieran dicha información para el desempeño de sus funciones, minimizando riesgos de seguridad y evitando exposiciones no autorizadas.

La asignación de privilegios se realiza bajo un control riguroso para garantizar el cumplimiento de los principios de seguridad fundamentales: **Integridad, Confidencialidad, Autenticidad y Trazabilidad**.

La implementación técnica de esta medida de seguridad se realiza a través del **servicio OCI IAM**, donde los derechos de acceso pueden ser gestionados eficazmente mediante políticas asignadas a recursos, familias de recursos, usuarios o grupos de usuarios, facilitando una administración centralizada, coherente y alineada con las mejores prácticas de seguridad.



Una **política de OCI IAM** está compuesta por una o varias declaraciones que especifican quién puede acceder a qué recursos, utilizando para ello una sintaxis básica o condicional:

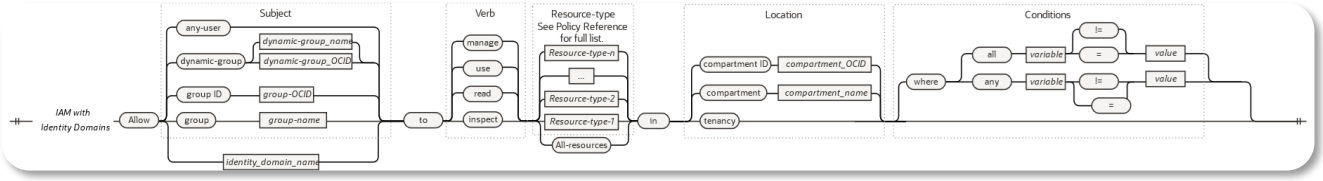
- Sintaxis Básica: Es una forma sencilla y directa de definir permisos, sin aplicar condiciones adicionales:

```
Allow <subject> to <verb><resource> in <location>
```

- Sintaxis Condicional: Permite añadir restricciones o reglas adicionales (condiciones) que deben cumplirse para que la política se aplique.

```
Allow <subject> to <verb><resource> in <location> where <conditions>
```

En el siguiente diagrama se explican brevemente los elementos de sintaxis:



Para una comprensión más detallada sobre el funcionamiento y la construcción de políticas IAM en Oracle Cloud Infrastructure, se recomienda consultar la documentación oficial, donde se explican en profundidad los elementos de la sintaxis y se proporcionan recursos adicionales para su correcta implementación.

Visión general de las políticas de IAM

Para obtener información detallada sobre la elaboración de políticas IAM específicas para la Infraestructura Roving Edge, se recomienda consultar la sección "*Permisos para Roving Edge Infrastructure*" en la documentación oficial. Esta sección aborda el proceso de creación de políticas que regulan el acceso a los siguientes servicios fundamentales dentro del entorno de Roving Edge:

- Block Volume
- Certificados
- Instancias de Cómputo
- Sincronización de Datos
- Diagnóstico
- Eventos
- IAM
- Monitorización
- Redes
- Almacenamiento de objetos
- Actualización del sistema

Permisos para Roving Edge Infrastructure

3.1.1.5 MECANISMOS DE AUTENTICACIÓN

El ENS establece directrices claras para la implementación de mecanismos de autenticación que aseguren un acceso controlado y una adecuada protección de los sistemas. En este sentido, se emplean mecanismos como el uso de contraseñas robustas y la validación mediante certificados para reforzar la seguridad.

En OCI Roving Edge Infrastructure se han adoptado mecanismos de autenticación adaptados tanto a las exigencias del ENS como a las particularidades funcionales y de seguridad del sistema:

i) **GESTIÓN DE USUARIOS Y PERMISOS:** Como se indica en secciones anteriores, el acceso a la consola del dispositivo se facilita mediante cuentas de usuario agrupadas en grupos, siguiendo los principios de segregación y control de acceso.

ii) **AUTENTICACIÓN EN LA CONSOLA DEL DISPOSITIVO:** El acceso a la consola del dispositivo Roving Edge requiere autenticación mediante usuario y contraseña. Las contraseñas tienen una vigencia máxima de 90 días, por lo que es obligatorio su cambio periódico. La gestión segura de estas credenciales dentro de la organización es fundamental, ya que la pérdida de estas imposibilita el acceso al dispositivo.

iii) **CLAVES API**: Las claves API se utilizan para interactuar con la Infraestructura Roving Edge a través de la interfaz de línea de comandos (CLI). Estas credenciales deben ser gestionadas de manera segura y regeneradas periódicamente para mantener un nivel elevado de seguridad.

iv) **AUTENTICACIÓN BASADA EN CERTIFICADOS**: Para establecer una conexión segura con los dispositivos Roving Edge, es necesario descargar e importar un certificado CA raíz. Este certificado es un requisito esencial para garantizar la comunicación entre el dispositivo y el *host*.

Para obtener información más detallada sobre los mecanismos de autenticación y los procedimientos de acceso, se recomienda consultar la guía completa disponible en el siguiente enlace:

Acceso a Infraestructura Roving Edge

3.1.2 EXPLOTACIÓN

Esta sección recoge las medidas relacionadas con el **control operativo y la gestión de los servicios** desplegados en la infraestructura. El ENS establece una serie de procesos y procedimientos que deben ser ejecutados por las entidades responsables con el fin de garantizar una explotación segura, eficiente y conforme con los principios de seguridad establecidos.

Estas medidas abarcan un conjunto de tareas técnicas, organizativas y de supervisión que deben ser implementadas por los responsables de los sistemas, principalmente los departamentos TIC, y tienen como objetivo asegurar la **disponibilidad, integridad y trazabilidad** del servicio durante su fase operativa.

3.1.2.1 INVENTARIO DE ACTIVOS

En cumplimiento con los requisitos de gestión y seguridad establecidos por el ENS, resulta imprescindible mantener un inventario actualizado de todos los activos, tanto a nivel de sistemas como de componentes, incluyendo su tipología, estado operativo y ubicación.

La existencia de un inventario completo y correctamente gestionado permite a las organizaciones disponer de una **visibilidad total sobre sus recursos tecnológicos**, facilitando su administración conforme

a las políticas internas de seguridad y control, y permitiendo la identificación de desviaciones, accesos no autorizados o configuraciones no deseadas.

