



# Unidad de distribución de alimentación para rack de Vertiv™ PowerIT

## Guía de uso e instalación

Serie M y serie D actualizables y no actualizables (equipadas con el firmware 6.x.x)

La información contenida en este documento está sujeta a cambios sin previo aviso y puede no ser adecuada para todas las aplicaciones. Si bien se han tomado todas las precauciones para garantizar la exactitud e integridad de la información incluida en el presente documento, Vertiv no asume ninguna responsabilidad y rechaza toda responsabilidad legal por los daños y perjuicios resultantes del uso de esta información o por cualquier error u omisión cometidos.

Consulte los códigos de edificación y los reglamentos locales en relación con la aplicación, la instalación y el funcionamiento de este producto. El ingeniero de consulta, el instalador o el usuario final son responsables de cumplir con todas las leyes y todos los reglamentos aplicables en cuanto a la aplicación, la instalación y el funcionamiento de este producto.

Vertiv es la empresa que fabrica o vende los productos incluidos en este manual de instrucciones. Este documento es propiedad de Vertiv y contiene información confidencial y patentada perteneciente a Vertiv. Queda terminantemente prohibido copiar, usar o divulgar tal información de cualquier modo sin el permiso por escrito de Vertiv.

Los nombres de las empresas y los productos son marcas comerciales o marcas registradas de sus respectivos propietarios. Toda pregunta relacionada con el uso de los nombres de marca registrada debe dirigirse al fabricante original.

### **Sitio de soporte técnico**

Si encuentra algún problema durante la instalación o el funcionamiento de su producto, consulte la sección pertinente del manual para ver si el problema se puede resolver siguiendo los procedimientos descritos.

Visite <https://www.vertiv.com/en-us/support/> para obtener ayuda adicional.

# ÍNDICE

<b>1 Instrucciones de seguridad importantes</b>	<b>1</b>
<b>2 Información general</b>	<b>3</b>
2.1 Condiciones ambientales	3
2.2 Sistema eléctrico	4
2.3 Red	4
2.3.1 Ethernet	4
2.3.2 Protocolos	4
2.3.3 Interfaces de usuario	5
<b>3 Instalación</b>	<b>7</b>
3.1 Montaje	8
3.2 Conexión de alimentación	20
3.2.1 Funcionamiento de U-Lock	20
3.2.2 Funcionamiento de P-Lock	22
<b>4 Prácticas de seguridad recomendadas</b>	<b>23</b>
4.1 Evaluación de riesgos	25
4.2 Seguridad física	25
4.3 Acceso a la cuenta	26
<b>5 Instalación</b>	<b>27</b>
5.1 Dispositivo de monitorización intercambiable	27
5.1.1 Básico	27
5.1.2 Medido	27
5.1.3 Unidad supervisada	28
5.1.4 Nivel de unidad y de salida conmutada y supervisada	30
5.1.5 Monitorizadas y conmutadas (IMD-5M)	32
5.1.6 Protocolo de árbol de expansión rápido (RSTP)	38
5.2 Configuración de red	41
5.3 Interfaz de usuario basada en web	45
5.3.1 Menú principal	45
5.4 Submenú Device	47
5.4.1 Información general	47
5.4.2 Alarmas y advertencias	55
5.4.3 Logging	60
5.4.4 CO2 Data	62
5.5 Submenú Provisioner	63
5.5.1 Discovery	64
5.5.2 File management	65
5.6 Submenú System	66

5.6.1 Users .....	66
5.6.2 Network .....	70
5.6.3 Web server .....	80
5.6.4 Remote Authentication .....	81
5.6.5 Time .....	88
5.6.6 SSH .....	88
5.6.7 USB .....	89
5.6.8 Serial Port .....	90
5.6.9 Email .....	90
5.6.10 SNMP .....	92
5.6.11 Modbus .....	94
5.6.12 SYSLOG .....	95
5.6.13 Admin .....	95
5.6.14 Locale .....	95
5.7 Submenú Utilities .....	95
5.7.1 Configuration Backup and Restore .....	96
5.7.2 Restore Defaults .....	97
5.7.3 Reboot .....	98
5.7.4 Reboot I/O Boards .....	99
5.7.5 Actualizaciones del firmware .....	100
5.7.6 Factory Access .....	101
5.8 Submenú Help .....	102
<b>6 Vertiv™ Intelligence Director .....</b>	<b>105</b>
6.1 Agregación .....	105
6.2 Administrador de matriz .....	107
6.3 Configuración de red .....	108
6.4 Vistas .....	111
6.4.1 Summary .....	112
6.4.2 Groups .....	114
6.4.3 List .....	116
6.4.4 Group Configuration .....	119
6.5 Interfaces .....	120
6.5.1 Datos SNMP del grupo .....	121
6.5.2 Consejos y resolución de problemas .....	121
<b>Apéndices .....</b>	<b>123</b>
Apéndice A: Asistencia técnica .....	123
Apéndice B: Sensores disponibles .....	127
Apéndice C: Adaptadores USB inalámbricos TP-Link .....	128
Apéndice D: LED de salida .....	130
Apéndice E: Códigos de pantalla del IMD .....	131

Apéndice F: Aprovevisionador: formato del archivo de ajustes de configuración .....	133
Apéndice G: Códigos de error API / CLI .....	153
Apéndice H: Un ejemplo de configuración de LDAP para las credenciales de Active Directory .....	157

Esta página se ha dejado en blanco intencionadamente.

# 1 Instrucciones de seguridad importantes

## Cumplimiento normativo

Los productos de Vertiv están regulados en cuanto a seguridad, emisiones e impacto medioambiental conforme a los siguientes organismos y políticas.

### Underwriters Laboratories (UL)

Las normas UL se utilizan para evaluar productos, probar componentes, materiales, sistemas y rendimiento, y evaluar productos con sostenibilidad medioambiental, energías renovables, productos alimentarios y de agua, sistemas de reciclaje y otras tecnologías innovadoras.

Las normas UL específicas de este equipo son las que se indican en la placa de identificación del dispositivo.

### CE

Si un producto incluye la marca CE, significa que dicho producto cumple con los requisitos europeos (UE) aplicables en cuanto a salud, seguridad y protección del medio ambiente, incluidas la legislación y las directivas sobre productos de la UE. La marca CE es necesaria para los productos que se ponen a la venta en el Espacio Económico Europeo (EEE).

Los reglamentos, directivas y normas específicas aplicables a cada producto se especifican en la declaración de conformidad.

### Comisión Federal de Comunicaciones (FCC, por sus siglas en inglés)

La Comisión Federal de Comunicaciones (FCC) regula las comunicaciones interestatales e internacionales por radio, televisión, alámbricas, satélite y cable en los 50 estados, el Distrito de Columbia y los territorios de los Estados Unidos. La FCC, organismo gubernamental estadounidense independiente y supervisado por el Congreso, es la principal autoridad de Estados Unidos en materia de leyes y reglamentos de comunicación, e innovación tecnológica.

Las normas de la FCC específicas para este equipo son:

- Este dispositivo de Clase A cumple con la sección 15 de las normas de la FCC.
- Su funcionamiento está sujeto a las dos condiciones siguientes:
  - Este dispositivo no debe causar interferencias perjudiciales.
  - Este dispositivo debe aceptar cualquier interferencia recibida, incluidas las interferencias que puedan provocar un funcionamiento no deseado.
- Este aparato digital de Clase A cumple con la normativa canadiense ICES-003.
- Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.



**¡ADVERTENCIA! Los cambios o modificaciones en esta unidad que no estén expresamente aprobados por la parte responsable del cumplimiento pueden anular la autorización del usuario para usar este equipo.**

**NOTA:** Visite <http://www.Vertiv.com/ComplianceRegulatoryInfo> para obtener información sobre seguridad importante antes de la instalación.

Esta página se ha dejado en blanco intencionadamente.

## 2 Información general

La unidad de distribución de alimentación para rack de Vertiv™ PowerIT (rPDU) ofrece a los administradores del centro de datos la flexibilidad necesaria para instalar la inteligencia que se exige hoy en día. Desde la alimentación básica hasta la supervisión de la alimentación o la conmutación de salidas, la línea de productos rPDU de Vertiv™ PowerIT se adapta a las necesidades de las empresas ahora y en el futuro.

Para establecer esta trayectoria de actualización, los ingenieros de Vertiv tomaron como punto de partida el sólido diseño de la rPDU de Vertiv™ PowerIT e incorporaron un dispositivo de supervisión intercambiable (IMD). Las PDU duran muchos años y, con el diseño del IMD, las empresas pueden actualizar sus PDU a nuevas tecnologías de supervisión en el futuro sin tener que reemplazar toda la rPDU de Vertiv™ PowerIT. En unos pocos pasos sencillos, el IMD se puede intercambiar en caliente sin interrumpir la alimentación de los servidores críticos.

### 2.1 Condiciones ambientales

Los límites del entorno operativo relativos a temperatura, humedad y elevación son los que se definen en las siguientes tablas.

**Tabla 2.1 Límites de temperatura**

Descripción	Mínimo	Máximo
En funcionamiento	0 °C (32 °F)	60 °C (140 °F)
Almacenamiento	-40 °C (-40 °F)	70 °C (158 °F)

**Tabla 2.2 Límites de humedad**

Descripción	Mínimo	Máximo
En funcionamiento	5%	95% (sin condensación)
Almacenamiento	5%	95% (sin condensación)

**Tabla 2.3 Límites de elevación**

Descripción	Mínimo	Máximo
En funcionamiento	0 m (0 ft)	3050 m (10000 ft)
Almacenamiento	0 m (0 ft)	15240 m (50000 ft)

## 2.2 Sistema eléctrico

Las características y el rendimiento de los productos eléctricos se definen en la **Tabla 2.4** abajo. Consulte también la placa de identificación del producto para ver los límites de clasificación adicionales.

**Tabla 2.4 Clasificaciones del receptáculo**

Tipo	Clasificaciones
Combinación C13/C19	250 VCA, 16 A (UL y CSA 16 A, 250 VCA) con cable C20 250 VCA, 10 A (UL y CSA 12 A, 250 VCA) con cable C14
Schuko alemán	250 VCA, 16 A
IEC-60320 C13	250 VCA, 10 A (UL y CSA 12 A, 250 VCA)
IEC-60320 C19	250 VCA, 16 A (UL y CSA 16 A, 250 VCA)
IEC309 PS6	230 VCA, 16 A
IEC309 PS56	230/400 VCA, 32 A
NEMA 5-15R o L5-15R	125 VCA, 12 A
NEMA 6-15R o L6-15R	250 VCA, 12 A
NEMA 5-20R o L5-20R	125 VCA, 16 A
NEMA 6-20R o L6-20R	250 VCA, 16 A
NEMA L5-30R	125 VCA, 24 A
NEMA L6-30R	250 VCA, 24 A
NEMA L7-15R	277 VCA, 12 A
NEMA L7-20R	277 VCA, 16 A
Saf-D-Grid	277 VCA, 16 A
Bloqueo U-Lock IEC-60320 C13	250 VCA, 10 A (UL y CSA 12 A, 250 VCA)
Bloqueo U-Lock IEC-60320 C19	250 VCA, 16 A (UL y CSA 16 A, 250 VCA)
United Kingdom BS1363	250 VCA, 13 A

## 2.3 Red

Los requisitos de comunicación del producto se definen en las siguientes secciones.

### 2.3.1 Ethernet

La velocidad del vínculo Ethernet para este producto es: 10/100/1000 Mb; dúplex completo.

### 2.3.2 Protocolos

Entre los protocolos de comunicaciones que admite este producto se incluyen: ARP, IPv4, IPv6, ICMP, ICMPv6, NDP, TCP, UDP, RSTP, STP, DNS, HTTP, HTTPS (TLSv1.3), SMTP, SMTPS, Modbus TCP/IP, DHCP, SNMP (V1/V2c/V3), LDAP, TACACS+, RADIUS, NTP, SSH, RS232 y Syslog.

### **2.3.3 Interfaces de usuario**

Este producto es compatible con las siguientes interfaces de usuario: SNMP, JSON-based Web GUI, JSON API e interfaz de línea de comandos que utilice SSH o serie (RS232).

Esta página se ha dejado en blanco intencionadamente.

## 3 Instalación

Haga uso de las imágenes de la sección de [Montaje](#) en la página siguiente, para instalar la rPDU de Vertiv™ PowerIT.

**NOTA:** Visite <http://www.Vertiv.com/ComplianceRegulatoryInfo> para obtener información sobre seguridad importante antes de la instalación.

### Para instalar la unidad:

1. Lleve todo el equipo de protección individual (EPI) pertinente. Considere la posibilidad de usar dos personas cuando levante e instale unidades más pesadas.
2. Para unidades horizontales, una los soportes de montaje con la tornillería suministrada y ajuste los sujetadores a 7 in/lb. Para unidades verticales, instale los botones de montaje sin herramientas suministrados en la parte trasera de la unidad y ajuste los sujetadores a 13,5 in/lb. Use la tornillería adecuada para acoplar la unidad al rack. Cuando corresponda, la instalación del equipo en un rack debe hacerse de forma que no peligre el aporte del caudal de aire necesario para el buen funcionamiento del equipo y los orificios de ventilación no queden obstruidos.
3. Conecte la rPDU de Vertiv™ PowerIT a un receptáculo de circuito derivado correctamente clasificado y protegido.



**PRECAUCIÓN:** Riesgo de que un objeto extraño caiga dentro de la carcasa de la rPDU. Se pueden producir daños en el equipo. Cuando se accede al compartimento de cableado durante la instalación para asegurarse de que ningún objeto extraño, como impurezas cae dentro del cuerpo de la rPDU. Si caen objetos extraños dentro de la rPDU durante la instalación y no se pueden extraer, **NO ACTIVE** la rPDU. Devuelva la rPDU a Vertiv para que la reparen.

Para unidades en estrella trifásicas, siempre verifique que haya una conexión neutral adecuada en el receptáculo de circuito derivado de instalación del edificio en el caso de unidades con cable o en el terminal de cableado de entrada de las unidades con cableado local. Una condición neutral abierta puede causar daños tanto a la rPDU como a cualquier equipo conectado.

4. Enchufe los dispositivos que van a recibir alimentación de la rPDU de Vertiv™ PowerIT.
5. Encienda cada dispositivo conectado a la rPDU de Vertiv™ PowerIT.

**NOTA:** Se recomienda el encendido secuencial para evitar una entrada de corriente alta.

## 3.1 Montaje

Se venden por separado soportes opcionales.

Figura 3.1 Soportes de longitud completa

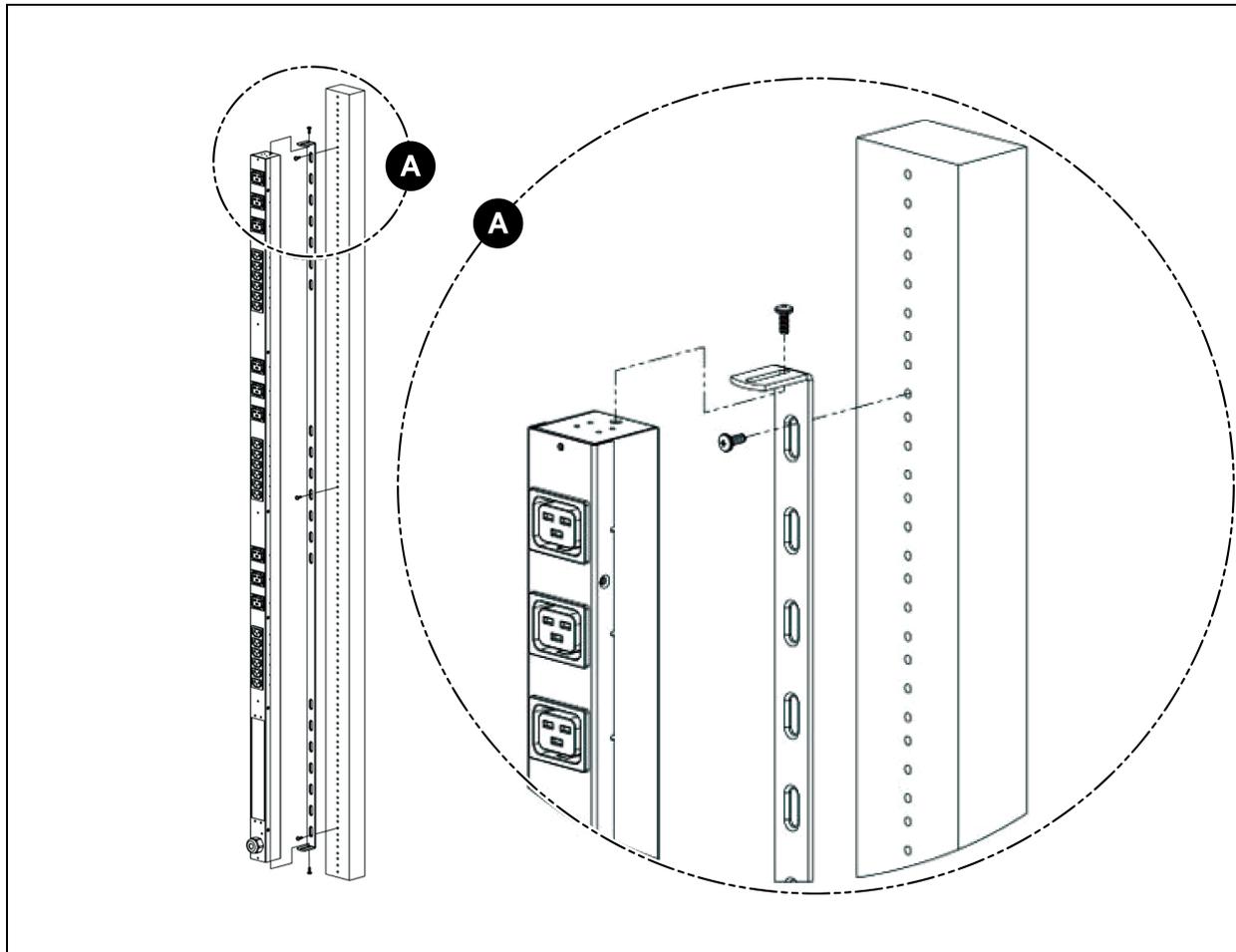


Figura 3.2 Soportes pequeños en L

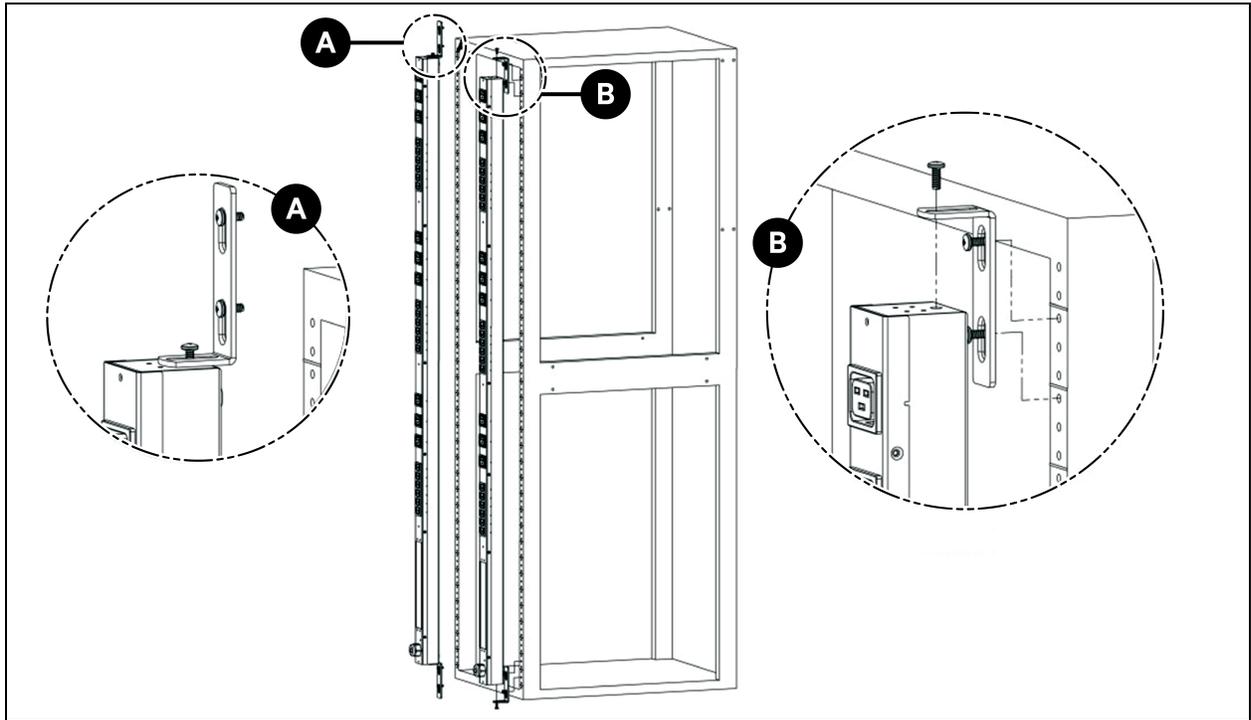
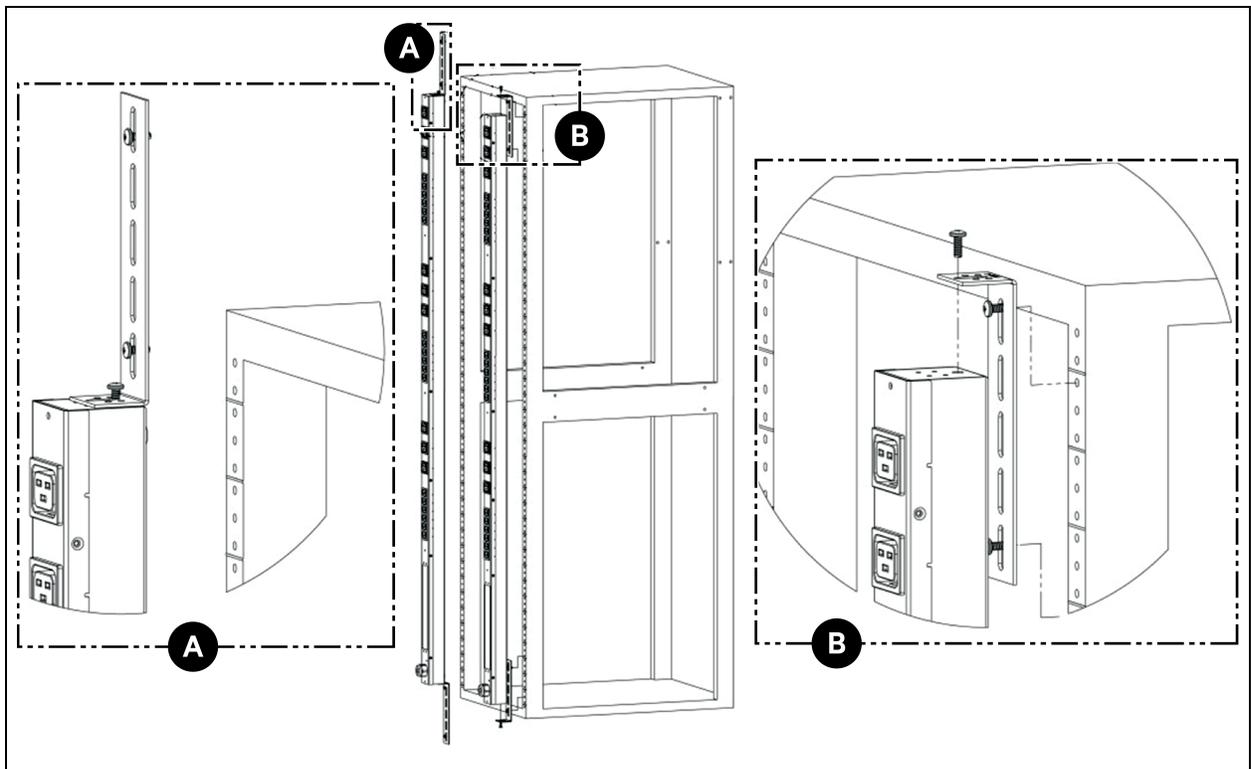


Figura 3.3 Soportes de extensión vertical



**Figura 3.4 Tornillería de montaje sin herramientas**

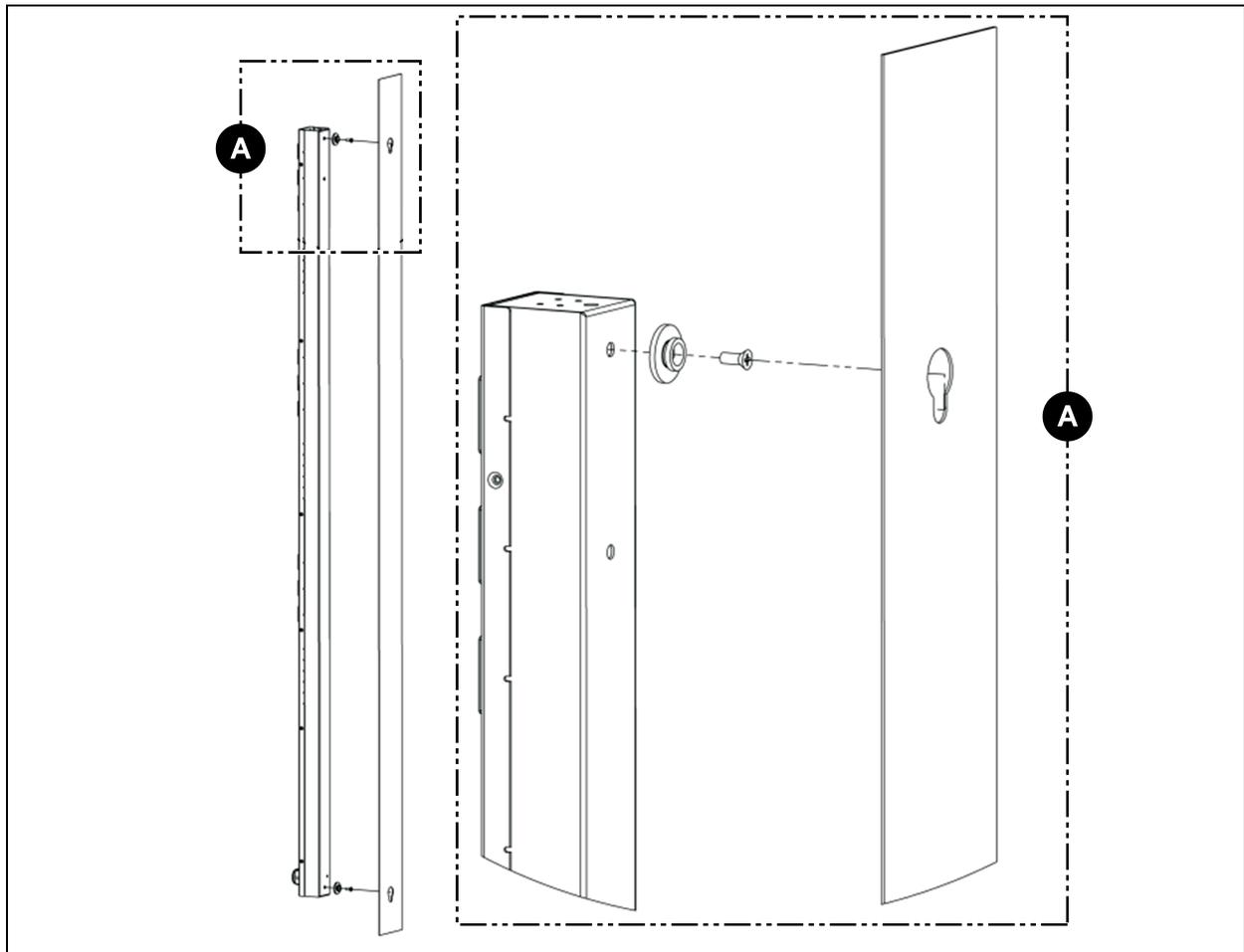
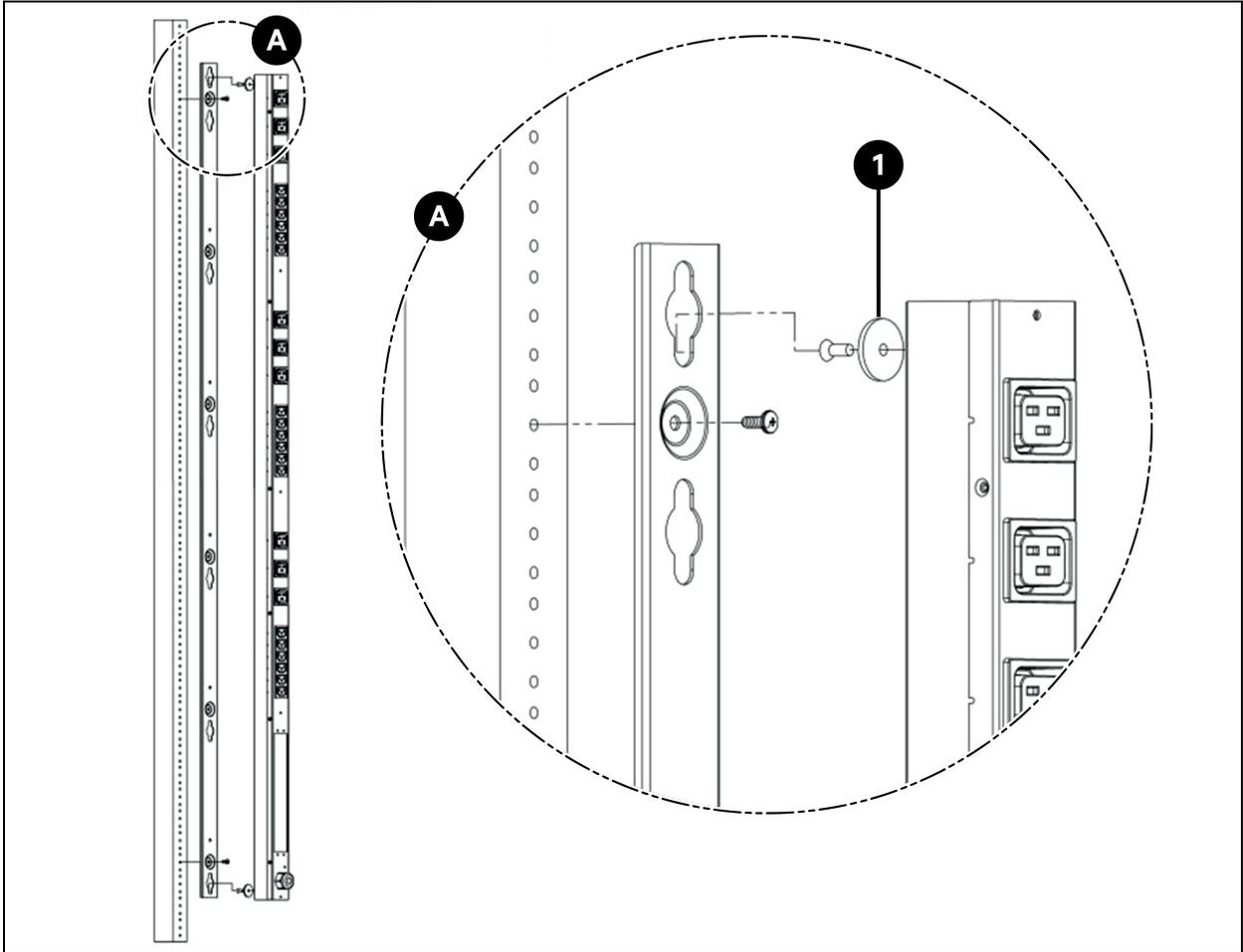


Figura 3.5 Soportes de longitud completa sin herramientas



Elemento	Descripción
1	Arandela de soporte de montaje sin herramientas

Figura 3.6 Soportes individuales de montaje lateral, dos unidades

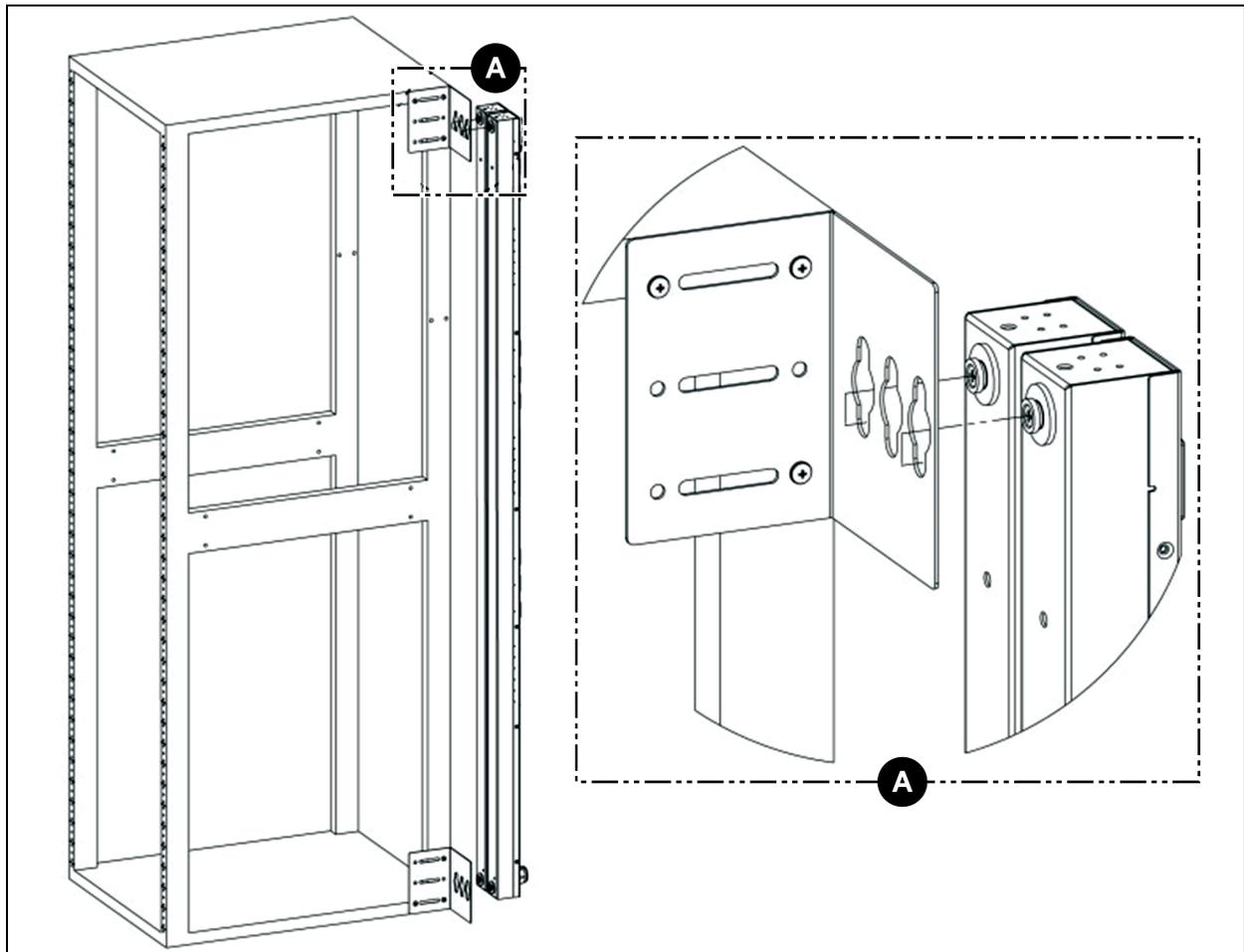
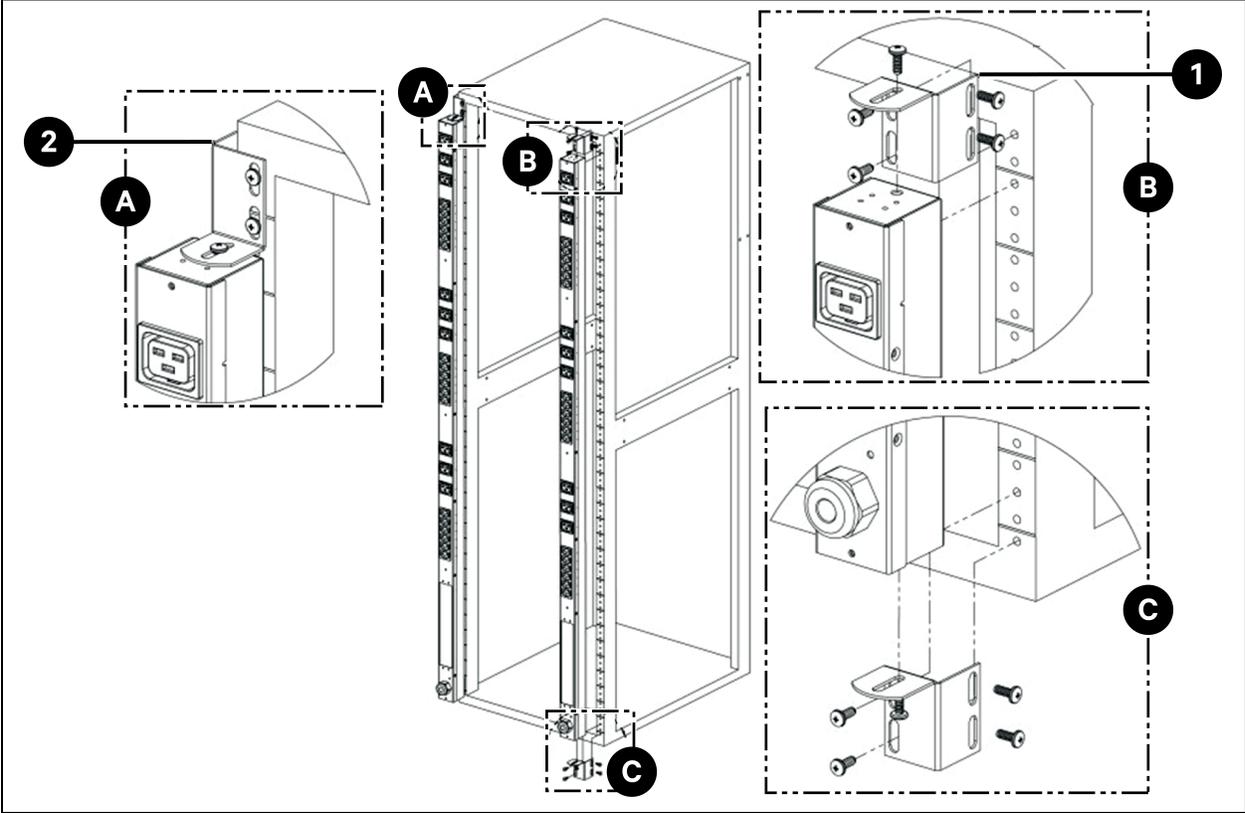


Figura 3.7 Soportes de desplazamiento/montaje lateral



Elemento	Descripción
1	Opción de lado derecho
2	Opción de lado izquierdo

Figura 3.8 Soportes de extensión de 7" (pulgadas)

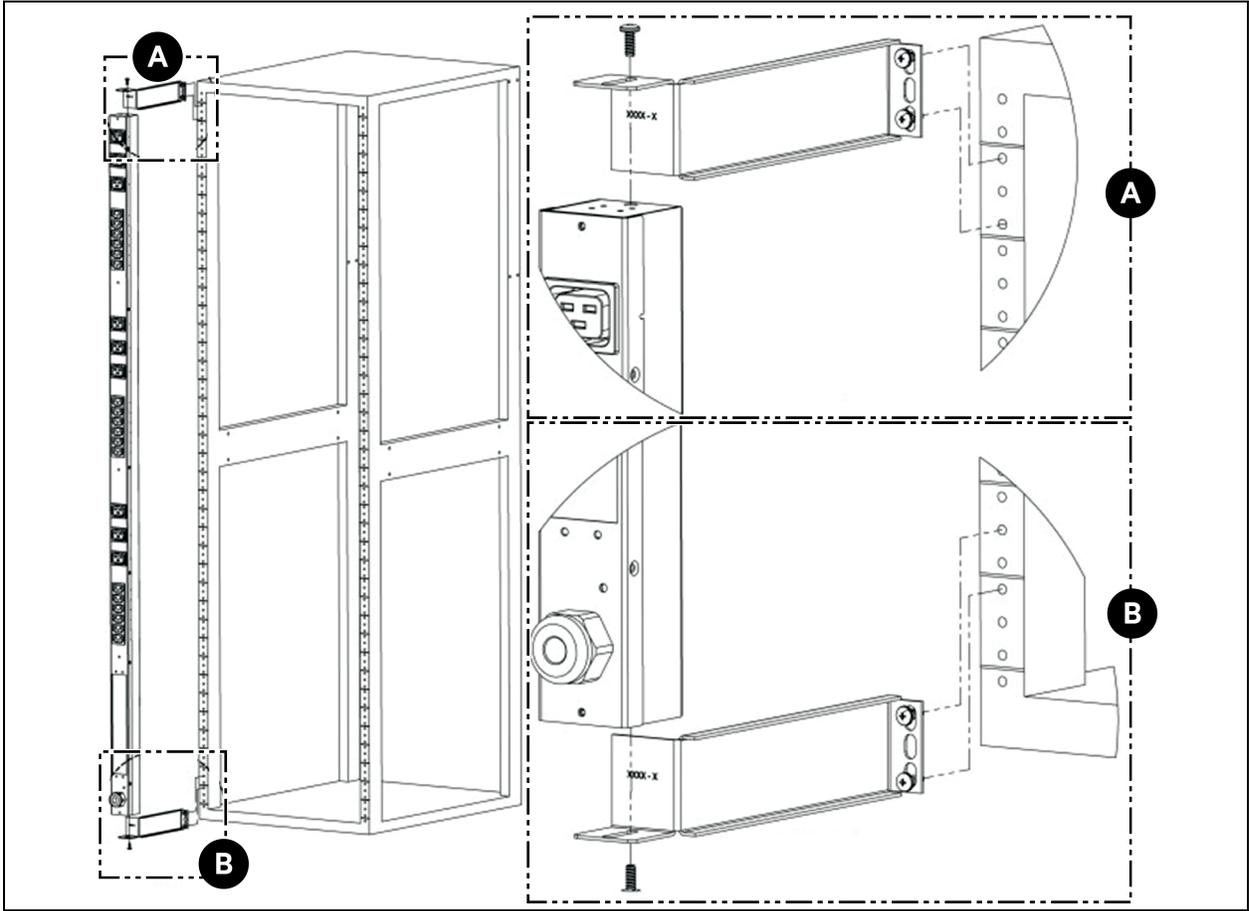


Figura 3.9 Soporte de montaje empotrado

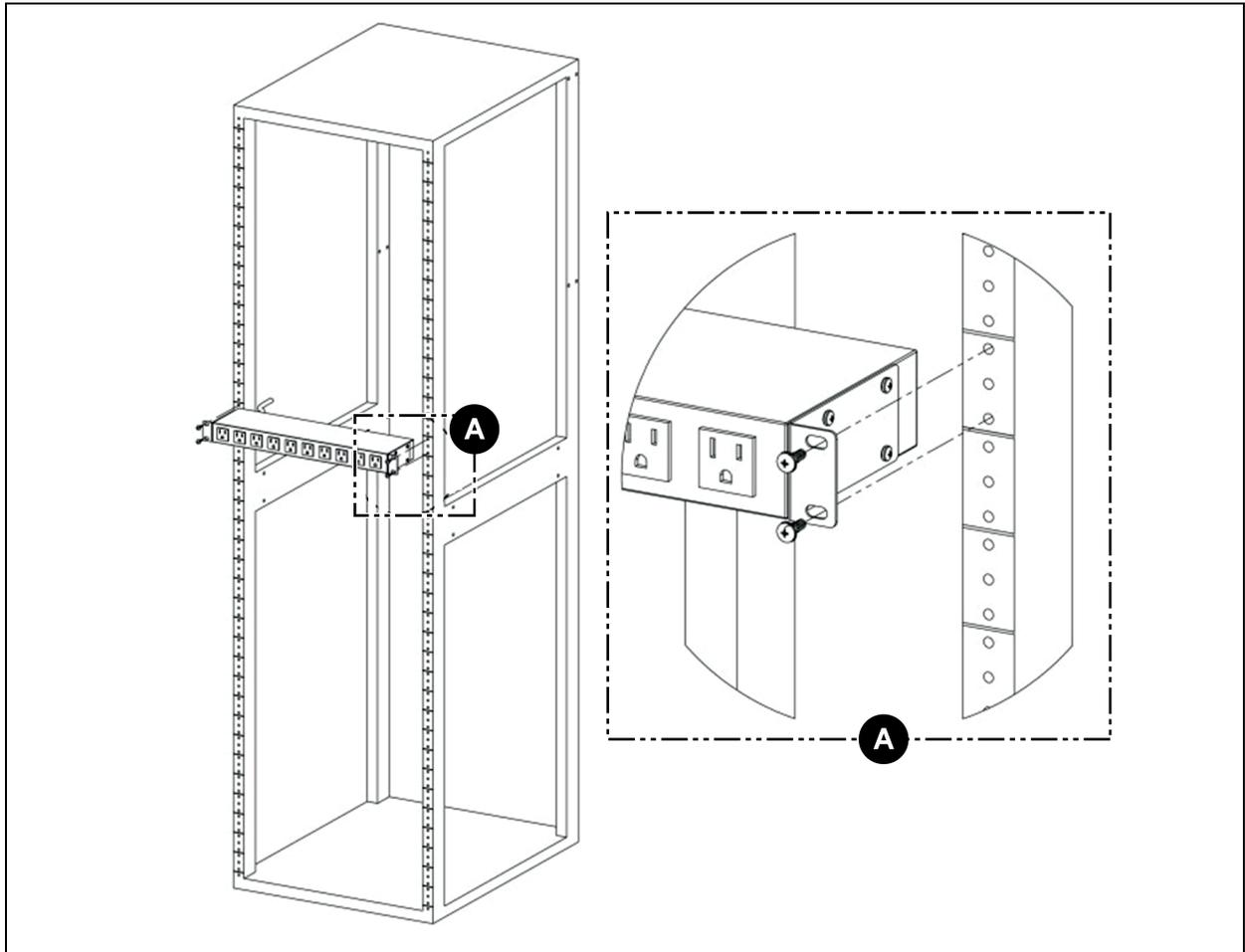


Figura 3.10 Soporte de montaje ajustable

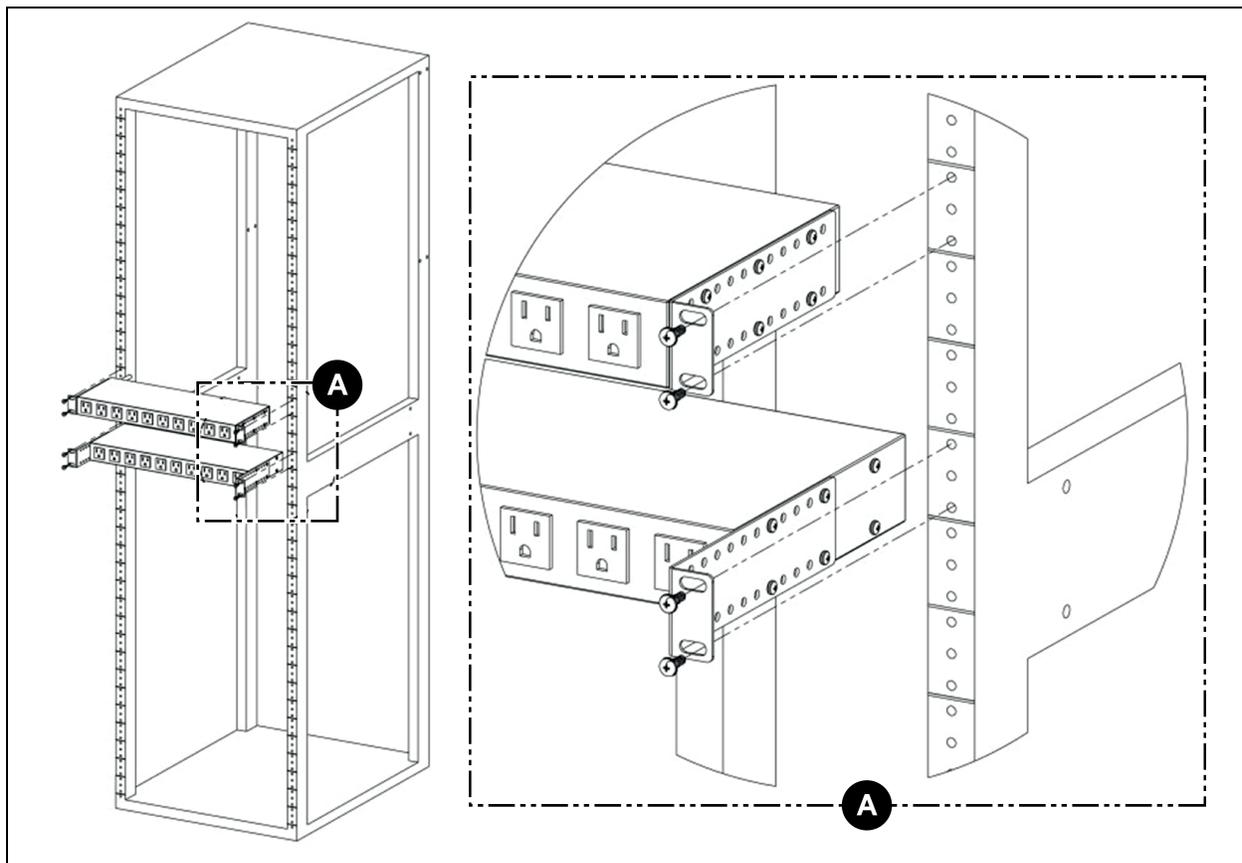


Figura 3.11 Soporte de montaje en panel

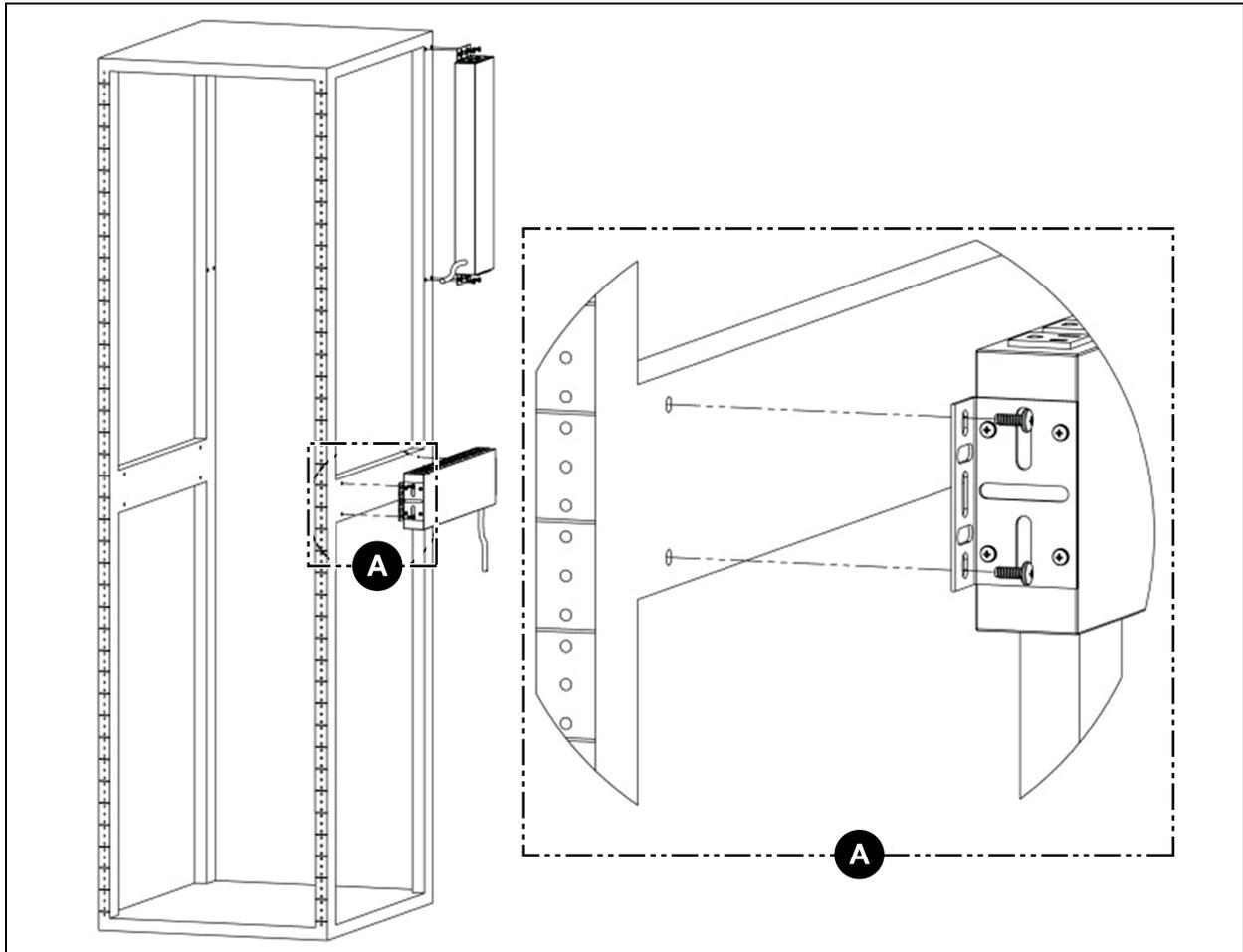


Figura 3.12 Soportes de montaje de conversión de 23" (pulgadas)

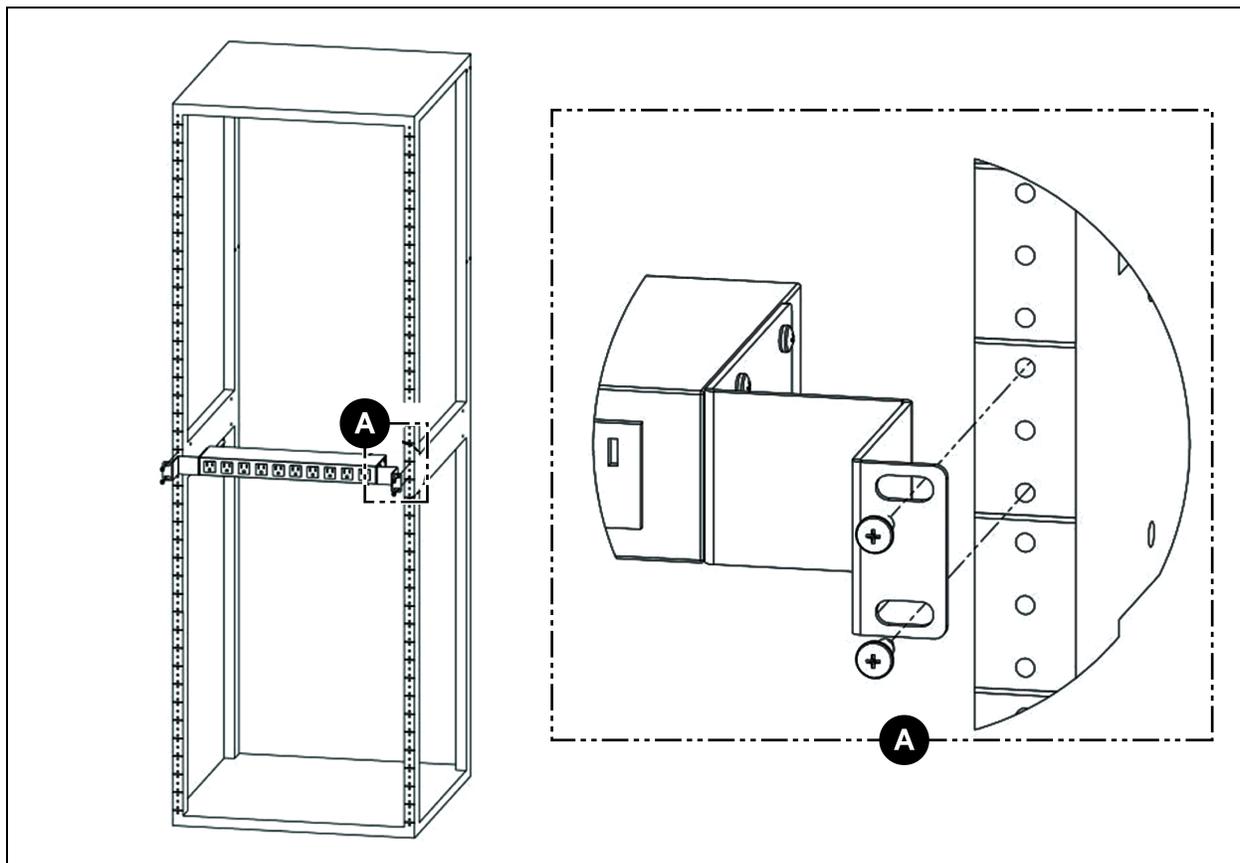
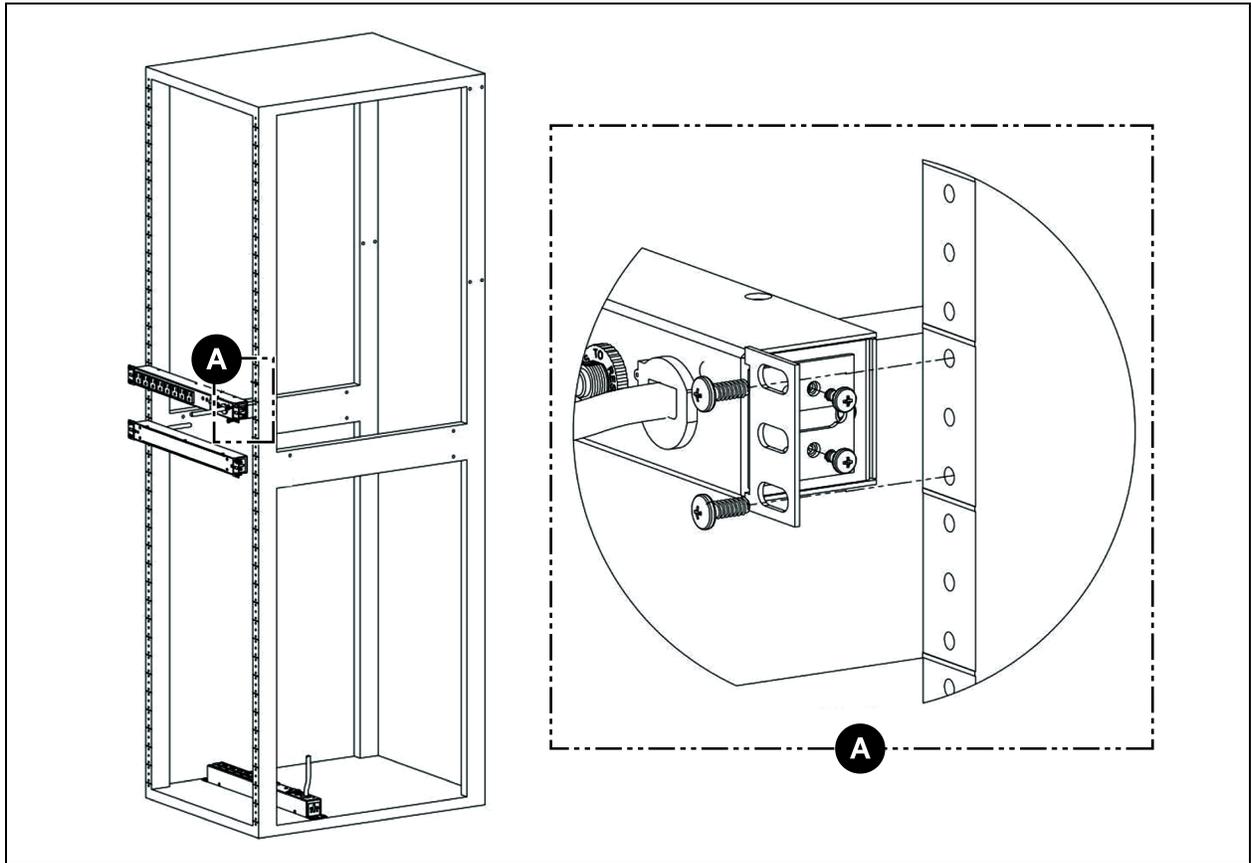
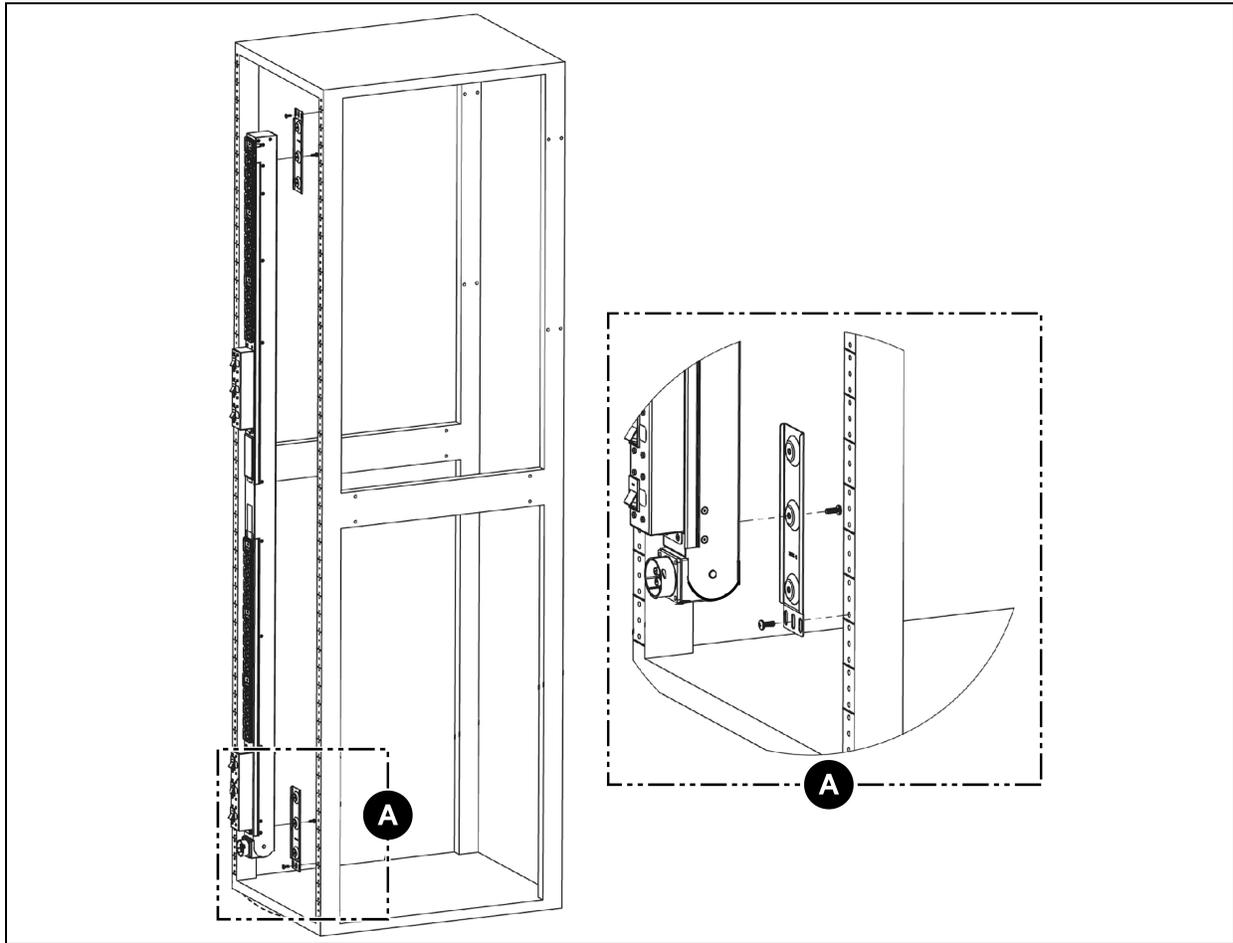


Figura 3.13 Soportes de montaje horizontal/en panel de 19" (pulgadas)



**Figura 3.14 Soportes de montaje para la unidad de distribución de alimentación universal (UPDU) Vertiv™ PowerIT con extremo giratorio**



## 3.2 Conexión de alimentación

Conecte la rPDU de Vertiv™ PowerIT a un receptáculo de circuito derivado correctamente clasificado y protegido. Asegúrese de que el cable de alimentación no supere el radio de curvatura del fabricante (8X).

### 3.2.1 Funcionamiento de U-Lock

Enchufe los dispositivos que van a recibir alimentación de la rPDU de Vertiv™ PowerIT.

- Retención del cable de alimentación U-Lock patentado por Vertiv.
- Utiliza cables de alimentación estándar.
- Al insertar el cable, se activa el sistema de bloqueo.
- El bisel es fácil de desbloquear con solo mantenerlo pulsado.

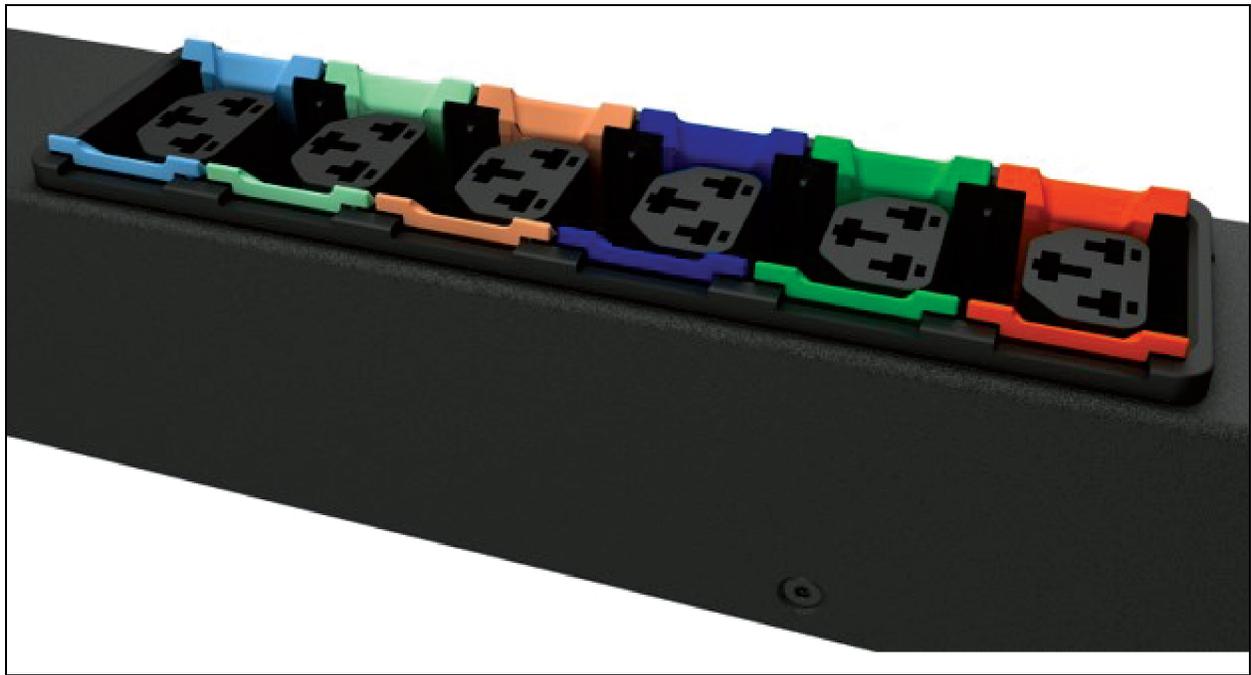
Figura 3.15 Funcionamiento de la retención del cable U-Lock



### 3.2.2 Funcionamiento de P-Lock

- Enchufe los dispositivos que van a recibir alimentación de la rPDU de Vertiv™ PowerIT.
- Vertiv™ Salida combinada C13/C19 con retención de cable de alimentación P-Lock.
- Compatible con cables de alimentación P-Lock.
- Mantenga presionadas las lengüetas del cable P-Lock para liberarlo de la salida.

Figura 3.16 Funcionamiento de la retención del cable P-Lock



## 4 Prácticas de seguridad recomendadas

Los ajustes predeterminados del soporte de la tarjeta se establecen en la configuración más segura para la implementación. A fin de que el equipo de infraestructura crítica cuente con la seguridad adecuada, es necesario configurar correctamente TODOS los servicios de comunicación. En esta sección se resumen los ajustes.

Vertiv se compromete a minimizar los riesgos de ciberseguridad en nuestros productos a través del ciclo de vida de nuestro producto Vertiv SECURE; para ello, implementa prácticas de ciberseguridad recomendadas en todo nuestro diseño de ingeniería de productos y soluciones, que los hace más seguros, fiables y competitivos de cara a nuestros clientes.

Véanse a continuación algunas recomendaciones sobre el ciclo de vida de la ciberseguridad. Las recomendaciones sobre ciberseguridad no tienen como objetivo proporcionar una guía completa sobre ciberseguridad, sino complementar los programas sobre ciberseguridad para clientes existentes. Véanse a continuación varios sitios disponibles, donde podrá obtener más información sobre prácticas recomendadas generales sobre ciberseguridad:

<https://www.cisa.gov/topics/cybersecurity-best-practices>

<https://www.vertiv.com/en-us/support/security-support-center/>

En la **Tabla 4.1** abajo se incluye una lista de los términos que hay que revisar. Cada uno de ellos debería revisarse y configurarse en función de las necesidades operativas que exige la gestión del equipo, y verificar que los ajustes proporcionen la funcionalidad operativa deseada sin añadir un acceso innecesario o no autorizado al equipo de infraestructura crítica. En la sección correspondiente de este documento, se incluye una referencia para configurar cada uno de ellos.

**Tabla 4.1 Ajustes que es necesario revisar y verificar para reducir el riesgo de acceso no autorizado**

Elemento	Descripción	Referencia
Cuentas y contraseñas	Cambie de inmediato los nombres del administrador y el usuario de la cuenta, y las contraseñas para eliminar el acceso mediante credenciales predeterminadas.	Consulte <a href="#">Users</a> en la página 66.
Acceso a red IP	Habilite/deshabilite el acceso a la red IPV4 y IPV6 de la tarjeta. Está deshabilitado cuando no se usa.	Consulte <a href="#">Network</a> en la página 70 .
Acceso SSHv2	Habilite/deshabilite el acceso SSHv2 para facilitar el diagnóstico y la configuración. Está deshabilitado cuando no se usa.	Consulte <a href="#">SSH</a> en la página 88.
Protocolo de servicio web	Seleccione HTTPS para usar el cifrado SSL cuando acceda a los datos a través de la interfaz de usuario basada en web.	Consulte <a href="#">Web server</a> en la página 80.
Certificados TLS	Cuando use HTTPS, instale sus propios certificados TLS desde una autoridad de certificación de confianza o genere certificados autofirmados alternativos.	Consulte <a href="#">SSL Certificate</a> : le permite cargar su propio archivo de certificado SSL firmado para reemplazar el predeterminado. El certificado puede estar autofirmado o firmado por una autoridad de certificación. El

**Tabla 4.1 Ajustes que es necesario revisar y verificar para reducir el riesgo de acceso no autorizado (continuación)**

Elemento	Descripción	Referencia
		<a href="#">certificado SSL debe tener formato PEM o PFX (PKCS12)</a> , en la página 81.
Acceso web de escritura remoto	<p>Para controlar/escribir a través de una interfaz de web, debe iniciar sesión de manera remota y tener una cuenta de usuario de nivel admin o control.</p> <p>Para prohibir el acceso remoto, deshabilite el HTTP y el HTTPS.</p>  <p><b>¡ADVERTENCIA! Al deshabilitar HTTP y HTTPS se finalizará de inmediato esta conexión y el acceso remoto solo estará disponible mediante SSH.</b></p>	Consulte <a href="#">Web server</a> en la página 80.
Protocolos de comunicación	Habilite/deshabilite el SNMP: deshabilite los protocolos no utilizados.	Consulte <a href="#">Modbus</a> en la página 94.
Ajustes de la versión SNMP	Habilite/deshabilite las versiones SNMP, considere la posibilidad de usar SNMPv3 con autenticación de usuario y cifrado.	Consulte <a href="#">SNMP</a> en la página 92.
Ajustes de la tabla de acceso SNMP	En cada entrada de la tabla de acceso SNMPv1/v2c, configure la opción SNMP Access Type a Read-Only para impedir que los hosts identificados en la entrada de la tabla efectúen cambios en el dispositivo.	Consulte <a href="#">SNMP</a> en la página 92.
Cadenas de comunidad SNMP	Use valores adecuados y sólidos para la comunicación SNMP en línea con la política de contraseñas de su organización.	Consulte <a href="#">SNMP</a> en la página 92.
Ajustes del SNMPv3	Use algoritmos hash y de cifrado adecuados para los ajustes de autenticación y privacidad del SNMPv3 para que las comunicaciones del SNMPv3 sean más seguras.	Consulte <a href="#">SNMP</a> en la página 92.
Cuenta de usuario invitado	Esta cuenta debe permanecer deshabilitada, salvo que sea necesaria, ya que proporciona acceso de solo lectura al dispositivo y puede facilitar contexto adicional para los parámetros del dispositivo si está habilitada.	Consulte <a href="#">Users</a> en la página 66.

Para una mayor seguridad, es posible restringir el firewall de red local y la puerta de enlace para que permitan solo el tráfico necesario en los puertos de red requeridos. Los puertos utilizados por la tarjeta MRIC-RP se enumeran en la tabla siguiente. El administrador puede cambiar algunos de los ajustes del puerto.

**Tabla 4.2 Puertos usados por la tarjeta MRIC-RP (v6.1 o posteriores)**

Servicio de red	Puerto utilizado	Predeterminado	Modificación necesaria
HTTP	TCP80	N	S
HTTPS	TCP443	S	S
DNS	TCP&UDP 53	S	N
NTP	TCP&UDP 123	S	N
SMTP	TCP25	S	S
SSH	TCP UDP 22	S	N

**Tabla 4.2 Puertos usados por la tarjeta MRIC-RP (v6.1 o posteriores) (continuación)**

Servicio de red	Puerto utilizado	Predeterminado	Modificación necesaria
SNMP	UDP 161, 162	N	Solo puede cambiarse el puerto de captura 162.
Modbus	TCP 502	N	S
VID/VIP	GDP/HTTP	N	N
DHCP Client	UDP 68	S	N
GDP (Geist Discovery Protocol)	UDP 6687	S	N
LDAP	TCP 389	N	S
RADIUS	UDP1812/1813/1645/1646	N	N
TACACS	TCP 49	N	N
Remote Syslog	TCP 514	N	S

Encontrará detalles de configuración de todas las opciones en el resto de esta guía.

## 4.1 Evaluación de riesgos

Vertiv recomienda llevar a cabo una evaluación de riesgos para identificar y evaluar de manera razonable los riesgos para la seguridad internos y externos previsible, la disponibilidad e integridad del sistema y su entorno. Esta tarea debería efectuarse de acuerdo con los marcos técnicos y regulatorios aplicables, como IEC 62443 y NERC-CIP. La evaluación de riesgos debe repetirse periódicamente.

## 4.2 Seguridad física

El IMD5 se ha diseñado para instalarse y funcionar en una ubicación físicamente segura. Vertiv recomienda efectuar una revisión de la seguridad física y del entorno de funcionamiento de la unidad. Dado que un atacante o una amenaza interna pueden causar graves trastornos, indicamos a continuación algunas mejores prácticas recomendadas, entre las que se incluyen:

- Acceso restringido a áreas, racks y unidades con tarjetas RFID cifradas, autenticación mediante clave de acceso multifactor exclusiva, dobles puertas de seguridad y escáneres biométricos para acceso físico al equipo.
- Personal de seguridad fiable y sin antecedentes con una presencia física 24/7, los 365 días del año y registros escritos para documentar y anotar el acceso físico al centro de datos, al edificio y al rack.
- Acceso físico restringido a equipo de telecomunicaciones y cableado de red. El acceso físico a las líneas de telecomunicación y al cableado de red debería restringirse para proteger contra ataques que pretenden interceptar o sabotear las comunicaciones. Entre las prácticas recomendadas se incluye el uso de conductos metálicos para el cableado de red que discurre entre los armarios del equipo.
- Todos los USB, RJ45 u otros puertos físicos deben estar restringidos en las unidades.

- No conecte medios extraíbles (como dispositivos USB y tarjetas SD) para ninguna tarea (como actualizaciones del firmware, cambios en la configuración o cambios en la aplicación de inicio) a menos que el origen del medio sea conocido y fiable. Antes de conectar algún dispositivo portátil a través de un puerto USB o una ranura para tarjeta SD, escanee el dispositivo en busca de malware o virus.

### 4.3 Acceso a la cuenta

Los privilegios de acceso a la cuenta del IMD5 deben administrarse con el objetivo de proporcionar el mínimo número de funciones posibles con las que el usuario final pueda desempeñar su trabajo. El inicio de sesión al IMD5 debería restringirse a los usuarios legítimos. Deberían adoptarse algunas de las siguientes prácticas recomendadas como parte de los procedimientos por escrito de la organización para el acceso a la red y el equipo:

- El primer inicio de sesión al IMD5 requiere la creación de credenciales.
- No deben compartirse la cuenta ni los inicios de sesión. Cada usuario debería tener sus cuentas y contraseñas específicas. Las funciones de inicio de sesión del IMD5 exigen que cada cuenta se corresponda a un usuario exclusivo no compartido.
- Los administradores deben restringir el acceso y los privilegios solo a las funciones requeridas para la tarea que desempeña el usuario.
- Restringir los privilegios de nivel de usuario (como actualizaciones del firmware, habilitación/deshabilitación del protocolo) únicamente a los administradores aprobados.
- Garantizar el cumplimiento de los requisitos de solidez, complejidad y longitud de la contraseña al máximo nivel de acuerdo con la política de TI de la empresa.
- Asegurarse de que los empleados que han sido despedidos tengan restringido de inmediato el acceso a la unidad. Algunos ejemplos incluyen al usuario de un proceso de autenticación de usuario AAA, TACACS+.
- Imponer el cierre de la sesión después de un periodo de inactividad.
- Usar syslog remoto para alertar de sucesos del sistema y de la red, amenazas a la seguridad y visibilidad del dispositivo para solucionar los problemas (puede también ser necesario para el cumplimiento de PCI-DSS/SOX/HIPAA).

## 5 Instalación

### 5.1 Dispositivo de monitorización intercambiable

El dispositivo de monitorización intercambiable (IMD) es la base de la línea de productos de alimentación actualizables del PowerIT Vertiv™ rPDU. El IMD se puede reemplazar y actualizar para permitir que los centros de datos puedan probar sus ubicaciones en el futuro. Instalar un IMD de reemplazo incorrecto en una rPDU puede provocar daños en el IMD.

#### 5.1.1 Básico

El rPDU Vertiv™ PowerIT actualizable básico está integrado al módulo IMD-01X y proporciona una distribución de alimentación de bajo coste con la opción de actualizarse para añadir características de medición local y/o monitorización remota, entre otras, en el futuro.

#### 5.1.2 Medido

El rPDU Vertiv™ PowerIT medido actualizable, una opción medida localmente, está integrado al módulo IMD-01D y proporciona una pantalla local para ver el consumo de corriente (amperios) con la opción de actualizarse para añadir monitorización y otras características en el futuro.

Figura 5.1 Módulo IMD-01D



Tabla 5.1 Descripciones del módulo IMD-01D

Elemento	Nombre	Descripción
1	Pantalla local	La pantalla local muestra los valores de fase, línea y corriente del circuito (en amperios).
2	Botones de la pantalla	Hay tres botones cerca de la pantalla del IMD: un botón para retroceder, otro para avanzar y otro para centrar. Las funciones de estos botones se describen en la <b>Tabla 5.2</b> en la página siguiente.

**Tabla 5.2 Funciones de los botones de la pantalla**

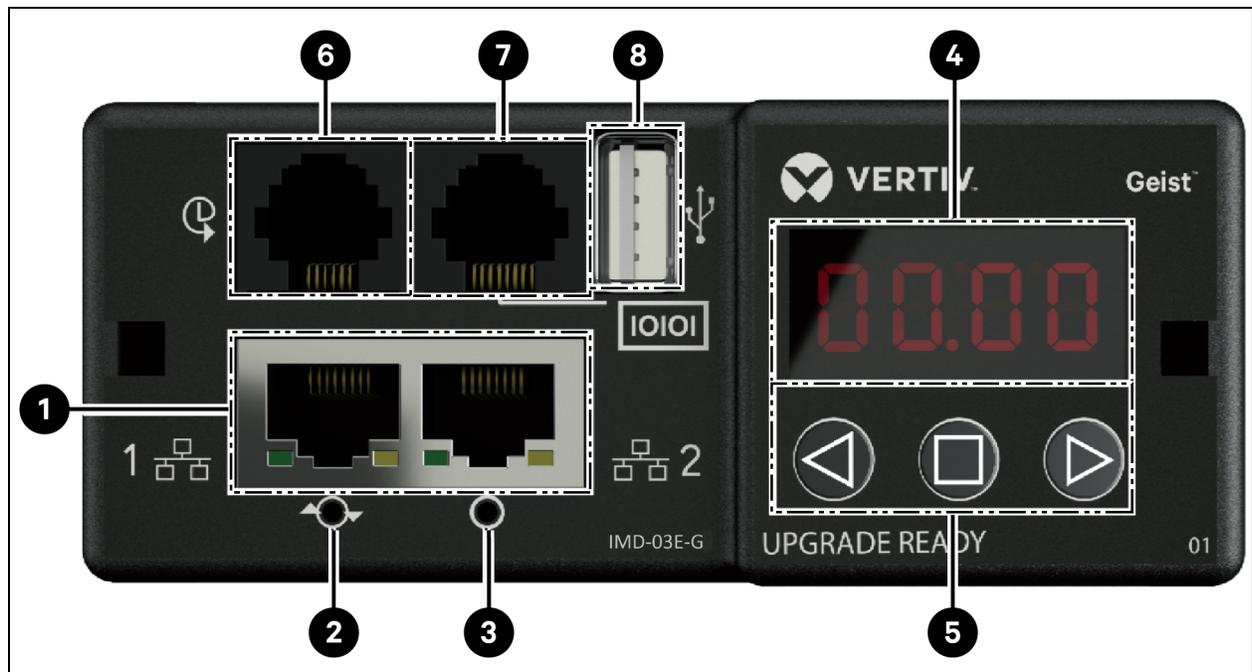
Botón	Símbolo	Descripción
Botón de retroceso		Volver al canal anterior.
Botón de avance		Avanzar al canal siguiente.
Botón de centrado		Alternar entre los modos de visualización de desplazamiento y estático. Si se mantiene pulsado este botón durante 10 segundos, se realizará un restablecimiento de red, lo cual restaurará la dirección IP predeterminada y restablecerá las cuentas de usuario.
Botón de centrado x3		Al pulsar este botón tres veces en dos segundos, se habilita el modo VLC. Al pulsar el botón mientras el modo VLC está activo, la unidad vuelve a la pantalla actual estándar.
Botones de avance y retroceso		Al pulsar ambos botones al mismo tiempo, la pantalla se voltea 180 grados.

**NOTA:** Las funciones de los botones de la pantalla pueden variar según la configuración de la unidad.

### 5.1.3 Unidad supervisada

Las versiones anteriores de las rPDU de Vertiv™ PowerIT de supervisión de nivel de unidad de Vertiv™ incluyen el módulo IMD-03E-G.

**Figura 5.2 Módulo IMD-03E-G**



**Tabla 5.3 Descripciones del módulo IMD-03E-G**

Número	Nombre	Descripción
1	Puertos Ethernet dobles	Los puertos Ethernet dobles actúan como un conmutador Ethernet de dos puertos, lo que permite conectar en cadena varios dispositivos. Los puertos Ethernet dobles se pueden configurar de forma independiente como interfaces de red Ethernet dobles, lo que permite que la rPDU se conecte a dos redes distintas.
2	Botón de reinicio por hardware	Al pulsar el botón de reinicio por hardware se reinicia el IMD. Actúa como una desconexión y conexión de la alimentación para el IMD y no cambia ni elimina información del usuario.
3	Botón de restablecimiento de red	Si se mantiene pulsado el botón de restablecimiento de red 5 segundos durante el funcionamiento normal, se restaurará la dirección IP predeterminada y se restablecerán las cuentas de usuario.
4	Pantalla local	La pantalla local muestra los valores de fase, línea y corriente del circuito (en amperios).
5	Botones de la pantalla	Hay tres botones cerca de la pantalla del IMD: un botón para retroceder, otro para avanzar y otro para centrar. Las funciones de estos botones se describen en la <b>Tabla 5.4</b> en la <b>página siguiente</b> .
6	Puerto del sensor remoto	Puerto RJ-12 para conectar sensores digitales remotos "plug-and-play" de Vertiv™ (se venden por separado). Cada sensor digital tiene un número de serie único y se detecta automáticamente. Las PDU de unidad supervisada admiten hasta 16 sensores. Se puede añadir el convertidor A2D opcional de Vertiv™ para admitir la detección analógica. El SN-ADAPTER opcional puede añadirse para dar cabida a los sensores integrados y modulares de Liebert. Para obtener más información, consulte <a href="#">Sensores disponibles</a> en la <b>página 127</b> .
7	Puerto serie	RS-232 a través del puerto RJ-45.
8	Puerto USB	Puerto USB que se utiliza para cargar el firmware, hacer una copia de seguridad/restaurar la configuración del dispositivo o ampliar la capacidad de registro a través de un dispositivo de almacenamiento USB o admitir adaptadores USB inalámbricos TP-Link. El puerto USB debe estar habilitado; consulte <a href="#">USB</a> en la <b>página 89</b> . Proporciona capacidad de alimentación de hasta 100 mA para dispositivos conectados por USB.

**NOTA: La conexión serie no permite el control de flujo.**

**Tabla 5.4 Funciones de los botones de la pantalla**

Botón	Símbolo	Descripción
Botón de retroceso		Pulse para volver al canal anterior. Si se mantiene pulsado el botón durante 3 segundos, se inicia una copia de seguridad de la configuración. La pantalla mostrará un mensaje <b>bcup</b> mientras se genera la copia de seguridad y luego se volverá al funcionamiento normal. La copia de seguridad se almacena en dispositivos de almacenamiento USB disponibles y no se pondrá en funcionamiento si dichas unidades no están disponibles.
Botón de avance		Pulse para avanzar al canal siguiente. Si se mantiene pulsado este botón durante 3 segundos, se inicia la restauración de la configuración. La pantalla mostrará el mensaje <b>load</b> seguido del mensaje <b>conf</b> y, a continuación, una cuenta atrás de 3 segundos. Una vez que termina la cuenta atrás, se muestra un mensaje <b>8888</b> y se aplica la copia de seguridad. La copia de seguridad se leerá desde dispositivos de almacenamiento USB. Si se suelta el botón en cualquier momento de esta secuencia, la restauración se anula. Una vez aplicada la copia de seguridad, o si no hay imágenes de copia de seguridad o no hay un dispositivo de almacenamiento USB conectado, la pantalla volverá a funcionar normalmente.
Botón de centrado		Alternar entre los modos de visualización de desplazamiento y estático. Si se mantiene pulsado este botón durante 3 segundos, se inicia una secuencia de restablecimiento de parámetros. La secuencia consiste en un mensaje <b>rset</b> seguido de un mensaje <b>dflit</b> y, a continuación, una cuenta atrás de 3 segundos. Una vez que termina la cuenta atrás, se muestra un mensaje <b>8888</b> y la información de red, <i>http</i> , cuentas de usuario y <i>LDAP/RADIUS</i> se restablece a los valores predeterminados. Si se suelta el botón en cualquier momento de esta secuencia, el restablecimiento se anula.
Botón de centrado x3		Al pulsar este botón 3 veces en 2 segundos, se habilita el modo VLC. Al pulsar el botón mientras el modo VLC está activo, la unidad vuelve a la pantalla actual estándar.
Botones de avance y retroceso		Al pulsar ambos botones al mismo tiempo, la pantalla se voltea 180 grados.
Botones de retroceso y centrado		Al pulsar ambos botones al mismo tiempo, se muestra la dirección IPv4 primaria de la unidad.

### 5.1.4 Nivel de unidad y de salida conmutada y supervisada

Las versiones anteriores de las rPDU de supervisión de nivel de unidad conmutada, supervisión de nivel de salida y supervisión de nivel de salida conmutada de Vertiv™ PowerIT incluyen el módulo IMD-3E-G.

Figura 5.3 Módulo IMD-3E-G

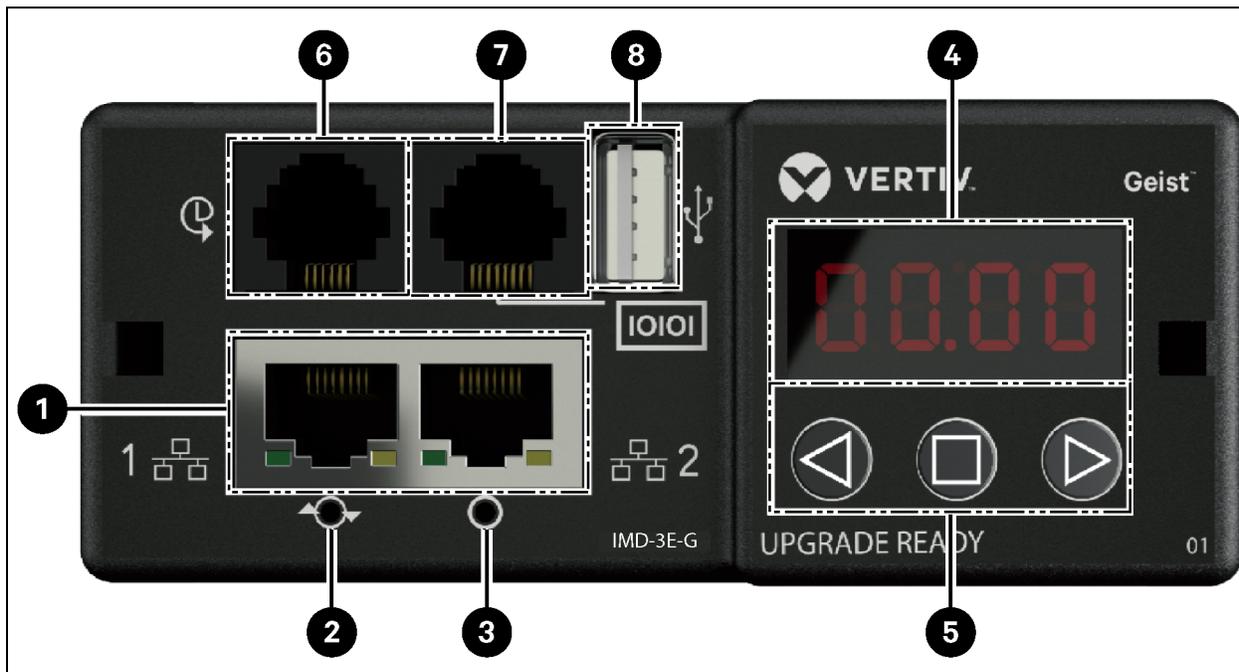


Tabla 5.5 Descripciones del módulo IMD-3E-G

Número	Nombre	Descripción
1	Puertos Ethernet dobles	Los puertos Ethernet dobles actúan como un conmutador Ethernet de dos puertos, lo que permite conectar en cadena varios dispositivos. Los puertos Ethernet dobles se pueden configurar de forma independiente como interfaces de red Ethernet dobles, lo que permite que la rPDU se conecte a dos redes distintas.
2	Botón de reinicio por hardware	Al pulsar el botón de reinicio por hardware se reinicia el IMD. Actúa como una desconexión y conexión de la alimentación para el IMD y no cambia ni elimina información del usuario.
3	Botón de restablecimiento de red	Si se mantiene pulsado el botón de restablecimiento de red 5 segundos durante el funcionamiento normal, se restaurará la dirección IP predeterminada y se restablecerán las cuentas de usuario.
4	Pantalla local	La pantalla local muestra los valores de fase, línea y corriente del circuito (en amperios).
5	Botones de la pantalla	Hay tres botones cerca de la pantalla del IMD: un botón para retroceder, otro para avanzar y otro para centrar. Las funciones de estos botones se describen en <a href="#">Funciones de los botones de la pantalla</a> en la página siguiente.
6	Puerto del sensor remoto	Puerto RJ-12 para conectar sensores digitales remotos "plug-and-play" de Vertiv (se venden por separado). Cada sensor digital tiene un número de serie único y se detecta automáticamente. Las PDU de salida conmutada y supervisada admiten hasta 16 sensores. Se puede añadir el convertidor A2D opcional de Vertiv™ para admitir la detección analógica. El SN-ADAPTER opcional puede añadirse para dar cabida a los sensores integrados y modulares de Liebert. Para obtener más información, consulte <a href="#">Sensores disponibles</a> en la página 127.
7	Puerto serie	RS-232 a través del puerto RJ-45.
8	Puerto USB	Puerto USB que se utiliza para cargar el firmware, hacer una copia de seguridad/restaurar la configuración del dispositivo o ampliar la capacidad de registro a través de un dispositivo de almacenamiento USB o admitir adaptadores USB inalámbricos TP-Link. El puerto USB debe estar habilitado; consulte <a href="#">USB</a> en la página 89. Proporciona capacidad de alimentación de hasta 100 mA para dispositivos conectados por USB.