En el caso de Infraestructura Roving Edge, esta medida se aplica específicamente a los nodos de dispositivos desplegados, tanto en su versión Roving Edge Device (RED) como Roving Edge Ultra. El entorno de Oracle proporciona varias interfaces para gestionar este inventario de forma flexible y trazable:

RED

Consulta de nodos de dispositivo de Roving Edge Infrastructure

Obtención de detalles de un nodo de Roving Edge Infrastructure

Ultra

Consulta de nodos de Roving Edge Ultra

Obtención de detalles de un nodo de Roving Edge Ultra

El objetivo de esta medida es garantizar que ningún recurso quede fuera del control de la organización, permitiendo así una gestión proactiva y alineada con los principios de seguridad establecidos. Tal y como se detalla en la documentación técnica oficial proporcionada, para facilitar la administración de los nodos desplegados la Infraestructura Roving Edge proporciona **herramientas** eficaces como la **Consola** Roving Edge, la Interfaz por línea de comando (**CLI**) y las **API**, que permiten la supervisión como el control de los dispositivos. Estas interfaces contribuyen de manera significativa a la creación y mantenimiento de un **inventario detallado**, elemento clave para cumplir con los estándares de seguridad y los requisitos de conformidad establecidos por el ENS.

3.1.2.2 MATENIMIENTO Y ACTUALIZACIONES DE SEGURIDAD

De acuerdo con lo establecido por el ENS, toda organización debe disponer de procedimientos formalizados para analizar, planificar y ejecutar la aplicación de **actualizaciones de seguridad**, parches, mejoras funcionales y nuevas versiones de software. Esta práctica resulta esencial para mantener la seguridad, disponibilidad y estabilidad del sistema a lo largo de su ciclo de vida.

En el caso de la Infraestructura Roving Edge, el mantenimiento de los dispositivos se basa en una gestión eficaz del **software de sistema**, lo que incluye: aplicación de actualizaciones de seguridad, implementación de nuevas versiones y mejoras y la posibilidad de revertir versiones en caso de incidencia. Este proceso puede llevarse a cabo tanto en modo **conectado** (online) como en modo **desconectado** (offline), según las condiciones de conectividad del entorno operativo.

Se recomienda realizar **comprobaciones periódicas de la versión del software instalada** en los dispositivos Roving Edge, con el fin de asegurar que estén ejecutando la versión más actualizada corrigiendo así posibles vulnerabilidades conocidas.

Para facilitar la gestión operativa, el sistema permite realizar las actualizaciones de seguridad en dos modalidades:

- Actualización en modo **conectado**. Cuando los dispositivos están conectados a OCI, el procedimiento de actualización se inicia verificando que el dispositivo esté alineado con la versión requerida. Si el dispositivo se encuentra a más de una versión de diferencia, las actualizaciones deben aplicarse de forma **secuencial**, versión por versión. El paquete de actualización tiene un tamaño comprendido entre 20 y 30 GB, por lo que el tiempo de descarga dependerá directamente de la velocidad de red disponible. Una vez completada la actualización, el sistema reiniciará automáticamente el dispositivo para aplicar los cambios.

Actualización del software del dispositivo Roving Edge mientras está conectado

- En entornos **desconectados**, el proceso se iniciará con la verificación de la versión actual del software a través de la consola del dispositivo. A continuación, desde la consola OCI en un entorno conectado, se descargará el **paquete de actualización** correspondiente, que será posteriormente transferido al dispositivo mediante un medio seguro. Una vez en el sistema, el paquete será importado y ejecutado, finalizando con el reinicio automático del dispositivo.

Actualización del software del dispositivo Roving Edge mientras está desconectado

Para obtener instrucciones detalladas sobre tareas como la identificación de la versión del software del dispositivo o la reversión a una versión anterior, se recomienda consultar la documentación oficial disponible en el siguiente enlace

Gestión de versiones de software de dispositivos Roving Edge

3.1.2.3 PROTECCIÓN FRENTE A CÓDIGO DAÑINO

La protección frente a código dañino constituye un pilar fundamental en el marco de las medidas de protección del ENS. Establece la necesidad de disponer de mecanismos tanto preventivos como reactivos frente a amenazas como virus, gusanos, spyware, troyanos u otras formas de programa maligno *(malware)*. Estos mecanismos son esenciales para preservar la integridad de los sistemas, evitar accesos no autorizados y mitigar riesgos asociados a fugas o alteración de la información y otras vulnerabilidades provocadas por código dañino.

En el caso de la Infraestructura Roving Edge, se implementan diversas medidas para garantizar una defensa en profundidad frente a código malicioso:

- A nivel preventivo, todo el código liberado es previamente analizado mediante **herramientas de detección de *malware*** en la plataforma SPLAT. Por otro lado, el sistema operativo del *host* **no permite acceso SSH** ni acceso directo por consola serial como principio de diseño, impidiendo su manipulación salvo mediante procesos oficiales de actualización controlada proporcionada por Oracle.
- A nivel reactivo, la Infraestructura Roving Edge incorpora de forma nativa una **funcionalidad de análisis antivirus** (ClamAV) cuya ejecución periódica permite detectar posibles amenazas

como virus o malware. Los registros generados por estos análisis están disponibles para el cliente a través de la interfaz web.

La adopción de estas medidas, tanto en su vertiente preventiva como reactiva, contribuye a que la infraestructura Roving Edge mantenga un nivel de seguridad elevado y resiliente frente a la evolución constante de amenazas asociadas a *malware* o código dañino.

3.1.2.4 GESTIÓN DE INCIDENTES

Esta medida indica la necesidad de registrar todas las actuaciones relacionadas con la gestión de incidentes, de forma que se registren las acciones realizadas tras un incidente, así como las evidencias para sustentar una postura de seguridad.