**NOTA: Se admiten dispositivos USB MSC, como unidades USB o discos duros externos. Los dispositivos de almacenamiento USB deben tener formato FAT32.**

**NOTA: La conexión serie no permite el control de flujo.**

## Botones de la pantalla

Hay tres botones cerca de la pantalla del IMD: un botón para retroceder, otro para avanzar y otro para centrar. Las funciones de estos botones se describen en la siguiente tabla.

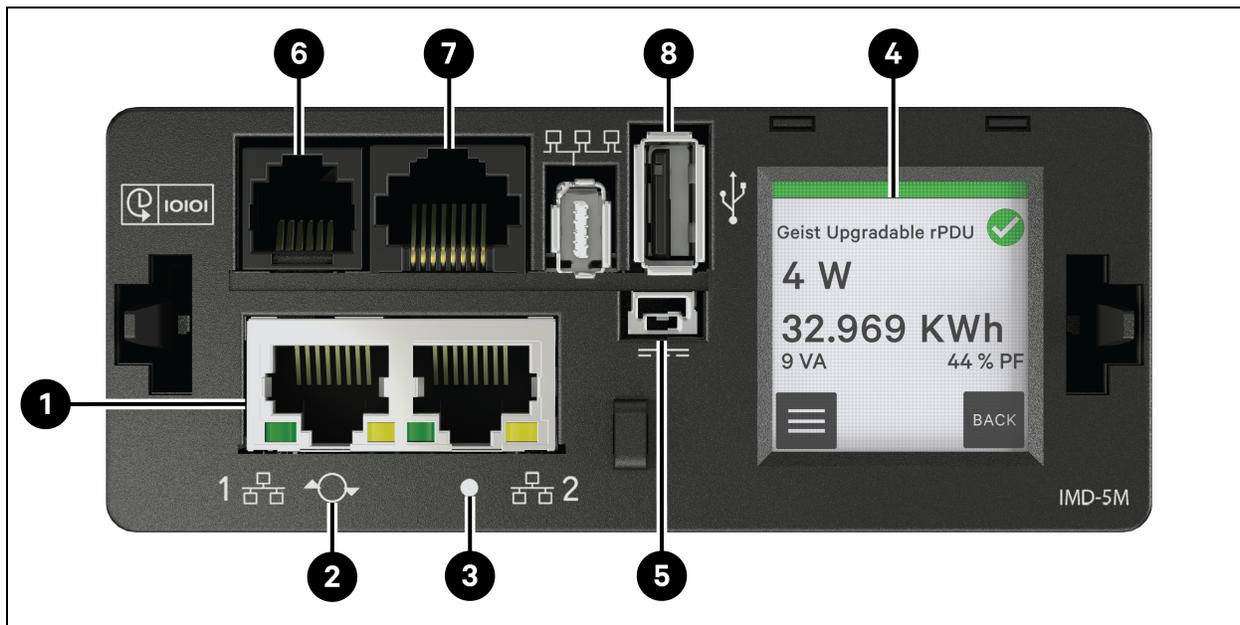
**Tabla 5.6 Funciones de los botones de la pantalla**

Botón	Símbolo	Descripción
Botón de retroceso		Pulse para volver al canal anterior. Si se mantiene pulsado este botón durante 3 segundos, se inicia una copia de seguridad de la configuración. La pantalla mostrará un mensaje <b>bcup</b> mientras se genera la copia de seguridad y luego se volverá al funcionamiento normal. La copia de seguridad se almacena en dispositivos de almacenamiento USB disponibles y no se pondrá en funcionamiento si dichas unidades no están disponibles.
Botón de avance		Pulse para avanzar al canal siguiente. Si se mantiene pulsado este botón durante 3 segundos, se inicia la restauración de la configuración. La pantalla mostrará el mensaje <b>load</b> seguido del mensaje <b>conf</b> y, a continuación, una cuenta atrás de 3 segundos. Una vez que termina la cuenta atrás, se muestra un mensaje <b>8888</b> y se aplica la copia de seguridad. La copia de seguridad se leerá desde dispositivos de almacenamiento USB. Si se suelta el botón en cualquier momento de esta secuencia, la restauración se anula. Una vez aplicada la copia de seguridad, o si no hay imágenes de copia de seguridad o no hay un dispositivo de almacenamiento USB conectado, la pantalla volverá a funcionar normalmente.
Botón de centrado		Alternar entre los modos de visualización de desplazamiento y estático. Si se mantiene pulsado este botón durante 3 segundos, se inicia una secuencia de restablecimiento de parámetros. La secuencia consiste en un mensaje <b>rset</b> seguido de un mensaje <b>dfit</b> y, a continuación, una cuenta atrás de 3 segundos. Una vez que termina la cuenta atrás, se muestra un mensaje <b>8888</b> y la información de red, http, cuentas de usuario y LDAP/RADIUS se restablece a los valores predeterminados. Si se suelta el botón en cualquier momento de esta secuencia, el restablecimiento se anula.
Botón de centrado x3		Al pulsar este botón tres veces en 2 segundos, se habilita el modo VLC. Al pulsar el botón mientras el modo VLC está activo, la unidad vuelve a la pantalla actual estándar.
Botones de avance y retroceso		Al pulsar ambos botones al mismo tiempo, la pantalla se voltea 180 grados.
Botones de retroceso y centrado		Al pulsar ambos botones al mismo tiempo, se muestra la dirección IPv4 primaria de la unidad.

## 5.1.5 Monitorizadas y conmutadas (IMD-5M)

Todas las rPDU de Vertiv™ PowerIT supervisadas y conmutadas se envían con el módulo IMD-5M.

Figura 5.4 Módulo IMD-5M



Elemento	Nombre	Descripción
1	Puertos Ethernet dobles	Los puertos Ethernet dobles actúan como un conmutador Ethernet de dos puertos, lo que permite conectar en cadena varios dispositivos. Los puertos Ethernet dobles se pueden configurar de forma independiente como interfaces de red Ethernet dobles, lo que permite que la rPDU se conecte a dos redes distintas.
2	Botón de reinicio/restablecimiento	Mantenga pulsado el botón durante 10 segundos para reiniciar el IMD. Actúa como una desconexión y conexión de la alimentación para el IMD y no cambia ni elimina información del usuario. Si se mantiene pulsado el botón 25 segundos durante el funcionamiento normal, se restaurará la dirección IP predeterminada y se restablecerán las cuentas de usuario.
3	LED de estado RGB (rojo, verde y azul)	LED verde: la unidad está en marcha y funcionando. LED amarillo: la unidad se está iniciando.
4	Menú táctil	Use el menú táctil para buscar los valores de fase, línea y corriente del circuito (en amperios).
5	Alimentación de entrada redundante	La alimentación redundante no funcionará con rPDU actualizables básicas, actualizables medidas más antiguas y rPDU de unidad supervisada actualizadas con el IMD-5M.

Elemento	Nombre	Descripción
6	Puerto del sensor remoto	Puerto RJ-12 para conectar sensores digitales remotos "plug-and-play" de Vertiv™ (se venden por separado). Cada sensor digital tiene un número de serie único y se detecta automáticamente. Las PDU monitorizadas y conmutadas admiten hasta 16 sensores. Se puede añadir el convertidor A2D opcional de Vertiv™ para admitir la detección analógica. El SN-ADAPTER opcional puede añadirse para dar cabida a los sensores integrados y modulares Liebert®. Para obtener más información, consulte <a href="#">Sensores disponibles</a> en la página 127.
7	Puerto serie	RS-232 a través del puerto RJ-45.
8	Puerto USB	Puerto USB que se utiliza para cargar el firmware, hacer una copia de seguridad/restaurar la configuración del dispositivo o ampliar la capacidad de registro a través de un dispositivo de almacenamiento USB o admitir adaptadores USB inalámbricos TP-Link. El puerto USB debe estar habilitado; consulte <a href="#">USB</a> en la <a href="#">página 89</a> . Proporciona hasta 0,5 vatios para el nivel supervisado de unidad y 5 vatios para el nivel de salida supervisada/nivel de unidad conmutada/nivel de salida conmutada.

**NOTA:** La conexión serie no permite el control de flujo.

## Flujo de trabajo del menú táctil

Cada sección se compone de uno o más grupos de páginas y cada grupo contiene una o más páginas. La mayoría de las páginas incluyen los botones Home, Enter y Next. Las únicas excepciones son la pantalla inicial, la página de inicio, las páginas que aparecen durante la actualización del firmware y las que aparecen momentáneamente para confirmar los resultados de una operación. El botón Home  lleva a la página de inicio. El botón Enter  pasa a la página siguiente del grupo de páginas. Si se está en la última página del grupo, se pasa a la primera página del grupo de páginas. El botón Next  pasa a la primera página del siguiente grupo de páginas. Si se está en el último grupo de páginas, se pasa al primer grupo.

La línea superior de cada página incluye la etiqueta del sistema sobre un fondo verde, amarillo o rojo que indica la alarma no reconocida de mayor prioridad, junto con un icono para indicar estados de alarma adicionales. Además, la medida de alarma se muestra en amarillo o rojo.

### Página de inicio

La página de inicio consta de enlaces a las tres secciones siguientes:

- System
- Devices
- Alarmas

La página de inicio es la única sin los botones de navegación Home, Next y Enter.

Figura 5.5 Flujo de trabajo del menú táctil

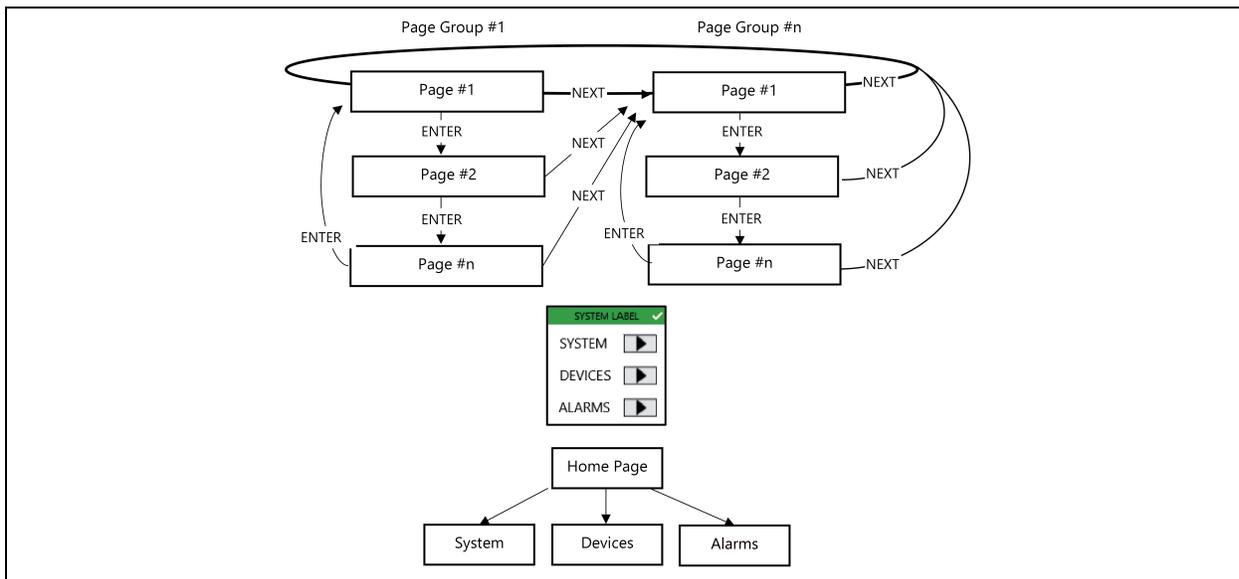


Figura 5.6 Sección System

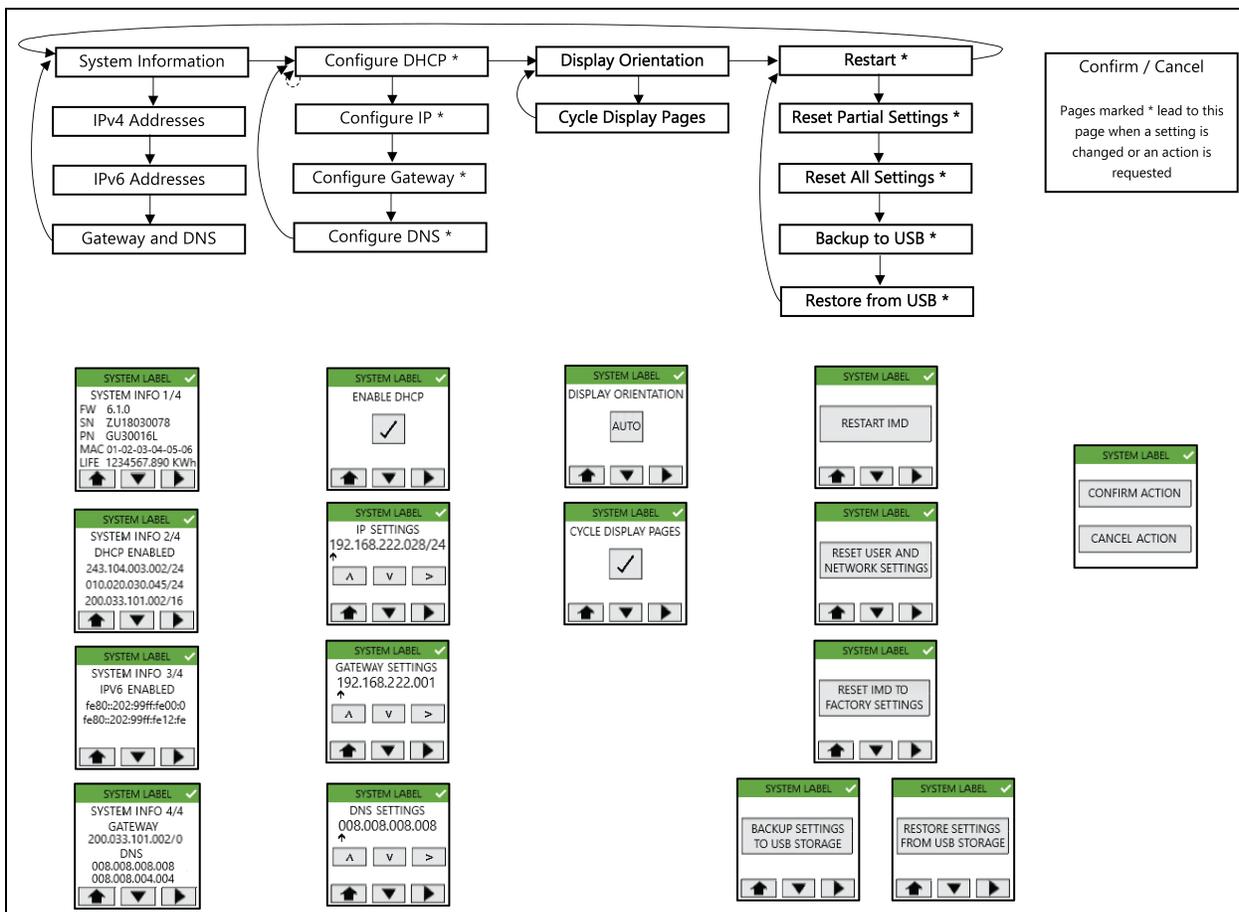


Figura 5.7 Sección Device

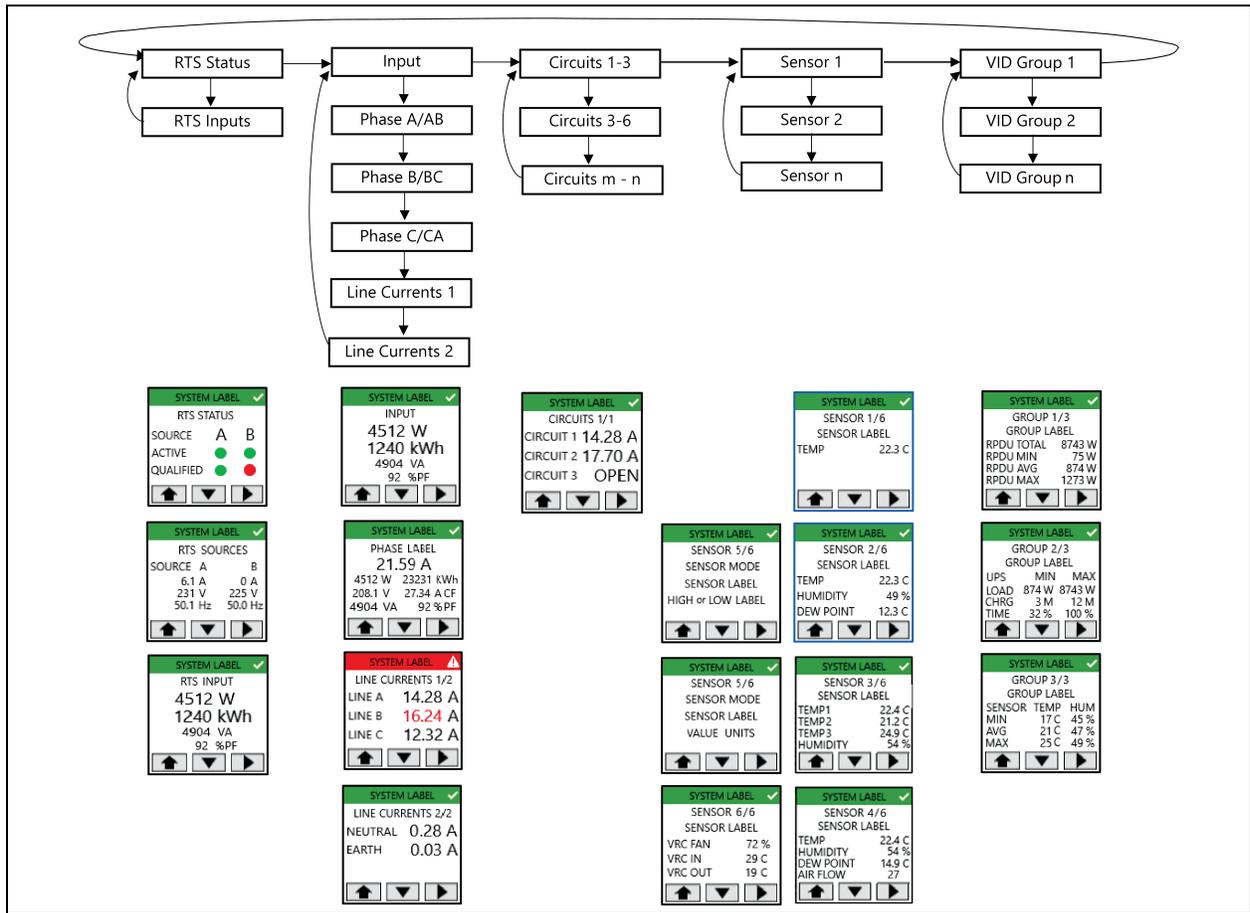
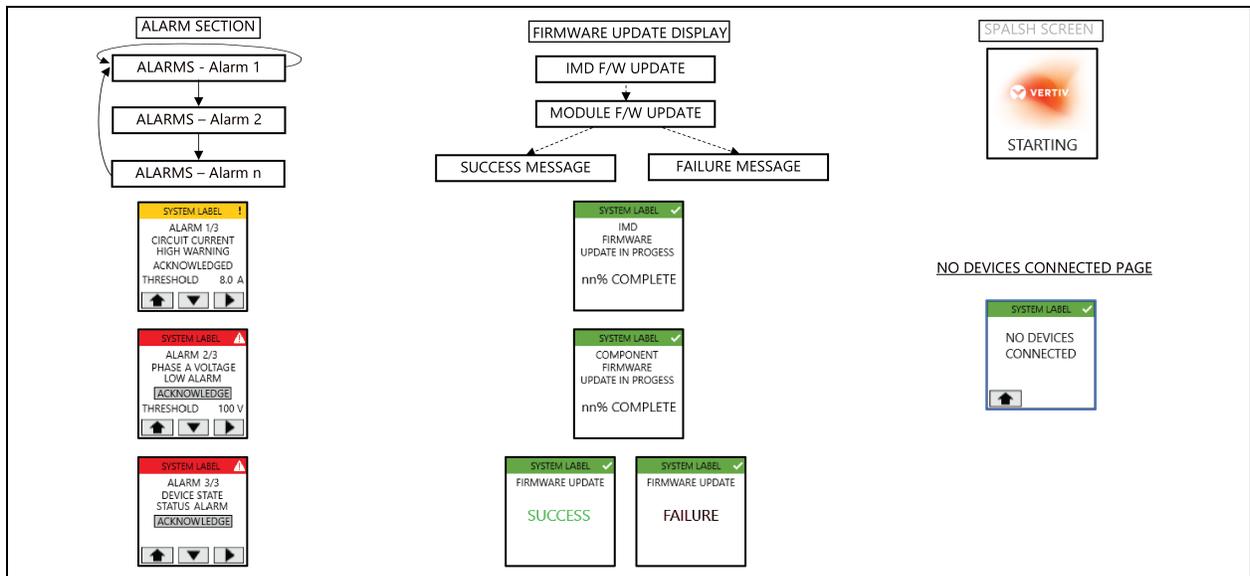


Figura 5.8 Sección Alarm y Firmware Update Display



## Funciones del menú táctil

- La página Splash Screen se muestra durante la inicialización del IMD.
- La página predeterminada que se muestra tras el encendido o tras un tiempo de inactividad del menú táctil de 60 segundos está determinada por el tipo de dispositivo:
  - **RTS:** página RTS Status
  - **PDU para rack:** página Input
  - **RDU202:** página Sensor 1
- La retroiluminación de la pantalla reducirá su intensidad tras 75 segundos de inactividad del menú táctil.
- En la mayoría de los casos, se muestran los nombres. La etiqueta del sistema se desplaza para mostrar la etiqueta completa. Otras etiquetas pueden aparecer truncadas si superan los 10 caracteres.
- Cada línea de encabezado de página tendrá un color de fondo verde, ámbar o rojo para indicar el estado de alarma no reconocida de mayor prioridad, y un icono para indicar los estados de advertencia y alarma.
- El punto de color de la página de salida indica el estado de la salida (verde=encendido, rojo=apagado) de las PDU para rack conmutadas de salida. No se muestra ningún punto cuando la rPDU no es capaz de conmutar salidas.
- Las páginas de ajustes IP solo harán referencia a la configuración IPv4 y la configuración de la dirección IP solo configura la primera dirección IP y dirección DNS.
- Cuando DHCP está activado, no se muestran las páginas de configuración de dirección IP, puerta de enlace y dirección DNS.
- La marca de verificación del botón de la página DHCP aparece/desaparece al pulsar el botón para indicar la opción seleccionada.
- La pantalla de actualización de firmware se muestra cuando comienza una actualización de firmware, independientemente de la fuente (UI web, CLI, API, SCP, USB). El porcentaje de progreso de actualización del firmware del componente se calculará como:  $(\text{tarjetas actualizadas hasta ahora}) / (\text{total de tarjetas por actualizar}) * 100$
- Una vez realizadas todas las actualizaciones de firmware, se muestra la página Firmware Update Success o Firmware Update Failure durante 15 segundos. A continuación, se muestra la página predeterminada.
- Durante la actualización del firmware, la retroiluminación de la pantalla se ajustará al 100% de intensidad. Al terminar, la retroiluminación de la pantalla reducirá su intensidad tras 75 segundos de inactividad del menú táctil.
- Solo se muestran las tres primeras direcciones IPv4 y/o IPv6 en el grupo de páginas System Information.
- Una acción pendiente, como esperar la confirmación de la acción o la confirmación de la dirección IP introducida, se cancelará por un evento asíncrono, por ejemplo, un tiempo de espera de la pantalla agotado (consulte [La página predeterminada que se muestra tras el encendido o tras un tiempo de inactividad del menú táctil de 60 segundos está determinada por el tipo de dispositivo](#): arriba) o una actualización de firmware.

- Al pulsar cualquier botón de navegación después de realizar cambios en la configuración de DHCP, dirección IP, puerta de enlace o DNS, se mostrará una página de acción de confirmación/cancelación. Al confirmar se ejecuta el cambio y se vuelve a la página anterior, en la que se muestran los ajustes modificados. Al cancelar se revoca el cambio y se vuelve a la página anterior, en la que se muestran los ajustes sin modificar.
- Cuando se selecciona la opción Cycle Display Pages, la pantalla predeterminada recorre las páginas del grupo de páginas del dispositivo, mostrando cada página durante 5 segundos. Por ejemplo, si se activa Cycle Display Pages en una PDU para rack, la pantalla recorrerá las páginas Input, Phase y Line Current.
- Cuando un grupo VID incluye más de un tipo de dispositivo (por ejemplo, PDU para rack y UPS), se mostrará una página de grupo VID para cada tipo de dispositivo dentro del grupo.
- El enlace Alarms de la página de inicio solo se muestra cuando se dispara una alarma.
- Las alarmas pueden confirmarse mediante el botón Acknowledge, que cambia al texto **Acknowledged** cuando se acciona.
- La página Display Orientation alterna entre Auto, 0 grados, 90 grados, 180 grados y 270 grados al pulsar un botón (con el ajuste de 270 grados volviendo a Auto). La acción es instantánea al pulsar el botón.
- Cuando se selecciona una acción Restart, Reset User/Network, Factory Reset, Backup o Restore, aparece una página de confirmación/cancelación. Si se confirma, la acción continúa; si se cancela, la pantalla vuelve a la página anterior. Al terminar la acción Reset User/Network, Factory Reset, Backup o Restore, se muestra la página Action Completed durante 5 segundos antes de que el menú táctil vuelva a la página predeterminada.
- La página No Devices Connected debería reemplazar a la página de menú táctil predeterminada (o a las páginas de menú táctil predeterminadas cíclicas) si no se detectan ramas api/dev en estado normal.
- Al seleccionar una acción del grupo de páginas de utilidades (como Restart), se muestra una página para confirmar/cancelar la acción. Si se confirma, se ejecuta la solicitud, tras lo cual la pantalla vuelve a la página de inicio. Si se cancela, se revoca la solicitud y se vuelve a la página anterior.

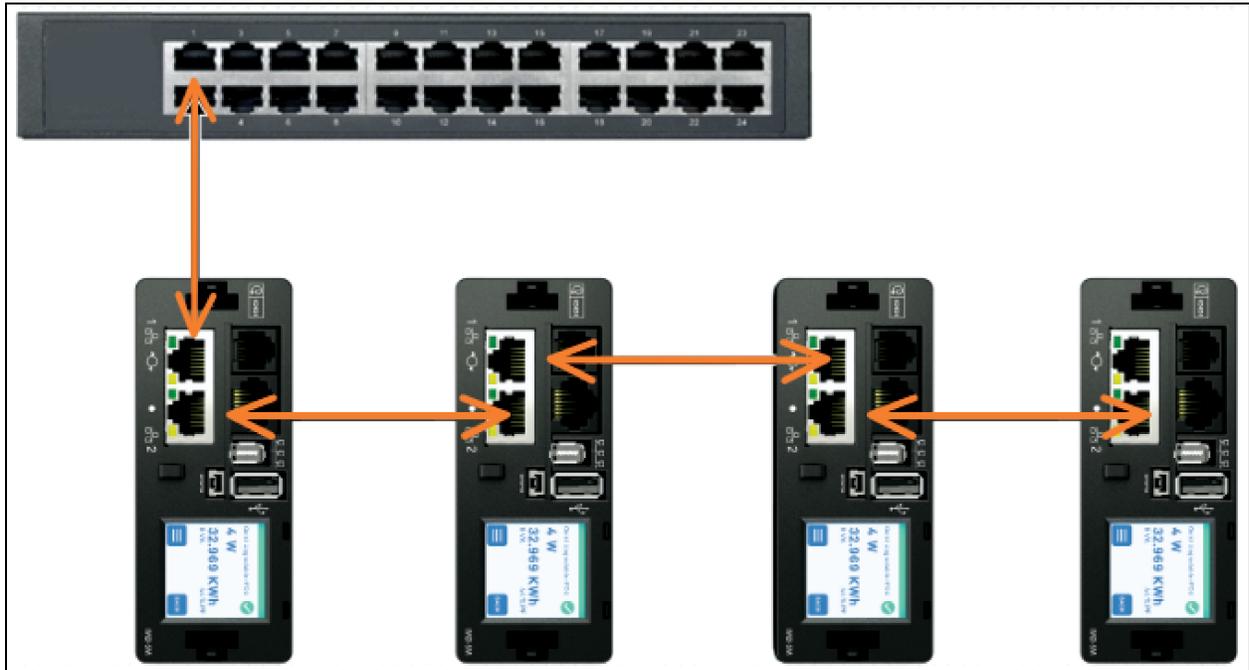
### 5.1.6 Protocolo de árbol de expansión rápido (RSTP)

Los dispositivos supervisados actualizables, que llevan integrados el IMD-5M, incluyen dos puertos Ethernet que funcionan juntos como un puente Ethernet interno. Uno de estos puertos se puede utilizar para conectar el IMD a una red existente o ambos puertos se pueden utilizar al mismo tiempo para conectar un IMD a otro en una configuración de conexión en cadena.

#### Conexión en cadena

- Utilice la conexión en cadena para reducir el número de puertos del conmutador de red.
- Las PDU para rack se conectan mediante una conexión en cadena Ethernet.
- La cabeza de la cadena de la PDU para rack se conecta a un puerto del conmutador de red.
- Cada PDU para rack tiene su propia dirección IP única.

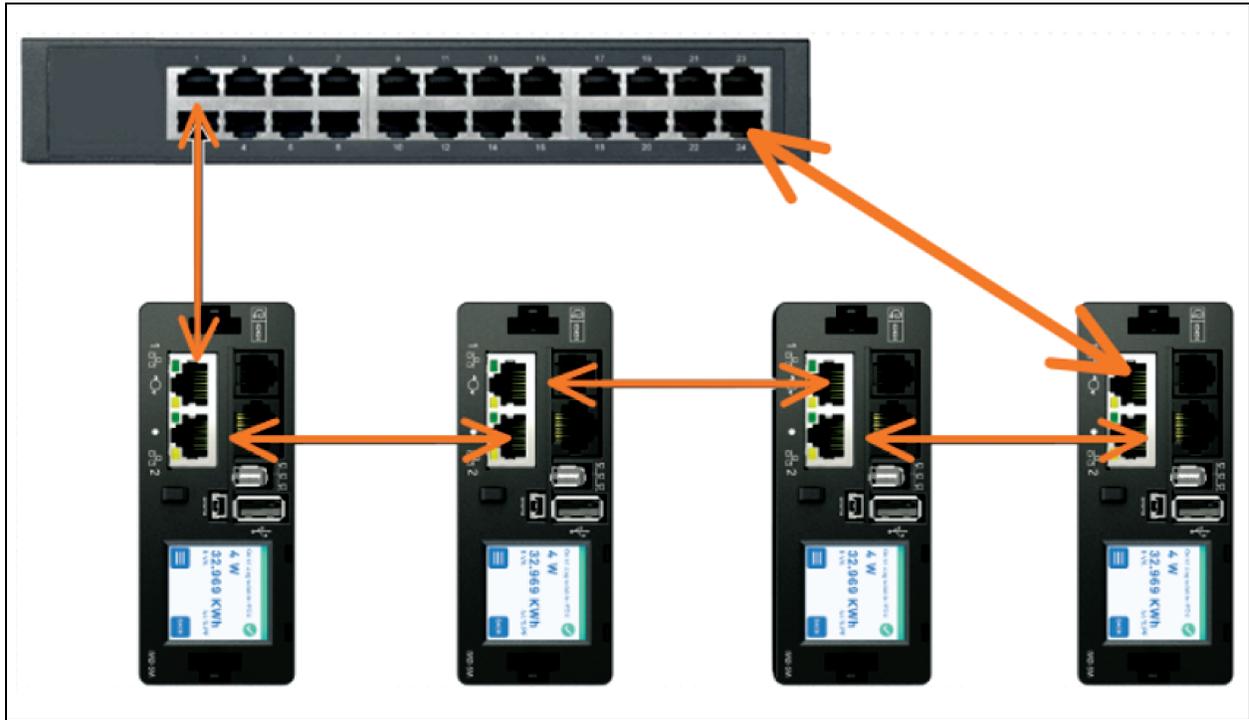
Figura 5.9 Conexión en cadena



### Conexión en cadena tolerante a errores

- Use una conexión en cadena tolerante a errores para proporcionar una conectividad de red resistente.
- Las PDU para rack se conectan mediante una conexión en cadena Ethernet.
- Tanto la cabeza como la cola de la cadena de las PDU para rack se conectan a los puertos del conmutador de red.
- Cada PDU para rack tiene su propia dirección IP única.
- El protocolo de árbol de expansión rápido (RSTP) debe configurarse de modo que pueda administrar la tolerancia a errores y mantener la conectividad en caso de que haya un fallo en el cable o una pérdida de alimentación por parte de la PDU para rack.

Figura 5.10 Conexión en cadena tolerante a errores



Cuando ambas interfaces de red están conectadas, el IMD implementa un protocolo de puente de red llamado protocolo de árbol de expansión rápido (RSTP). El RSTP es un estándar de IEEE que se aplica en todos los puentes administrados. Si se utiliza el RSTP, los puentes de la red intercambian información para encontrar rutas o bucles redundantes. IPv6 debe estar desactivado cuando se usa conectividad de red redundante.

Cuando se detecta un bucle, los puentes de la red trabajan simultáneamente para deshabilitar de forma temporal las rutas redundantes. Esto permite a la red evitar las tormentas de difusión provocadas por los bucles. Además, el RSTP comprueba periódicamente los cambios en la topología de la red. Cuando se pierde una conexión, el RSTP permite que los puentes cambien rápidamente a una ruta redundante.

**NOTA: El protocolo RSTP impone un límite de 40 enlaces entre puentes, incluidos los IMD.**

**NOTA: Vertiv Intelligence Director no se puede usar conjuntamente con el RSTP y la conectividad de red redundante.**

## 5.2 Configuración de red

El IMD actualizable tiene una dirección IP predeterminada para la configuración inicial y el acceso.

**Para restaurar la dirección IP predeterminada y restablecer toda la información de la cuenta de usuario:**

1. Si se mantiene pulsado el botón RESET/RESTART (orificio de la primera clavija) junto a la pantalla LCD durante 25 segundos, también se restablece la información de la red y de cuenta del usuario.
2. Si se mantiene pulsado el botón RESET/RESTART (orificio de la primera clavija) junto a la pantalla LCD durante 10 segundos, se apagará y encenderá el IMD sin cambiar información del usuario.

La página Network, ubicada en la pestaña System, permite asignar las propiedades de la red manualmente o utilizar DHCP para conectarse a la red. Para acceder a la unidad es necesario conocer la dirección IP. Se recomienda el uso de una IP estática o un DHCP reservado. La dirección predeterminada se muestra en la parte delantera de la unidad.

- **IP Address:** 192.168.123.123
- **Subnet Mask:** 255.255.255.0
- **Gateway:** 192.168.123.1

Para acceder a la unidad por primera vez, debe cambiar temporalmente la configuración de la red del ordenador para que coincida con la subred **192.168.123. xxx**. Para configurar la unidad, conéctela al puerto Ethernet del ordenador y siga las instrucciones adecuadas para el sistema operativo del ordenador.

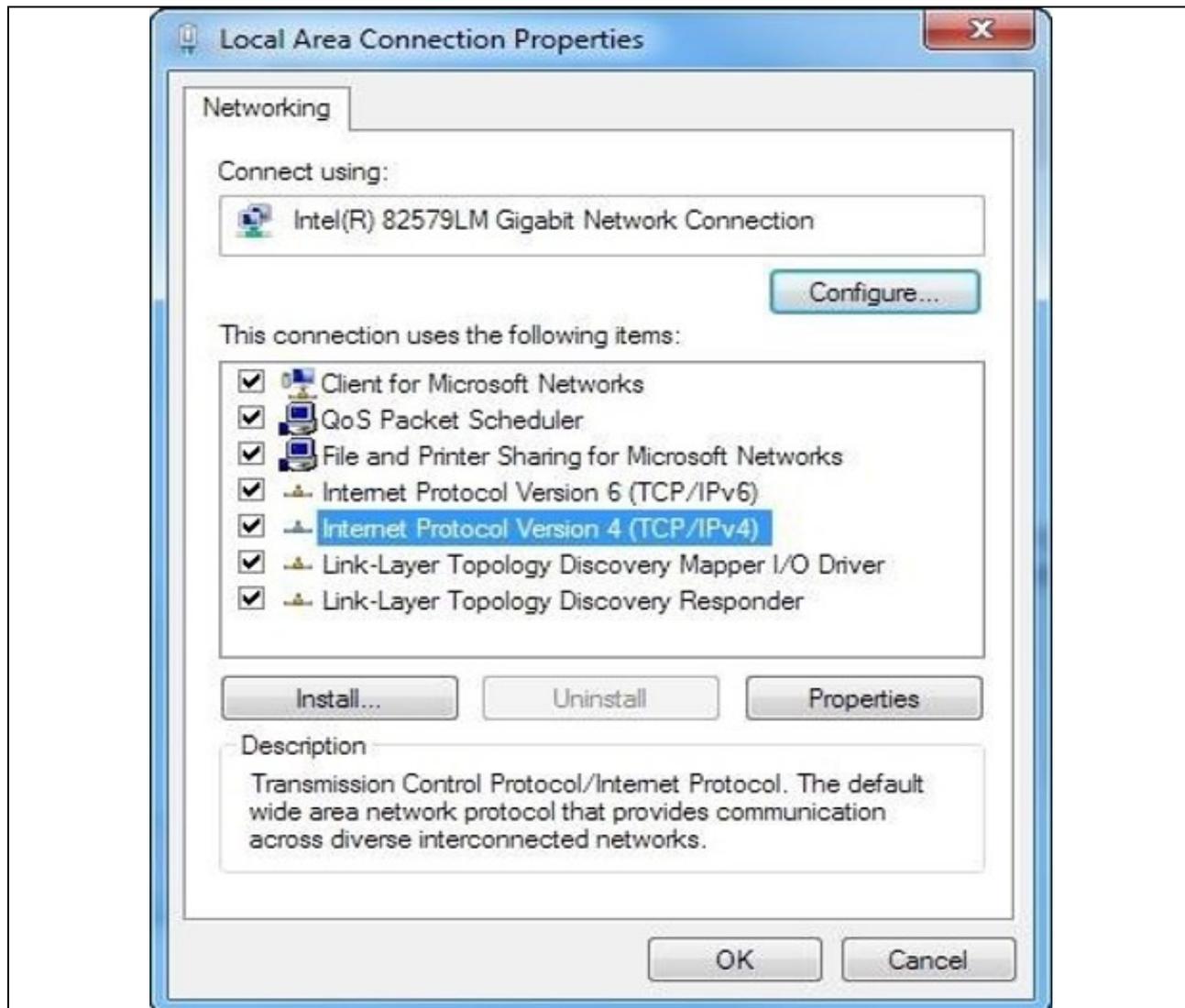
**Para configurar la red para un sistema operativo Windows:**

1. Acceda a la configuración de red de su sistema operativo.
  - Windows Server 2022 y 2019.
  - En Microsoft Windows 10, haga clic en *Start>Network and Internet>Change Adapter Settings*.
  - En Microsoft Windows 11, haga clic en *Start>Network and Internet>Change Adapter Settings*.
2. Localice la entrada bajo la LAN, Internet de alta velocidad o conexión de área local que corresponda a la tarjeta de red (NIC). Haga doble clic en la entrada del adaptador de red en la lista Network Connections.

**NOTA: La mayoría de los ordenadores tendrán una sola NIC Ethernet instalada, pero un adaptador WiFi o de datos celulares también aparece como NIC en esta lista. Asegúrese de elegir la entrada correcta.**

3. Haga clic en *Properties* para abrir la ventana Local Properties.

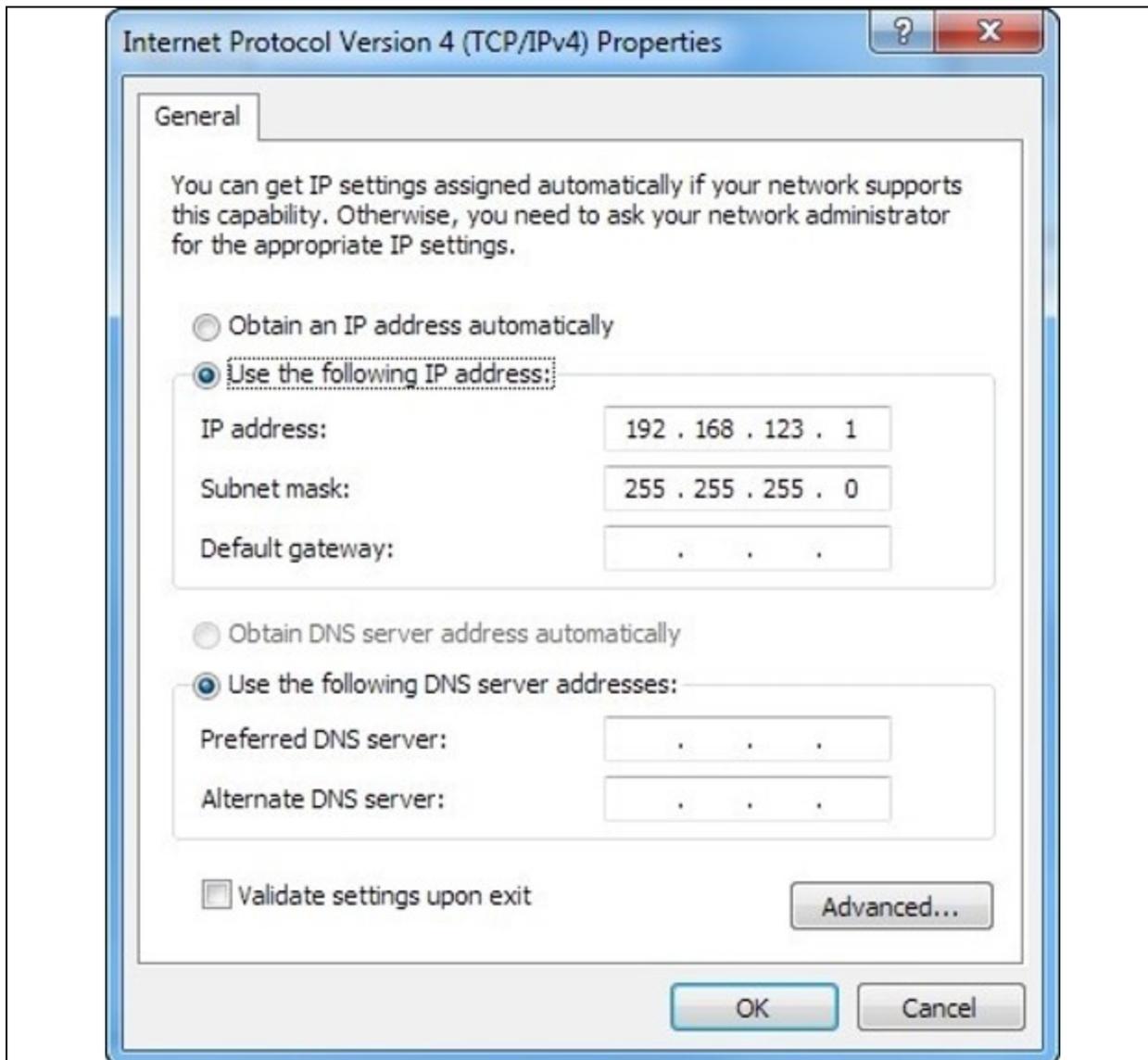
Figura 5.11 Local Area Connection Properties



4. En la lista, seleccione *Internet Protocol Version 4 (TCP/IPv4)* y haga clic en *Properties*.

**NOTA:** Si ve más de una entrada TCP/IP, como en el ejemplo anterior, el ordenador puede estar configurado para compatibilidad con IPv6, así como con IPv4; asegúrese de seleccionar la entrada para el protocolo IPv4. Anote la configuración actual de la tarjeta NIC para que pueda restaurarla a la normalidad después de haber terminado el procedimiento de configuración.

Figura 5.12 Internet Protocol Version 4



5. Elija *Use the following IP address*, configure la dirección IP a **192.168.123.1** y Subnet Mask a **255.255.255.0**. Durante la configuración inicial, Default Gateway y las entradas de DNS Server pueden dejarse en blanco. Seleccione *OK* - *OK* para cerrar las ventanas Internet Protocol Properties y Local Properties.
6. En un navegador web, introduzca **http://192.168.123.123** para acceder a la unidad. Si es la primera vez que configura la unidad, debe crear una cuenta de administrador y una contraseña antes de poder continuar.
7. Una vez creada la cuenta Admin, inicie sesión en la unidad.
8. De forma predeterminada, se muestra la página de sensores predeterminados. Desplácese a la *pestaña System* y luego a la *página Network* para configurar las propiedades de la red del dispositivo. Los ajustes para IP address, Subnet Mask, Gateway y DNS de la unidad se pueden asignar manualmente o adquirirse a través de DHCP.