La gestión de incidentes es un proceso crítico para garantizar la seguridad y continuidad operativa de la Infraestructura Roving Edge de Oracle, alineado con los requisitos del Esquema Nacional de Seguridad (ENS). A través de ***My Oracle Support (MOS)***, el personal autorizado puede crear, clasificar y gestionar incidentes, asegurando que la información sensible esté protegida según las políticas de seguridad y privacidad vigentes. En caso de un incidente, es necesario documentar todos los detalles y clasificarlo según su severidad y prioridad, escalando cuando sea necesario a niveles superiores de soporte.

Para obtener instrucciones detalladas sobre cómo gestionar las solicitudes de soporte técnico, consulte la documentación oficial a través del siguiente enlace:

Solicitudes de Soporte

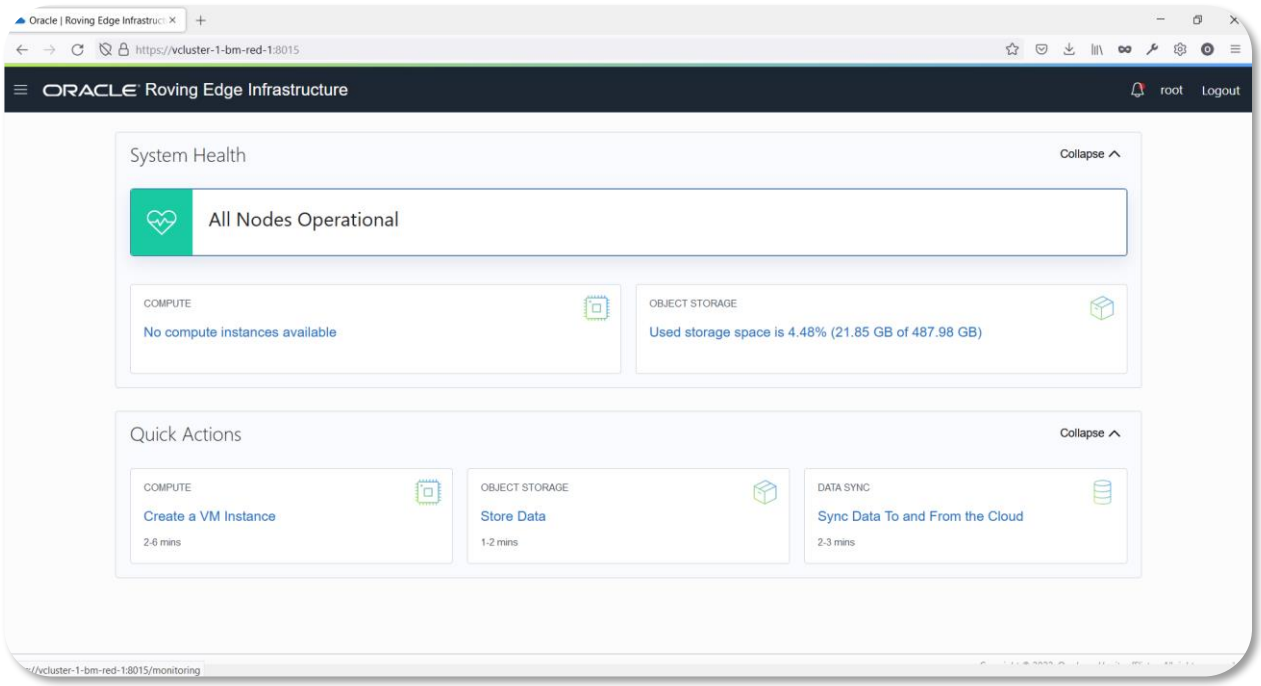
Una vez gestionado el incidente, es crucial seguir el proceso de seguimiento, resolución y cierre, garantizando que las acciones correctivas restauren la seguridad y funcionalidad de la infraestructura. Además, se debe documentar el incidente conforme a las normativas del ENS, incluyendo las lecciones aprendidas y las medidas preventivas adoptadas. Todo el proceso debe cumplir con los principios de confidencialidad, integridad y disponibilidad establecidos en el ENS, asegurando que la infraestructura esté protegida frente a futuros riesgos.

3.1.2.5 REGISTRO DE LA ACTIVIDAD

De acuerdo con los requisitos establecidos por el ENS, el registro efectivo de la actividad de los usuarios constituye un elemento clave para garantizar la responsabilidad, trazabilidad, y la seguridad en los sistemas de información. La infraestructura Roving Edge dispone de los mecanismos que aseguren la generación, almacenamiento y protección de registros de actividad, permitiendo su posterior análisis:

- **Actividad de los usuarios**: Registro de la identidad del usuario, la fecha y la hora de la acción y los recursos o servicios afectados. Esto permite reconstruir el historial de operaciones y detectar comportamientos anómalos no autorizados.
- **Actividad del dispositivo**: Los registros incluyen eventos relevantes del sistema, como el estado operativo del dispositivo.
- **Mensajes de error y acciones fallidas**: Registros de errores e intentos fallidos que facilitan la detección de incidentes de seguridad, errores de configuración o intentos de intrusión.

La consola de gestión de Roving Edge ofrece una vista consolidada del estado del sistema a través del componente denominado ***System Health***.



System Health: Consulta en tiempo real del estado general del nodo

Desde el apartado Node Management, es posible acceder al detalle de cada nodo individual, incluyendo el estatus operativo, métricas clave y **logs asociados** a ese nodo. La opción de Logging permite descargar localmente los registros de actividad generados por el nodo, tanto para su análisis manual como para su procesamiento mediante soluciones SIEM y análisis forense.

Estos registros se organizan en tres categorías principales:

- **Hardware Information**
- **Network**
- **Storage**

En el marco de esta infraestructura, el bloque ***Hardware Information*** permite acceder a los registros directamente relacionados con la operativa del nodo, incluyendo trazas de servicios críticos como:

- **AIDE**

  verificación de la integridad del sistema
- **compute-api**

  interacción con recursos de cómputo
- **firewall**

  eventos relacionados con el tratamiento de tráfico entrante y saliente
- **console**

  eventos de consola
- **identity-control-plane**

  gestión y autenticación de identidades

- **metrics**
- **…**

La gestión y disponibilidad adecuada de los registros de actividad resulta fundamental para garantizar la trazabilidad y la capacidad de auditoría conforme a los estándares del Esquema Nacional de Seguridad. Para ampliar información sobre la gestión de registros, se recomienda consultar la documentación técnica oficial:

Registros del dispositivo Roving Edge

3.1.2.6 PROTECCIÓN DE CLAVES CRIPTOGRÁFICAS

La protección de claves criptográficas es fundamental para salvaguardar la información sensible y garantizar la confidencialidad e integridad de los datos. El ENS establece una serie de requisitos específicos para la gestión segura de claves, que abarcan desde su generación, transporte y custodia, hasta su archivado y destrucción.

Asimismo, el ENS recomienda que las claves se mantengan aisladas de los sistemas operativos en los que se utilizan, evitando cualquier acceso no autorizado. Para ello, es imprescindible el uso de algoritmos criptográficos certificados que aseguren robustez y fiabilidad del sistema criptográfico en su conjunto.

Los dispositivos Roving Edge pueden configurarse para utilizar claves criptográficas gestionadas por Oracle (***Oracle-managed***) o gestionadas por el cliente (***customer-managed***). Cuando se emplean claves gestionadas por el cliente, este asume la responsabilidad de almacenar y administrar de manera segura claves maestras, que son fundamentales para proteger información sensible como contraseñas y claves de recuperación.

La clave maestra (***master key***) de un dispositivo Roving Edge es un componente crítico de seguridad. Esta clave controla el acceso *root*, garantizando que únicamente usuarios autorizados puedan desbloquear y operar el dispositivo. Hasta que la Consola Serie no se desbloquee mediante la ***passphrase*** de la clave maestra, el dispositivo permanecerá inoperativo.

La gestión de la **Master Key** depende del método de aprovisionamiento del dispositivo.

- En **dispositivos aprovisionados de fábrica**, por defecto estos dispositivos utilizan una Clave Maestra generada y gestionada por Oracle, aunque existe la posibilidad de emplear una clave personalizada. Si es necesario, la clave maestra puede ser eliminada para inutilizar el dispositivo, hasta su recuperación con otra clave.
- En dispositivos **auto aprovisionados**, la gestión completa de la clave maestra, así como de la passphrase y contraseñas, es responsabilidad exclusiva del usuario, sin intervención alguna por parte de Oracle.

Configurar credenciales en dispositivos auto aprovisionados

Consideraciones de Seguridad

Para evitar accesos no autorizados, es imprescindible garantizar la protección del acceso *root* mediante una adecuada gestión de la **Clave Maestra**. Se deben implementar las siguientes medidas de seguridad:

- Restringir el acceso a la clave maestra únicamente a personal autorizado

- Utilizar mecanismos seguros para el almacenamiento de la clave
- Establecer políticas claras de recuperación en caso de pérdida de la clave

En cuanto a la gestión de la **Clave Maestra**, se contemplan las siguientes operaciones principales:

1. **Uso de una Clave Maestra personalizada**

   En los dispositivos proporcionados por Oracle, la protección de la información secreta se gestiona mediante una clave maestra basada en el Servicio de Gestión de Claves (KMS) y un módulo de seguridad hardware (HSM).

   Para un mayor control sobre la información confidencial, es posible configurar una clave maestra basada en KMS proporcionada por el cliente desde la *tenancy* de OCI.

   Esta clave personalizada proporcionada por el usuario solo puede especificarse en el momento de **creación del nodo**, no es posible modificar posteriormente un nodo creado originalmente con una clave proporcionada por Oracle.

   Para más información sobre la configuración de claves maestras personalizadas, se puede consultar la documentación oficial:

   
   Uso de su propia clave maestra con dispositivos de Roving Edge Infrastructure

2. **Destrucción de la Clave Maestra**

   La protección de la seguridad en los dispositivos de Roving Edge *Infrastructure* es fundamental, especialmente en situaciones donde un dispositivo pueda estar comprometido o en riesgo. La **destrucción** de la clave maestra es una acción crítica para evitar accesos no autorizados y garantizar que los datos sensibles permanezcan seguros.

   Este procedimiento elimina de forma irreversible la clave maestra, dejando el dispositivo inoperativo para evitar posibles vulnerabilidades futuras.

   Para instrucciones detalladas sobre cómo realizar de forma segura la destrucción de la clave maestra, consulte el siguiente enlace:

   
   Destrucción de la Clave Maestra para los dispositivos de Roving Edge Infrastructure

3. **Recuperación de un Dispositivo Después de la Destrucción de la Clave Maestra**

   Aunque la destrucción de la clave maestra asegura el dispositivo al prevenir accesos no autorizados, también deshabilita su funcionalidad. Para restaurar el dispositivo y volver a un estado operativo, es necesario recuperar la clave maestra.

   Los pasos detallados para la recuperación se pueden encontrar en el siguiente enlace:

   
   Recuperación del dispositivo de Roving Edge Infrastructure después de destruir la Clave Maestra

3.1.3 MONITORIZACIÓN DEL SISTEMA

En cumplimiento con el Esquema Nacional de Seguridad, los sistemas deben estar sujetos a medidas de monitorización que garanticen la **integridad, disponibilidad y confidencialidad de la información** que procesan. El sistema de monitorización debe incorporar mecanismos capaces de recopilar datos relevantes conforme a la clasificación del sistema, permitiendo evaluar los controles de seguridad a lo largo del tiempo.

Diseñada para operar como una extensión de los servicios en la nube de Oracle en entornos remotos, la Infraestructura Roving Edge incorpora funcionalidades de monitorización que permiten tanto el control del rendimiento operativo como la supervisión del estado de seguridad. Si bien la herramienta ***System Health*** se centra en el rendimiento, también puede utilizarse para identificar comportamientos atípicos que advierten de posibles amenazas de seguridad.

Para obtener más información sobre cómo monitorizar el estado del sistema consulte el siguiente enlace:

Supervisión del dispositivo de Roving Edge Infrastructure

Las métricas ofrecen información valiosa sobre el rendimiento del sistema, lo que permite a los administradores detectar anomalías, optimizar el uso de recursos y garantizar el cumplimiento de los requisitos de seguridad y operación. Al habilitar la recopilación de métricas, es posible analizar tendencias, identificar comportamientos inusuales y ajustar la infraestructura para lograr un funcionamiento más eficiente.