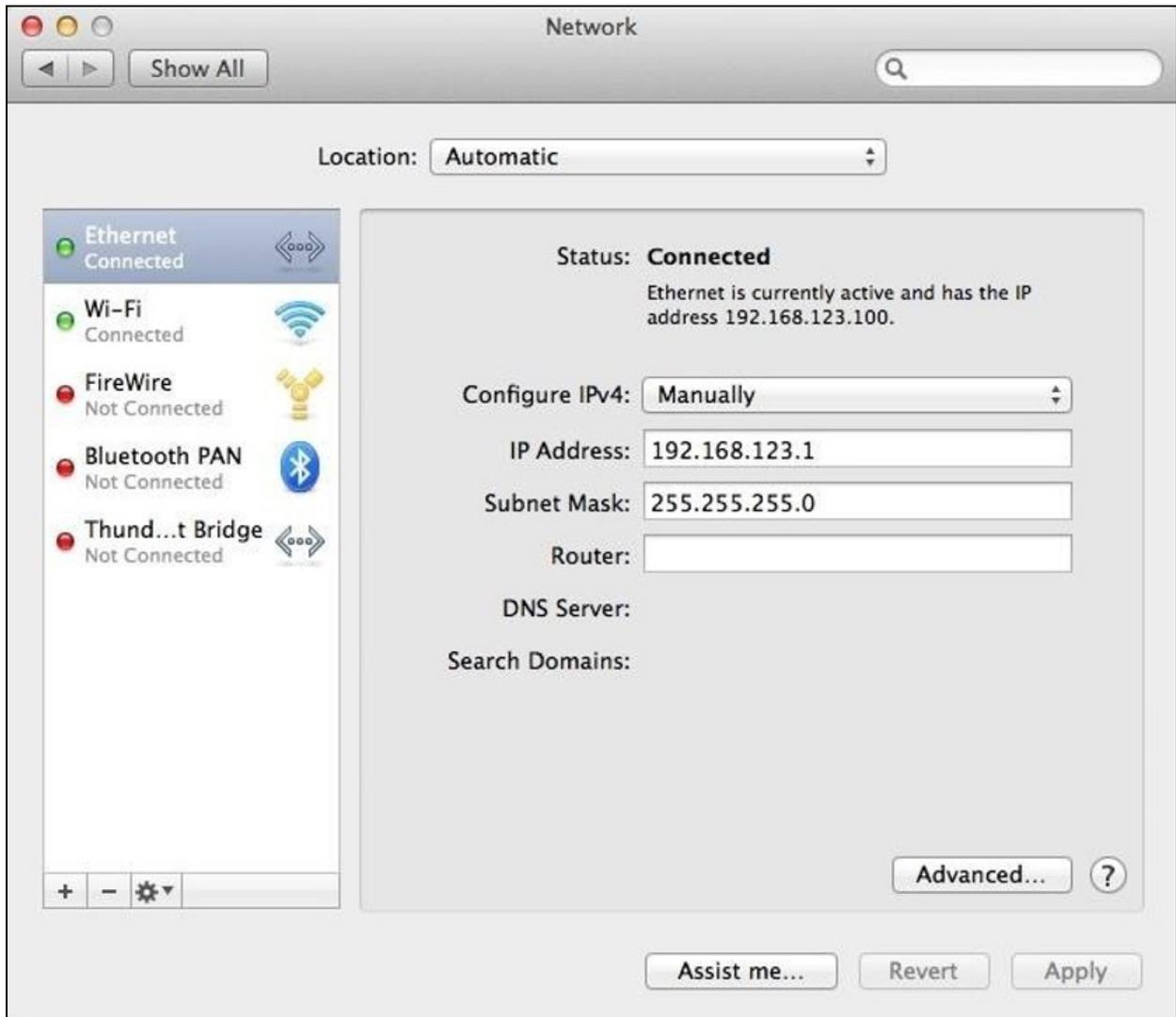
9. Haga clic en *Save*.

**NOTA:** Una vez guardados los cambios, el navegador ya no podrá recargar la página web desde la dirección **192.168.123.123** y muestra el mensaje **Page not Found** o **Host Unavailable**; esto es normal. Cuando termine de configurar la dirección IP de la unidad, repita los pasos anteriores cambiando la configuración de la tarjeta NIC Ethernet del ordenador a la que anotó antes de cambiarla.

**Para configurar la red para un Mac:**

1. Haga clic en el icono System Preferences en el Dock y elija *Network*.

**Figura 5.13** Preferencias del sistema de Mac



2. Asegúrese de que esté resaltada la opción Ethernet en el lado izquierdo de la ventana NIC. En la mayoría de los casos, habrá una entrada Ethernet en un Mac. Anote la configuración actual para que pueda restaurarla a la normalidad después de haber terminado el procedimiento de configuración.

3. Seleccione *Manually* en la lista desplegable Configure IPv4 y, a continuación, establezca la opción IP address en **192.168.123.1** y Subnet Mask en **255.255.255.0**, y haga clic en *Apply*.

**NOTA: La configuración del router y del servidor DNS se puede dejar en blanco para esta configuración inicial. En un navegador web, introduzca <http://192.168.123.123> para acceder a la unidad. Si es la primera vez que configura la unidad, debe crear una cuenta de administrador y una contraseña antes de poder continuar.**

4. Una vez creada la cuenta Admin, inicie sesión en la unidad.
5. De forma predeterminada, se muestra la página de sensores predeterminados. Desplácese a la pestaña *System* y luego a la página *Network* para configurar las propiedades de la red del dispositivo. Los ajustes para IP address, Subnet Mask, Gateway y DNS de la unidad se pueden asignar manualmente o adquirirse a través de DHCP.
6. Haga clic en *Save*.

**NOTA: Una vez guardados los cambios, el navegador ya no podrá recargar la página web desde la dirección **192.168.123.123** y muestra el mensaje **Page not Found** o **Host Unavailable**; esto es normal. Cuando termine de configurar la dirección IP de la unidad, repita los pasos anteriores cambiando la configuración de la tarjeta NIC Ethernet del ordenador a la que anotó antes de cambiarla.**

## 5.3 Interfaz de usuario basada en web

**NOTA: Vertiv™ PowerIT es el mismo producto que Vertiv™ Geist™. Use este manual tanto para el producto etiquetado Vertiv™ PowerIT como Vertiv™ Geist™. Próximamente se actualizarán los gráficos con el nuevo nombre.**

Se puede acceder a la unidad a través de una conexión HTTP estándar no cifrada, así como mediante una conexión HTTPS (TLS) cifrada. Las unidades se establecerán de manera predeterminada en HTTP y se redirigirán a HTTPS, a menos que el administrador las habilite específicamente como HTTP.

**NOTA: Se debe crear una cuenta de administrador (nombre de usuario y contraseña) al acceder al dispositivo por primera vez.**

**NOTA: Si el mensaje **Clock not set** aparece en la parte inferior derecha de la página, siga los procedimientos en **Time** en la página 88.**

**NOTA: La frecuencia de actualización de los datos en la interfaz web es de 5 segundos. Esto no debe confundirse con los cálculos de contabilización de energía continua y las notificaciones de alarma instantáneas.**

### 5.3.1 Menú principal

El menú principal está colocado verticalmente en el extremo izquierdo. Consulte la **Figura 5.14** en la página siguiente para el menú principal.

**!** ¡ADVERTENCIA! No conecte radiadores eléctricos, aparatos de calefacción eléctricos o cualquier otro aparato eléctrico que puedan provocar incendios, descargas eléctricas o lesiones cuando funcionan sin supervisión.

Figura 5.14 Menú principal

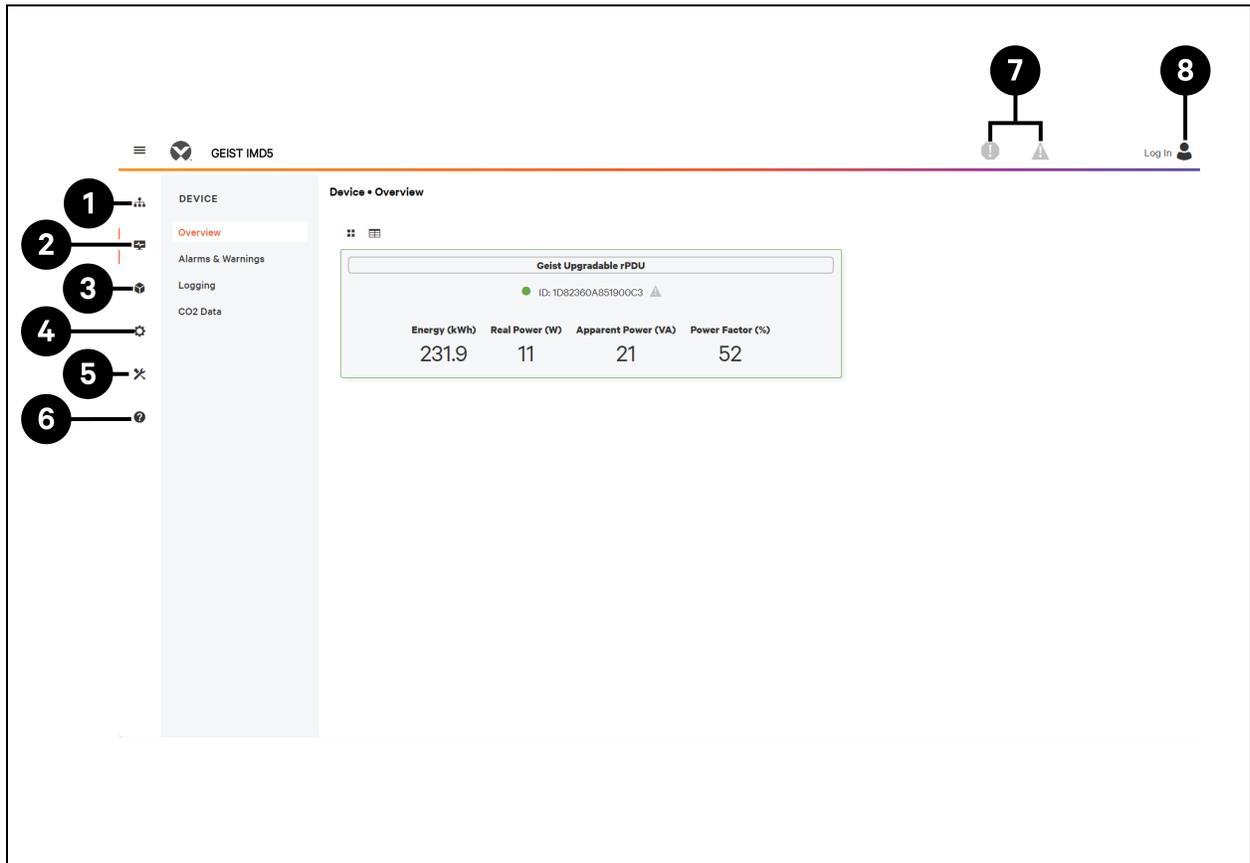


Tabla 5.7 Descripciones del menú principal

Elemento	Descripción
1	Agregación
2	Dispositivo
3	Aprovisionador
4	System
5	Utilidades
6	Ayuda
7	Alarmas y advertencias
8	Log In/Log Out

## 5.4 Submenú Device

Haga clic en el submenú Device para acceder a los menús *Overview*, *Alarms & Warnings*, *Logging* y *CO2 Data*.

### 5.4.1 Información general

Debe iniciar sesión antes de efectuar algún cambio. Solo los usuarios con autorizaciones de nivel de control o superiores tienen acceso a esta configuración.

Figura 5.15 Descripciones del submenú Device Overview

The screenshot shows the 'Device Overview' page for a 'GEIST UPGRADABLE RPDU'. The page is divided into several sections, each highlighted with a numbered callout:

- 1:** Device header area showing 'GEIST UPGRADABLE RPDU' and 'DEVICE ID 1D82380A851900C3'.
- 2:** Summary table for overall device statistics.
- 3:** Table for 'Current (A<sub>ass</sub>)' showing a value of 0.18.
- 4:** Table for 'Residual Current' showing 'Residual Current Aggregate (Arms)' at 10 and 'Residual Current DC (rms)' at 6.
- 4:** Table for 'Current (A<sub>ass</sub>)' for individual circuits (Circuit 1 to Circuit 6), all showing 0.00.
- 6:** Table for 'Outlet' statistics (Outlet 1, Outlet 2, Outlet 3).
- 7:** Callout pointing to the 'Outlet 3' row in the table.
- 8:** Callout pointing to the 'Overview' menu item in the left sidebar.

State	Label	Energy (kWh)	Real Power (W)	Apparent Power (VA)	Power Factor (%)	Voltage (V <sub>ass</sub> )	Current (A <sub>ass</sub> )	Current Crest Factor	Balance (%)
▲	Total	235.3	10	22	45				
▲	Phase A	222.7	10	22	48	122.3	0.18	4.95	100
▲	Phase B	12.64	0	0	100	122.3	0.00	1.00	0
▲	Phase C	0.000	0	0	100	122.3	0.00	1.00	0

State	Label	Current (A <sub>ass</sub> )
▲	Line	0.18

State	Label	Residual Current Aggregate (Arms)	Residual Current DC (rms)
▲	Residual Current	10	6

State	Label	Current (A <sub>ass</sub> )
● ▲	Circuit 1	0.00
● ▲	Circuit 2	0.00
● ▲	Circuit 3	0.00
● ▲	Circuit 4	0.00
● ▲	Circuit 5	0.00
● ▲	Circuit 6	0.00

State	Label	Energy (kWh)	Real Power (W)	Apparent Power (VA)	Power Factor (%)	Voltage (V <sub>ass</sub> )	Current (A <sub>ass</sub> )	Current Crest Factor
● ▲	Outlet 1	0.000	0	0	100	122.8	0.00	1.00
● ▲	Outlet 2	0.000	0	0	100	122.5	0.00	1.00
● ▲	Outlet 3	0.000	0	0	100	122.6	0.00	1.00

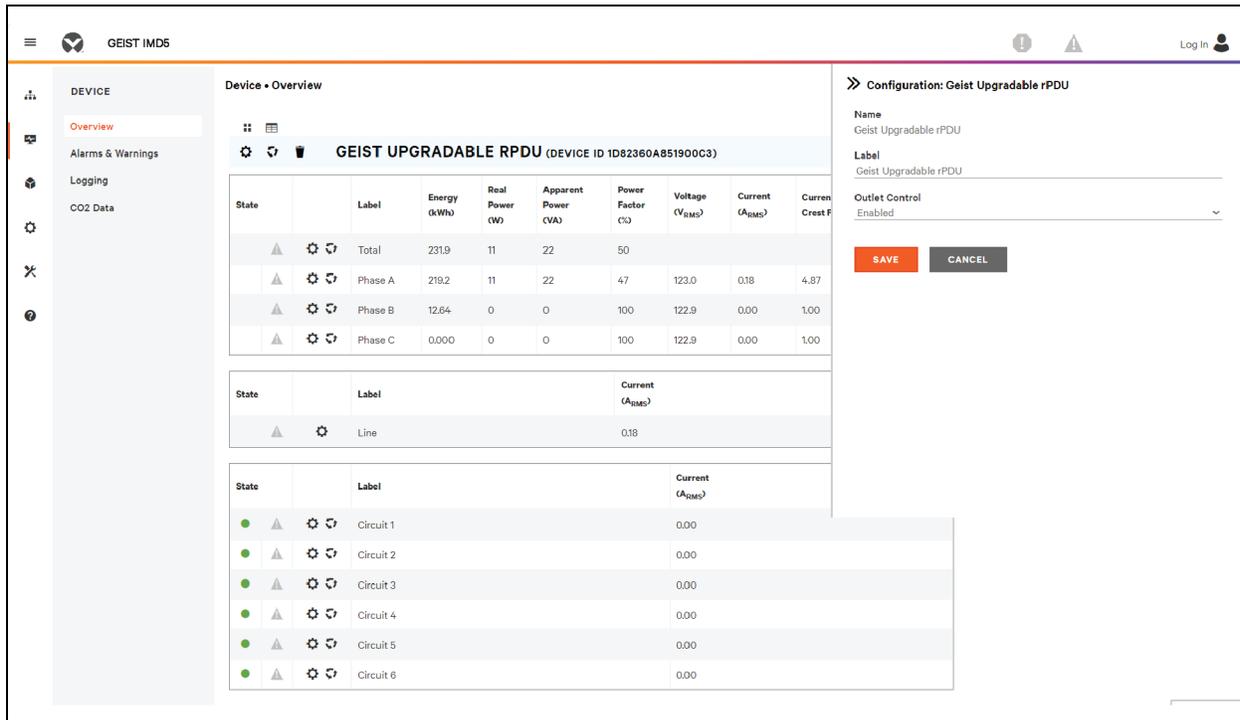
**Tabla 5.8 Descripciones del submenú Device Overview**

Número	Nombre	Descripción
1	Device ID	La identificación del producto es única y no se puede modificar. Puede ser necesario para recibir asistencia técnica.
2	Monitor de fase total e individual	Muestra las estadísticas de corriente alterna, voltaje y potencia de cada fase individual y del total de todas las fases combinadas. También se indican el factor de cresta actual y el equilibrio de fase (%).
3	Line	Muestra la corriente (en amperios RMS) en las unidades trifásicas en estrella. Esto no se muestra en las unidades monofásicas y trifásicas delta.
4	Residual Current	Solo para rPDU con la función RCM-B. Muestra los valores para Residual Current Aggregate (mA) y Residual Current DC (mA). Cuando sea pertinente, se debe mostrar la corriente residual para cada fase.
5	Monitor de corriente	Muestra las estadísticas de consumo de corriente alterna para cada circuito individual en la rPDU.
6	Monitor de salida	Se aplica SOLO a las rPDU de salida supervisada/salida conmutada: muestra las estadísticas de corriente alterna, voltaje y alimentación de cada circuito y salida. También se indica el factor de cresta actual (solo monitorización de alimentación de nivel de salida y monitorización de nivel de salida conmutada). Muestra el estado de salida (solo monitorización de alimentación de nivel de salida y monitorización de nivel de salida conmutada).
7	Icono de operación	Se aplica SOLO a las rPDU de salida supervisada/salida conmutada: modificar configuración.
8	Icono de configuración	Se aplica SOLO a las rPDU de salida supervisada/salida conmutada: modificar nombre de etiqueta.

**Para cambiar la etiqueta de un dispositivo:**

- Haga clic en el icono de configuración  para cambiar la etiqueta de la rPDU de Vertiv™ PowerIT y cambie la etiqueta. El nombre es el nombre de fábrica o el modelo de la rPDU y no se puede cambiar.
- Haga clic en **SAVE**.

Figura 5.16 Cambio de la etiqueta de un dispositivo



**Para cambiar la operación del dispositivo:**

1. Haga clic en el icono de operación
2. Seleccione la operación que desea realizar:
  - **On/Off:** activa o desactiva todas las salidas.
  - **Reboot:** para las salidas que están actualmente activadas, el reinicio desactiva las salidas y luego vuelve a activarlas después del retardo de espera de reinicio. Las salidas que actualmente estén desactivadas se activan al reiniciar.
  - **Cancel:** cancela la operación actual si no se ha completado.
  - **Reset Energy:** restablece la energía total medida en kWh.
  - **Restore Defaults:** restaura la configuración del dispositivo a sus valores predeterminados de fábrica. Esto incluye las etiquetas, los retardos y las acciones de encendido del dispositivo.

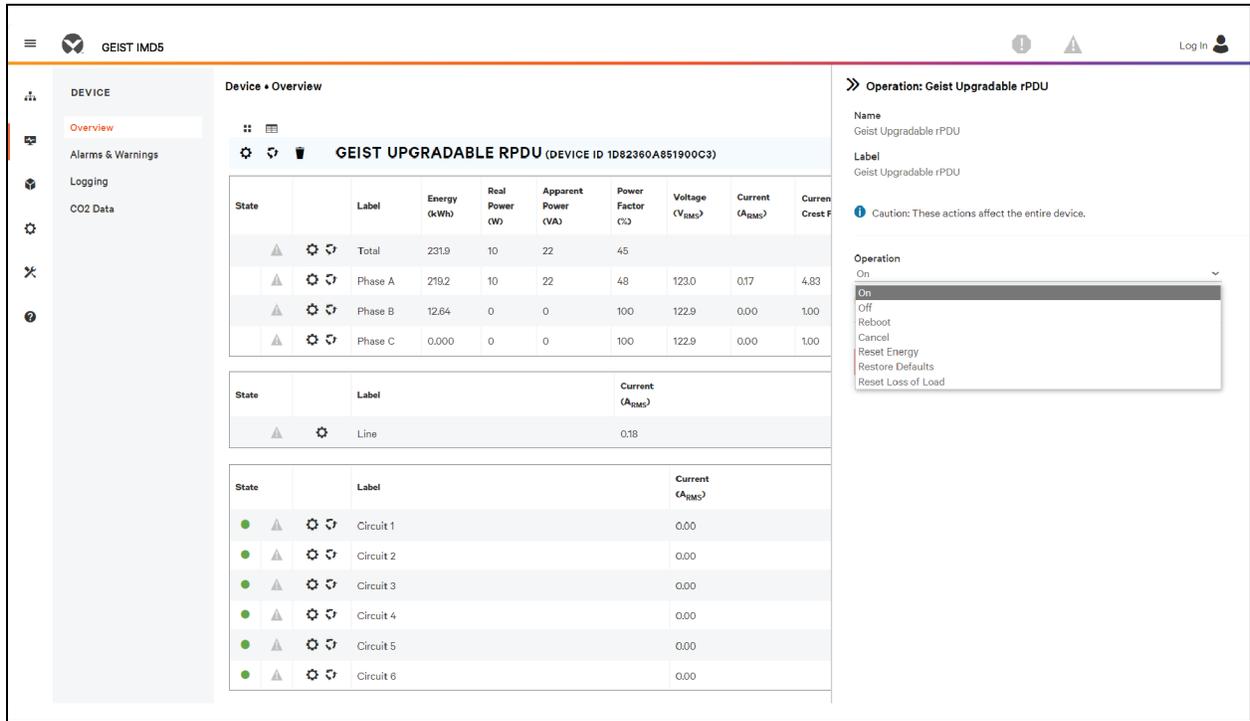
**NOTA:** Estas acciones afectan al dispositivo en su totalidad.

**NOTA:** Las operaciones de activación/desactivación y reinicio solo se aplican a las rPDU Vertiv™ PowerIT de salida conmutada.

3. Para las operaciones relacionadas con el estado de las salidas, al ajustar Delay en *True* se utiliza la configuración de retardo actual para cada salida al realizar la operación seleccionada.
4. Seleccione *SAVE* para iniciar la acción.

**NOTA:** Los retardos en la acción de encendido están relacionados con el tiempo transcurrido desde que se enchufó la unidad, no con el tiempo transcurrido desde que se completó el inicio. Se pueden ejecutar antes de que la unidad se inicie por completo.

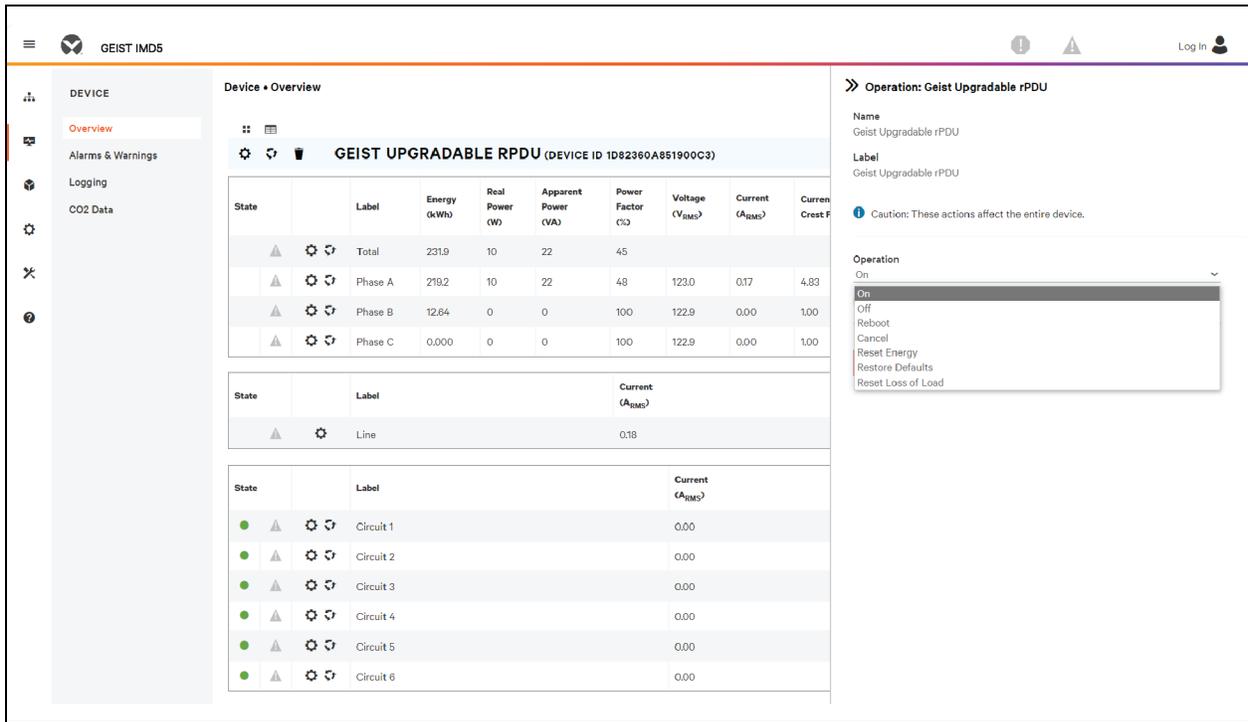
Figura 5.17 Cambio de operación del dispositivo



**Para cambiar una etiqueta de fase o circuito:**

1. Haga clic en el icono de configuración  de la fase o el circuito, y cambie la etiqueta. El nombre es la fase física o el nombre del circuito y no se puede cambiar.
2. Haga clic en *SAVE*.

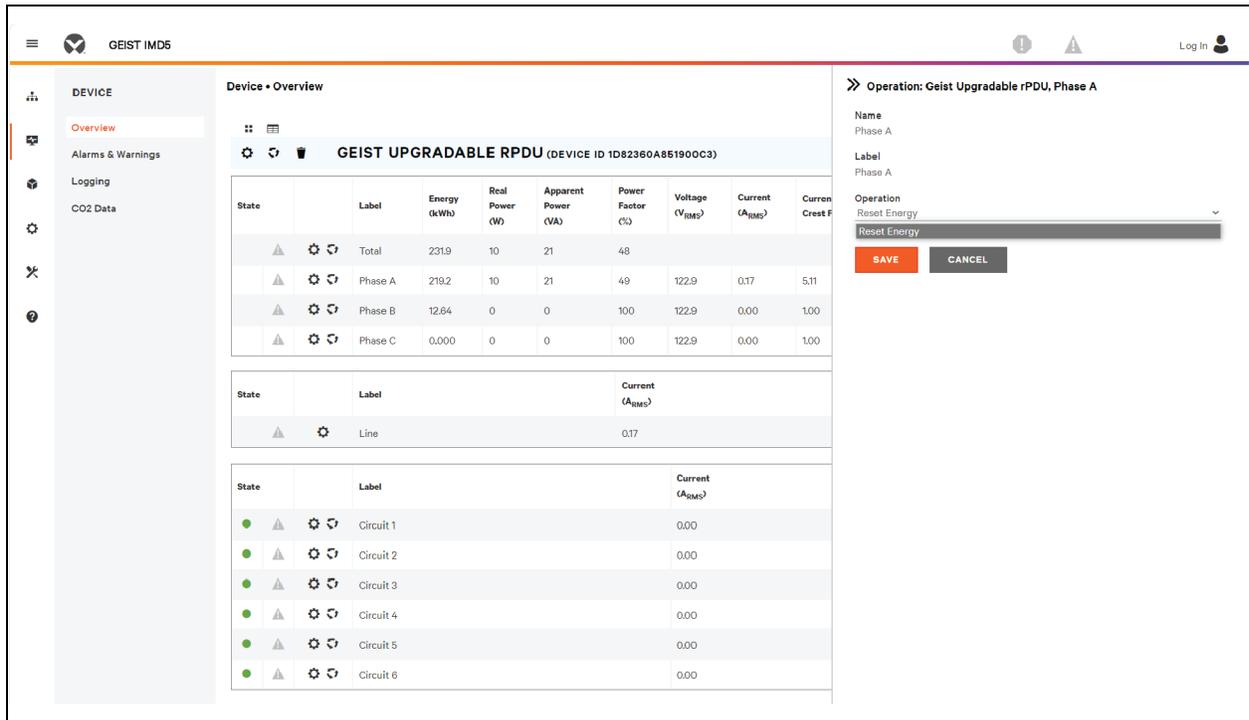
Figura 5.18 Cambio de una etiqueta de fase o circuito



**Para cambiar la operación de la fase:**

1. Haga clic en el icono de operación .
2. Seleccione *Reset Energy*, para restablecer la energía total medida en kWh para la fase seleccionada.
3. Seleccione *SAVE* para iniciar la acción.

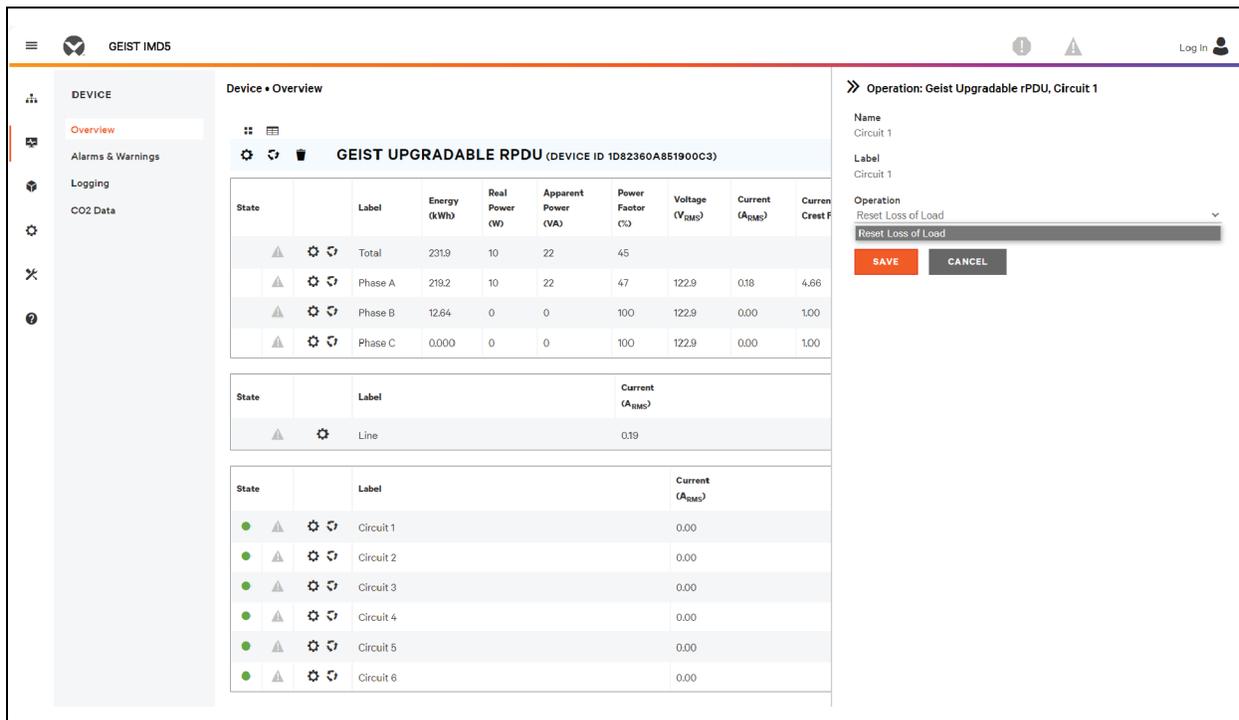
Figura 5.19 Cambio de la operación de la fase



**Para cambiar la operación del circuito:**

1. Haga clic en el icono de operación .
2. Seleccione *Reset Loss of Load* para restablecer la alarma de pérdida de carga.
3. Seleccione *SAVE* para iniciar la acción.

Figura 5.20 Cambio de la operación del circuito



**NOTA:** Este paso es necesario cuando la opción State muestra una alarma de pérdida de carga y el problema ya se ha resuelto. La alarma de pérdida de carga se activa por una caída repentina de corriente detectada por el transductor de medición de corriente del disyuntor cuando funciona cerca del límite de carga del circuito. Para las unidades horizontales conmutables actualizables, la alarma de pérdida de carga se activa adicionalmente por la pérdida de voltaje del disyuntor (independientemente de la carga del circuito).

Para configurar una salida:

**NOTA:** se aplica únicamente a las rPDU de Vertiv™ PowerIT de salida supervisada/salida conmutada.

1. Haga clic en el icono de configuración  de la salida.
2. Cambie la configuración, según sea necesario.
  - a. Etiqueta de la salida.

**NOTA:** Los pasos 2b a 2k se aplican solo a salidas conmutadas.

- b. **State:** el estado actual de la salida (On u Off).
- c. **Mode:** modo en que se controlará la salida:
  - **Manual Control:** el estado de salida se controla mediante la interfaz de usuario de web, SNMP o la API.
  - **Alarm Control (normalmente desactivado, se activa al activarse una alarma relacionada):** el estado de salida está normalmente desactivado y se activa cuando se active cualquier suceso de la alarma de la salida.

- **Alarm Control (normalmente activado, se desactiva al activarse una alarma relacionada):** el estado de salida está normalmente activado y se desactiva cuando se active cualquier suceso de la alarma de la salida.
  - **Alarm Control (normalmente desactivado, se activa al activarse todas las alarmas relacionadas):** el estado de salida está normalmente desactivado y se activa cuando se active cualquier suceso de la alarma de la salida.
  - **Alarm Control (normalmente activado, se desactiva al activarse todas las alarmas relacionadas):** el estado de salida está normalmente activado y se desactiva cuando se active cualquier suceso de la alarma de la salida.
- d. **Pending State:** estado al que está pasando la salida.
  - e. **Time To Action:** tiempo que queda antes de que se lleve a cabo la acción pendiente. Esto se ajusta con los retardos.
  - f. **On Delay:** el tiempo, en segundos, que la unidad espera antes de activar una salida.
  - g. **Off Delay:** el tiempo, en segundos, que la unidad espera antes de desactivar una salida.
  - h. **Reboot Delay:** el tiempo, en segundos, que la unidad espera antes de reiniciar una salida.
  - i. **Reboot Hold Delay:** el tiempo, en segundos, que la unidad espera después de apagar la salida antes de volver a encenderla durante un reinicio.
  - j. **Power-On Action:** define el estado en que se iniciará la salida cuando se encienda (On, Off o Last). De manera predeterminada, la configuración inicial es **Last** y las salidas están configuradas como ON de fábrica.
  - k. **Power-On Delay:** el tiempo, en segundos, que la unidad espera después del encendido antes de activar una salida.

3. Haga clic en **SAVE**.

**Figura 5.21 Configuración de la salida**

State	Label	Energy (kWh)	Real Power (W)	Apparent Power (VA)	Power Factor (%)	Voltage (V <sub>RMS</sub> )	Current (A <sub>RMS</sub> )
● ▲ ⚙️	Outlet 1	0.000	0	0	100	123.3	0.00
● ▲ ⚙️	Outlet 2	0.000	0	0	100	123.0	0.00
● ▲ ⚙️	Outlet 3	0.000	0	0	100	123.1	0.00
● ▲ ⚙️	Outlet 4	0.000	0	0	100	123.1	0.00
● ▲ ⚙️	Outlet 5	0.000	0	0	100	0.0	0.00
● ▲ ⚙️	Outlet 6	0.000	0	0	100	123.1	0.00
● ▲ ⚙️	Outlet 7	0.000	0	0	100	123.3	0.00
● ▲ ⚙️	Outlet 8	0.000	0	0	100	0.0	0.00
● ▲ ⚙️	Outlet 9	0.000	0	0	100	0.0	0.00
● ▲ ⚙️	Outlet 10	0.000	0	0	100	123.0	0.00
● ▲ ⚙️	Outlet 11	8.334	0	0	100	123.1	0.00
● ▲ ⚙️	Outlet 12	0.000	0	0	100	123.1	0.00
● ▲ ⚙️	Outlet 13	0.000	0	0	100	123.0	0.00
● ▲ ⚙️	Outlet 14	0.000	0	0	100	122.9	0.00
● ▲ ⚙️	Outlet 15	0.000	0	0	100	122.9	0.00
● ▲ ⚙️	Outlet 16	25.28	0	0	100	122.9	0.00
● ▲ ⚙️	Outlet 17	0.000	0	0	100	122.8	0.00
● ▲ ⚙️	Outlet 18	0.000	0	0	100	122.9	0.00
● ▲ ⚙️	Outlet 19	0.000	0	0	100	123.3	0.00

**Configuration: Geist Upgradable rPDU, Outlet 1**

Label: Outlet 1

State: On

Mode: Manual Control

Pending State: None

Time To Action: 0

Delays are in seconds.

On Delay: 5

Off Delay: 5

Reboot Delay: 5

Reboot Hold Delay: 10

Power-On Action: Last

Power-On Delay: 0.25

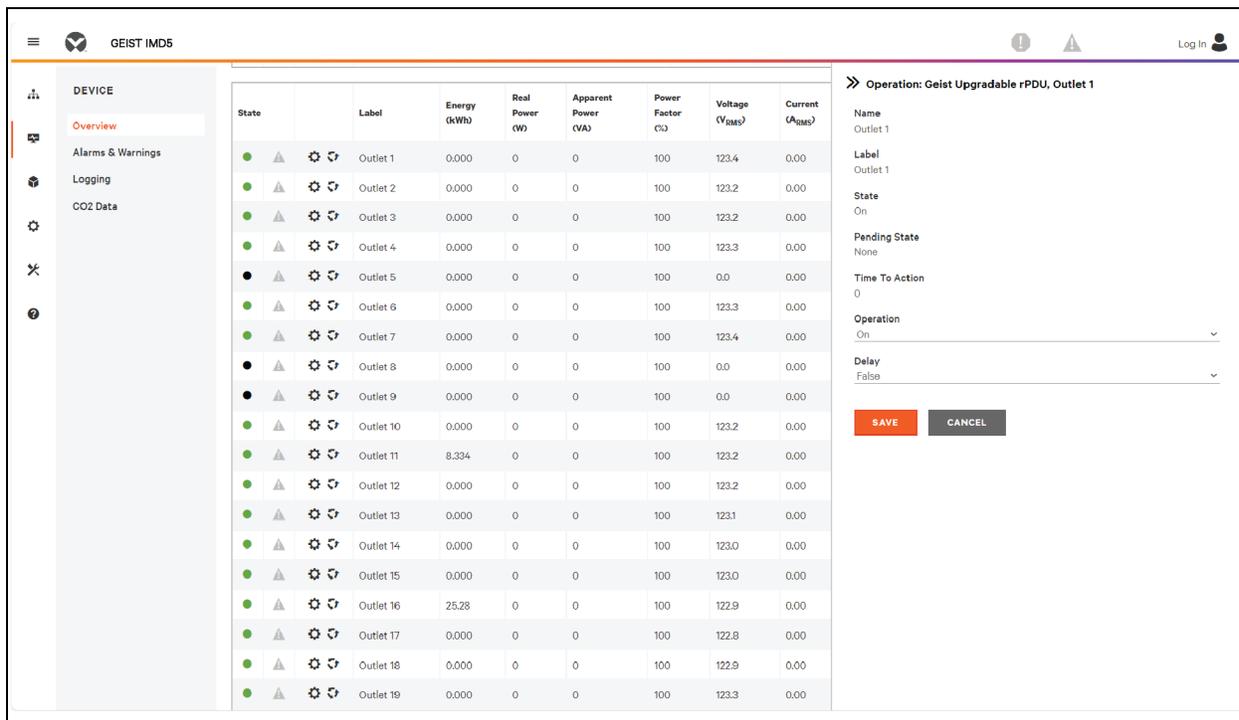
**SAVE** **CANCEL**

**Para cambiar la operación de la salida:**

**NOTA:** se aplica únicamente a las rPDU de Vertiv™ PowerIT de salida supervisada/salida conmutada.

1. Haga clic en el icono de operación  de la salida deseada.
2. Seleccione la operación que desea realizar:
  - **On/Off:** activa o desactiva la salida seleccionada.
  - **Reboot:** para las salidas que están actualmente activadas, el reinicio desactiva las salidas y luego vuelve a activarlas después del retardo de espera de reinicio. Las salidas que actualmente estén desactivadas se activan al reiniciar.
  - **Cancel:** cancela la operación actual si no se ha completado.
  - **Reset Energy:** restablece la energía total medida en kWh para la salida seleccionada.
3. Para las operaciones relacionadas con el estado de las salidas, al ajustar Delay en *True* se utiliza la configuración de retardo actual para cada salida al realizar la operación seleccionada.
4. Seleccione *SAVE* para iniciar la acción.

**Figura 5.22 Cambio de la operación de la salida**



### 5.4.2 Alarmas y advertencias

La página Alarms & Warnings permite establecer condiciones de alarma o de advertencia (sucesos) para cada lectura de alimentación y de circuito. Los sucesos se desencadenan cuando una medición supera un umbral definido por el usuario, ya sea porque asciende por encima del umbral (activación alta) o cae por debajo de él (activación baja). Los sucesos se muestran en diferentes secciones, según el dispositivo o la medición a la que se asocia el suceso. Cada suceso puede implicar llevar a cabo una o más acciones cuando este tiene lugar.

Figura 5.23 Página Alarms & Warnings

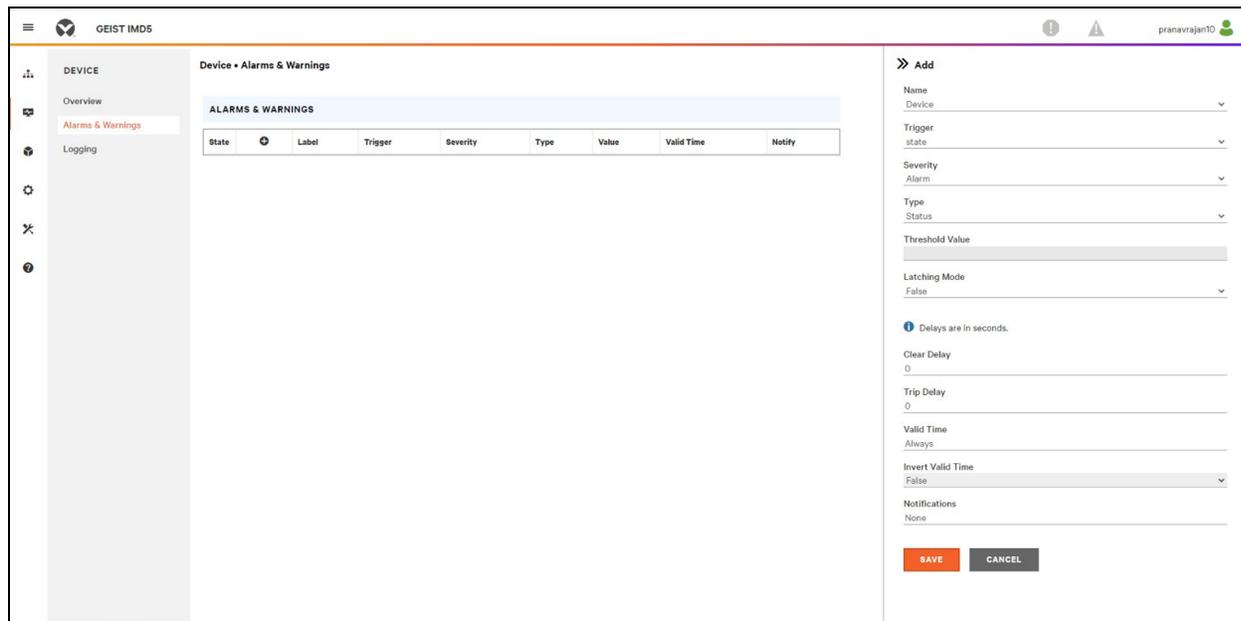


Tabla 5.9 Descripciones de Alarms & Warnings

Número	Descripción	Símbolo	Descripción
1	Estado de cada suceso.		Símbolo de advertencia. El suceso se muestra en naranja.
			Símbolo de alarma. La alarma se muestra en rojo.
			Símbolo de suceso confirmado. El símbolo permanece hasta que la condición medida vuelve a la normalidad.
2	Añadir/eliminar/modificar alarmas y advertencias.		Añadir nuevas alarmas y advertencias.
			Modificar alarmas y advertencias existentes.
			Eliminar alarmas y advertencias existentes.
3	Notificar al usuario sucesos activados y solicitar confirmación.	N/A	Vacío, si no hay una condición de alerta.
			Cuando se produce un suceso de advertencia o alarma, puede hacer clic en este símbolo para confirmar el suceso e impedir que la unidad envíe más notificaciones sobre el mismo. <b>NOTA: Al hacer clic en este símbolo, no se borra el suceso de advertencia o alarma; solo se evita que se repitan las notificaciones.</b>
4	Muestra las condiciones de la configuración de alarmas y advertencias.		

**Para añadir un nuevo suceso de alarma o advertencia:**

1. Haga clic en *Add/Modify Alarms* y en el botón *Warnings*.
2. Establezca las condiciones para este suceso de la siguiente manera:
  - a. En las listas desplegadas, seleccione el nombre de la fase o circuito, la medición de activación, la gravedad y el tipo.