La Infraestructura Roving Edge Infrastructure admite la generación de **métricas** de rendimiento y estado. Estas métricas se recopilan desde los servicios del sistema y por defecto, se almacenan en compartimentos de ***Object Storage***.

Para su análisis y visualización a lo largo del tiempo, Roving Edge está preconfigurado para interactuar con *InfluxDB*, una base de datos de series temporales diseñada para manejar datos de alta frecuencia. Al redirigir las métricas hacia InfluxDB, los administradores obtienen una visión más profunda del comportamiento del sistema, lo que permite anticiparse a posibles incidencias y asegurar un funcionamiento seguro y eficiente de los dispositivos.

Las instrucciones detalladas para configurar la recopilación de métricas y su envío a InfluxDB están disponibles en el siguiente enlace:

Métricas de dispositivo

3.2 MEDIDAS DE PROTECCIÓN

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

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

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

3.2.1 PROTECCIÓN DE LOS EQUIPOS

El marco establecido por el Esquema Nacional de Seguridad determina que deben implementarse medidas de protección que garanticen la seguridad, integridad y disponibilidad de los **sistemas de información**, así como del **equipamiento que los sustenta**. Estas medidas comprenden todos los mecanismos necesarios para asegurar la configuración segura del sistema, preservando al mismo tiempo la confidencialidad de las operaciones realizadas.

Estas medidas de protección abarcan tanto la seguridad física, como la seguridad lógica y las salvaguardas operativas. Como extensión de la infraestructura *cloud* de Oracle, diseñada para operar en entornos remotos, los dispositivos Roving Edge requieren un enfoque de seguridad que contemple no solo la protección de los sistemas del usuario final, sino también salvaguardas adicionales específicas de la computación en el borde (*edge computing*).

Aunque muchas de las medias de seguridad aplicables a estaciones de trabajo tradicionales siguen siendo pertinentes, deben complementarse con controles diseñados para afrontar los riesgos particulares asociados a la movilidad del dispositivo, la conectividad intermitente y la posible exposición a entornos no controlados.

Las medidas de protección que deben aplicarse a los dispositivos de la Infraestructura Roving Edge incluyen diferentes capas de seguridad:

- **Protección Física:** Se deben implementar controles de acceso que aseguren que únicamente el personal autorizado pueda manipular los dispositivos y acceder a su entorno operativo.
- **Seguridad Lógica:** Es fundamental aplicar mecanismos de autenticación robustos, así como el cifrado de la información almacenada y transmitida. Estas medidas protegen la confidencialidad e integridad de los datos frente a accesos no autorizados o interceptación.
- **Medidas Operativas:** Deben establecerse políticas de uso seguro, como la desconexión automática de sesiones tras períodos de inactividad, la limitación de privilegios por rol y la restricción del acceso mediante métodos no autorizados.

El acceso a los dispositivos Roving Edge debe realizarse conforme a las políticas de seguridad definidas por la organización, siguiendo siempre las mejores prácticas y principios de mínimo privilegio. Los mecanismos de acceso disponibles se describen en la sección "*Acceso al Dispositivo*", e incluyen principalmente:

i) Gestión de los nodos desde la consola Oracle Cloud Infraestructura. Requiere conectividad a internet.

ii) Acceso a la consola del dispositivo Roving Edge Infrastructure. Acceso local directo a la interfaz de administración.

iii) Interfaz de línea de Comandos (CLI). Permite la administración a través de comandos.

iv) Acceso mediante API. Integración segur a través de llamadas programáticas, con autenticación y control de permisos.

Acceso a Roving Edge

Aplicar correctamente estas medidas de protección es clave para garantizar la integridad operativa de los dispositivos Roving Edge y minimizar el riesgo de accesos no autorizados.

3.2.2 BLOQUEO DEL PUESTO DE TRABAJO

Si bien la protección del puesto de trabajo suele centrarse en la interacción directa del usuario con sistemas individuales, en el caso de la Infraestructura Roving Edge, los dispositivos forman parte de una red distribuida que extiende los servicios en la **nube a ubicaciones periféricas remotas**. En este contexto, la gestión robusta de sesiones adquiere una importancia aún mayor, ya que es fundamental para proteger tanto la infraestructura como los datos procesados, especialmente en entornos donde la seguridad física puede no estar plenamente garantizada y el control de acceso digital se convierte en un componente crítico de la seguridad.

Para mitigar estos riesgos, la Consola del Dispositivo Roving Edge establece restricciones sobre las sesiones de usuario:

- Se permite un máximo de **tres sesiones concurrentes** por usuario, contadas por navegador.
- Las sesiones se **finalizan automáticamente** tras **15 minutos de inactividad o 4 horas de uso activo**, lo que ayuda a prevenir accesos no autorizados.

Estas políticas de gestión de sesión están diseñadas para reducir la exposición a amenazas internas o externas, alineándose con los principios de mínima exposición y control de sesiones definidos en el Esquema Nacional de Seguridad (ENS).

Para más información sobre la configuración y el comportamiento de las sesiones en la consola del dispositivo, se puede consultar el siguiente enlace:

Sesiones de consola de dispositivos

3.2.3 PROTECCIÓN DE LAS COMUNICACIONES

La **protección de las comunicaciones** tiene como objetivo garantizar la confidencialidad, integridad y disponibilidad de la información en tránsito. En el contexto de Roving Edge Infrastructure, esto implica asegurar los **datos transmitidos a través de la red,** protegiéndolos contra accesos no autorizados e implementando mecanismos capaces de detectar y bloquear posibles intrusiones.

Para lograr este objetivo, es fundamental aplicar controles y herramientas de red que garanticen una **comunicación segura** entre los dispositivos RED y los distintos puntos de acceso, tanto locales como remotos. Asimismo, es necesario configurar los **parámetros de red** siguiendo las mejores prácticas de seguridad, con especial atención a la segmentación, cifrado de tráfico y filtrado de conexiones.