**NOTA: Activaciones altas si la medición rebasa el umbral y activaciones bajas si la medición desciende por debajo del umbral.**

- b. Introduzca el valor de Threshold Value deseado (cualquier número entre -999,0 y 999,0).
- c. Introduzca el tiempo para Clear Delay deseado en segundos. Cualquier valor distinto de 0 significa que una vez que este suceso se active, la medición debe volver a la normalidad durante este número de segundos antes de que el suceso se borre y se restablezca. El valor para Clear Delay puede ser de hasta 14.400 segundos (4 horas).
- d. Introduzca el tiempo para Trip Delay deseado en segundos. Cualquier valor distinto de 0 significa que la medición debe superar el umbral durante este número de segundos antes de que el suceso se active. El valor para Trip Delay puede ser de hasta 14.400 segundos (4 horas).
- e. Latching Mode, si está habilitado, este suceso y sus acciones asociadas permanecen activos hasta que se confirme el suceso, incluso si la medición vuelve posteriormente a la normalidad.
- f. Para especificar dónde se envían las notificaciones de alerta cuando se produce este suceso de alarma o alerta, haga clic en el icono de añadir para crear una nueva acción.
- g. Seleccione una de las opciones que desee en el menú desplegable:
  - El campo Target es la dirección de correo electrónico o el administrador de SNMP donde se envían las notificaciones cuando el suceso se activa. Para obtener más información sobre cómo configurar una dirección de correo electrónico de destino, consulte [Email](#) en la página 90.
  - O bien, cuando se selecciona un número de salida como objetivo, el estado de salida cambia cuando se activa un suceso y permanece en el estado de cambio hasta que el suceso se reinicia o se reconoce. En el caso de esta opción, el modo de salida debe estar configurado para el control de la alarma, consulte [Alarmas y advertencias](#) en la página 55.

**NOTA: Los valores de Target, Delay y Repeat se comparten en todas las alarmas. Si se necesitan varios valores de Delay o Repeat para objetivos específicos, cada uno de ellos se debe añadir a la lista de Target y luego se debe marcar la casilla correspondiente como Enabled en cada alarma.**

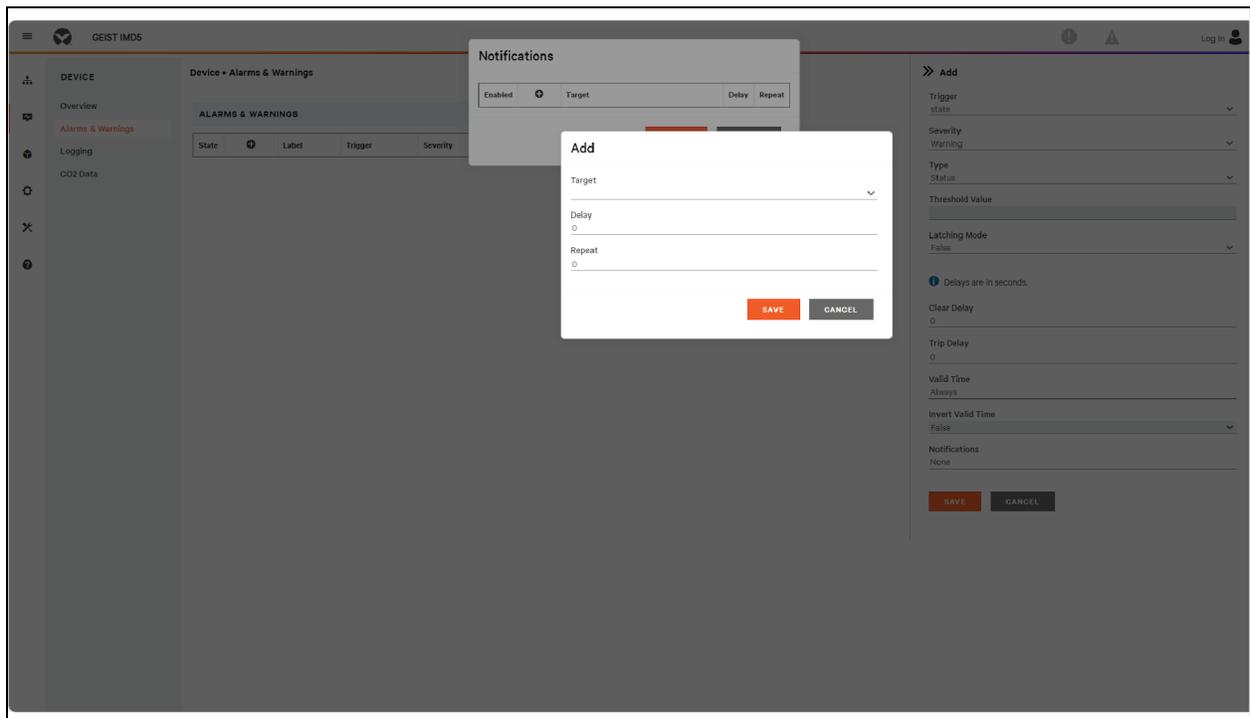
**NOTA: se aplica únicamente a las rPDU de salida supervisada/salida conmutada de Vertiv™ PowerIT.**

- El campo Delay determina el tiempo durante el que este suceso debe permanecer activado antes de que se envíe la primera notificación de esta acción. Este valor es distinto del valor de Trip Delay anterior. El campo Trip Delay determina el tiempo durante el que se debe superar el valor umbral antes de que se active el suceso en sí. Este retardo determina el tiempo durante el que el suceso debe permanecer activado antes de que tenga lugar esta acción. El retardo puede ser de hasta 14.400 segundos (4 horas). Un retardo de 0 enviará la notificación inmediatamente.

- El campo Repeat determina si se enviarán varias notificaciones para esta acción. Las notificaciones repetidas se envían a los intervalos especificados hasta que el suceso se confirme o hasta que el suceso se borre y se restablezca. El intervalo para Repeat puede ser de hasta 14.400 segundos (4 horas). Un valor de 0 deshabilita esta característica y solo se envía una notificación.
3. Haga clic en **SAVE** para guardar esta acción de notificación.

**NOTA:** Se puede configurar más de una acción para una alarma o advertencia. Para añadir varias acciones, solo hay que hacer clic de nuevo en el icono de añadir y establecer cada una como se desee. Cada alerta puede tener hasta 32 acciones asociadas.

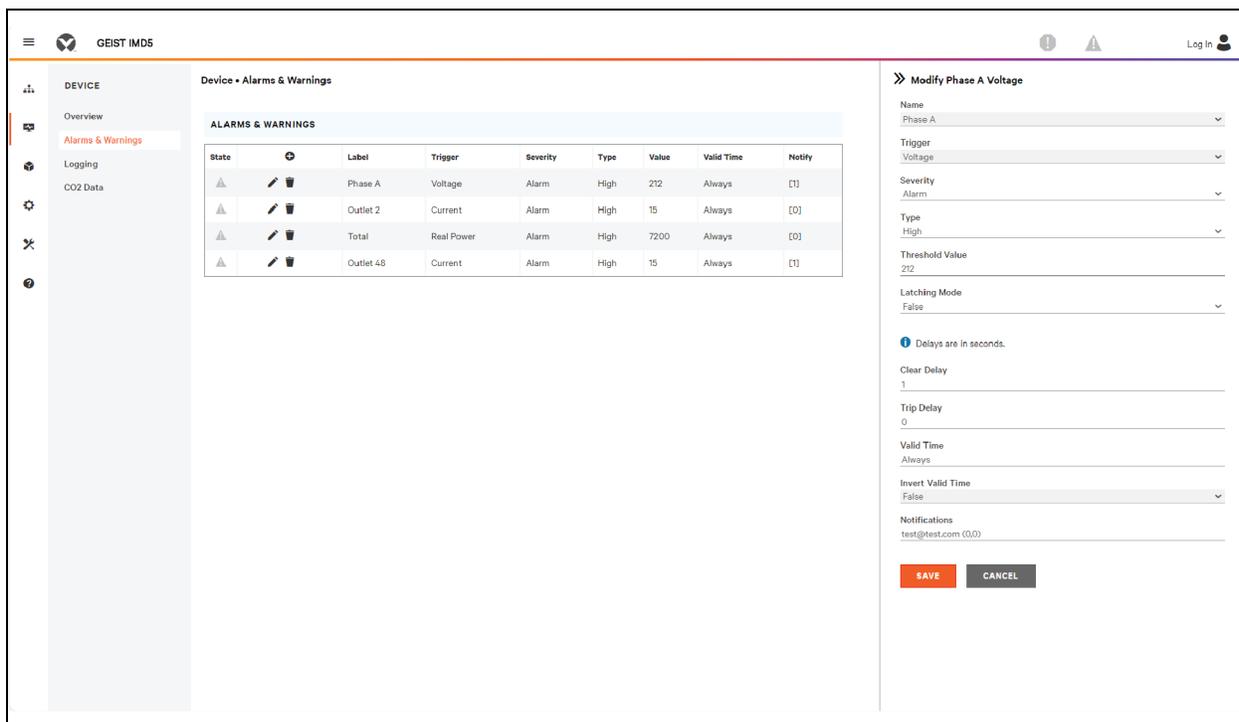
**Figura 5.24** Ventana Add de Alarms & Warnings



**Para cambiar una alarma o un suceso de advertencia existente:**

1. Haga clic en el icono de modificar situado junto al suceso de alarma o advertencia que desee cambiar.
2. Modifique la configuración según sea necesario y haga clic en **SAVE**.
3. Después de añadir una acción, esta tiene una casilla de verificación en la columna de habilitado en el extremo izquierdo. De forma predeterminada, cuando se agrega una acción, esta está sin marcar (deshabilitada). Haga clic en la *casilla de verificación* para habilitarla. Esto permite activar y desactivar selectivamente distintas acciones para probarlas.

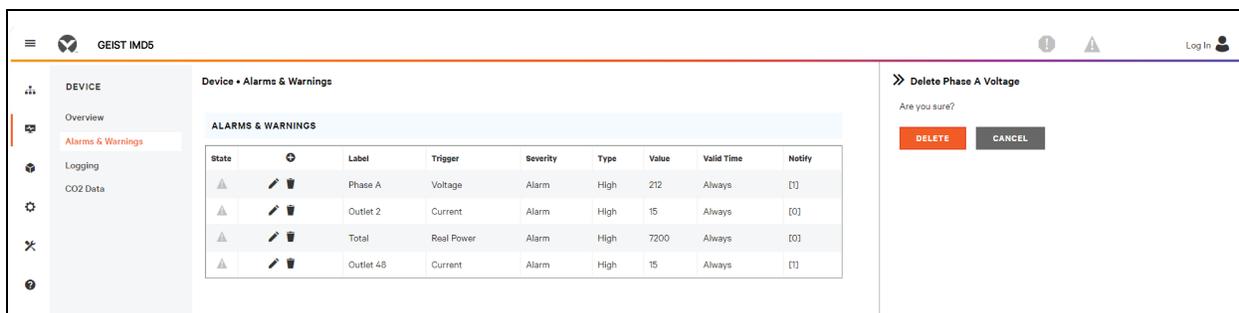
**Figura 5.25 Cambio de la ventana Alarms & Warnings**



**Para eliminar una alarma o un suceso de advertencia existente:**

1. Haga clic en el icono de eliminar situado junto al suceso de alarma o advertencia que desee quitar.
2. Haga clic en **DELETE** y **SAVE** para confirmar.

**Figura 5.26 Eliminación del suceso Alarms & Warning**



### 5.4.3 Logging

La página Logging permite acceder a los datos históricos registrados por la rPDU de Vertiv™ PowerIT; para ello, es necesario seleccionar los sensores y el intervalo de tiempo deseados para su registro. La página Logging permite seleccionarlo todo o no seleccionar nada.

**Para seleccionar o anular la selección del valor de medición:**

1. Haga clic en el icono de dispositivo y en el submenú Logging.
2. En la página Logging, haga clic en *Select All* para seleccionar el valor de medición y haga clic en *Select None* para anular la selección del valor de medición.

**Figura 5.27** Página Logging

The screenshot shows the 'Device + Logging' page in the GEIST IMDS interface. It features a 'DATA LOG' section with a dropdown menu for downloading logs (set to '.JSON'), a 'SUBMIT' button, a warning about clearing logs when the interval changes, a 'Log Interval (minutes)' field set to '15', a 'SAVE' button, and a 'CLEAR THE LOG' button. Below this is the 'LOGGING' section, which includes a 'SAVE' button, a device name 'GEIST UPGRADABLE RPDU (DEVICE ID FE394028990200C3)', and two data tables. The first table shows Phase A data, and the second table shows Circuit 1 data. Both tables have columns for Energy (kWh), Real Power (W), Apparent Power (VA), Power Factor (CF), Voltage (V<sub>RMS</sub>), Current (A<sub>RMS</sub>), Current Crest Factor, and Balance (CF). The 'Circuit 1' table also includes a 'Current (A<sub>RMS</sub>)' column.

Label	Energy (kWh)	Real Power (W)	Apparent Power (VA)	Power Factor (CF)	Voltage (V <sub>RMS</sub> )	Current (A <sub>RMS</sub> )	Current Crest Factor	Balance (CF)
Phase A	88.864	4	9	48	125.1	0.07	4.07	100

Label	Current (A <sub>RMS</sub> )
Circuit 1	0.00

Label	Energy (kWh)	Real Power (W)	Apparent Power (VA)	Power Factor (CF)	Voltage (V <sub>RMS</sub> )	Current (A <sub>RMS</sub> )	Current Crest Factor
Outlet 1	0.047	0	0	100	120.7	0.00	1.00
Outlet 2	1.386	0	0	100	120.7	0.00	1.00
Outlet 3	0.001	0	0	100	120.7	0.00	1.00
Outlet 4	0.023	0	0	100	120.7	0.00	1.00
Outlet 5	0.000	0	0	100	120.7	0.00	1.00
Outlet 6	0.087	0	0	100	120.6	0.00	1.00

**Tabla 5.10 Descripciones de la página Logging**

Elemento	Nombre	Descripción
1	Download the data log	Haga clic en el menú desplegable y seleccione una de las opciones: <i>JSON</i> para el formato <i>JSON</i> . <i>CSV</i> para el formato <i>.csv</i> en el programa de hoja de cálculos. Haga clic en el botón <i>SUBMIT</i> para descargar el registro de datos.
2	Log interval	Frecuencia con la que se escriben los datos en el archivo de registro. El intervalo de registro puede ser de 1 a 600 minutos; el ajuste predeterminado es de 15 minutos.  <b>¡ADVERTENCIA! Los datos de registro se eliminarán permanentemente.</b>
3	Clear the log	Para eliminar el archivo de registro.  <b>¡ADVERTENCIA! Los datos de registro se eliminarán permanentemente.</b>
4	Select All/Select None	Haga clic en <i>Select All</i> para seleccionar el valor de medición y haga clic en <i>Select None</i> para anular la selección del valor de medición.
5	Logging	Haga clic en el valor de medición para seleccionar o anular la selección de los parámetros de registro deseados. De forma predeterminada, se seleccionan todas las mediciones. Haga clic en <i>SAVE</i> para guardar los cambios.

**NOTA:** El periodo de tiempo de registro máximo está determinado por el número de mediciones que se registran y el intervalo en el que se escriben los datos en el archivo de registro.

## 5.4.4 CO2 Data

Figura 5.28 Página de inicio de CO2

The screenshot shows the 'CO2 Data' page for a GEIST IMD5 device. The page includes a sidebar with navigation options: Overview, Alarms & Warnings, Logging, and CO2 Data (highlighted). The main content area displays the device name 'GEIST UPGRADABLE RPDU (DEVICE ID D792850A851900C3)' and two tables of CO2 data.

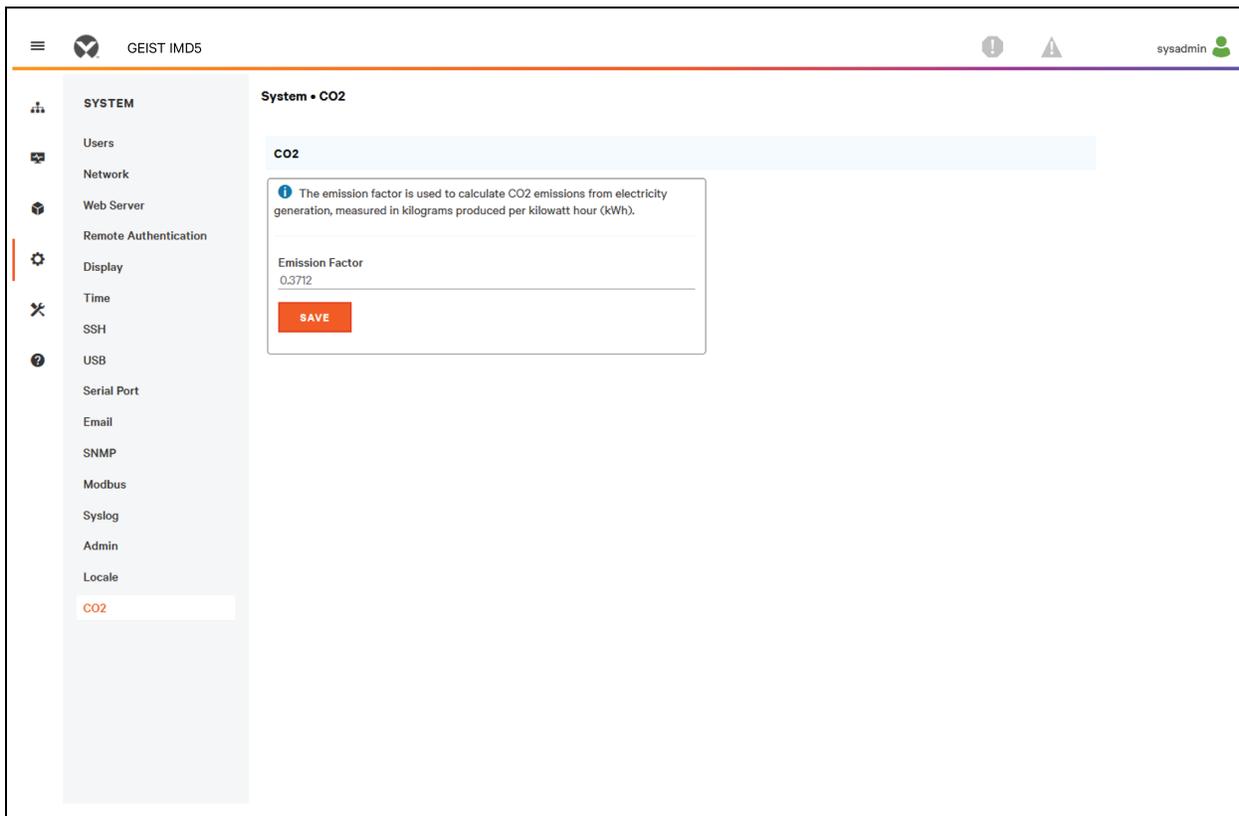
**Table 1: Phase A CO2 Data**

Label	Accumulated CO2 (kg)	Instantaneous CO2 (kg/h)
Phase A	0.826	0.002

**Table 2: Outlet CO2 Data**

Label	Accumulated CO2 (kg)	Instantaneous CO2 (kg/h)
Outlet 1	0.000	0.000
Socket B	0.000	0.000
Outlet 3	0.000	0.000
Outlet 4	0.000	0.000
Outlet 5	0.000	0.000
Outlet 6	0.000	0.000
Outlet 7	0.000	0.000
Outlet 8	0.000	0.000
Outlet 9	0.000	0.000
Outlet 10	0.000	0.000
Outlet 11	0.000	0.000
Outlet 12	0.403	0.000

Figura 5.29 Pestaña System de CO2



**NOTA:** Hay tres páginas asociadas con la página CO2. La primera página es la página de datos de CO2 en Device (Figura 5.28 en la página anterior), que muestra los cálculos acumulados e instantáneos para las fases y las salidas. La segunda es la página CO2 en System donde usted configura la opción Emission Factor para calcular el CO2 por kWh. El factor de emisión de CO2 predeterminado se configurará a 0.3712. La tercera página está en la página de información de ayuda; el periodo de duración del CO2 se basa en el periodo de duración de la energía. Si un usuario restablece el uso de energía de una PDU o una salida específica, el valor volverá a 0. No obstante, el periodo de duración de la energía de ese componente no volverá a 0.

## 5.5 Submenú Provisioner

El submenú Provisioner permite que el usuario detecte las rPDU de Vertiv™ PowerIT conectadas localmente. El usuario puede cargar un archivo de configuración para actualizar su firmware y configurarlo.

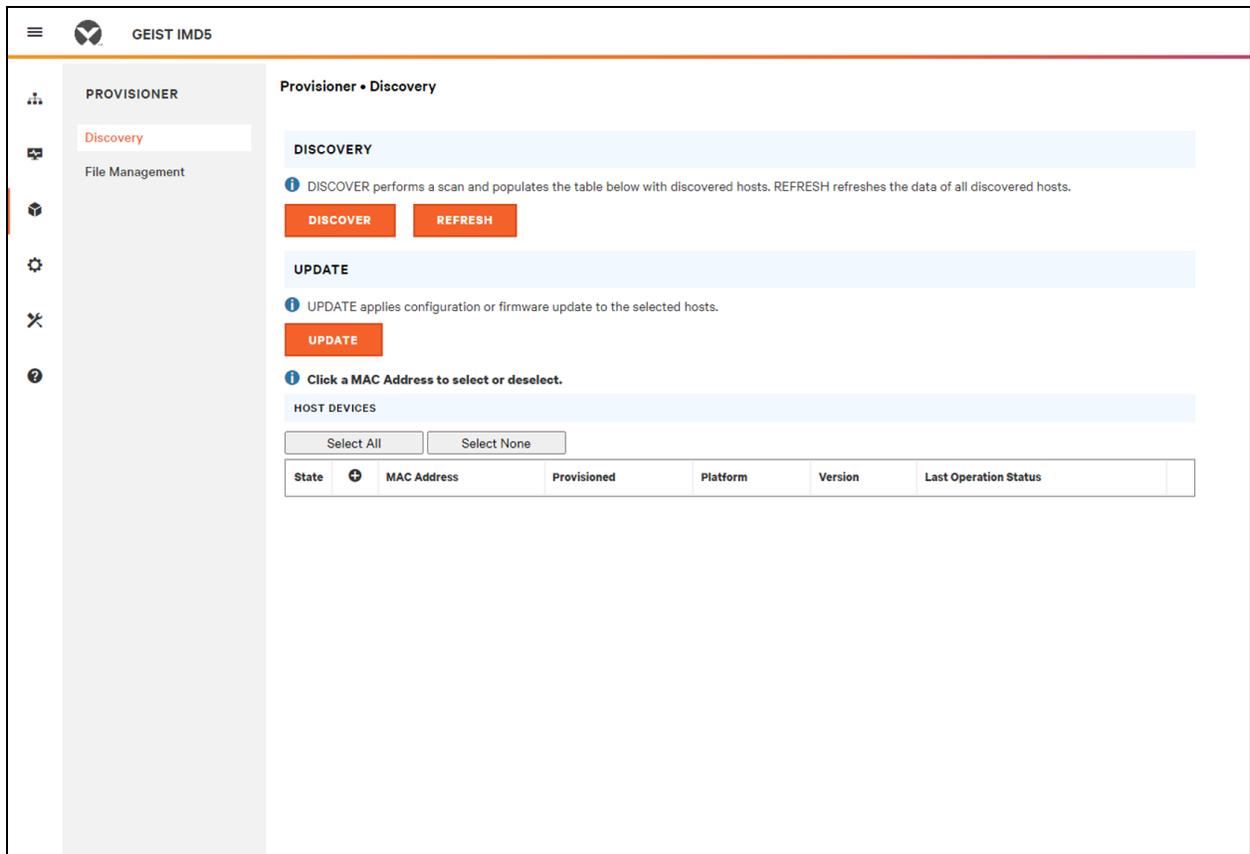
El submenú Provisioner ofrece la capacidad de configurar los ajustes del dispositivo (por ejemplo, alarmas) y los ajustes del sistema. Esta funcionalidad puede aprovisionar:

- IMD-5M que ejecuten el firmware 6.x.x.
- rPDU que ejecuten el firmware 5.x.x (modelos de IMD 3E, 03E, 3E-S y 03E-S)
- rPDU Vertiv™ PowerIT nuevas de fábrica o previamente configuradas con 6.1.0.
- PDU para rack conectadas directamente a la red local o conectadas como parte de una red de Vertiv Intelligence Director (agregación).

- Todas las rPDU Vertiv™ PowerIT o algunas de las que se han detectado.

**NOTA:** Debe haber iniciado sesión como usuario de nivel de administrador para poder usar la opción Provisioner. IPV6 debe estar activado en el rPDU Vertiv™ PowerIT que se está descubriendo. Es posible configurar la mayoría de los elementos en el menú de la interfaz de usuario System. Otros ajustes, como la configuración de los sensores y las alarmas, no se pueden configurar con esta versión de la herramienta de aprovisionamiento.

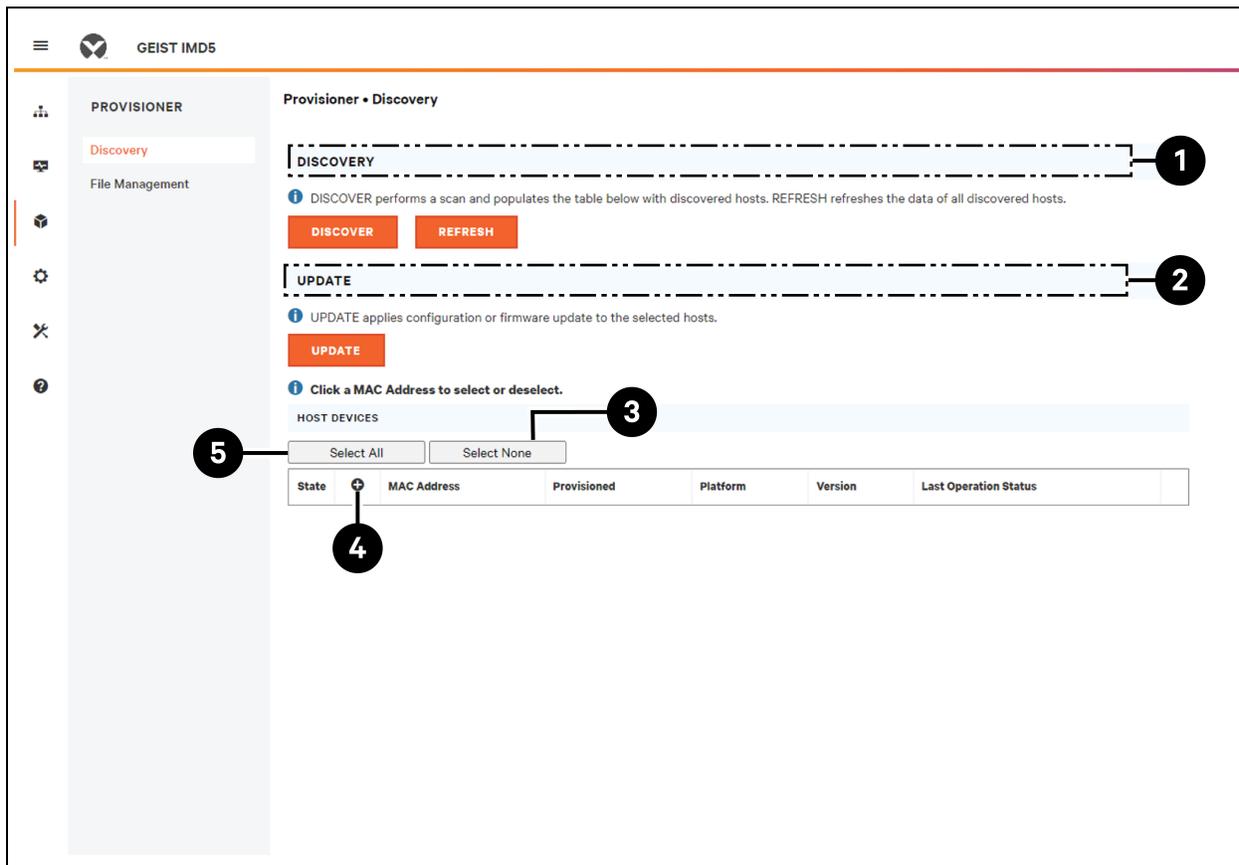
Figura 5.30 Página del submenú Provisioner



## 5.5.1 Discovery

1. Haga clic en *DISCOVER* para identificar las rPDU Vertiv™ PowerIT conectadas localmente.
2. Haga clic en todas las rPDU Vertiv™ PowerIT de la lista para las que desee actualizar el firmware y/o la configuración. Las unidades seleccionadas aparecerán resaltadas de color verde. También puede hacer clic en la opción *Select All* para actualizar todas las rPDU Vertiv™ PowerIT que aparecen en la lista.
3. Haga clic en *UPDATE* para actualizar todas las rPDU Vertiv™ PowerIT seleccionadas con el archivo de firmware y/o el archivo de configuración.

Figura 5.31 Discovery



Número	Nombre	Descripción
1	Discover	Identifica las PDU para rack locales y conectadas a la red
2	Update	Actualiza el firmware y/o la configuración de las rPDU seleccionadas
3	Select None	Seleccione ninguno para cancelar todas las selecciones
4	Add MAC address	Permite añadir la rPDU de forma manual por su dirección MAC
5	Select All	Selecciona todas las rPDU conectadas

**NOTA:** Debe cargar los archivos de firmware y de configuración antes de realizar este paso en la pestaña File Management.

## 5.5.2 File management

Firmware Files:

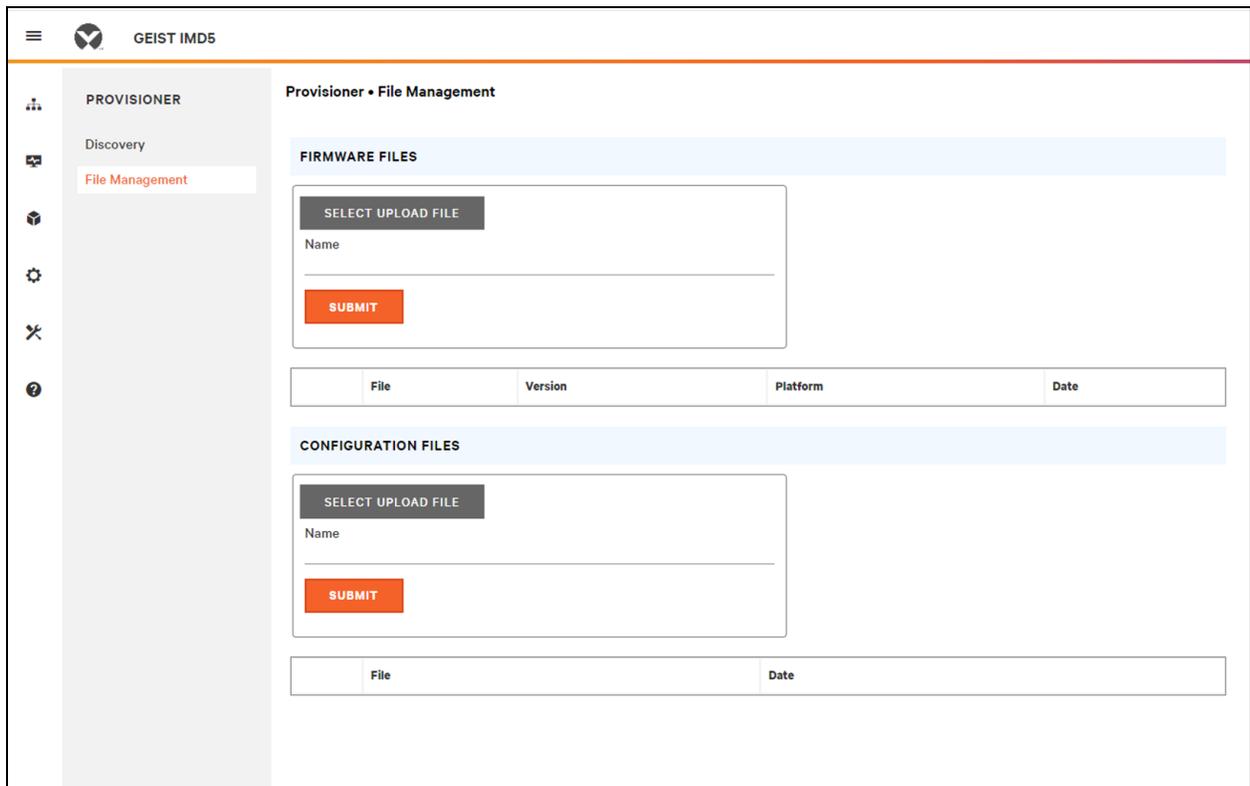
1. Haga clic en *SELECT UPLOAD FILE* y seleccione *.firmware file* en la ventana Open.
2. Haga clic en *SUBMIT*. El archivo del firmware aparecerá en la lista.

Configuration Files:

1. Haga clic *SELECT UPLOAD FILE* y seleccione *.config file* en la ventana Open.

2. Haga clic en *SUBMIT*. El archivo de configuración aparecerá en la lista.

**Figura 5.32** Página File Management



Consulte [Aprovisionador: formato del archivo de ajustes de configuración](#) en la página 133 para ver ejemplos de archivos de ajustes de configuración usados por el aprovisionador y el formato necesario para el archivo.

## 5.6 Submenú System

**NOTA:** Debe haber iniciado sesión como administrador para modificar la configuración de la pestaña System.

### 5.6.1 Users

La página Users en el menú System permite gestionar o restringir el acceso a las funciones de la unidad mediante la creación de cuentas para diferentes usuarios.

**NOTA:** Política de bloqueo de cuenta Web/SSH/CLI: una cuenta se bloquea durante 30 minutos tras realizar 10 intentos de inicio de sesión consecutivos sin éxito en un plazo de 60 minutos. Se puede editar con la última versión del firmware.

El ámbito permite que una cuenta de nivel de administrador restrinja los usuarios a la visibilidad de la información de la salida especificada.

Figura 5.33 Página Users

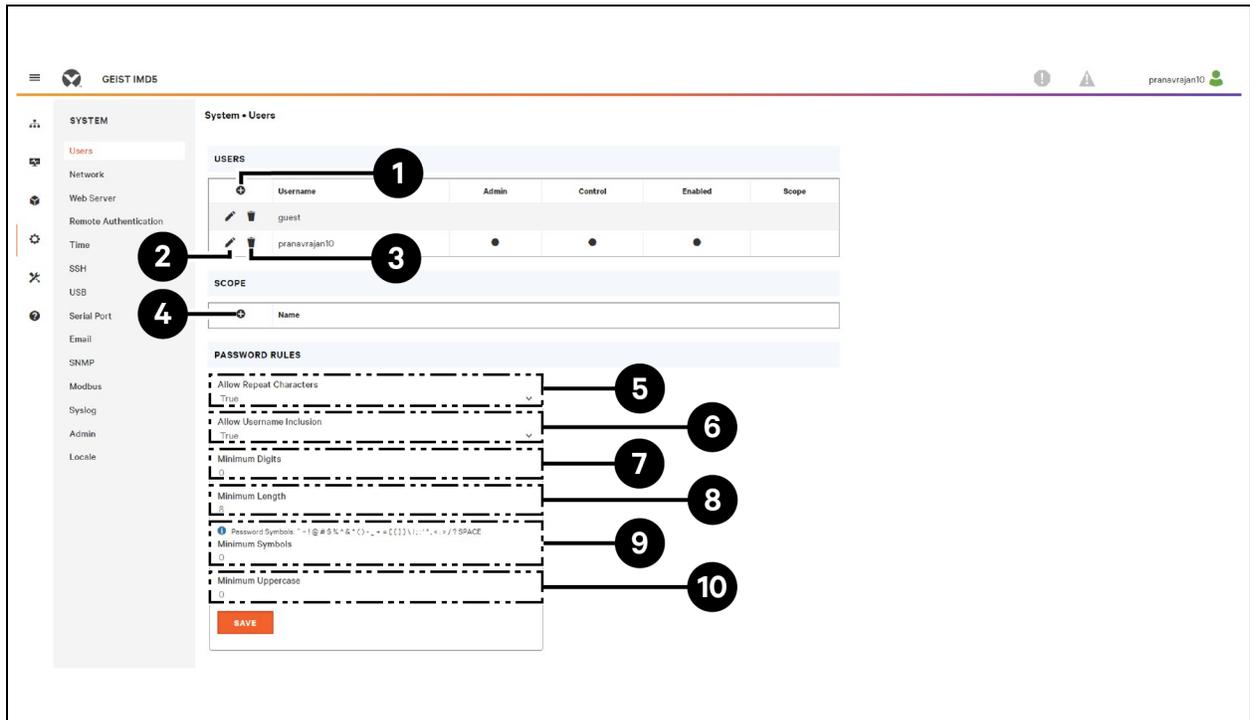


Tabla 5.11 Descripciones de la página Users

Número	Descripciones
1	Añadir nueva cuenta de usuario
2	Modificar cuenta de usuario
3	Eliminar cuenta de usuario
4	Añadir un ámbito de usuario: Solo es visible cuando se ha iniciado sesión como administrador*
5	Allow Repeat Characters: restrinja el uso de más de 2 caracteres repetidos (el valor predeterminado es false)*
6	Allow Username Inclusion: restrinja la inclusión del nombre de usuario en la contraseña (el valor predeterminado es false)*
7	Minimum Digits: introduzca los caracteres de dígitos numéricos mínimos (el valor predeterminado es 0)*
8	Minimum Length: introduzca el número mínimo de caracteres de la contraseña (el valor predeterminado es 8 y el mínimo es 6)*
9	Minimum Symbols: introduzca los caracteres de símbolos mínimos (el valor predeterminado es 0)*
10	Minimum Uppercase: introduzca los caracteres de mayúsculas mínimos (el valor predeterminado es 0)*

**NOTA:** \*Solo es visible cuando se ha iniciado sesión como administrador.

**NOTA: Solo una cuenta de nivel de administrador permite añadir, modificar o eliminar usuarios, además de añadir, modificar o eliminar ámbitos. Las cuentas de nivel de control y solo visualización permiten cambiar sus propias contraseñas mediante el icono de modificar usuario, pero no pueden añadir, eliminar ni modificar otras cuentas. La cuenta de invitado no permite añadir, eliminar o modificar ninguna cuenta, ni siquiera la propia.**

**Para añadir o modificar una cuenta de usuario:**

1. Haga clic en el icono de añadir o modificar usuario.
2. Cree o modifique la información de la cuenta según sea necesario.
  - a. **Username:** el nombre de la cuenta. Los nombres de usuario pueden tener un máximo de 24 caracteres, distinguen entre mayúsculas y minúsculas, y no pueden contener espacios ni ninguno de estos caracteres prohibidos: \$& ` :<> [ ] { } "+%@/ ; =? \ ^ | ~ ' ,

**NOTA: No se puede cambiar un nombre de usuario después de crear la cuenta.**

- b. **Administrator:** si se establece en *True*, esta cuenta tiene acceso de nivel de administrador a la unidad y puede cambiar cualquier configuración.
  - c. **Control:** si se establece en *True*, esta cuenta tiene acceso de nivel de control. Si el administrador se establece en *True*, el control también se establecerá automáticamente en *True*. Si se establece en *False*, la cuenta pasa a ser una cuenta habilitada, que es de solo visualización.
  - d. **Scope:** si se ha creado un ámbito de usuario, seleccione el ámbito aplicable a la cuenta. Consulte el paso [Para añadir o modificar un ámbito de usuario:](#) en la página opuesta.
  - e. **New Password:** los nombres de usuario pueden tener un máximo de 24 caracteres, distinguen entre mayúsculas y minúsculas, y no pueden contener espacios.
  - f. **Account Status:** establezca la cuenta en *Enabled* o *Disabled*. Al deshabilitar una cuenta, se impide que se utilice para iniciar sesión, pero no se elimina de la lista de cuentas.
3. Haga clic en *SAVE*.

## Tipos de cuentas de usuario

- **Administrator:** las cuentas de administrador (cuentas en las cuales tanto la autoridad de administrador como la autoridad de control están establecidas en *True*, como se ha indicado anteriormente) tienen un control total sobre todas las funciones y configuración disponibles en el dispositivo, incluida la capacidad de modificar la configuración del sistema y de añadir, modificar o eliminar las cuentas de otros usuarios.
- **Control:** las cuentas de control (cuentas con solo control establecido en *True*) tienen el control de todos los ajustes pertenecientes a los sensores del dispositivo. Pueden añadir, modificar o borrar alarmas y sucesos de advertencia y acciones de notificación, y pueden cambiar los nombres o etiquetas del dispositivo y sus sensores. Las cuentas de control no pueden modificar la configuración del sistema ni hacer cambios en las cuentas de otros usuarios.
- **View-Only:** si Administrator y Control están establecidos en *False*, la cuenta es una cuenta habilitada, que es de solo visualización. Los únicos cambios que se le permiten a una cuenta de solo visualización son el cambio de la contraseña de su propia cuenta y el cambio del idioma de preferencia para su propia cuenta. Las cuentas de solo visualización no pueden cambiar la configuración de ningún dispositivo o sistema.

- **Guest:** cualquier usuario que vea la página web de la unidad sin iniciar sesión en ella, la verá automáticamente como invitado. De forma predeterminada, la cuenta Guest es una cuenta de solo visualización y no puede realizar cambios en ningún ajuste. Esta cuenta no permite cambios en los nombres, etiquetas, eventos de alarma y notificaciones. La cuenta Guest no se puede eliminar, pero se puede desactivar, lo que obligaría al usuario a iniciar sesión para ver el estado del sistema.

**Para cambiar una contraseña de usuario:**

1. Inicie sesión en su cuenta.
2. Haga clic en el icono de modificar usuario.
3. Haga clic en Username, en la esquina superior derecha de la página.
4. Introduzca una contraseña nueva y verifíquela introduciéndola en el campo Verify Password.
5. Haga clic en *SAVE*.

**Figura 5.34** Página de cambio de contraseña del usuario

The screenshot shows a web interface titled 'Modify' with a double arrow icon. It contains several form fields and a table:

- Username:** A text input field.
- Administrator:** A dropdown menu with 'True' selected.
- Control:** A dropdown menu with 'True' selected.
- Scope:** A dropdown menu with '--' selected.
- New Password:** A text input field.
- Verify Password:** A text input field.
- Account Status:** A dropdown menu with 'Enabled' selected.
- Language Preference:** A dropdown menu with 'English' selected.
- SSH Public Key:** A table with columns for adding a key, a label, and the key itself.
 

	Label	SSH Public Key
+		

At the bottom, there are two buttons: a red 'SAVE' button and a grey 'CANCEL' button.

**Para añadir o modificar un ámbito de usuario:**

1. Haga clic en el icono de añadir o modificar ámbito. Consulte la **Figura 5.35** en la página siguiente.

2. Cree o modifique la información del ámbito según sea necesario.
  - a. **Label:** introduzca el nombre deseado para el ámbito seleccionado.
  - b. **Remote Authentication Attribute:** se usa para todos los tipos de autenticación remota.
  - c. Haga clic en las salidas aplicables para un usuario especificado (resaltado en verde).
3. Haga clic en *OK* para guardar los cambios.

Figura 5.35 Añadir ámbito

SCOPE	
+	Name

## Normas de la contraseña y ajustes de la política de cuentas

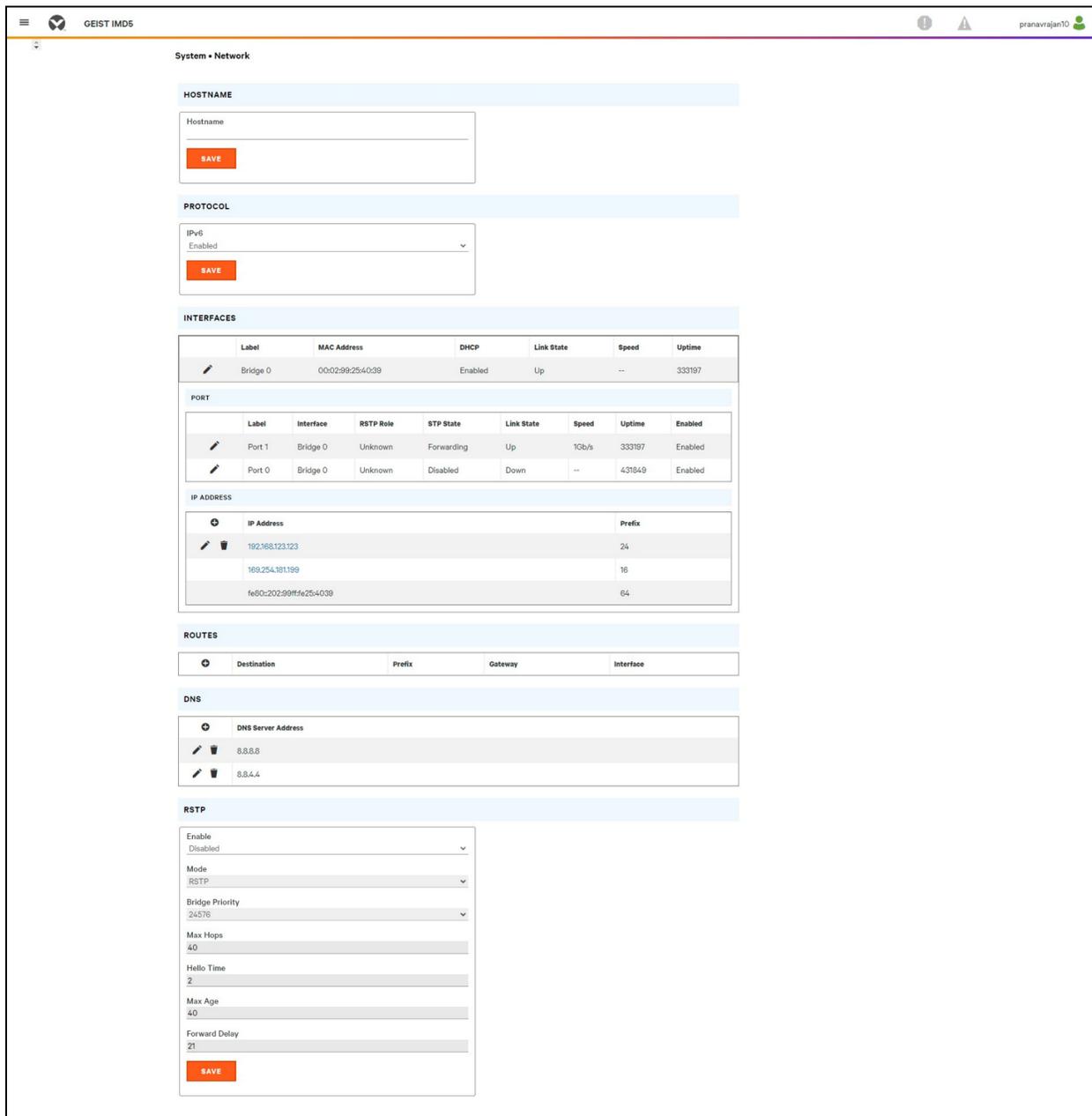
**NOTA:** La sesión de un usuario se cerrará automáticamente tras 10 minutos de inactividad.

### 5.6.2 Network

La configuración de red de la unidad se establece en la pestaña *Network* del menú *System*. La configuración correspondiente a la conexión de red de la unidad es:

- **Hostname:** el nombre del host se puede utilizar como método de identificación del dispositivo en la red.
- **Protocol:** haga clic en el menú desplegable de IPv6, seleccione *Enabled* o *Disabled* y haga clic en *Save*.
- **Interfaces:** se utiliza para configurar la dirección IP de la rPDU Vertiv™ PowerIT, habilitar/deshabilitar el DHCP y ver el estado del enlace y el tiempo de funcionamiento. El dispositivo admite hasta ocho entradas de direcciones IP configuradas por el usuario.
- **Ports:** Se utilizan para ver y/o modificar las siguientes configuraciones de puerto Ethernet: etiqueta, interfaz, rol RSTP, estado del RSTP, estado del STP, estado del enlace, velocidad, tiempo de funcionamiento y habilitar/deshabilitar.
- **IP Address:** se utiliza para añadir o modificar las direcciones IP.
- **Routes:** muestra las rutas configuradas y es aquí donde configurará la dirección de la puerta de enlace para la rPDU Vertiv™ PowerIT. Las rutas predeterminadas se distinguen porque tienen los siguientes valores: para *destination* es **0.0.0.0** o **::**, para *Prefix* es **0** y para *Interface* es **all**. Solo puede haber una ruta predeterminada para IPv4 y otra para IPv6.
- **DNS:** permite a la unidad resolver nombres de host para los servidores de correo electrónico, **NTP** y **SNMP**.
- **RSTP:** se utiliza para ver y modificar el estado del RSTP, *Mode*, *Bridge Priority*, *Max Hops*, *Hello Time*, *Max Age* y *Forward Delay*.

Figura 5.36 Página de configuración de Network

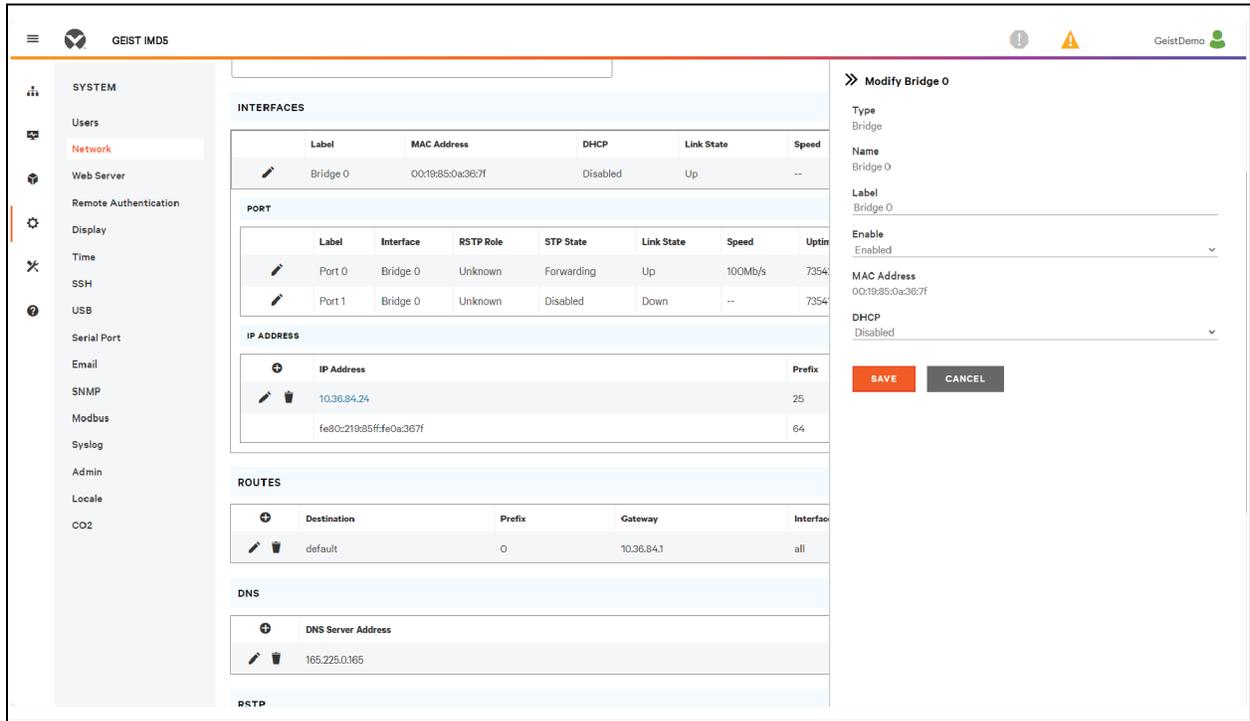


**Para editar los parámetros de la interfaz:**

1. Haga clic en el icono de modificar.
2. Modifique los campos deseados.
  - a. **Label:** cambie el nombre deseado de la interfaz seleccionada.
  - b. **Enable:** habilite/deshabilite la interfaz seleccionada. Si solo hay una interfaz disponible, al deshabilitarla se limita el acceso al dispositivo que requiere el restablecimiento de la red.
  - c. **DHCP:** habilite/deshabilite DHCP en la interfaz seleccionada.
3. Haga clic en SAVE.

**NOTA:** los cambios realizados en la configuración de la interfaz de red se aplican una vez que se hace clic en el botón **Save**. Si ha cambiado la dirección IP, aparecerá como si la unidad ya no respondiera porque el navegador no podrá recargar la página web. Cierre la ventana del navegador, escriba la nueva dirección IP en la barra de direcciones del navegador y podrá acceder a la unidad.

**Figura 5.37** Parámetros de la interfaz



**Para añadir una interfaz para un adaptador USB inalámbrico:**

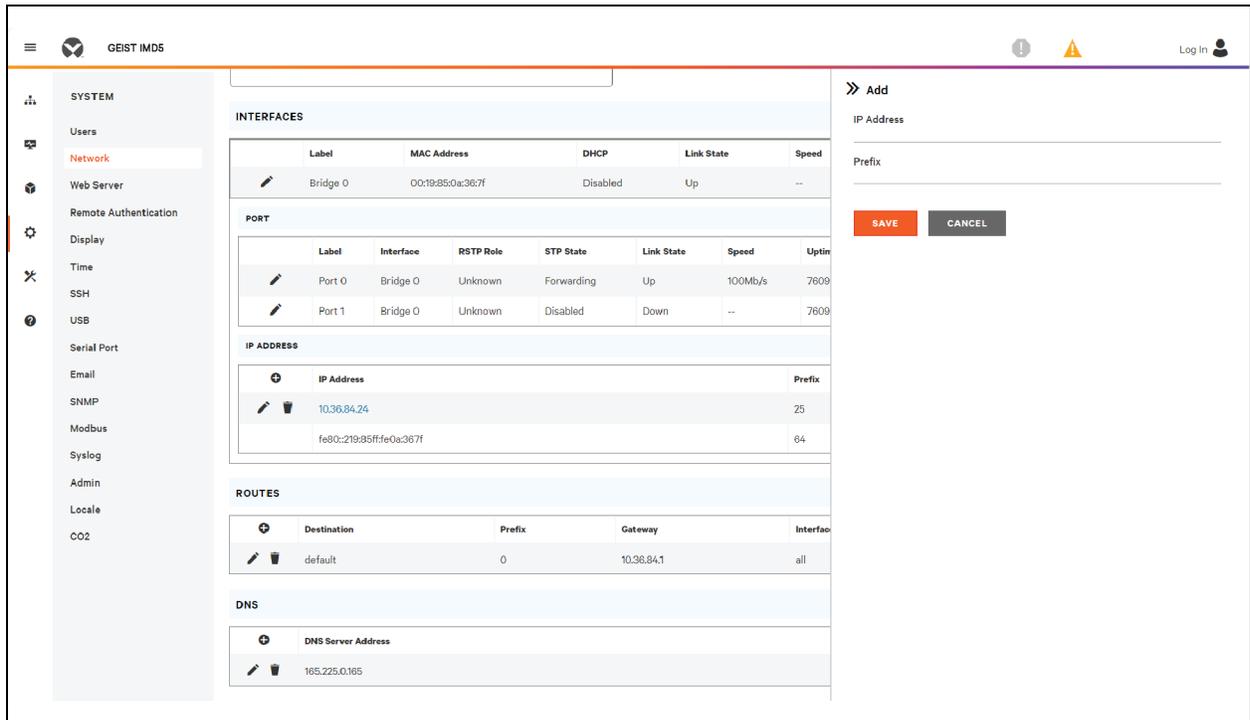
1. Introduzca el adaptador USB inalámbrico en el puerto USB (no se podrá acceder a la rPDU durante unos segundos mientras la pila de red se reconfigura automáticamente.)
2. Después de detectar automáticamente el adaptador, aparecerá una interfaz wifi.
3. Haga clic en el icono de modificar. Seleccione el SSID aplicable del menú desplegable Detected SSIDs.

**NOTA:** Consulte [Adaptadores USB inalámbricos TP-Link](#) en la **página 128** para obtener una lista de los adaptadores inalámbricos TP-Link.

**Para añadir una nueva dirección IP:**

1. Haga clic en el icono de añadir.
2. Introduzca la dirección IPv4 o IPv6 y el prefijo/máscara de subred en los campos correspondientes. Se pueden asignar estadísticamente hasta ocho direcciones IP.
3. Haga clic en **SAVE**.

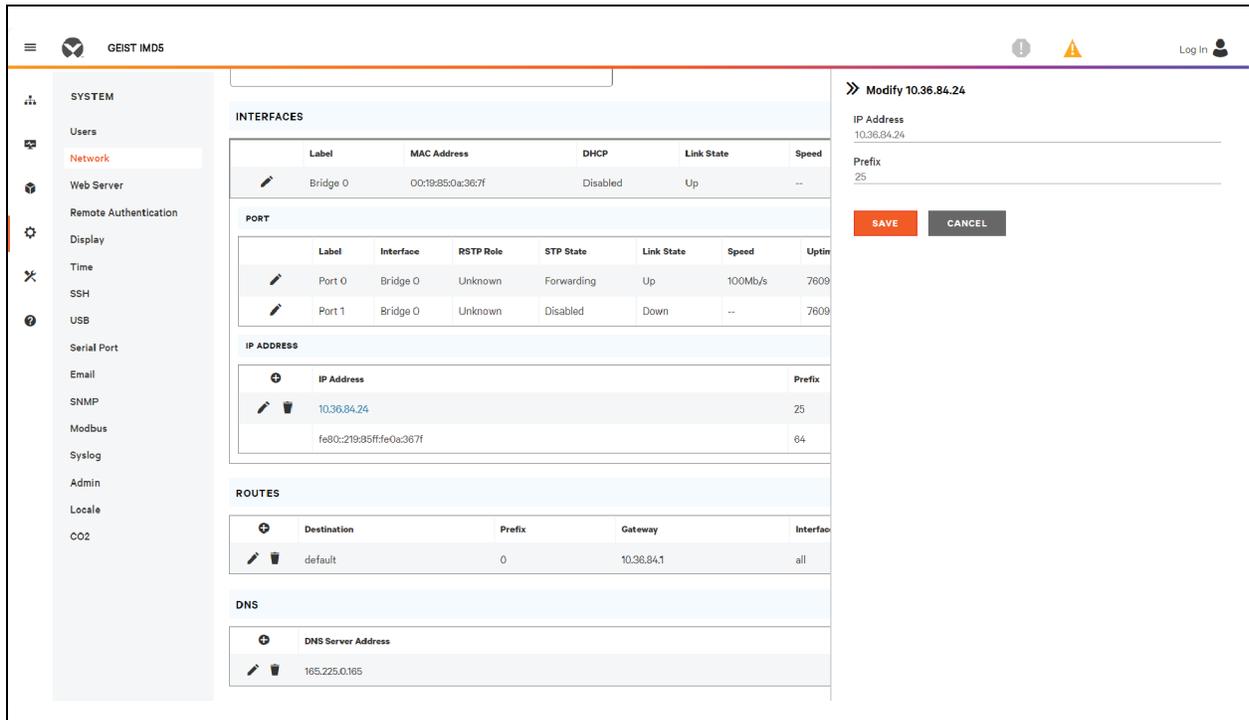
Figura 5.38 Añadir una nueva dirección IP



**Para modificar una dirección IP existente:**

1. Haga clic en el icono de modificar.
2. Edite los campos IP Address y Prefix/Subnet Mask, según sea necesario.
3. Haga clic en SAVE.

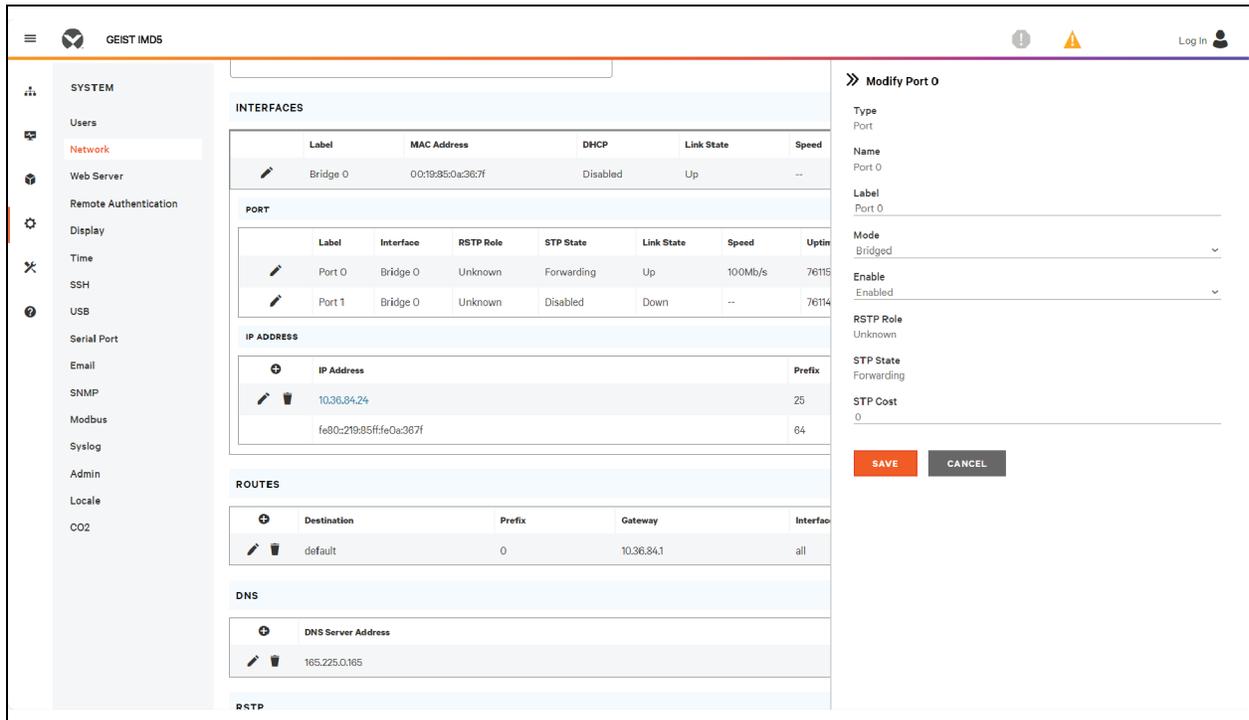
Figura 5.39 Modificación de una dirección IP



**Para modificar la configuración del puerto:**

1. Haga clic en el icono de modificar.
2. Introduzca la información correspondiente.
  - a. Cambie la etiqueta del puerto si lo desea.
  - b. Seleccione el modo Bridged o Independent.
  - c. Habilite/deshabilite el puerto.
  - d. Asigne el STP State. De este modo se designa la contribución de esta interfaz al coste de la ruta raíz cuando sirve como puerto raíz.
3. Haga clic en *SAVE*.

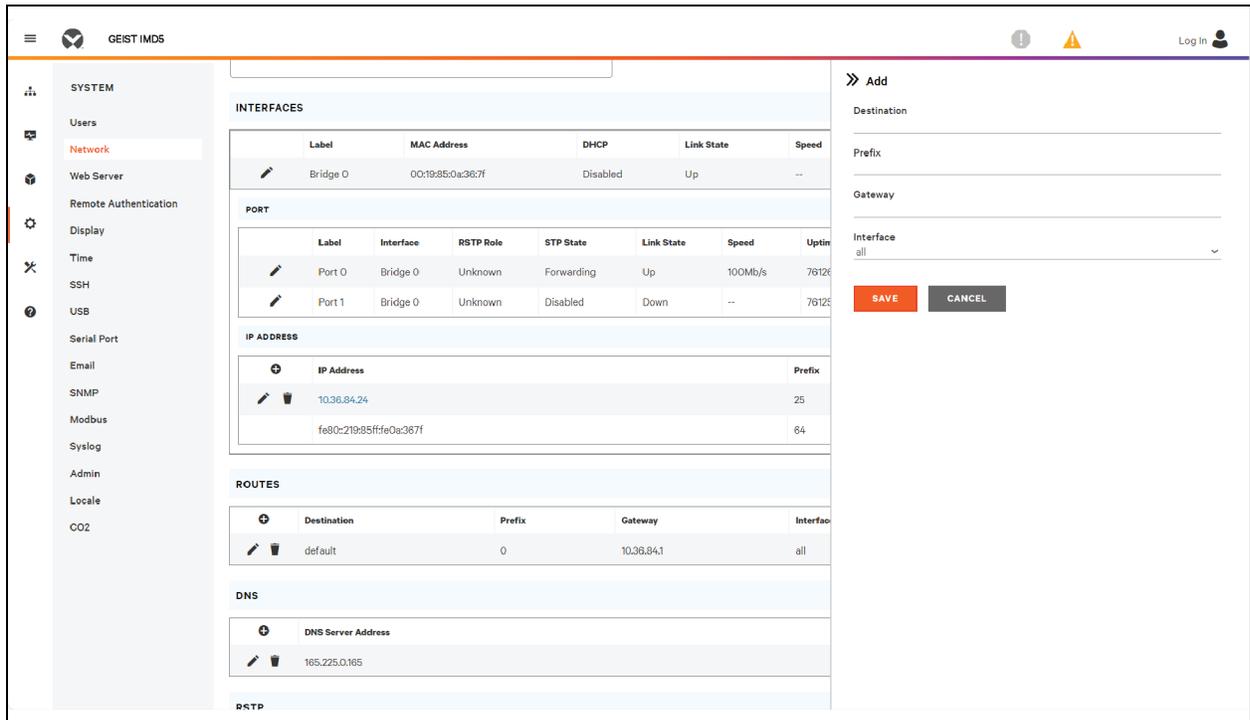
Figura 5.40 Modificación de la configuración del puerto



**Para añadir una ruta nueva:**

1. Haga clic en el icono de añadir.
2. Introduzca la información correspondiente.
  - a. La dirección IP en el campo Destination para la ruta deseada.
  - b. Introduzca el valor de *Prefix* para la ruta deseada.
  - c. Introduzca la dirección IP en el campo Gateway.
  - d. Seleccione la *Interface* que se aplique a la ruta.
3. Haga clic en **SAVE**.

Figura 5.41 Adicción de ruta



**Para modificar una ruta existente:**

1. Haga clic en el icono de modificar.
2. Edite los campos deseados.
3. Haga clic en *SAVE*.

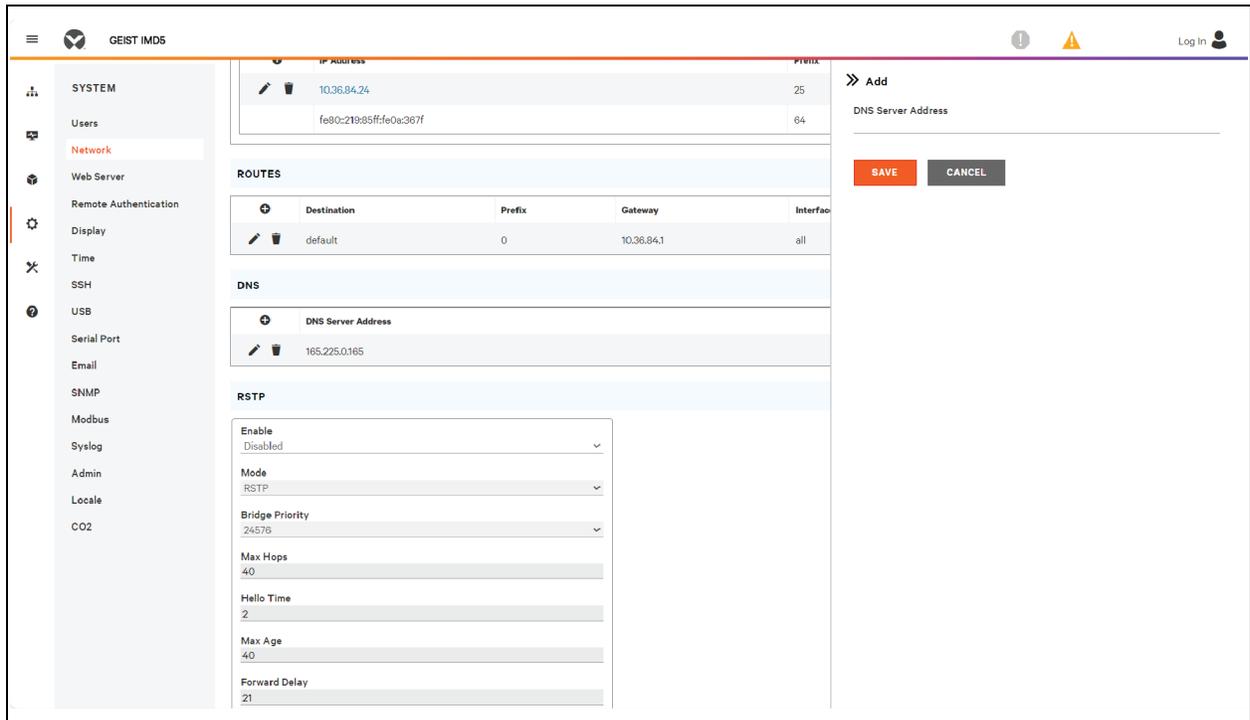
Figura 5.42 Modificación de ruta

The screenshot shows the GEIST IMDS web interface. On the left is a navigation menu with categories like SYSTEM, Network, Web Server, Remote Authentication, Display, Time, SSH, USB, Serial Port, Email, SNMP, Modbus, Syslog, Admin, Locale, and CO2. The main content area is divided into several sections: INTERFACES (with a table for Bridge 0), PORT (with a table for Port 0 and Port 1), IP ADDRESS (with a table for 10.36.84.24 and fe80::219:85:ff:fe0a:367f), ROUTES (with a table for default), and DNS (with a table for 165.225.0.165). On the right, a 'Modify 0.0.0.0' dialog box is open, showing fields for Destination (0.0.0.0), Prefix (0), Gateway (10.36.84.1), and Interface (all). There are 'SAVE' and 'CANCEL' buttons at the bottom of the dialog.

**Para añadir una nueva dirección de servidor DNS:**

1. Haga clic en el icono de añadir.
2. Introduzca la IP del servidor DNS que desee. Se pueden añadir hasta dos servidores DNS.
3. Haga clic en SAVE.

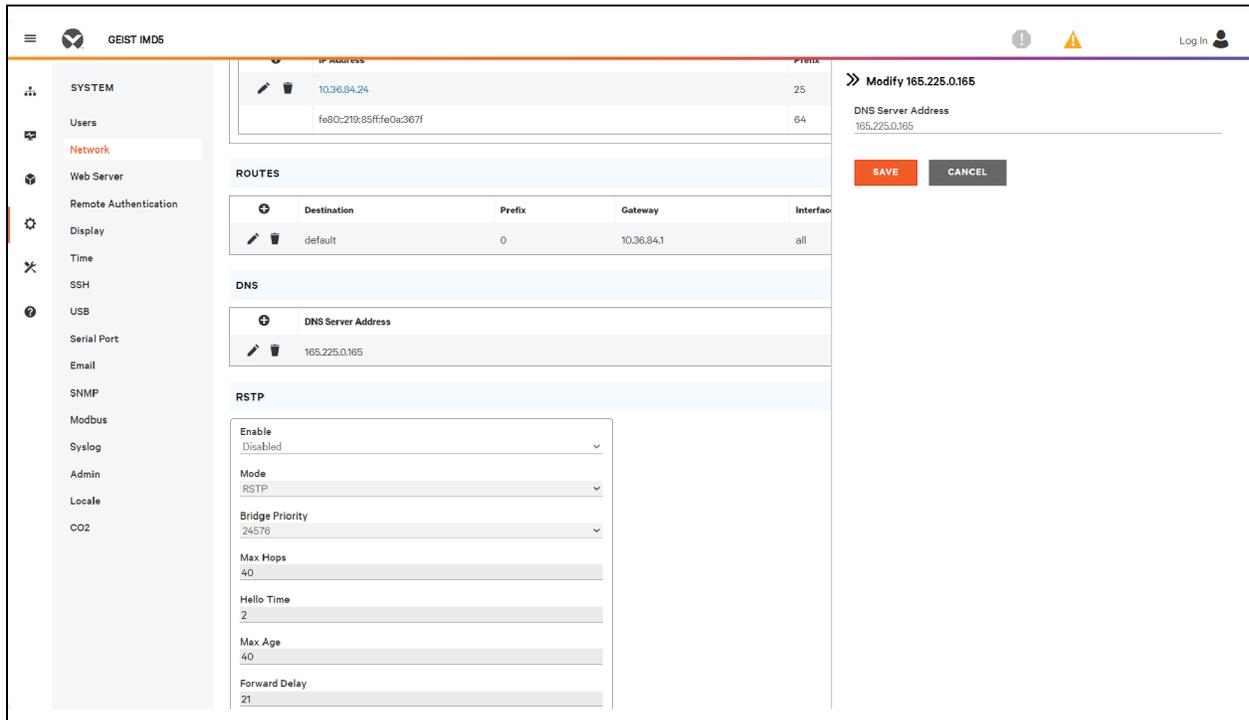
Figura 5.43 Adición de una nueva dirección de servidor DNS



**Para modificar una dirección de servidor DNS existente:**

1. Haga clic en el icono de modificar.
2. Edite el campo DNS Server Address según sea necesario.
3. Haga clic en SAVE.

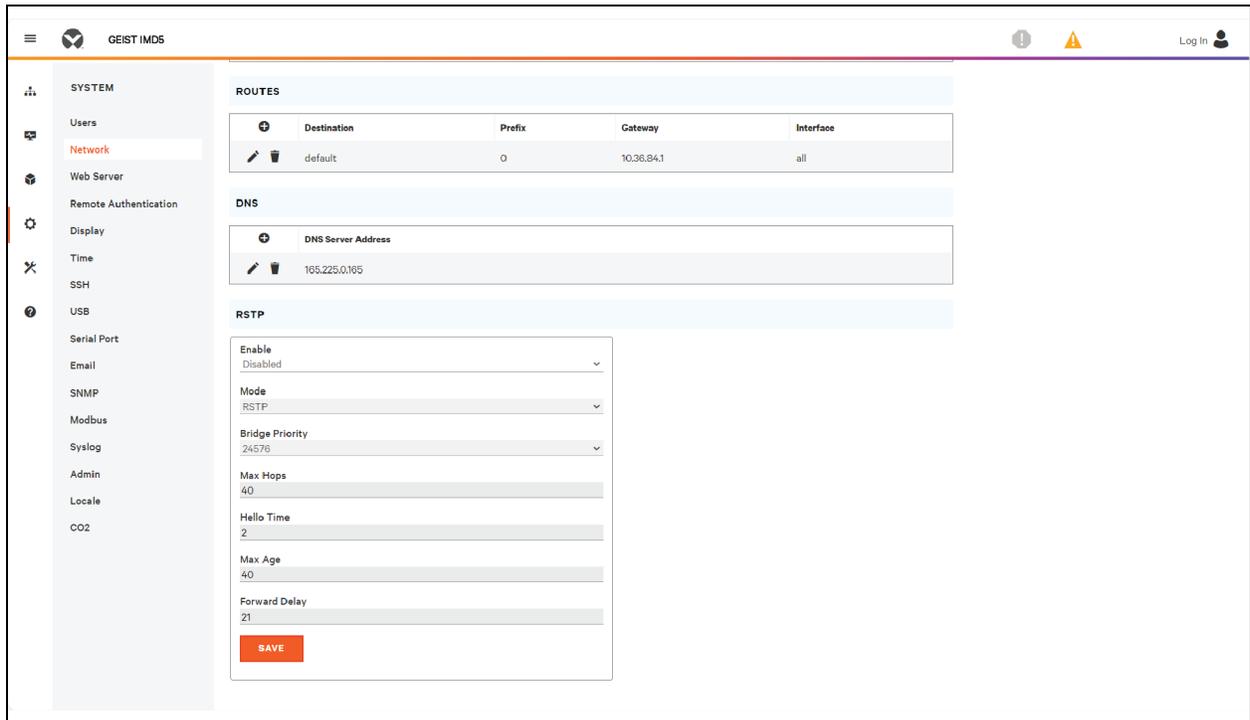
Figura 5.44 Modificación de una dirección de servidor DNS



**Para cambiar la configuración de RSTP:**

1. Cambie la configuración como desee.
  - a. **Enable:** habilite o deshabilite el protocolo RSTP.
  - b. **Mode:** el modo RSTP permite volver a STP cuando sea necesario.
  - c. **Bridge Priority:** haga clic en el menú desplegable, seleccione el valor adecuado y haga clic en Save.
  - d. **Max Hops:** se usa cuando el modo está habilitado para RSTP.
  - e. **Hello Time:** intervalo, en segundos, entre las transmisiones periódicas de los mensajes de configuración por los puertos designados.
  - f. **Max Age:** antigüedad máxima, en segundos, de la información transmitida por esta interfaz, cuando sirve como puente de raíz. Establecido en 2 segundos.
  - g. **Forward Delay:** retardo, en segundos, que utilizan los puentes para hacer la transición del puente raíz y los puertos designados al modo de reenvío. Establecido en 21 segundos.
2. Haga clic en **SAVE**.

**Figura 5.45 Cambio de la configuración de RSTP**



### 5.6.3 Web server

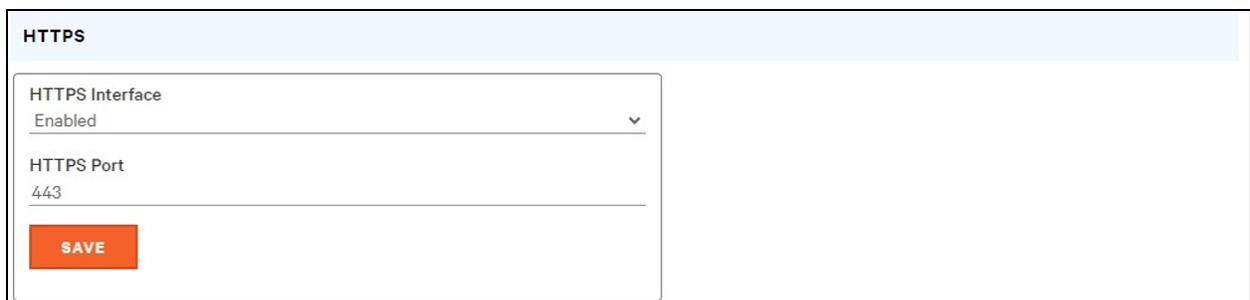
La configuración del servidor web de la unidad se puede actualizar en la pestaña Web Server del menú System.

- **HTTP Interface:** se habilita o redirige a HTTPS, mientras que la interfaz de HTTPS puede estar habilitada o deshabilitada. Cuando la interfaz de HTTP se redirige a HTTPS y la interfaz de HTTPS está deshabilitada, la interfaz de HTTP también se puede deshabilitar eficazmente.

**NOTA:** Téngase en cuenta que no es posible deshabilitar los protocolos HTTP, HTTPS y SSH al mismo tiempo.

- **HTTP/HTTPS Server Port:** le permite cambiar los puertos TCP a los que escuchan los servicios HTTP y HTTPS para las conexiones entrantes. Los valores predeterminados son el puerto 80 para HTTP y el puerto 443 para HTTPS.

**Figura 5.46 Página de configuración de HTTP**



- **SSL Certificate:** le permite cargar su propio archivo de certificado SSL firmado para reemplazar el predeterminado. El certificado puede estar autofirmado o firmado por una autoridad de certificación. El certificado SSL debe tener formato *PEM* o *PFX* (PKCS12).

**Figura 5.47 SSL Certificate**

- **Formato *PEM*:**
  - El certificado público y la clave privada deben residir en el mismo archivo.
  - El certificado debe seguir el estándar x.509.
  - La clave privada debe estar generada con el algoritmo RSA o el algoritmo ECDSA. Debe estar en el formato *PEM*.
    - No se admite un algoritmo RSA de 2048 bits o más pequeño.
    - P-384 es el tamaño admitido para el algoritmo ECDSA.
  - La clave privada *PEM RSA* puede estar protegida por una contraseña.
- **Formato *PFX*:** también se dispone de compatibilidad con el estándar PKCS12 (*.pfx*), que es una combinación binaria cifrada de un certificado público *PEM* y de su clave privada *PEM*. Cuando se genera un certificado *PFX*, se le pide una contraseña opcional.

## 5.6.4 Remote Authentication

La página Remote Authentication permite designar uno de los tres protocolos de autenticación para el acceso remoto al dispositivo. De forma predeterminada, el dispositivo utiliza la base de datos local para autenticar a los usuarios. La autenticación remota permite al dispositivo autenticar a un usuario con un servidor remoto. Si la autenticación remota falla, volverá a la autenticación local.

### Para cambiar la configuración de Remote Authentication:

1. Seleccione el modo necesario en el menú desplegable.
  - **Disabled:** autenticación local.
  - **LDAP:** protocolo ligero de acceso a directorios.
  - **TACACS+:** sistema de control de acceso del controlador de acceso a terminales plus.
  - **RADIUS:** servicio de autenticación remota telefónica de usuario.
2. Haga clic en *SAVE*.

## LDAP

El protocolo ligero de acceso a directorios (LDAP) se puede configurar a través de este menú.

**NOTA: Es necesario conocer la configuración del servidor LDAP para configurar el dispositivo de rPDU Vertiv™ PowerIT para este protocolo de autenticación remota. Si no está familiarizado con esta configuración, consulte al administrador del servidor LDAP.**

Configuración para la autenticación remota mediante LDAP.

- **LDAP Server Address:** especifique la dirección del host para el LDAP. El *HOST* puede ser una dirección IPv4, una dirección IPv6 entre paréntesis (p. ej., *[2001:0DB8:AC10:FE01::]*) o un nombre de host.
- **LDAP Server Port:** se utiliza para establecer el número de puerto LDAP. El puerto predeterminado para LDAP es 389; para Security Type utilice *None* o *StartTLS*. Use 636 para Security Type SSL.
- **LDAP Mode:** en el menú desplegable, seleccione *Active Directory* u **OpenLDAP**. Consulte [Un ejemplo de configuración de LDAP para las credenciales de Active Directory](#) en la página 157.
- **Security Type:** en el menú desplegable, seleccione *None*, *SSL* o *StartTLS*.
- **Bind DN:** nombre distintivo utilizado como enlace al servidor de directorios. La cadena en blanco para el DN de enlace y la contraseña implican un enlace anónimo.
- **Bind Password:** contraseña utilizada como enlace al servidor de directorios.
- **Base DN:** DN para usar para la base de búsqueda.

Los campos restantes proceden del esquema NIS, definido en RFC2307. Se utilizan para autenticar a los usuarios en LDAP. Si se dejan en blanco se utilizará el valor predeterminado.

- **User Filter:** filtro LDAP para seleccionar usuarios.
- **"uid" Mapping:** nombre del atributo de servidor que corresponde al atributo *uid* en el esquema.
- **"uidNumber" Mapping:** nombre del atributo de servidor que corresponde al atributo *uidNumber* en el esquema.
- **Group Filter:** filtro LDAP para seleccionar grupos.
- **"gid" Mapping:** nombre del atributo de servidor que corresponde al atributo *gid* en el esquema.
- **"memberUid" Mapping:** nombre del atributo de servidor que corresponde al atributo *memberUid* en el esquema.

**NOTA: Los usuarios *deben* rellenar el campo **uidNumber**. Si el valor es nulo o falta, fallará el inicio de sesión válido. El **uidNumber** del usuario *debe* ser 1000 o superior. Si el valor es inferior a 1000, fallará el inicio de sesión válido.**

- **Enabled Group:** los usuarios de este grupo tienen privilegios de solo visualización, como se describe en la sección Usuarios de este manual.
- **Control Group:** los usuarios de este grupo tienen privilegios de control, como se describe en la sección Usuarios de este manual.
- **Admin Group:** los usuarios de este grupo tienen privilegios de administrador, como se describe en la sección Usuarios de este manual. Los usuarios de LDAP no cuentan para calcular el número mínimo de usuarios de administración requeridos.

Haga clic en *SAVE*.

Los campos Enabled Group, Control Group y Admin Group indican cómo asignar grupos a los permisos de usuario. Un usuario debe pertenecer a uno de estos grupos para acceder al dispositivo. Si un usuario pertenece a más de un grupo, se utiliza el grupo con los permisos más elevados.

Figura 5.48 Menú LDAP

The image shows a web-based configuration interface for LDAP. The title is "LDAP". The form contains the following fields and options:

- LDAP Server Address: [Text input]
- LDAP Server Port: 389
- LDAP Mode: Active Directory (dropdown)
- Security Type: None (dropdown)
- Bind DN: [Text input]
- Bind Password: [Text input]
- Verify Password: [Text input]
- Base DN: [Text input]
- User Filter: (objectClass=posixAccount)
- \*uid\* Mapping: uid
- \*uidNumber\* Mapping: uidNumber
- Group Filter: (objectClass=posixGroup)
- \*gid\* Mapping: gidNumber
- \*memberUid\* Mapping: memberOf
- Enabled Group: enabled
- Control Group: control
- Admin Group: admin

At the bottom of the form is a red "SAVE" button.

## TACACS+

El sistema de control de acceso del controlador de acceso a terminales plus (TACACS+) se puede configurar a través de este menú.

**NOTA: Es necesario conocer la configuración del servidor TACACS+ para configurar el dispositivo de rPDU Vertiv™ PowerIT para este protocolo de autenticación remota. Si no está familiarizado con esta configuración, consulte al administrador del servidor de TACACS+.**

Configuración para la autenticación remota mediante TACACS+.

Figura 5.49 Menú TACACS+

**TACACS+**

Primary Authentication Server  
\_\_\_\_\_

Alternate Authentication Server  
\_\_\_\_\_

Primary Accounting Server  
\_\_\_\_\_

Alternate Accounting Server  
\_\_\_\_\_

Shared Secret (Password)  
\_\_\_\_\_

Verify Password  
\_\_\_\_\_

Service  
PPP ▼

Admin Attribute  
\_\_\_\_\_

Control Attribute  
\_\_\_\_\_

Enabled Attribute  
\_\_\_\_\_

SAVE

- **Primary Authentication Server:** el servidor de autenticación/autorización primario, que puede ser una dirección IPv4, una dirección IPv6 entre corchetes (p. ej., [2001:0DB8:AC10:FE01::]) o un nombre de host. El servidor de autenticación primario se utiliza tanto para la autenticación como para la autorización. Este nombre/dirección de host del servidor AA es necesario.
- **Alternate Authentication Server:** el servidor de autenticación/autorización alternativo, que puede ser una dirección IPv4, una dirección IPv6 entre corchetes o un nombre de host. El servidor de autenticación secundario se utiliza tanto para la autenticación como para la autorización.
- **Primary Accounting Server:** el servidor de cuentas primario, que puede ser una dirección IPv4, una dirección IPv6 entre corchetes o un nombre de host. El servidor de cuentas primario es opcional. Si está configurado, se notifica al servidor cuando se autoriza a un usuario.
- **Alternate Accounting Server:** el servidor de cuentas alternativo, que puede ser una dirección IPv4, una dirección IPv6 entre corchetes o un nombre de host. El servidor de cuentas secundario es opcional. Si está configurado, se notifica al servidor cuando se autoriza a un usuario.
- **Shared Secret (Password):** introduzca una palabra o frase secreta en el campo Shared Secret (se aplica tanto a los servidores de autenticación y cuentas primarios como a los secundarios).
- **Service:** el valor que se debe utilizar para el campo de servicio en las solicitudes TACACS+. Las opciones válidas son *PPP* y *raccess*.

- **Admin Attribute:** un usuario con este atributo tendrá privilegios *admin*, como se describe en la sección Usuarios de este manual. Los usuarios de TACACS+ no cuentan para calcular el número mínimo de usuarios de administración requeridos.
- **Control Attribute:** los usuarios con este atributo tendrán privilegios de control, como se describe en la sección Usuarios de este manual.
- **Enabled Attribute:** los usuarios con este atributo tendrán privilegios de solo visualización, como se describe en la sección Usuarios de este manual.

Haga clic en *SAVE*.

**NOTA:** Los pares atributo-valor (AVP) que devuelve el servidor durante la autenticación/autorización determinan los permisos del usuario. El campo Group Attribute indica al sistema que AVP contiene el grupo de acceso del usuario. Si el valor de AVP coincide con el campo Admin Group, el usuario tiene acceso Admin (completo). Si el valor de AVP coincide con el campo Control Group, el usuario tiene acceso de control. Si el valor de AVP coincide con el campo Enabled Group, el usuario tiene acceso de solo visualización. Si no se encuentran coincidencias, el usuario no tendrá acceso a la unidad. Un campo de grupo en blanco no coincidirá con ningún AVP.

## RADIUS

El protocolo de servicio de autenticación remota telefónica de usuario (RADIUS) se puede configurar a través de este menú.

**NOTA:** Es necesario conocer la configuración del servidor RADIUS para configurar el dispositivo de rPDU Vertiv™ PowerIT para este protocolo de autenticación remota. Si no está familiarizado con esta configuración, consulte al administrador del servidor RADIUS.

Configuración para la autenticación remota mediante RADIUS.

Figura 5.50 Menú RADIUS

**RADIUS**

Primary Authentication Server

---

Alternate Authentication Server

---

Shared Secret (Password)

---

Verify Password

---

Group Attribute  
filter-id

---

Admin Group

---

Control Group

---

Enabled Group

---

SAVE

- **Primary Authentication Server:** introduzca la dirección IP del servidor de autenticación/autorización/cuentas primario. El servidor de autenticación primario puede ser una dirección IPv4, una dirección IPv6 entre corchetes (p. ej., [2001:0DB8:AC10:FE01::]) o un nombre de host. El servidor de autenticación primario se utiliza para autenticación, autorización y cuentas. Este servidor AA es obligatorio.
- **Alternate Authentication Server:** si corresponde, introduzca la dirección IP del servidor de autenticación/autorización/cuentas alternativo. el servidor de autenticación alternativo puede ser una dirección IPv4, una dirección IPv6 entre corchetes o un nombre de host. El servidor de autenticación secundario se utiliza para autenticación, autorización y cuentas.
- **Shared Secret (Password):** introduzca una palabra o frase secreta en el campo Shared Secret (se aplica tanto a los servidores de autenticación y cuentas primarios como a los secundarios).
- **Group Attribute:** identifica el par de atributo-valor (AVP) que indica a qué grupo de acceso pertenece el usuario. Los valores válidos son *filter-id* y *management-privilege-level*.
- **Admin Group:** un usuario perteneciente a este grupo tiene privilegios de administrador, como se describe en la sección Usuarios del manual.
- **Control Group:** un usuario perteneciente a este grupo tiene privilegios de control, como se describe en la sección Usuarios del manual.
- **Enabled Group:** un usuario perteneciente a este grupo tiene privilegios de solo visualización **Enabled**, como se describe en la sección Usuarios del manual.

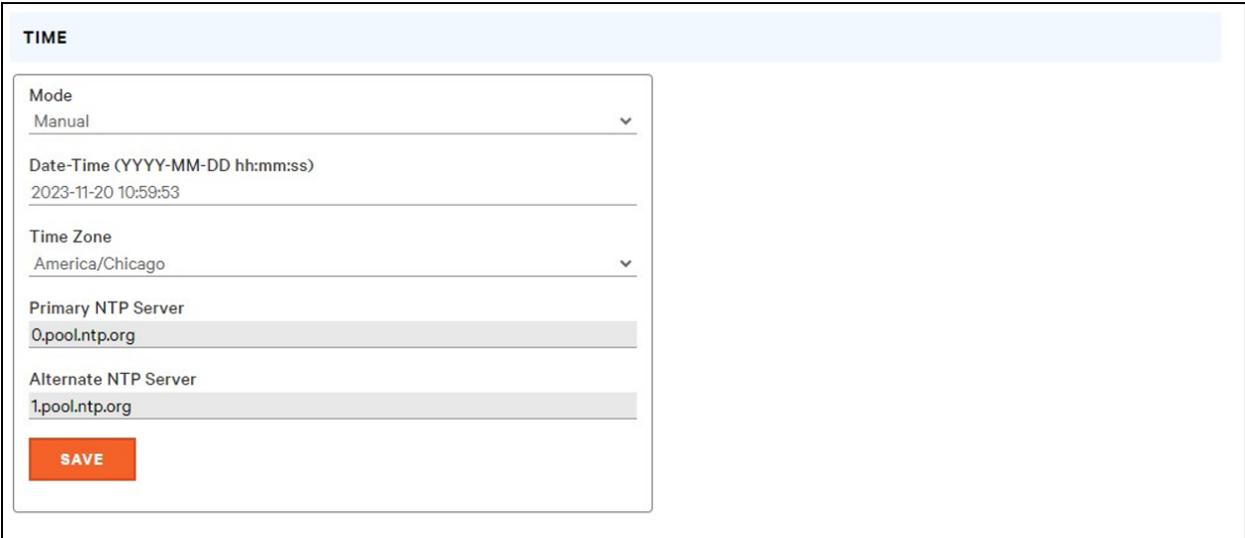
Haga clic en **SAVE**.