La protección de las comunicaciones internas dentro de la infraestructura Roving Edge también es clave para salvaguardar los datos en tránsito y prevenir accesos no autorizados a sistemas internos. Un componente esencial para lograr este aislamiento y control es el uso de **Virtual Cloud Networks (VCNs),** que constituyen la base para la creación de entornos de red seguros y aislados dentro del ecosistema RED. Para ello es necesario llevar a cabo una serie de acciones clave en la configuración y gestión de los recursos de red:

- **Gestión de Subredes**: La configuración adecuada de subredes es fundamental para definir entornos de red aislados dentro de la Infraestructura Roving Edge, permitiendo la segmentación de recursos y facilitando un control de seguridad más granular. Para más detalle sobre la configuración de subredes en dispositivos Roving Edge se puede consultar la documentación oficial:


Subredes para dispositivos de Roving Edge Infrastructure

- **Enrutamiento**: La correcta configuración de las tablas de *enrutamiento* asegura que el tráfico dentro del dispositivo se dirija de forma segura entre las diferentes subredes y hacia sistemas externos según sea necesario. Para información adicional sobre la gestión de tablas de enrutamiento en una VCN se puede consultar la siguiente entrada:


Trabajar con tablas de rutas y reglas de rutas

- **Listas de Seguridad**: Las Listas de Seguridad (*Security Lists*) desempeñan un papel crucial, funcionando como un firewall virtual a nivel de la interfaz de red virtual (VNIC). Permiten definir reglas de entrada (*ingress*) y salida (*egress*) para permitir o denegar tipos específicos de tráfico, aplicando reglas tanto con estado (*stateful*) como sin estado (*stateless*). Para obtener información más detallada sobre la configuración y el funcionamiento de las listas de seguridad en la protección de la red, se puede consultar el siguiente enlace:


Listas de seguridad

3.2.3.1 PROTECCIÓN DE LA INTEGRIDAD Y LA AUTENTICIDAD

Esta medida requiere verificar la autenticidad de la entidad remota antes de intercambiar cualquier información fuera del dominio de seguridad de la organización.

Aunque los dispositivos Roving Edge Infrastructure están diseñados para operar en modos conectado, semi-conectado y desconectado respecto a la nube de Oracle, la sincronización de datos entre los dispositivos RED y la *tenancy* de Oracle Cloud Infrastructure (OCI) es una tarea esencial para mantener la coherencia y disponibilidad de la información.

Tal y como se menciona en secciones anteriores de la presente guía, la sincronización de datos entre los dispositivos Roving Edge y OCI es una funcionalidad preconfigurada que facilita la transferencia eficiente de datos, soportando una sincronización bidireccional para garantizar una gestión fluida y coherente de la información en ambos entornos.

Las tareas de sincronización de datos se pueden realizar en ambas vías de la siguiente manera:

i) De un *bucket* del dispositivo Roving Edge a un *bucket* en OCI.

ii) De un *bucket* en OCI a un *bucket* del dispositivo Roving Edge.

Para información detallada sobre los requisitos previos, así como instrucciones para la creación, edición y monitorización de tareas de sincronización de datos, se puede consultar el siguiente enlace:


Sincronización de datos de Roving Edge Infrastructure

Los **certificados** en Oracle Roving Edge Infrastructure (RED) garantizan la autenticidad y seguridad de las comunicaciones entre los dispositivos y Oracle Cloud Infrastructure (OCI). Estos certificados son esenciales para autenticar los dispositivos, prevenir accesos no autorizados y asegurar la transferencia segura de datos.

Cada dispositivo RED recibe un certificado digital único, que contiene un par de claves RSA.

Estos certificados son firmados por una **Autoridad Certificadora (CA),** lo que garantiza su confianza y validez. Solo se admiten claves RSA firmadas mediante algoritmos de firma basados en SHA.

Durante la comunicación entre un dispositivo RED y OCI, ambas partes verifican la autenticidad de los certificados respectivos, asegurando así un canal de comunicación seguro y confiable.

Para una guía detallada sobre la configuración y gestión de certificados, se puede consultar el siguiente enlace:

Gestión de certificados

Para la **Gestión de Nodos Roving Edge** en la consola de OCI, el acceso se realiza principalmente a través de Internet. Oracle emplea el protocolo estándar de la industria Transport Layer Security (TLS) para asegurar la comunicación con los servicios en la nube de Oracle.

Las conexiones TLS se establecen utilizando un cifrado mínimo de 128 bits, con claves privadas de al menos 2048 bits para la generación de las claves criptográficas, garantizando así la confidencialidad e integridad de los datos en tránsito.

Además, es posible acceder a los servicios de Oracle Cloud a través de una **VPN** o por medio de **FastConnect** con IPSec para acceder a los servicios de Oracle Cloud.

3.2.4 PROTECCIÓN DE LA INFORMACIÓN

Este conjunto de medidas abarca todo lo relacionado con la **protección de la información**, en cumplimiento con la legislación nacional y la normativa europea vigente. Incluye diversos aspectos fundamentales como la clasificación de la información, los controles de acceso, la responsabilidad en el tratamiento de datos, al almacenamiento seguro y la eliminación o destrucción segura de la información cuando ya no es necesaria.

Estas medidas están diseñadas para garantizar que la información sensible sea gestionada respetando la privacidad, la seguridad y los requisitos legales durante todo su ciclo de vida.

Dado que los dispositivos Roving Edge se utilizan principalmente para la recopilación y procesamiento de datos en el punto de generación, la protección de los datos almacenados en estos dispositivos es de máxima prioridad, especialmente cuando se trata de información sensible o crítica para el objetivo al que están dedicados.

Para asegurar la confidencialidad y seguridad de los **datos almacenados**, el servicio de ***Object Storage*** cifra automáticamente todos los datos en reposo. Este proceso de cifrado es obligatorio y está habilitado por defecto, sin posibilidad de desactivación, ni siquiera mediante API, garantizando que toda la información permanezca protegida cuando se almacena localmente en los dispositivos Roving Edge.

Los dispositivos de almacenamiento *flash* utilizados en Roving Edge Device y Roving Edge Ultra son unidades de borrado seguro instantáneo (*Instant Secure Erase, ISE*). Estos dispositivos funcionan como unidades de cifrado completo de disco (*Full Disk Encryption, FDE*), ya que los datos se cifran mediante una

clave de hardware al escribirlos y se descifran al ser leídos. Cuando se envía el comando de borrado criptográfico (*Crypto Erase*), la clave de cifrado/descifrado se sobrescribe, impidiendo que los datos almacenados puedan ser descifrados.

Los módulos criptográficos TPM empleados en los dispositivos Roving Edge Device y Roving Edge Ultra cuentan con certificación FIPS 140-2, asegurando el cumplimiento de estándares de seguridad reconocidos internacionalmente. Esta información puede ser consultada en el siguiente enlace de la documentación oficial:

Cifrado automático

Adicionalmente, debido a que los dispositivos RED pueden desplegarse en entornos remotos o en escenarios de uso temporal, es fundamental contar con medidas robustas para la **sanitización o saneamiento de datos** cuando los dispositivos son dados de baja o devueltos. En estos casos, Oracle ofrece una funcionalidad de sanitización que garantiza la eliminación permanente y segura de los datos almacenados en el dispositivo, haciendo que sean irrecuperables.

Para obtener más información sobre los procesos de sanitización, se puede consultar el siguiente enlace:

Sanitización de un dispositivo

3.2.5 COPIAS DE SEGURIDAD

El marco del ENS establece la obligatoriedad de implementar procedimientos de copia de seguridad que permitan la recuperación de datos perdidos, ya sea de forma accidental o intencionada, conforme a las políticas internas de la organización. Estos procedimientos deben definir claramente la frecuencia de realización de las copias, los requisitos de almacenamiento tanto local (*on-site*) como en ubicaciones externas (*off-site*), y los controles necesarios para garantizar el acceso autorizado a las copias de respaldo.

Es fundamental que los procedimientos de copia de seguridad sean sometidos a pruebas regulares para verificar su eficacia. La periodicidad de estas pruebas debe establecerse en función de la criticidad de los datos y del impacto potencial de su indisponibilidad. Como requisito mínimo, al menos una copia de seguridad debe almacenarse en una ubicación física distinta a la del original, asegurando que un incidente no afecte simultáneamente a ambos repositorios.

En el entorno de OCI Roving Edge Infrastructure, los procesos de respaldo pueden optimizarse mediante funcionalidades específicas, tales como:

- **Copias de Seguridad de Volúmenes de Bloque (*Block Volumes*)**. OCI ofrece mecanismos automatizados para la gestión de copias de seguridad de volúmenes de bloque, garantizando que los datos críticos almacenados en estos volúmenes se respalden de forma segura y puedan ser restaurados cuando sea necesario. Se pueden realizar snapshots periódicos que se almacenan en *Object Storage*, facilitando una recuperación eficiente y segura.
- **Sincronización de datos para respaldo en la Región OCI**. La funcionalidad de sincronización de datos permite la transferencia segura y fluida de información entre los dispositivos Roving Edge Infrastructure y el almacenamiento en Oracle Cloud Infrastructure, como se mencionó anteriormente. (Ver sección "*2.6.5 Sincronización de Datos*")

- **Soluciones de respaldo para entornos sin conectividad:** En escenarios donde la conectividad directa con la nube no está disponible, resulta esencial implementar una estrategia robusta de respaldo. En lugar de depender únicamente de un dispositivo RED, se recomienda un enfoque redundante mediante el uso de al menos dos dispositivos o una solución alternativa de respaldo local en un dispositivo separado. Esta práctica asegura la protección de datos críticos y su sincronización con Oracle Cloud una vez que se restablezca la conectividad, minimizando así el riesgo de pérdida de información en entornos aislados o remotos.

4. GLOSARIO

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

Término	Definición
AIDE	Advanced Intrusion Detection Environment.
API	Application Programming Interfaces.
ATE	Application Test Environment.
B2B	Business-to-Business.
B2C	Business-to-Consumer.
CA	Certificate Authority
CapEx	Capital Expenditures.
CCN	Centro Criptológico Nacional.
CCN-CERT	Centro Criptológico Nacional – *Computer Emergency Response Team*
CDaaS	Content Delivery as a Service.
CIS	Center for Internet Security.
CLI	Command Line Interface
CPQ	Configure, Price, Quote.
CRM	Customer Relationship Management.
CX	Customer Experience.
DDoS	Distributed Denial of Service.
DISA	Defense Information Systems Agency.
DoS	Denial of Service.
ELSA	Enterprise Linux Security Advisory.
ENS	Esquema Nacional de Seguridad.
EPM	Enterprise Perfomance Management.
ERM	Enterprise Risk Management.
ERP	Enterprise Resource Planning.
EURA	Acceso Restringido a la Unión Europea. European Union Restricted Access
GDS	Global Desktop Strategy.
GIS	Geographical Information System.
HCM	Human Capital Management.
IA	Inteligencia Artificial.
IaaS	Infrastructure as a Service.
IAM	Identity and Access Management.
IBPX	Integrated Business Planning and Execution.
IDCS	Identity Cloud Service.
IDS	Intrusion Detection System.
IEC	International Electrotechnical Commission.
IoT	Internet of Things.
IPS	Intrusion Prevention System.
ISO	International Organization for Standardization.
JRE	Java Runtime Environment.
JSON	JavaScript Object Notation.