**NOTA:** los pares atributo-valor (AVP) que devuelve el servidor durante la autenticación/autorización determinan los permisos del usuario. El campo Group Attribute indica al sistema que AVP contiene el grupo de acceso del usuario. Si el valor de AVP coincide con el campo Admin Group, el usuario tiene acceso Admin (completo). Si el valor de AVP coincide con el campo Control Group, el usuario tiene acceso de control. Si el valor de AVP coincide con el campo Enabled Group, el usuario tiene acceso de solo visualización. Si no se encuentran coincidencias, el usuario no tendrá acceso a la unidad. Un campo de grupo en blanco no coincidirá con ningún AVP.

## 5.6.5 Time

La fecha y hora de la unidad se establecen en esta página.

Figura 5.51 Página de configuración de Time



The screenshot shows a configuration page titled "TIME". It contains several fields: "Mode" set to "Manual", "Date-Time (YYYY-MM-DD hh:mm:ss)" set to "2023-11-20 10:59:53", "Time Zone" set to "America/Chicago", "Primary NTP Server" set to "0.pool.ntp.org", and "Alternate NTP Server" set to "1.pool.ntp.org". A red "SAVE" button is located at the bottom of the form.

Hay dos modos disponibles:

- **Protocolo de tiempo de red (NTP):** sincroniza la fecha y la hora de la unidad con la zona horaria especificada utilizando los servidores NTP enumerados. Los servidores NTP se pueden reconfigurar.
- **Manual:** en este modo, la fecha y la hora deben escribirse como se indica a la izquierda del campo.

## 5.6.6 SSH

El menú SSH permite configurar los parámetros para el acceso de SSH al dispositivo.

**Figura 5.52** Página de configuración de SSH



- **SSH Access:** habilita o deshabilita el acceso a través de SSH.
- **SSH Port:** le permite cambiar el puerto al que el servicio SSH escucha para las conexiones entrantes. El puerto predeterminado es el 22.

**NOTA:** La sesión de un usuario de SSH se cerrará automáticamente tras 10 minutos de inactividad.

## 5.6.7 USB

**Para habilitar o deshabilitar el puerto USB:**

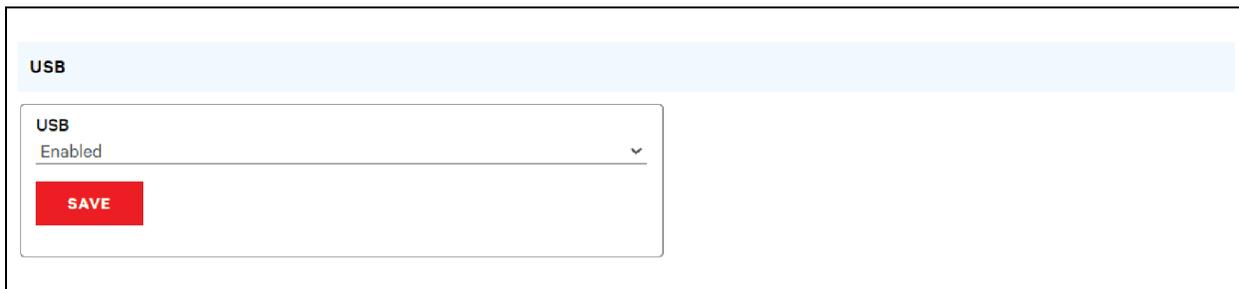
1. Seleccione Enable o Disable en el menú desplegable.
2. Haga clic en el botón *SAVE*.

Cuando el puerto USB está habilitado, los dispositivos USB conectados se muestran en la interfaz web.

**NOTA:** El dispositivo USB debe tener formato FAT32.

Si se detecta un dispositivo de almacenamiento USB válido y se están registrando datos históricos, estos datos también se almacenan en un archivo en la unidad de almacenamiento USB. Si aún no existe, se crea un archivo llamado **log-1.csv** bajo un directorio **log** en el nivel superior del sistema de archivos. Si ya existen archivos de registro, se utiliza como punto de partida el que tiene el identificador numérico más alto en el título. Cada periodo de registro, se agregan nuevos datos a este archivo en el mismo formato que la recuperación CSV. Si se crean o eliminan puntos de datos en relación con los enumerados en el encabezado CSV, se crea un nuevo archivo con un nombre con el siguiente número secuencial. Si el sistema de archivos se llena, este registro se interrumpirá.

**Figura 5.53** USB



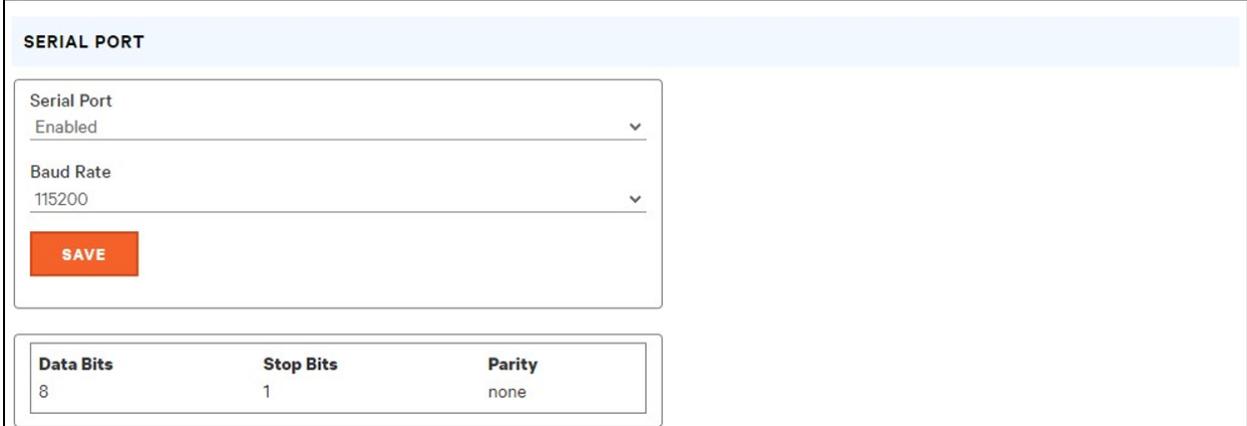
## 5.6.8 Serial Port

**NOTA:** La conexión serie no permite el control de flujo.

El menú Serial Port permite configurar los ajustes del puerto serie, habilitar o deshabilitar el puerto, y establecer la velocidad en baudios.

1. Haga clic en el menú desplegable Serial Port y seleccione *Enabled/Disabled*.
2. Haga clic en el menú desplegable Baud Rate y seleccione el valor *Baud Rate*.
3. Haga clic en *SAVE*.

**Figura 5.54** Menú desplegable System: Serial Port



The screenshot shows a configuration window titled "SERIAL PORT". It contains two dropdown menus: "Serial Port" set to "Enabled" and "Baud Rate" set to "115200". Below these is an orange "SAVE" button. At the bottom, there is a table with three columns: "Data Bits" (8), "Stop Bits" (1), and "Parity" (none).

Data Bits	Stop Bits	Parity
8	1	none

## 5.6.9 Email

La unidad tiene capacidad para enviar notificaciones de correo electrónico a un máximo de diez (10) direcciones de correo electrónico cuando se produce un suceso de alarma o de advertencia.

Figura 5.55 Página de configuración de Email

**System • Email**

**EMAIL**

**1** Leave Username and Password blank for relay-only (no authentication).

SMTP Server

Port  
25

"From" Email Address

Username

Password

Verify Password

**SAVE**

**1**

**3**

Target Email Address

username@server.com

**2**

**4**

Tabla 5.12 Descripciones de la página de configuración de Email

Elemento	Descripción
1	Añadir nueva dirección de correo electrónico de destino.
2	Modificar dirección de correo electrónico de destino existente.
3	Eliminar dirección de correo electrónico de destino existente.
4	Enviar correo electrónico de prueba.

Para enviar correos electrónicos, la unidad debe estar configurada para acceder al servidor de correo, de la siguiente manera:

- **SMTP Server:** el nombre o la dirección IP de un servidor SMTP o ESMTP adecuado.
- **Port:** el puerto TCP que el servidor SMTP utiliza para proporcionar servicios de correo. Los valores típicos serían Port 25 para una conexión no cifrada o 465 y 587 para una conexión cifrada mediante TLS/SSL, pero estos pueden variar dependiendo de la configuración del servidor de correo.
- **From Email Address:** la dirección de la que parecen proceder los correos electrónicos de la unidad. Muchos servicios de correo electrónico hospedados, como Gmail, requieren que sea la cuenta de correo electrónico de un usuario válido.
- **Username y Password:** las credenciales de inicio de sesión para el servidor de correo electrónico. Si el servidor no requiere autenticación (relé abierto), pueden dejarse en blanco.

Los servidores de Microsoft Exchange deben estar configurados para permitir el relé SMTP desde la dirección IP de la unidad. Además, el servidor de Exchange debe estar configurado para permitir una autenticación básica, de modo que la unidad pueda iniciar sesión con el método AUTH LOGIN para enviar sus credenciales de inicio de sesión. Otros métodos, como AUTH PLAIN y AUTH MD5 no son compatibles.

**Para añadir o modificar una dirección de correo electrónico de destino:**

1. Haga clic en el icono de añadir o modificar.
2. Introduzca la dirección de correo electrónico y luego haga clic en Save.

**Para eliminar una dirección de correo electrónico de destino:**

1. Haga clic en el icono de eliminar situado junto a la dirección que desee eliminar.
2. Haga clic en *Delete* en la ventana emergente para confirmar.

**Para enviar un correo electrónico de prueba:**

1. Haga clic en el icono de correo electrónico de prueba situado junto a la característica que desee probar.
2. Una ventana emergente indica que se está enviando el correo electrónico de prueba; haga clic en OK para descartar la ventana emergente.

## 5.6.10 SNMP

El protocolo simple de administración de redes (SNMP) se puede usar para monitorizar las mediciones y el estado de la unidad. Se admiten SNMP V1, V2c y V3. Además, las capturas de alarma se pueden enviar hasta a diez direcciones IP.

Haga clic en **ZIP** para descargar el archivo *mib.zip* que contiene tanto el archivo MIB como la hoja de cálculo con formato CSV.

El servicio de SNMP-V1/V2c y SNMP-V3 se puede habilitar o deshabilitar de forma independiente. El servicio escucha las peticiones de lectura de datos en el puerto 161, que es el valor predeterminado habitual para los servicios SNMP; esto también se puede cambiar.

La base de datos de información de administración (MIB) se puede descargar desde la unidad a través del vínculo ZIP en la parte superior de la página web. Al hacer clic en este vínculo, se descarga un archivo .zip que contiene tanto el archivo MIB como una hoja de cálculo en formato CSV que describe los OID disponibles en lenguaje natural para ayudarle a configurar su administrador SNMP para que lea los datos de la unidad.

**Figura 5.56** Página de configuración de SNMP

**Figura 5.57** Página de configuración de Users de SNMP

USERS				
	Type	Name	Authentication	Privacy
	V1/V2c Read Community	public	—	—
	V1/V2c Write Community	private	—	—
	V1/V2c Trap Community	private	—	—
	V3 Read		None	None
	V3 Read/Write		None	None
	V3 Trap		None	None

La sección Users permite configurar las distintas comunidades de lectura, escritura y captura para los servicios SNMP. También puede configurar los tipos de autenticación y los métodos de cifrado que se utilizan para SNMP V3 si lo desea. Haga clic en el icono de modificar para cambiar la configuración.

Las capturas permiten definir los tipos de SNMP que desea enviar y las direcciones IP de los destinatarios.

**Para configurar un destino de captura:**

1. Localice la sección *Traps* de la página SNMP y pulse el icono de añadir.
2. Introduzca la dirección IP a la que se debe enviar la captura en el campo Host.
3. Cambie el número de puerto si lo desea.
4. Seleccione la versión de la captura que se utilizará (V1, V2c o V3) y haga clic en *SAVE*.

Se puede enviar una captura de prueba haciendo clic en el icono de prueba junto a la dirección IP del host. También puede actualizar/cambiar la configuración de la captura. Haga clic en el icono de modificación junto a la dirección IP del host.

**Figura 5.58 Trap**

TRAPS			
	Host	Port	Version
   	192.168.123.111	162	2c

### 5.6.11 Modbus

El protocolo de comunicación Modbus TCP se puede usar para monitorizar las mediciones y el estado de la unidad. También permite al usuario ajustar los ajustes de la unidad.

El mapa de registro se puede descargar desde la unidad a través del vínculo ZIP en la parte superior de la página web. Al hacer clic en este vínculo, se descarga un archivo **.zip** que contiene una hoja de cálculo en formato CSV que describe la asignación de Modbus en lenguaje natural para ayudarle a configurar su administrador Modbus de modo que pueda leer/escribir los datos de la unidad.

El protocolo de comunicación Modbus se puede habilitar o deshabilitar. El acceso Modbus a la unidad puede ser *Read* o *Read/Write*. Las solicitudes de lectura o escritura de datos se realizan en el puerto 502, que es el valor predeterminado habitual para el protocolo Modbus; este puerto también se puede cambiar.

**Figura 5.59 Modbus**

**MODBUS**

Download the Register Map  
[modbus.zip](#)

Modbus  
 Disabled ▼

Access  
 Read ▼

Port  
 502

**SAVE**

## 5.6.12 SYSLOG

Los datos de Syslog se pueden capturar de forma remota, pero primero se deben configurar y habilitar a través de la página SYSLOG.

**Figura 5.60 SYSLOG**

**NOTA:** Esta función es principalmente útil para fines de diagnóstico y normalmente debe dejarse deshabilitada, a menos que la asistencia técnica de Vertiv™ aconseje habilitarla para resolver problemas específicos.

Para poder usar el botón Download the Event Log CSV, es necesario que el usuario tenga acceso de administrador.

## 5.6.13 Admin

La página Admin permite al administrador del dispositivo guardar su información de contacto junto con la descripción y la ubicación del dispositivo. En cuanto un administrador guarde la información, otros usuarios (no administradores) podrán verla. Además, la etiqueta del sistema se puede modificar en esta página. Esta etiqueta suele aparecer en la barra de título de la ventana del navegador web y/o en la(s) pestaña(s) del navegador en el que se está viendo el dispositivo.

## 5.6.14 Locale

La página Locale establece el idioma y las unidades de temperatura predeterminados para el dispositivo. Esta configuración se convertirá en las opciones de visualización predeterminadas del dispositivo, aunque los usuarios individuales pueden cambiar estas opciones para sus propias cuentas. La cuenta de invitado solo podrá ver el dispositivo con las opciones establecidas aquí.

## 5.7 Submenú Utilities

El submenú Utilities del menú System ofrece la posibilidad de restaurar los valores predeterminados, reiniciar el sistema de comunicación y realizar actualizaciones de firmware.

## 5.7.1 Configuration Backup and Restore

Guarde los ajustes de la configuración actual y restaure los ajustes de la configuración anterior si es necesario.

**Tabla 5.13 Opciones de copia de seguridad y restauración**

Opción	Descripción
Download Configuration Backup File	Las descargas no requieren autenticación del usuario. El nombre del archivo descargado es <b>backup_XXX.bin</b> , donde XXX es una representación de cadena de la dirección MAC para la interfaz <b>Ethernet</b> de la unidad sin los caracteres :
Backup File	Carga el archivo de copia de seguridad de configuración. Se requiere la autenticación del usuario y el usuario debe tener privilegios de administrador. Un archivo de copia de seguridad solo puede usarse para cargar la configuración en unidades con el mismo número de modelo.

**Para guardar los ajustes de la configuración actual:**

1. Seleccione *Download Configuration Backup File*.
2. Haga clic en *BIN*.

**NOTA:** Para guardar la configuración no se requiere la autenticación del usuario.

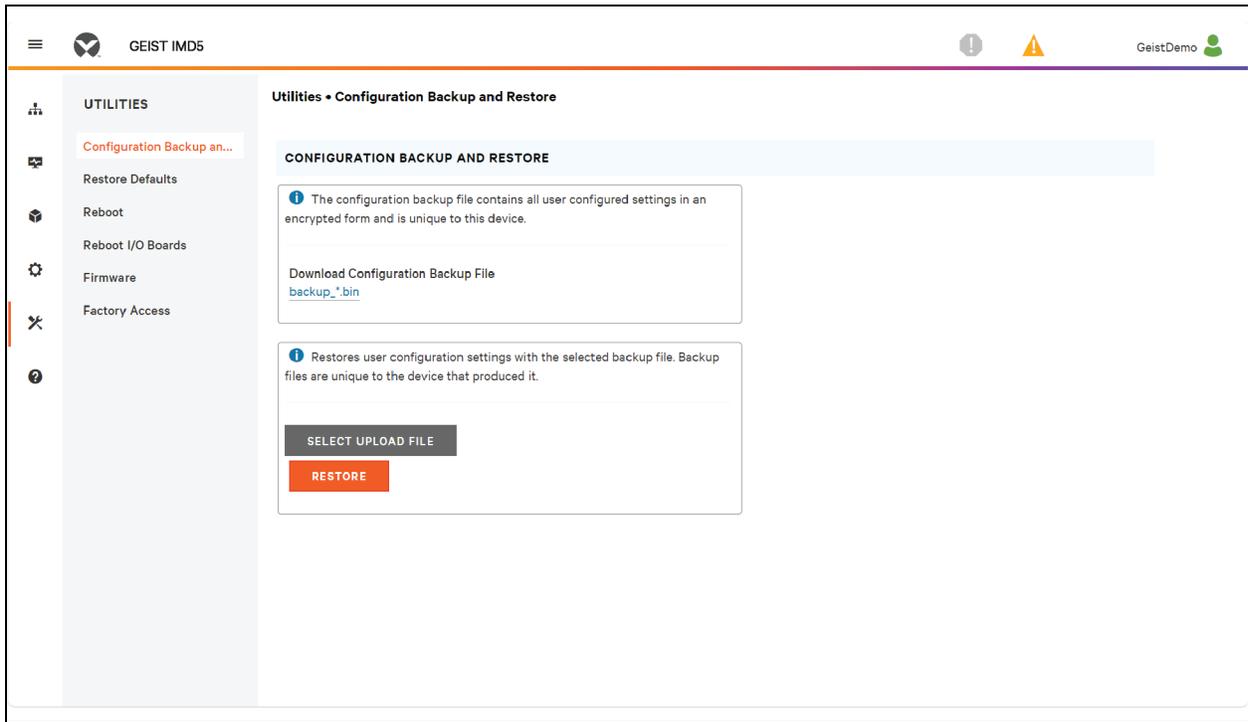
**Para restaurar los ajustes de la configuración anterior:**

1. Haga clic en *Backup File*.
2. Haga clic en *SELECT UPLOAD FILE*.
3. Seleccione el Backup File.
4. Haga clic en *RESTORE*.

**NOTA:** Para restaurar la configuración se requiere la autenticación del usuario, y el usuario debe tener privilegios de administrador.

**NOTA:** Un archivo de copia de seguridad solo puede usarse para cargar la configuración en unidades con el mismo número de modelo.

Figura 5.61 Información general sobre Configuration Backup and Restore



### 5.7.2 Restore Defaults

Permite restaurar la configuración predeterminada.

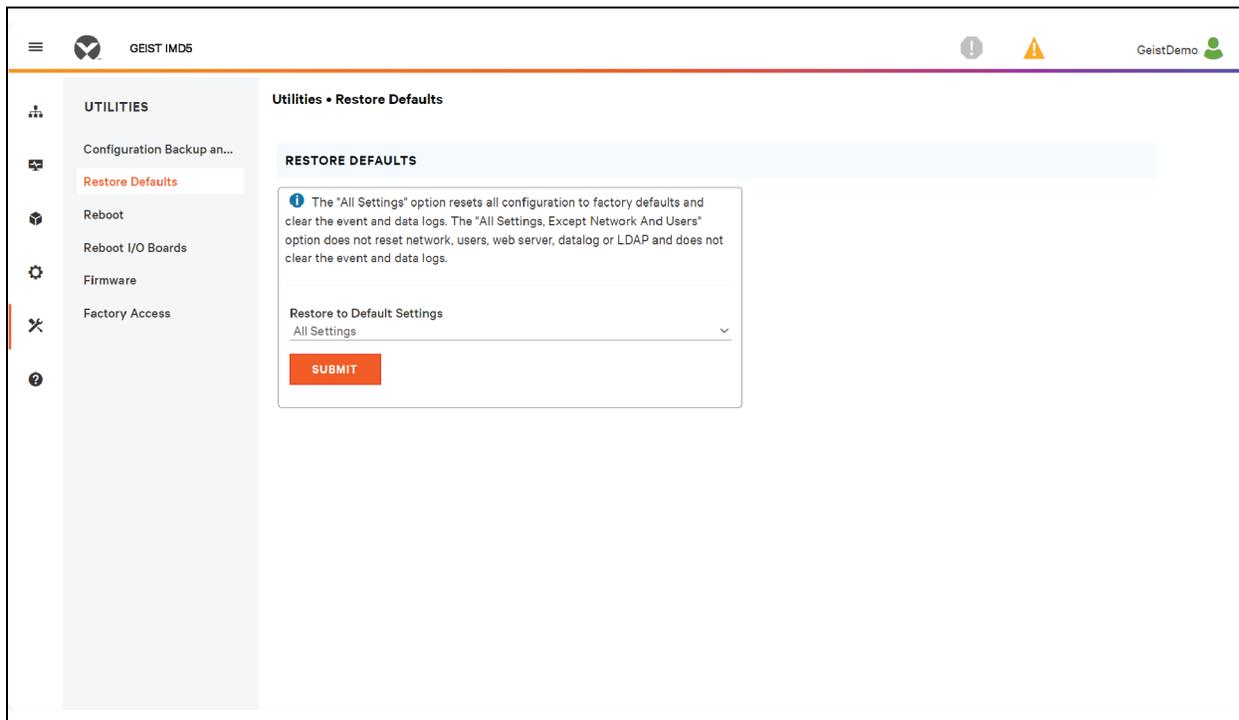
Tabla 5.14 Opciones de Restore Default

Opción	Descripción
All Settings	Restablece toda la configuración de /conf, /alarm y /dev a los valores de fábrica. También se borrarán el registro de sucesos y el registro de datos, y se ejecutará el comando de eliminación en cualquier dispositivo con estado <b>unavailable</b> . Esto hará que partes del sistema se reinicialicen. Se realizará correctamente y le seguirá un breve periodo en el que no se podrá acceder al sistema.
All Settings, Except Networks And Users	Como la opción <b>defaults</b> anterior, pero no restablece /conf/network, /conf/http, /conf/datalog, /auth ni /conf/ldap, y no borra el registro de sucesos ni el registro de datos. Esto hará que partes del sistema se reinicialicen. Se realizará correctamente y le seguirá un breve periodo en el que no se podrá acceder al sistema.

Para restaurar la configuración predeterminada:

1. Seleccione una de las opciones *All Settings* o *All Settings, Except Networks And Users* en el menú desplegable.
2. Haga clic en *SUBMIT*.

Figura 5.62 Información general sobre Restore Defaults

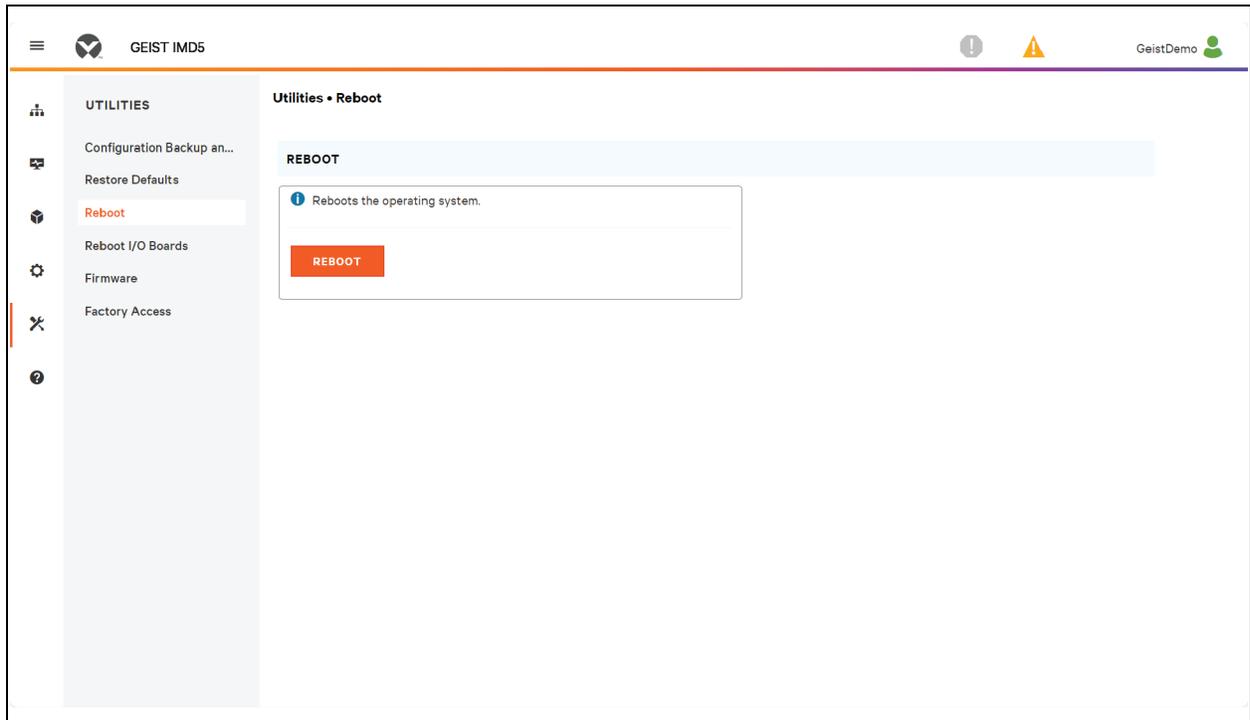


### 5.7.3 Reboot

Permite reiniciar el sistema operativo. Restablece el procesador del IMD que hace que el IMD se reinicie. Haga clic en *REBOOT* para reiniciar el sistema operativo.

**NOTA:** La alimentación de los dispositivos conectados no se ve afectada.

Figura 5.63 Información general sobre Reboot



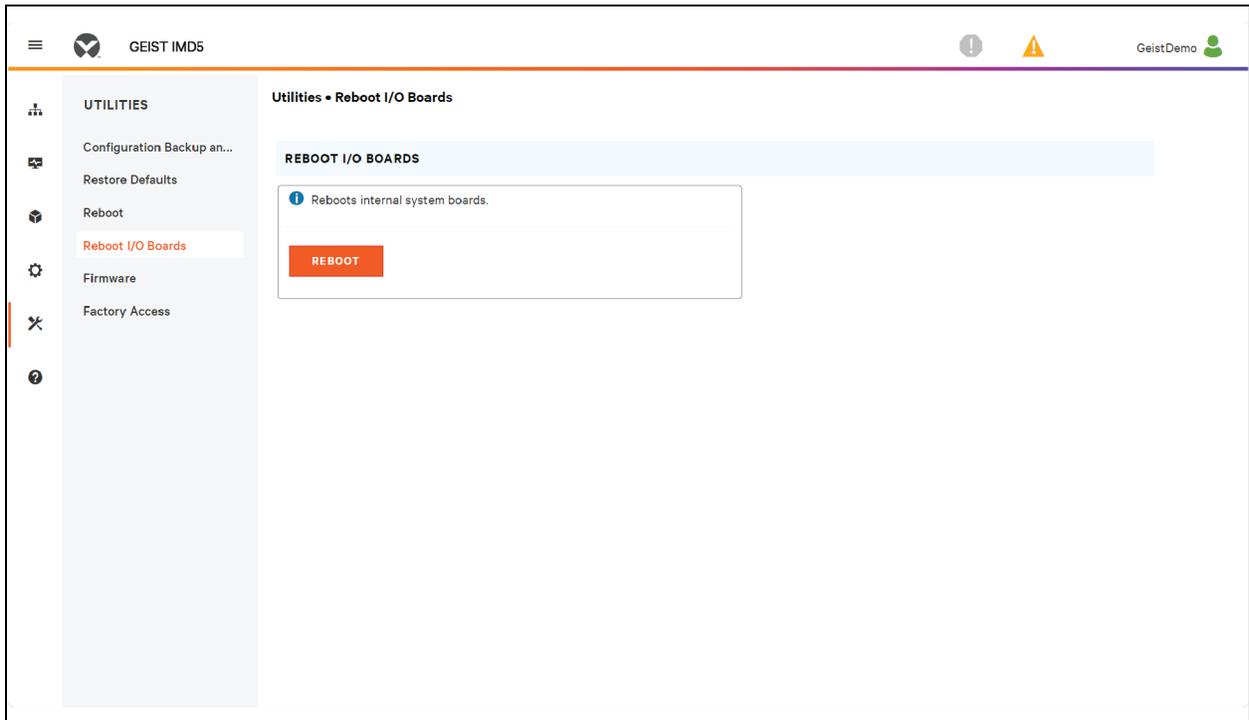
## 5.7.4 Reboot I/O Boards

Si la rPDU de Vertiv™ PowerIT no responde o no muestra todos los valores, al reiniciar las placas internas se reiniciará el sistema. De este modo, se restablecerán los procesadores de la placa de entrada interna y de las placas de salida, lo que hará que se reinicien.

Haga clic en *REBOOT* para reiniciar las placas internas del sistema.

**NOTA:** La alimentación de los dispositivos conectados no se ve afectada.

Figura 5.64 Información general sobre Reboot I/O Boards



## 5.7.5 Actualizaciones del firmware

Carga un archivo de firmware que actualiza el sistema. Esta acción requiere la autenticación del usuario y el usuario debe tener privilegios de administrador. Las actualizaciones de firmware normalmente se incluyen en un archivo .zip que contiene varios archivos, incluido el propio paquete de firmware, una copia del MIB de SNMP, un archivo de texto readme donde se explica cómo instalar el firmware y varios otros archivos de soporte según sea necesario. Asegúrese de descomprimir el archivo y siga las instrucciones incluidas.

### Para actualizar el firmware a través del archivo del paquete de firmware:

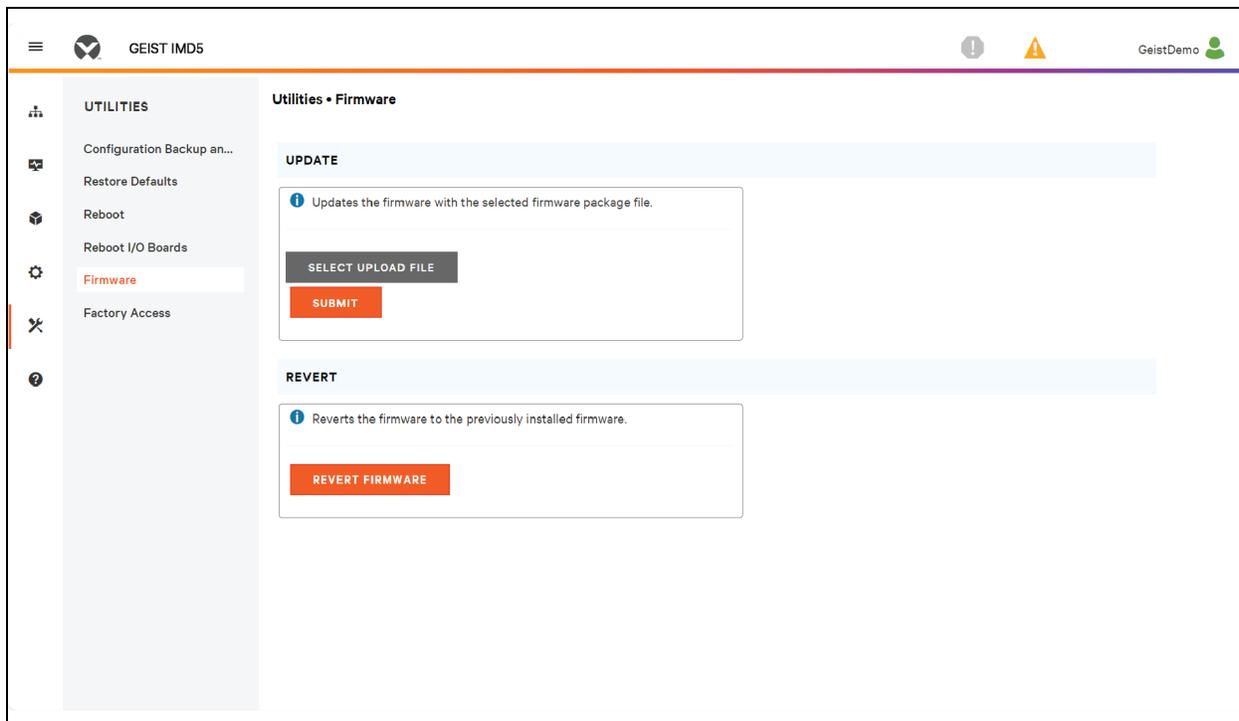
1. Haga clic en *SELECT UPLOAD FILE* y seleccione el archivo *.firmware* en la ventana *Open*.
2. Haga clic en *SUBMIT*.
3. Si hay algún problema (la unidad no se comporta correctamente) tras instalarse satisfactoriamente el firmware, haga clic en *REVERT FIRMWARE*.

### Para actualizar el firmware a través de una unidad flash USB:

1. Descargue el firmware más reciente en <https://www.vertiv.com/en-us/support/software-download/power-distribution/geist-upgradeable-series-v5-firmware/> y descomprima la carpeta.
2. Obtenga una unidad flash USB y aplíquelo el formato FAT32.
3. Cree un directorio en la unidad flash USB llamado *FIRMWARE* (no tiene que estar en mayúsculas).
4. Abra la carpeta del firmware descomprimido y copie el archivo *.firmware*.
5. Pegue este archivo en la carpeta *FIRMWARE* de la unidad flash.
6. Conecte la unidad flash USB en la PDU.

Durante la actualización, el IMD dejará de desplazar datos. Una vez completada la actualización, aparecerá un mensaje de inicio en la pantalla. Después del reinicio, el IMD reanudará el desplazamiento de datos en la pantalla.

**Figura 5.65 Información general sobre Firmware**



## 5.7.6 Factory Access

Factory Access proporciona información para el soporte técnico.

**Tabla 5.15 Opciones de Factory Access**

Opción	Descripción
Download Factory Support Package	Descarga un paquete de diagnóstico cifrado que se puede enviar al personal de asistencia técnica.
Factory Access	Permite el acceso de la fábrica a la unidad a través de SSH (para propósitos de depuración).

### Para descargar un paquete de soporte de fábrica:

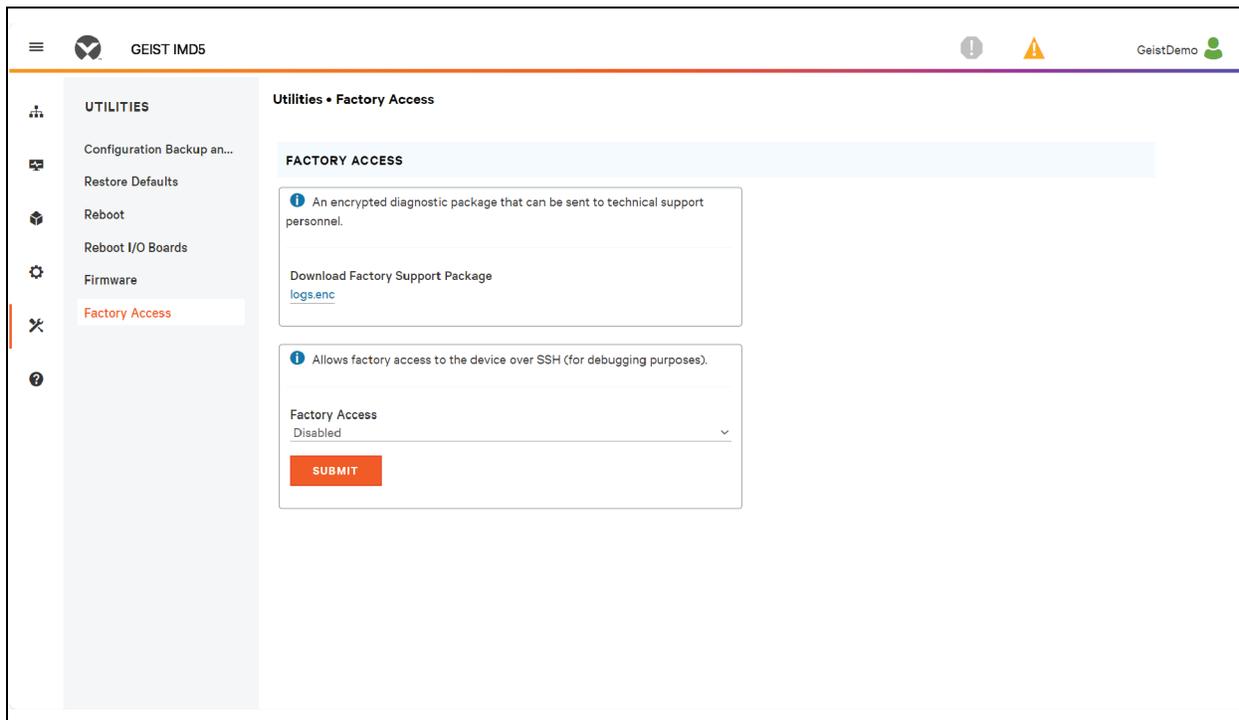
1. Haga clic en *Download Factory Support Package*.
2. Haga clic en *ENC*.

### Para habilitar/deshabilitar el acceso de fábrica:

1. Seleccione *Enable* o *Disable* en el menú desplegable.
2. Haga clic en *SUBMIT*.

**NOTA:** Se requiere la autenticación del usuario y el usuario debe tener privilegios de administrador.

Figura 5.66 Información general sobre Factory Access

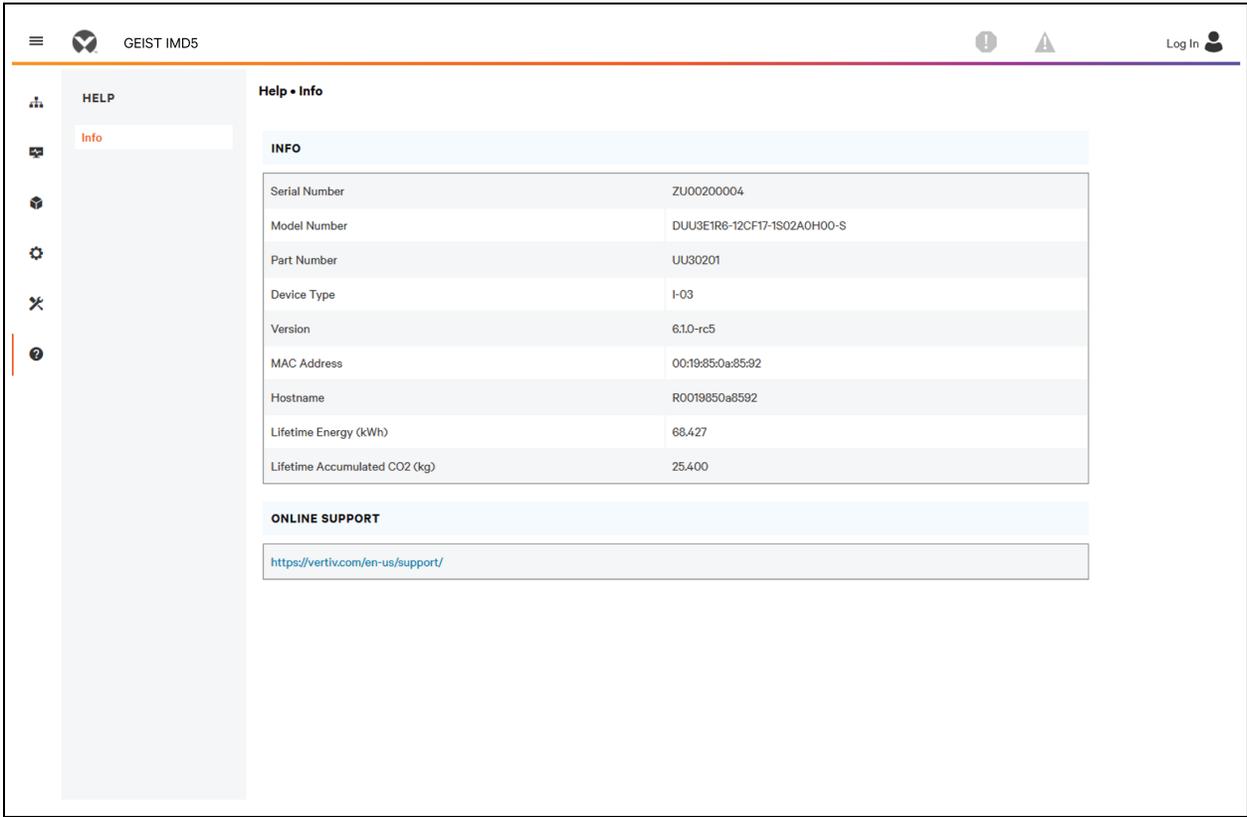


## 5.8 Submenú Help

### Página Info

La página Info muestra la información de configuración actual de la unidad, incluidos el nombre y el ID del dispositivo, el tipo de IMD instalado, la versión del firmware actual de la unidad y la información de red. La información de soporte del fabricante también está aquí.

Figura 5.67 Página Info



Esta página se ha dejado en blanco intencionadamente.

## 6 Vertiv™ Intelligence Director

Vertiv Intelligence Director incorpora una capa de visualización única y unificada para pequeñas implementaciones de las rPDU de Vertiv™PowerIT, los UPS de Vertiv™, los sensores de entorno y las salidas de la rPDU de Vertiv™PowerIT. Una vez implementado, Vertiv Intelligence Director ofrece una funcionalidad mejorada a través de la rPDU Vertiv™ PowerIT, no como un dispositivo autónomo, sino como una puerta de acceso para comprender el amplio ecosistema de dispositivos en el que está instalado.

### 6.1 Agregación

El elemento inicial de Vertiv Intelligence Director, disponible con las rPDU Vertiv™ PowerIT que ejecutan la versión de firmware 5.3.0 o posterior, se denomina agregación. Este elemento único permite:

- Utilizar la agregación para reducir el recuento de direcciones IP, agregar datos de varias PDU de montaje en rack y habilitar la administración de grupos de salidas de PDU de montaje en rack.
- Las PDU para rack se conectan mediante una conexión en cadena Ethernet, como en el ejemplo anterior de conexión en cadena.
- La cabeza de la PDU para rack en cadena está configurada como un administrador de matrices.
- La red de dispositivos de matriz puede incluir conmutadores de red.
- Se puede utilizar una única dirección IP asignada al administrador de matriz para acceder a un máximo de 50 dispositivos (el administrador de matriz y 49 dispositivos de matriz).
- Los ajustes de red del dispositivo de matriz se configuran automáticamente.
- A los dispositivos de matriz se accede mediante la dirección IP del administrador de matriz y un número de puerto. El número de puerto se puede obtener navegando por la página *Device>List* y pasando el cursor sobre el dispositivo.
- Los usuarios pueden definir grupos de dispositivos, por ejemplo, representando racks.
- El administrador de matriz genera mediciones agregadas como la potencia total del grupo y la potencia total, incluidos promedios, mínimos y máximos.
- Cuando se usa Vertiv Intelligence Director no se permite la conexión en cadena tolerante a errores.