Término	Definición
JWT	JSON Web Token.
KPI	Key Perfomance Indicator.
LDAP	Lightweight Directory Access Protocol.
LLDD	Landing Zones
LoB	Line of Business.
MES	Manufacturing Execution System.
Namespace	Domino lógico que permite aislar y organizar los datos almacenados en Object Storage.
NIDS	Network Intrusion Detection System.
NIST	National Institute of Standards and Technology.
OAuth	Open Authorization.
OCI	Oracle Cloud Infrastructure.
OCID	Oracle Cloud Identifier.
OELZ	Oracle Enterprise Landing zone
OFA	Oracle Fusion Applications.
OKE	Oracle Container Engine for Kubernetes.
OKEOM	OKE Oracle-Managed.
OOTB	Out-Of-The-Box.
OpEx	Operating Expenses.
OPSS	Oracle Platform Security Services.
Oracle ME	Oracle My Experience.
OS	Operating System.
OTP	One-Time Password.
OWASP	Open Web Application Security Project.
PaaS	Platform as a Service.
PAM	Pluggable Authentication Module.
PAR	Pre-Authenticated Request.
PCI-DSS	Payment Card Industry Data Security Standard.
PGP	Pretty Good Privacy.
PLM	Product Lifecycle Management.
RBAC	Role based Access control.
RED	Roving Edge Device
RPM	Red Hat Package Manager.
S&OP	Sales and Operations.
SaaS	Software as a Service.
SCIM	System for Cross-domain Identity Management.
SCM	Supply Chain Management.
SFA	Sales Force Automation.
SFC	System File Checker.
SIEM	Security Information and Event Management.
SOC	Security Operations Center.
SQL	Structured Query Language.
SSO	Single Sign-On.

Término	Definición
STIG	Security Technical Implementation Guide.
TLS	Transport Layer Security.
VCN	Virtual Cloud Network.
VM	Virtual Machine
VPN	Virtual Private Network.
WAF	Web Application Firewall.
WSUS	Windows Server Update Service.
XSS	Cross Site Scripting.

5. RESUMEN Y APLICACIÓN DE MEDIDAS

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

Control ENS	Medidas y Configuración	Estado	
OP	MARCO OPERACIONAL		
OP.ACC	CONTROL DE ACCESOS		
op.acc.1	Identificación	Aplica	Cumple
	Se ha configurado el uso de cuentas OCI IAM para la gestión de recursos de la Infraestructura Roving Edge y la gestión de nodos en la Región OCI	☐Si ☐No	☐Si ☐No
		Observaciones:	
op.acc.2	Requisitos de acceso	Aplica	Cumple
	Se han establecido políticas de custodia y rotación periódica de la *passphrase* de acceso a la Consola Serie.	☐Si ☐No	☐Si ☐No
op.acc.2	Requisitos de acceso	Aplica	Cumple

	Se han diseñado reglas de acceso en OCI IAM que limiten acciones por tipo de recurso y asigna sólo los necesarios según el rol del usuario.	☐Si ☐No	☐Si ☐No
		Observaciones:	
op.acc.3	Segregación de funciones y tareas	Aplica	Cumple
	Se han creado los grupos de seguridad basados en roles (RBAC) para los recursos de la Infraestructura Roving Edge y para la propia gestión de los nodos desde la OCI Region.	☐Si ☐No	☐Si ☐No
		Observaciones:	
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 a través del servicio OCI IAM	☐Si ☐No	☐Si ☐No
		Observaciones:	
op.acc.5	Mecanismos de autenticación	Aplica	Cumple
	Se cambian las credenciales con la periodicidad marcada por la política de la organización y de aquellos recursos que acceden a los servicios de la infraestructura de Roving Edge	☐Si ☐No	☐Si ☐No
		Observaciones:	
	Se retiran y deshabilitan las credenciales cuando la entidad (persona, equipo o proceso) que se autentica termina su relación con el sistema de infraesç Edge.	☐Si ☐No	☐Si ☐No
		Observaciones:	

OP.EXP	EXPLOTACIÓN		
op.exp.1	Inventario de Activos	Aplica	Cumple
	Se revisa periódicamente el detalle de nodos de Roving Edge desplegados desde la OCI Region	☐Si ☐No	☐Si ☐No
		Observaciones:	
	Se revisa periódicamente el detalle de los recursos desplegados en la Infraestructura de Roving Edge	☐Si ☐No	☐Si ☐No
		Observaciones:	
op.exp.2	Mantenimiento y Actualizaciones de Seguridad	Aplica	Cumple
	Se han establecido y documentado procedimientos formales para la gestión de parches, actualizaciones y versiones de la Infraestructura Roving Edge	☐Si ☐No	☐Si ☐No
		Observaciones:	
	Se realizan comprobaciones periódicas de la versión del sistema operativo en los dispositivos Roving Edge	☐Si ☐No	☐Si ☐No
		Observaciones:	

	Se registra cada intervención (actualización, reversión, parche) en el sistema de gestión de cambios de la organización.	☐Si ☐No	☐Si ☐No
		Observaciones:	
OP.MON	MONITORIZACIÓN DEL SISTEMA		
op.mon.1	Sistema de métricas	Aplica	Cumple
	Se está realizando un seguimiento del estado de los servicios mediante la supervisión de uso de los recursos, métricas sobre dichos recursos y métricas de facturación.	☐Si ☐No	☐Si ☐No
		Observaciones:	
MP	MEDIDAS DE PROTECCIÓN		

MP.COM	PROTECCIÓN DE LAS COMUNICACIONES		
mp.com.1	Protección de las comunicaciones	Aplica	Cumple
	Se han diseñado y configurado subredes aisladas para segmentar la red dentro de la Infraestructura Roving Edge Se aplican tablas de enrutamiento para controlar el tráfico interno y externo Se implementan listas de seguridad para filtrar tráfico entrante y saliente en la Infraestructura RED.	☐Si ☐No	☐Si ☐No
		Observaciones:	
mp.com.2	Protección de la integridad y de la autenticidad	Aplica	Cumple
	Se utilizan certificados digitales únicos por dispositivo, firmados por una Autoridad Certificadora (CA)	☐Si ☐No	☐Si ☐No
		Observaciones:	
MP.INFO	PROTECCIÓN DE LA INFORMACIÓN		
mp.info.1	Sanitización	Aplica	Cumple
	Se han definido procedimientos para la sanitización de dispositivos RED antes de su devolución o baja operativa	☐Si ☐No	☐Si ☐No
		Observaciones:	

mp.info.2	Copias de seguridad	Aplica	Cumple
	Se han definido políticas de backup que incluyen frecuencia, retención y ubicación (local y externa) de las copias, estableciendo controles de acceso a las copias de seguridad por personal autorizdo	☐Si ☐No	☐Si ☐No
		Observaciones:	


CCN
centro criptológico nacional