Figura 6.1 Pestaña Aggregation

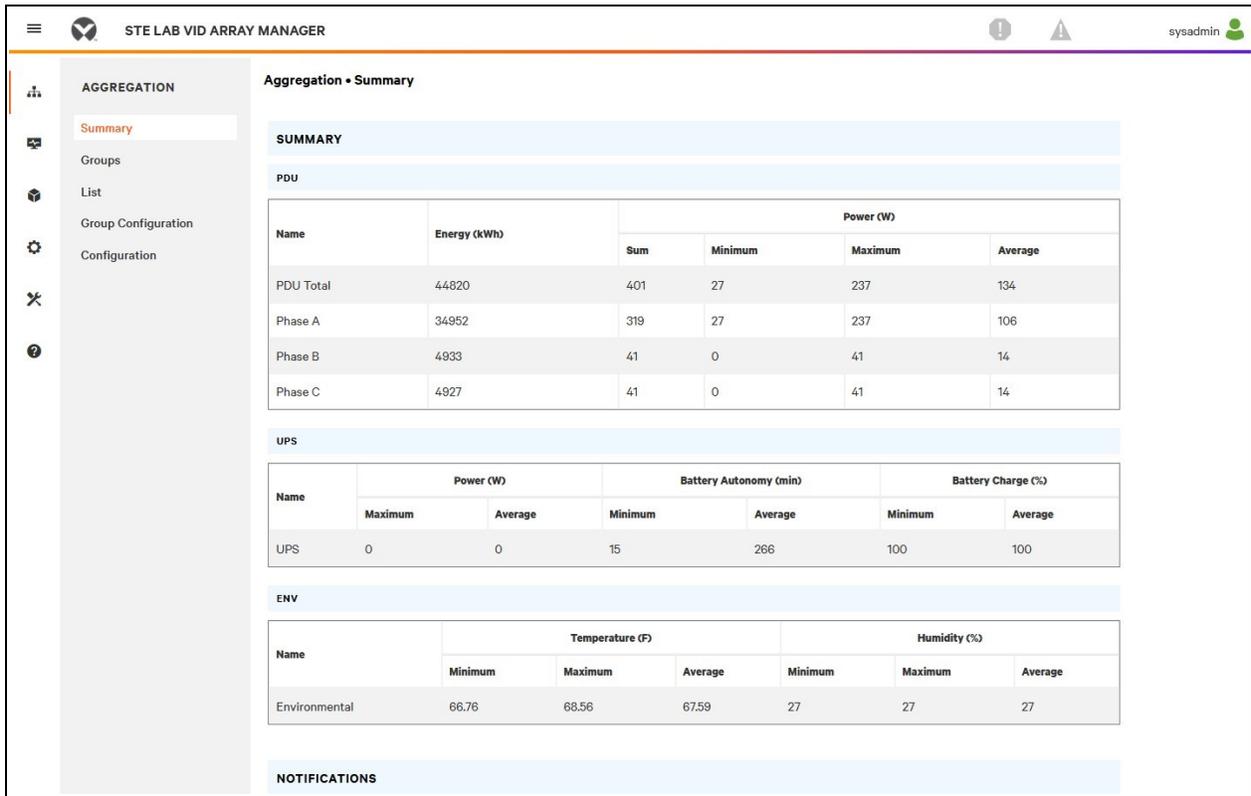
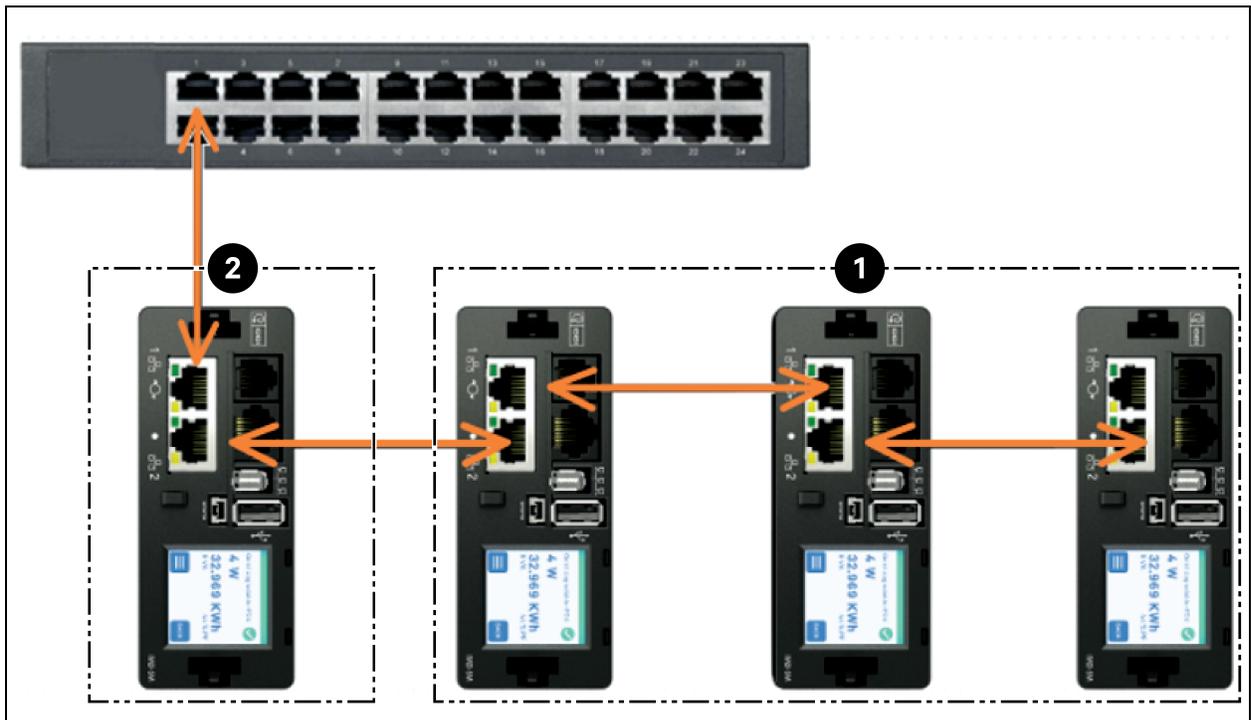


Figura 6.2 Agregación





Elemento	Descripción
1	Vertiv™ Liebert® GXT4
2	Dispositivos aguas abajo
3	Red del dispositivo
4	Dispositivos de matriz (rPDU PowerIT)
5	Red de administración
6	Administrador de matriz (rPDU PowerIT)
7	Conmutador Ethernet

Ya no es posible incorporar las nuevas PDU para rack IMD-02x cuando se utiliza un administrador de matriz que ejecuta el firmware 6.3.0 o posterior.

## 6.3 Configuración de red

En la versión inicial de agregación, los dispositivos de matriz se definen como rPDU de Vertiv™ PowerIT dentro de las plataformas de productos Vertiv™ PowerIT monitorizadas y conmutadas (3E, 03E, 3E-S, 03E-S, 3E-G, 03E-G and 5M) de Vertiv™ PowerIT, así como PDU de montaje en rack Vertiv™ MPH2™ y Vertiv™ MPX™, UPS Vertiv™ Liebert® GXT4, Vertiv™ Liebert® GXT5, Vertiv™ Liebert® PSI5, Vertiv™ Liebert® EXM, Vertiv™ Liebert® APM y Vertiv™ Liebert® ITA2, unidad de refrigeración en fila Vertiv™ Liebert® CRV y unidad de refrigeración Vertiv™ Liebert® VRC conectada mediante USB. Cada administrador de matriz puede admitir hasta 49 dispositivos de matriz, por lo que el número de administradores depende del tamaño general de la instalación y de la arquitectura de red de preferencia.

El administrador de matriz debe ponerse en marcha antes de conectarse a la red de administración primaria o a la red de dispositivos de matriz. Esta puesta en marcha se realiza habitualmente mediante un ordenador portátil o una máquina local conectada directamente al puerto 1 en el IMD.

Una vez establecida la conectividad local, puede poner en marcha el administrador de matriz.

### Para poner en marcha el administrador de matriz:

1. Desplácese a *System>Locale*. Seleccione las unidades de idioma y temperatura predeterminadas que correspondan en los menús desplegables. Esta configuración se deriva a los dispositivos de matriz de su red.
2. Desplácese a *System>Network*. En el protocolo IPv6, elija *Enabled* en el menú desplegable.
3. Desplácese a *Aggregation>Configuration*. Cambie la configuración como desee.
  - a. **Aggregation:** elija *Enabled* en el menú desplegable.
  - b. **Array device Username:** define el nombre de usuario que se va a configurar en todos los dispositivos de matriz.
  - c. **Array device Password:** define la contraseña que se va a configurar en todos los dispositivos de matriz.
  - Introduzca la nueva contraseña, confírmela y haga clic en *Submit*. Al configurar la opción *Aggregation*, asegúrese de que la contraseña del dispositivo gestionado cumpla con todas las reglas de complejidad de la contraseña del dispositivo de matriz. A menos que el usuario las haya cambiado, estas requieren una contraseña con una longitud mínima de 8 caracteres con las rPDU que ejecuten firmware 5.9.0 o posterior.

4. Haga clic en *Submit*.

Una vez que se active la agregación en el administrador de matriz, configure los ajustes restantes del administrador de matriz. Conecte el administrador de matriz a la red de administración (puerto 1) del IMD y a la red de dispositivos (puerto 2).

**NOTA: El administrador de matriz tiene una red DHCP incorporada para asignar direcciones a sus dispositivos de matriz. Esta red DHCP utiliza direcciones 192.168.123/192.168.124, que no se pueden utilizar para la red de administración.**

## Dispositivos de matriz

En la versión inicial de la agregación, los dispositivos de matriz se definen como rPDU de Vertiv™ PowerIT dentro de las plataformas del producto monitorizadas y conmutadas de Vertiv™ PowerIT, así como PDU de montaje en rack Vertiv™ MPH2™ y Vertiv™ MPX™, UPS Vertiv™ Liebert® GXT4, Vertiv™ Liebert® GXT5, Vertiv™ Liebert® PSI5, Vertiv™ Liebert® EXM, Vertiv™ Liebert® APM y Vertiv™ Liebert® ITA2, unidad de refrigeración en fila Vertiv™ Liebert® CRV y unidad de refrigeración Vertiv™ Liebert® VRC conectada mediante USB. Todos los rPDU de Vertiv™ PowerIT (modelos de IMD 02, 02E) deben estar ejecutando el firmware Versión 3.4 o posterior; los rPDU de Vertiv™ PowerIT (3E, 03E, 3E-S, 03E-S, 3E-G, 03E-G) y los rPDU para rack R-Series deben estar ejecutando el firmware versión 5.3.0 o posterior. Los dispositivos de matriz de la oración anterior no se pueden incorporar a los controladores de matriz con firmware 6.3.0 o posterior. En todos los casos, se recomienda encarecidamente que todas las rPDU se actualicen a la última versión de firmware disponible. Si las rPDU Vertiv™ PowerIT se instalan por primera vez y nunca se han configurado, ya están listas para la agregación. Si las rPDU Vertiv™ PowerIT se han implementado en un entorno de computación y se han puesto en marcha con la configuración de la LAN local y las cuentas de usuario, cada rPDU de Vertiv™ PowerIT debe restablecerse a sus valores de fábrica mediante *Utilities>Restore Defaults*. Seleccione *All Settings* y haga clic en *Submit*. A continuación, el administrador de matriz derivará los datos de configuración a los dispositivos de matriz.

### Para configurar una nueva instalación con un administrador de matriz:

1. Instale los dispositivos de matriz en racks y conecte los racks.
2. Encadene los dispositivos de matriz entre sí cuando sea apropiado utilizando los puertos con las etiquetas 1 y 2 en el IMD.
  - Si se usan conexiones de rPDU en cadena, asegúrese de que ninguna conexión incluya más de 20 rPDU.
  - Los dispositivos de matriz se pueden conectar en red mediante conexiones en cadena, conexiones en estrella o una combinación de ambas.
3. Instale el administrador de matriz en un rack. Mediante un portátil o una máquina local, conéctese al puerto 1 para configurar la agregación.
4. Conecte el administrador de matriz a la red de administración a través del puerto 1.
5. Conecte el administrador de matriz a la red del dispositivo de matriz a través del puerto 2.

### Para configurar una instalación existente con un administrador de matriz:

**NOTA: utilice las siguientes instrucciones si hay rPDU de Vertiv™ PowerIT conectadas en cadena.**

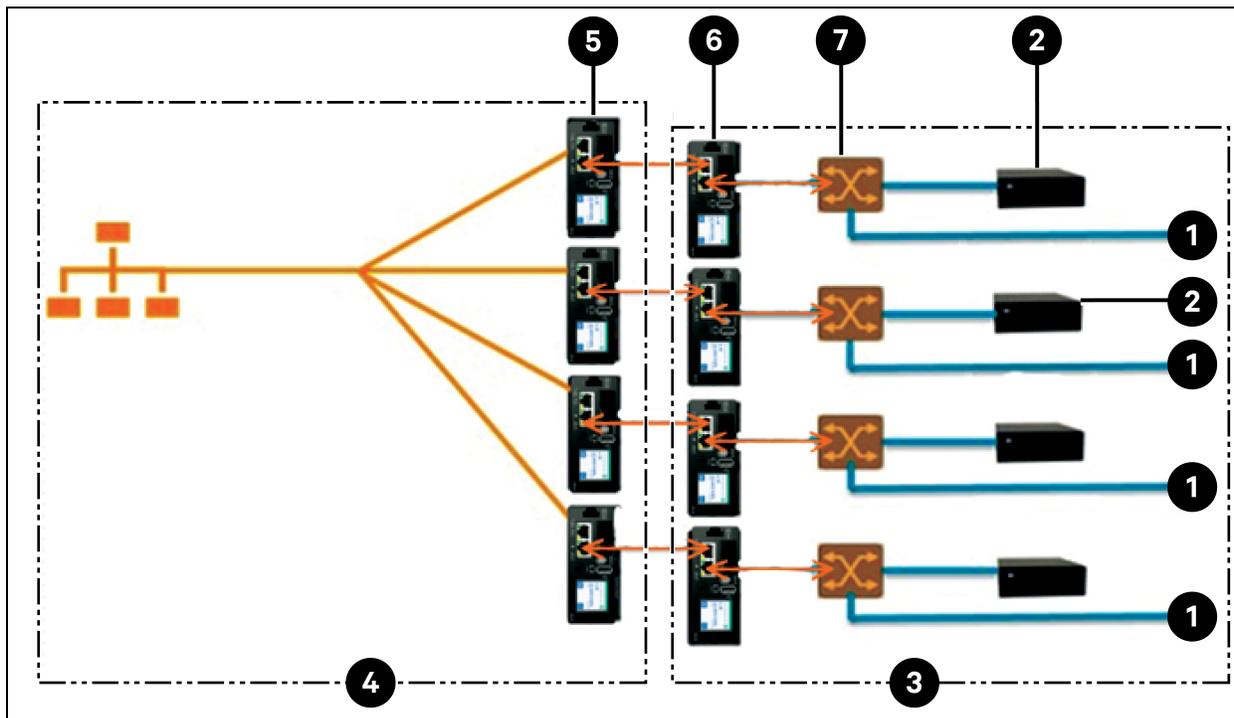
1. Designe un administrador de matriz y desconéctelo de la red de administración.

2. Restablezca todos los dispositivos de matriz a los valores predeterminados de fábrica. Las conexiones físicas de Ethernet en la conexión en cadena pueden permanecer iguales; sin embargo, si se conectan previamente en una configuración en bucle, la rPDU de Vertiv™ PowerIT final de la cadena se debe desconectar del conmutador de red.
3. Habilite la opción Aggregation en el administrador de matriz.
4. Conecte el administrador de matriz a la red de administración a través del puerto 1.
5. Conecte el administrador de matriz a la red de matrices a través del puerto 2.

## Varios administradores de matriz

Para instalaciones con varios administradores de matriz, tenga en cuenta que cada red de dispositivos debe funcionar como una red autónoma y aislada. Veamos un ejemplo de 200 rPDU, representado en la **Figura 6.4** en la página opuesta. Esta instalación requeriría un mínimo de cuatro administradores de matriz, cada uno de los cuales administra su propia red de dispositivos. Cada administrador de matriz es visible en la red de administración y actúa como un servidor DHCP para sus dispositivos de matriz. Un usuario de la red de administración puede desplazarse a través de cada administrador de matriz para llegar a la interfaz de un dispositivo de matriz. Otras consideraciones pueden afectar a la cantidad de administradores de matriz. Si tiene una arquitectura de red en filas, es posible que prefiera un administrador de matriz al comienzo de cada fila, en lugar de un administrador de matriz que atraviese varias filas. Dependiendo de cómo estén divididos estos 200 armarios en filas, puede que tenga más de cuatro administradores de matriz. Una vez decidida la configuración, siga el proceso correspondiente para la agregación.

Figura 6.4 Ejemplo de configuración de red



Elemento	Descripción
1	Otros dispositivos
2	UPS
3	Red del dispositivo
4	Red de administración
5	Administradores de matriz (rPDU PowerIT)
6	Dispositivos de matriz (rPDU PowerIT)
7	Conmutador Ethernet

**NOTA:** Solo se requerirá un conmutador Ethernet de red de dispositivos cuando se conecte más de un dispositivo de puerto de red único al final de una conexión en cadena de rPDU o cuando no se utilicen conexiones en cadena.

## 6.4 Vistas

Cuando se establece la comunicación entre el administrador de matriz y los dispositivos de matriz, se rellenan automáticamente varias vistas en la interfaz de usuario. Las nuevas vistas en la pestaña Device de la barra de navegación superior son:

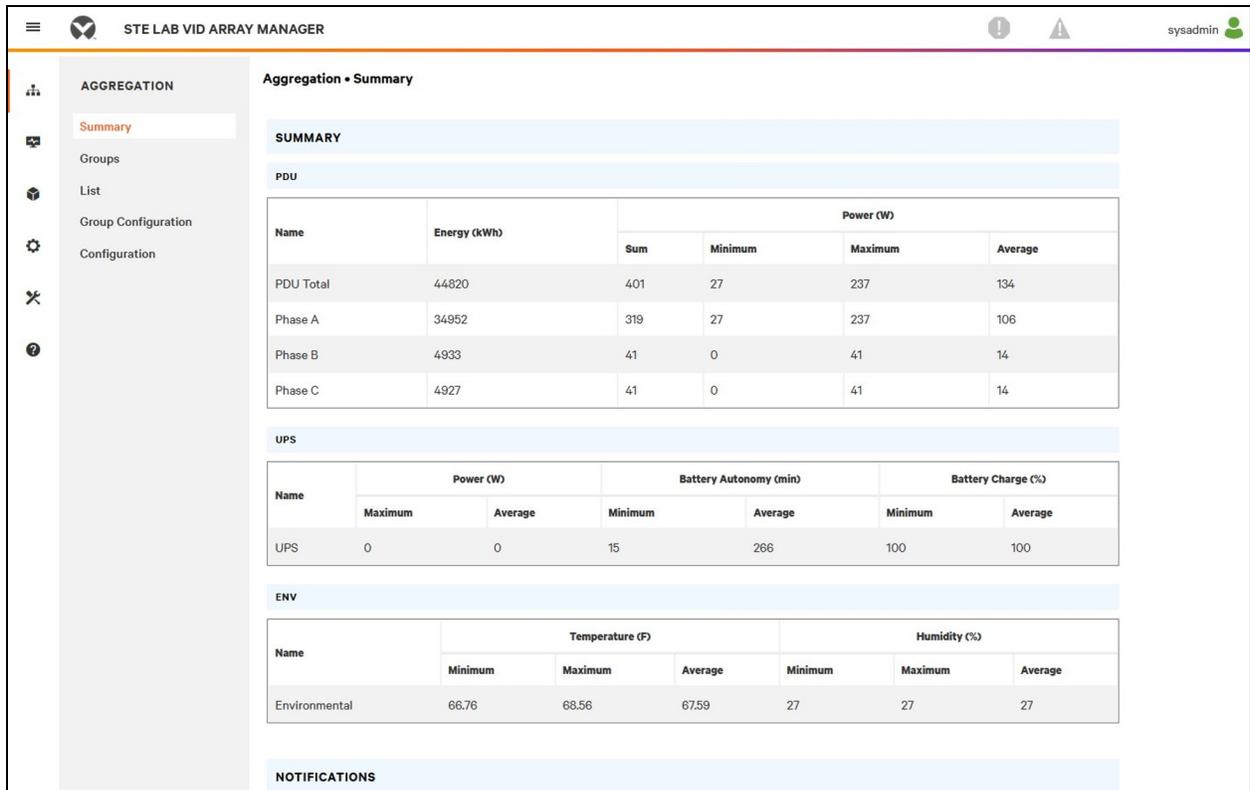
- Summary
- Groups
- List

- Group Configuration
- Configuración

## 6.4.1 Summary

La vista Summary recopila los datos de todos los dispositivos de matriz mediante un esquema conciso de los detalles relevantes de alimentación, entorno y alarmas.

Figura 6.5 Pestaña Summary



## PDU de montaje en rack

La red de la rPDU de Vertiv™ PowerIT se resume en los siguientes puntos de datos:

- **Energy (kWh):** la energía total de la rPDU de Vertiv™ PowerIT dentro de la red de dispositivos.
- **Power (W) Sum:** la carga energética total de la rPDU de Vertiv™ PowerIT dentro de la red de dispositivos.
- **Power (W) Minimum:** la carga energética más baja de grupo de la rPDU de Vertiv™ PowerIT dentro de la red de dispositivos.
- **Power (W) Maximum:** la carga energética más alta de grupo de la rPDU de Vertiv™ PowerIT dentro de la red de dispositivos.
- **Power (W) Average:** la carga energética promedio de grupo de la rPDU de Vertiv™ PowerIT dentro de la red de dispositivos.

**NOTA: estas lecturas se repiten por fase (se muestran cuando solo hay rPDU de Vertiv™ PowerIT trifásicas).**

## UPS

La red de UPS se resume en los siguientes puntos de datos:

- **Power (W) Maximum:** la carga energética más alta del UPS dentro de la red de dispositivos.
- **Power (W) Average:** la carga energética promedio del UPS dentro de la red de dispositivos.
- **Battery Autonomy (min) Minimum:** el tiempo de funcionamiento más bajo de la batería del UPS dentro de la red de dispositivos.
- **Battery Autonomy (min) Average:** el tiempo de funcionamiento promedio de la batería del UPS dentro de la red de dispositivos.
- **Battery Charge (%) Minimum:** la carga más baja de la batería del UPS dentro de la red de dispositivos.
- **Battery Charge (%) Average:** la carga promedio de la batería del UPS dentro de la red de dispositivos.

## Sensores de entorno (ENV)

La categoría de entorno se resume en los siguientes puntos de datos:

**NOTA: Los valores de humedad estarán en blanco cuando se utilicen sensores solo de temperatura.**

- **Temperature (F) Minimum:** la temperatura más baja dentro de la red de dispositivos.
- **Temperature (F) Maximum:** la temperatura más alta dentro de la red de dispositivos.
- **Temperature (F) Average:** la temperatura promedio dentro de la red de dispositivos.
- **Humidity (%) Minimum:** la humedad más baja dentro de la red de dispositivos.
- **Humidity (%) Maximum:** la humedad más alta dentro de la red de dispositivos.
- **Humidity (%) Average:** la humedad promedio dentro de la red de dispositivos.

## Refrigeración térmica

- **Fan Speed (%) Minimum:** la velocidad del ventilador del dispositivo térmico más baja dentro de la red de dispositivos.
- **Fan Speed (%) Maximum:** la velocidad del ventilador del dispositivo térmico más alta dentro de la red de dispositivos.
- **Fan Speed (%) Average:** la velocidad del ventilador del dispositivo térmico promedio dentro de la red de dispositivos.
- **Temperature (F) Minimum:** la temperatura del dispositivo térmico más baja dentro de la red de dispositivos.
- **Temperature (F) Maximum:** la temperatura del dispositivo térmico más alta dentro de la red de dispositivos.
- **Temperature (F) Average:** la temperatura del dispositivo térmico promedio dentro de la red de dispositivos.
- **Capacity (%) Minimum:** la capacidad del dispositivo térmico más baja dentro de la red de dispositivos.

- **Capacity (%) Maximum:** la capacidad del ventilador del dispositivo térmico más alta dentro de la red de dispositivos.
- **Capacity (%) Average:** la capacidad del dispositivo térmico promedio dentro de la red de dispositivos.

## Notificaciones

Las notificaciones muestran alarmas pendientes de dispositivos en la red de dispositivos.

## 6.4.2 Groups

Una vez establecidos los grupos dentro de Group Configuration, la vista Groups resume los datos de alimentación y entorno.

Figura 6.6 Pestaña Groups

The screenshot shows the 'Groups' tab in the STE LAB VID ARRAY MANAGER. The main content area displays a table for 'GROUP W' with the following data:

Name	Energy (kWh)	Power (W)			
		Sum	Minimum	Maximum	Average
PDU Total	3657	28	28	28	28
Phase A	3657	28	28	28	28
Phase B	0.000	0	0	0	0
Phase C	0.000	0	0	0	0

Below this table, there is a section for 'Outlet' with the following data:

Name	Energy (kWh)	Power (W)			
		Sum	Minimum	Maximum	Average
Outlet	1858	82	0	82	16

There is also a section for 'UPS' with the following data:

Name	Power (W)		Battery Autonomy (min)		Battery Charge (%)	
	Maximum	Average	Minimum	Average	Minimum	Average
UPS	0	0	440	440	100	100

At the bottom, there is a section for 'GROUP K7' with a table structure similar to the others.

Los puntos de datos disponibles son:

### Group rPDU

- **Energy (kWh):** la energía total de la rPDU de Vertiv™ PowerIT dentro del grupo.
- **Power (W) Sum:** la carga energética total de la rPDU de Vertiv™ PowerIT dentro del grupo.
- **Power (W) Minimum:** la carga energética más baja de la rPDU de Vertiv™ PowerIT dentro del grupo.
- **Power (W) Maximum:** la carga energética más alta de la rPDU de Vertiv™ PowerIT dentro del grupo.

- **Power (W) Average:** la carga energética promedio de la rPDU de Vertiv™ PowerIT dentro del grupo.

**NOTA: Estas lecturas se repiten por fase (se muestran cuando solo hay rPDU trifásicas).**

### Group rPDU Outlet

- **Energy (kWh):** la energía total de la salida de la rPDU de Vertiv™ PowerIT dentro del grupo.
- **Power (W) Sum:** la carga energética total de la salida de la rPDU de Vertiv™ PowerIT dentro del grupo.
- **Power (W) Minimum:** la carga energética más baja de la salida de la rPDU de Vertiv™ PowerIT dentro del grupo.
- **Power (W) Maximum:** la carga energética más alta de la salida de la rPDU de Vertiv™ PowerIT dentro del grupo.
- **Power (W) Average:** la carga energética promedio de la salida de la rPDU de Vertiv™ PowerIT dentro del grupo.

Estas lecturas se repiten para cada grupo de salidas de la rPDU de Vertiv™ PowerIT presente en el grupo cuando hay, por lo menos, una salida supervisada. Si en el grupo existe una combinación de PDU de montaje en rack con salidas monitorizadas y salidas no monitorizadas, las lecturas solamente proporcionarán el total de las PDU de montaje en rack con salidas monitorizadas.

Estas lecturas se repiten por fase (se muestran cuando solo hay PDU trifásicas).

**NOTA: Las lecturas de energía reflejan la suma de las lecturas de energía de las salidas y al restablecer la lectura de energía de cada salida también se restablecerá la energía total del grupo de salidas.**

El icono de operación  se muestra para cada grupo que incluya, por lo menos, una salida de PDU de montaje en rack con capacidad de conmutación.

#### Para cambiar la operación del grupo de salidas:

1. Haga clic en el icono de operación.
2. Seleccione la operación que se debe realizar (se aplica solo a las salidas de PDU de montaje en rack con capacidad de conmutación asignadas al grupo):
  - **On/Off:** activa o desactiva todas las salidas.
  - **Reboot:** para las salidas que están actualmente activadas, el reinicio desactiva las salidas y luego vuelve a activarlas después del retardo de espera de reinicio.  
  
Las salidas que actualmente estén desactivadas se activan al reiniciar.
  - **Cancel:** cancela la operación actual si no se ha completado.
3. Para las operaciones relacionadas con el estado de las salidas, al ajustar Delay en True se utiliza la configuración de retardo actual para cada salida.
4. Seleccione *Submit* para iniciar la acción.

### Group UPS

- **Power (W) Maximum:** la carga energética más alta del UPS dentro del grupo.
- **Power (W) Average:** la carga energética promedio del UPS dentro del grupo.

- **Battery Autonomy (min) Minimum:** el tiempo de funcionamiento más bajo de la batería del UPS dentro del grupo.
- **Battery Autonomy (min) Average:** el tiempo de funcionamiento promedio de la batería del UPS dentro del grupo.
- **Battery Charge (%) Minimum:** la carga más baja de la batería del UPS dentro del grupo.
- **Battery Charge (%) Average:** la carga promedio de la batería del UPS dentro del grupo.

### **Group Environmental**

- **Temperature (F) Minimum:** la temperatura más baja dentro del grupo.
- **Temperature (F) Maximum:** la temperatura más alta dentro del grupo.
- **Temperature (F) Average:** la temperatura promedio dentro del grupo.
- **Humidity (%) Minimum:** la humedad más baja dentro del grupo.
- **Humidity (%) Maximum:** la humedad más alta dentro del grupo.
- **Humidity (%) Average:** la humedad promedio dentro del grupo.

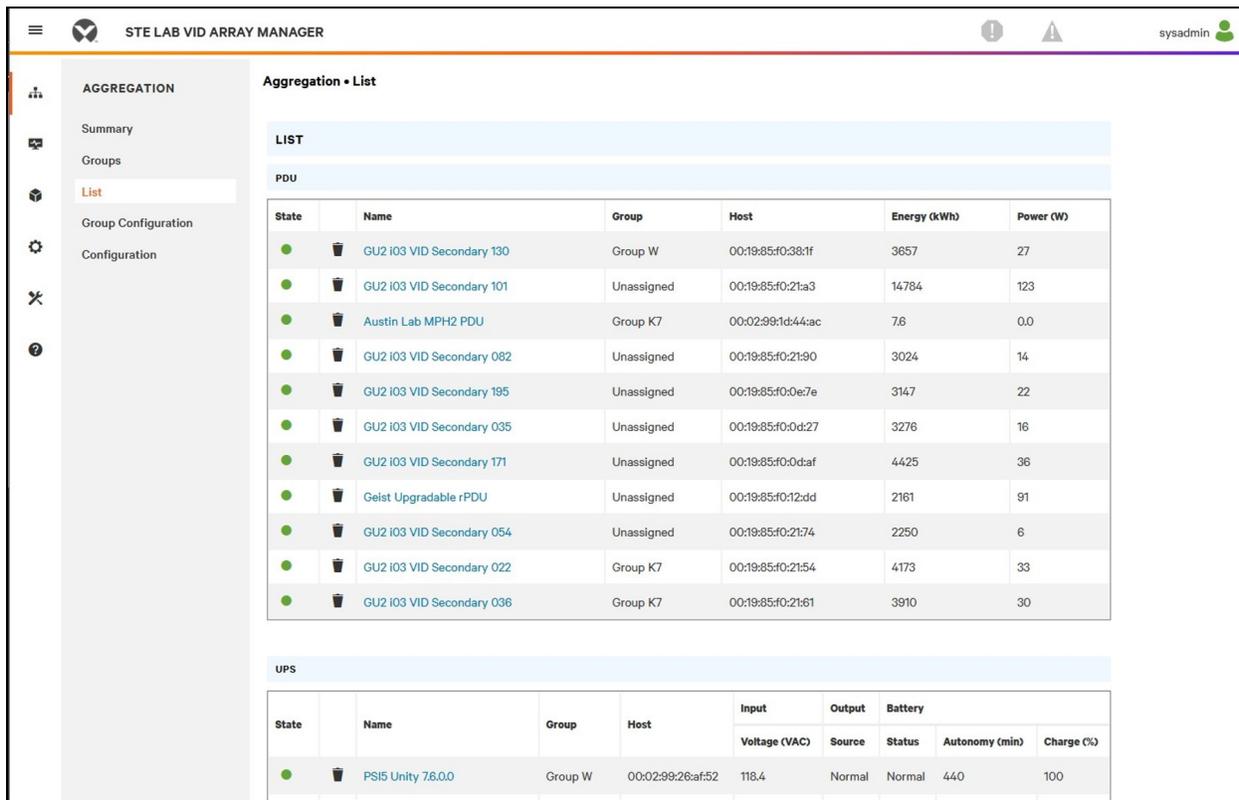
### **Group Thermal Cooling**

- **Fan Speed (%) Minimum:** la velocidad del ventilador del dispositivo térmico más baja dentro del grupo.
- **Fan Speed (%) Maximum:** la velocidad del ventilador del dispositivo térmico más alta dentro del grupo.
- **Fan Speed (%) Average:** la velocidad del ventilador del dispositivo térmico promedio dentro del grupo.
- **Temperature (F) Minimum:** la temperatura del dispositivo térmico más baja dentro del grupo.
- **Temperature (F) Maximum:** la temperatura del dispositivo térmico más alta dentro del grupo.
- **Temperature (F) Average:** la temperatura del dispositivo térmico promedio dentro del grupo.
- **Capacity (%) Minimum:** la capacidad del dispositivo térmico más baja dentro del grupo.
- **Capacity (%) Maximum:** la capacidad del dispositivo térmico más alta dentro del grupo.
- **Capacity (%) Average:** la capacidad del dispositivo térmico promedio dentro del grupo.

### **6.4.3 List**

La vista List presenta un inventario de todos los dispositivos dentro de la red de dispositivos del administrador de matriz.

Figura 6.7 Pestaña List



El inventario se subdivide en las siguientes categorías:

### PDU de montaje en rack

Todas las rPDU de Vertiv™ PowerIT de la red de dispositivos entran en esta categoría y presentan los siguientes puntos de datos:

- **State:** el estado de la rPDU de Vertiv™ PowerIT. El estado es Normal o Unavailable (pérdida de conectividad).
- **Name:** etiqueta de la rPDU de Vertiv™ PowerIT. Al hacer clic en el nombre, se abre una pestaña del navegador para acceder al dispositivo.
- **Group:** el nombre del grupo. Si no hay un grupo creado por el usuario, el nombre del grupo es Unassigned.
- **Energy:** energía de la rPDU de Vertiv™ PowerIT.
- **Power:** carga energética total de la rPDU de Vertiv™ PowerIT.

### UPS

Todos los dispositivos UPS de la red de dispositivos entran en esta categoría y presentan los siguientes puntos de datos:

- **State:** el estado del UPS. El estado es Normal o Unavailable (pérdida de conectividad).
- **Name:** etiqueta del UPS. Al hacer clic en el nombre, se abre una pestaña del navegador para acceder al dispositivo.

- **Group:** el nombre del grupo. Si no hay un grupo creado por el usuario, el nombre del grupo es Unassigned.
- **Input Voltage:** voltaje de entrada del UPS.
- **Output Source:** el modo de funcionamiento del UPS, que puede ser: Normal, Bypass, Battery, Booster, Reducer, Off u Other.
- **Status:** el estado de la batería, que puede ser: Normal, Low, Depleted o Unknown.
- **Battery Autonomy:** tiempo de funcionamiento de la batería del UPS.
- **Charge:** carga de la batería del UPS.

## Sensores de entorno (ENV)

Todos los sensores de entorno de la red de dispositivos entran en esta categoría y presentan los siguientes puntos de datos:

- **State:** el estado del sensor. El estado es Normal o Unavailable (pérdida de conectividad).
- **Name:** etiqueta del sensor. Al hacer clic en el nombre, se abre una pestaña del navegador para acceder al dispositivo.
- **Group:** el nombre del grupo. Si no hay un grupo creado por el usuario, el nombre del grupo es Unassigned.
- **Device:** muestra la dirección MAC y la etiqueta de la rPDU de Vertiv™ PowerIT principal del sensor.
- **Temperature (F):** lectura de la temperatura (temperatura principal solo con sensores GT3HD).
- **Humidity (%):** lectura de humedad. Este campo está en blanco si solo se despliegan los sensores de temperatura SRT.

Los sensores de entorno comunican sus valores a través de la MIB de las rPDU de Vertiv™ PowerIT a las que están conectados. No son sensores independientes con sus propias direcciones IP. En esta versión, los únicos sensores válidos son los sensores SRT, GTHD o GTHD3 de Vertiv™ PowerIT conectados a la rPDU de Vertiv™ PowerIT.

**NOTA: La etiqueta de cualquier dispositivo puede personalizarse iniciando sesión en el dispositivo y editarse a través del icono de configuración.**

**NOTA: Para eliminar un dispositivo que se ha quitado de la red, seleccione el icono de la papelera situado junto al dispositivo. Al seleccionar el icono de eliminar, se elimina el dispositivo y cualquier sensor de entorno conectado al mismo.**

## Refrigeración térmica

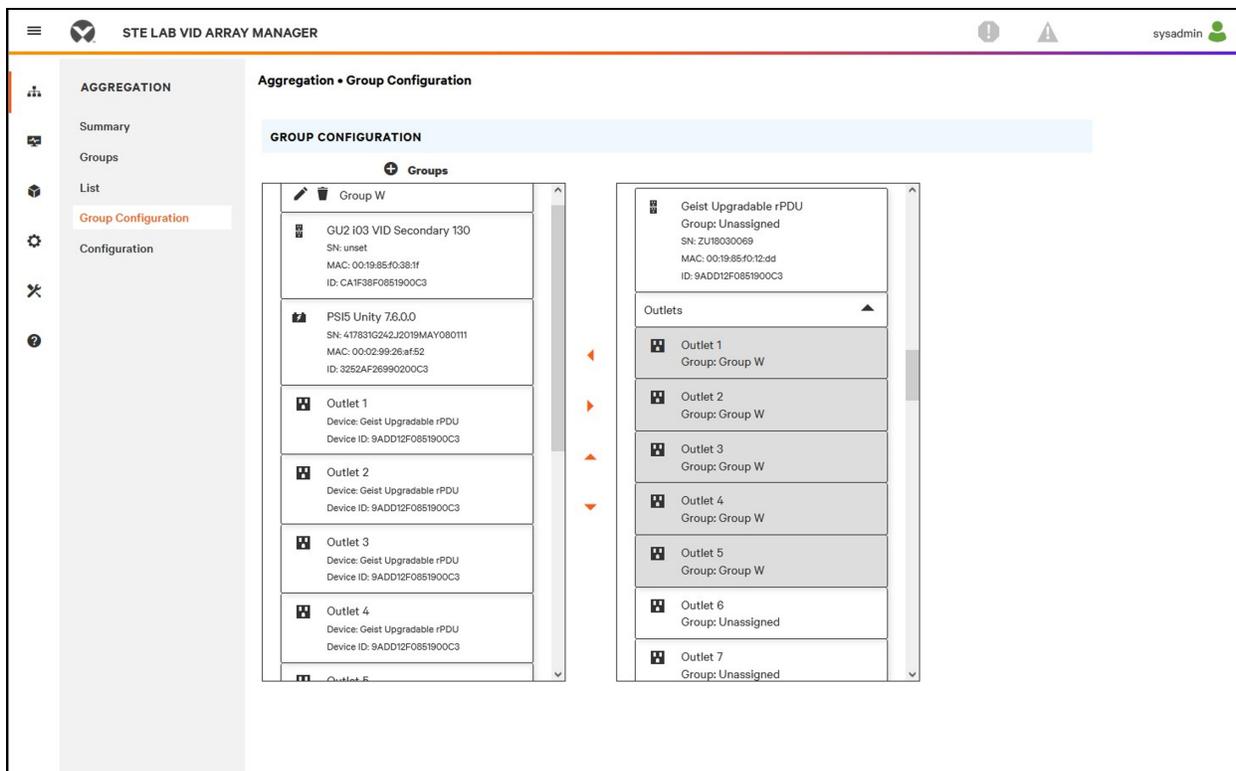
- **State:** el estado de la refrigeración. El estado es normal o no disponible (pérdida de conectividad).
- **Name:** etiqueta del dispositivo de refrigeración térmica. Al hacer clic en el nombre, se abre una pestaña del navegador para acceder al dispositivo.
- **Group:** el nombre del grupo. Si no hay un grupo creado por el usuario, el nombre del grupo es Unassigned.
- **Host:** dirección MAC.
- **Fan Speed (%):** velocidad del ventilador del dispositivo térmico.
- **Temperature (F):** temperatura del dispositivo térmico.

- **Capacity (%):** capacidad del dispositivo térmico.

### 6.4.4 Group Configuration

En la página Group Configuration, puede definir grupos de dispositivos con fines de agregación de datos y analíticos. Un grupo, a menudo, hace referencia a una unidad de medida dentro de un entorno de computación que incluye varios dispositivos de matriz, como un rack con dos rPDU de Vertiv™ PowerIT, dispositivos UPS y sensores de entorno o una fila que incluye varios racks.

Figura 6.8 Group Configuration



La página Group Configuration muestra una lista de los dispositivos detectados automáticamente bajo la columna *Unassigned* que muestra:

- Uno o varios iconos que definen el tipo de dispositivo, como rPDU de Vertiv™ PowerIT, sensor de entorno, UPS o salida de la rPDU de Vertiv™ PowerIT.
- Etiqueta del dispositivo
- N.º de serie
- Dirección MAC
- ID

A la izquierda se muestran los grupos de dispositivos configurados (que normalmente representan racks).

**Para crear un nuevo grupo:**

1. Haga clic en el *signo más (+)* a la izquierda de Groups, para añadir un nuevo grupo, bajo Groups.
2. Haga clic en el icono de configuración para cambiar el nombre de la etiqueta de grupo.

3. Edite la etiqueta, si lo desea, y haga clic en *Save*.
4. Para asignar dispositivos al grupo, resalte el grupo deseado (dentro de la categoría *Groups*) y resalte los dispositivos deseados dentro de la categoría *Unassigned*.

**NOTA: Debe hacer clic en la flecha hacia abajo debajo de la PDU para ver su lista de salidas.**

5. Haga clic en la *flecha a la derecha* para asignar los dispositivos al grupo.
6. Repita el proceso para otros grupos, según sea necesario.

**NOTA: Los grupos se pueden reordenar haciendo clic en las flechas arriba o abajo.**

**Para quitar dispositivos de un grupo:**

Resalte los dispositivos y haga clic en la *flecha a la derecha*.

**Para eliminar un grupo:**

Haga clic en el icono de la papelera situado junto al nombre del grupo.

**NOTA: Al eliminar un grupo, todos sus dispositivos vuelven al grupo *Unassigned*.**

## 6.5 Interfaces

Los dispositivos de matriz se combinan para formar grupos; cada dispositivo conserva su propia interfaz de usuario y datos de SNMP independientes.

**Para acceder a la interfaz de usuario del dispositivo de matriz:**

1. En la vista *List*, use el ratón para desplazar el cursor por encima de las entradas de la tabla. Al pausar los dispositivos, aparecen un resaltado amarillo y un cuadro de texto. El cuadro de texto muestra la dirección IP y el número de puerto del dispositivo.
2. Desplácese a una dirección IP y al número de puerto para acceder a la interfaz del servidor web del dispositivo.  
  
- O bien -
3. Haga clic en el nombre del dispositivo para acceder al hipervínculo para la interfaz web del dispositivo.

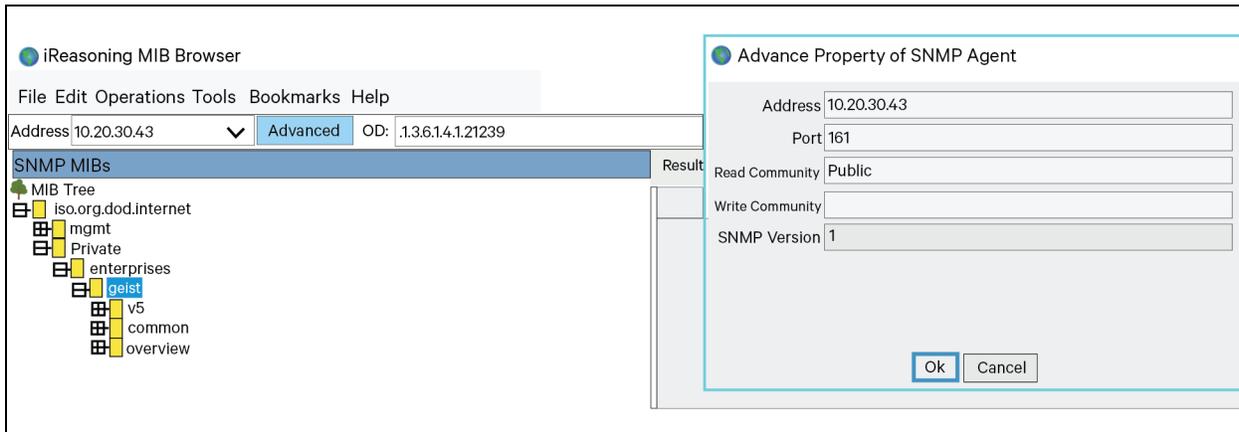
**Para acceder a los datos de SNMP del dispositivo de matriz:**

Se puede acceder a los datos de la PDU para rack PowerIT de SNMP mediante el puerto asignado a través de la dirección IP del administrador de matriz usando la MIB de Vertiv™ PowerIT v5. El archivo MIB puede descargarse desde la página SNMP del administrador de matriz.

1. En la vista *List*, use el ratón para desplazar el cursor por encima de las entradas de la tabla. Al pausar un dispositivo, aparecen un resaltado amarillo y un cuadro de texto con el puerto SNMP del dispositivo.
2. En el navegador de MIB, introduzca el puerto SNMP que aparece en la lista.

**NOTA: El software para monitorizar los dispositivos de matriz individuales debe poder admitir un número de puerto SNMP único por cada dispositivo monitorizado.**

Figura 6.9 Navegador de MIB



### 6.5.1 Datos SNMP del grupo

Los datos agregados, tanto el resumen (como los kWh totales y kW máximos) como los datos del grupo, están disponibles a través de la dirección IP de la rPDU Vertiv™ PowerIT del administrador de matriz y el puerto SNMP preterminado 161. Hay dos MIBS disponibles para la PDU para rack PowerIT del controlador de matriz:

- **v5:** contiene puntos de datos de la rPDU de Vertiv™ PowerIT principal individual.
- **Overview:** contiene puntos de datos para datos agregados en todos los dispositivos de matriz.

### 6.5.2 Consejos y resolución de problemas

- Se recomienda actualizar todos los dispositivos a la última versión de firmware antes de configurar la agregación.
- Asegúrese de que la PDU para rack designada como administrador de matriz esté completamente configurada y que la agregación esté habilitada antes de conectar cualquier dispositivo de matriz.
- Asegúrese de que todos los dispositivos de matriz tengan el estado predeterminado de fábrica antes de conectarlos al administrador de matriz. Si los ajustes se han cambiado previamente o si se han definido algunos usuarios en un dispositivo, el dispositivo debe restablecerse a los valores predeterminados de fábrica antes de conectarlo al administrador de matriz.
- Si va a restablecer una PDU para rack a los valores predeterminados de fábrica, asegúrese de usar la función *Utilities>Restore defaults>All Settings*. Al usar el botón central del IMD o el interruptor de restablecimiento de agujero de alfiler que se encuentra debajo del puerto de red 2 para restablecer los ajustes, no se restablecen todos los ajustes y es posible que los dispositivos de matriz no se identifiquen correctamente.
- Después de restablecer una PDU para rack a los valores predeterminados de fábrica, y antes de conectarla como un dispositivo de matriz, desconecte la PDU para rack de la red y reiníciela mediante el botón situado debajo del puerto de red 1. De este modo, se garantiza que cualquier dirección DHCP asignada durante el procedimiento de restablecimiento a los valores predeterminados de fábrica se libere.
- Pueden pasar hasta 20 minutos hasta que se lleguen a reconocer los dispositivos del dispositivo de matriz tras la configuración inicial.

- Los datos agregados, tanto resumidos como de grupo, no pueden generar alarmas.
- La herramienta Provisioner (*Provisioner>Discovery and Provisioner>File Management*) se puede utilizar para actualizar fácilmente el firmware de la PDU para rack del dispositivo de matriz y del administrador de matriz.
- Los datos agregados, tanto resumidos como de grupo, no se pueden utilizar para generar capturas de SNMP.
- Los nombres de la comunidad SNMP están configurados en cada dispositivo. Siga los vínculos de los dispositivos que se muestran en la página List en el menú Devices e inicie sesión en cada dispositivo para configurar el SNMP.
- No cambie el número de puerto SNMP predeterminado, los ajustes de la red o del servidor web cuando esté conectado a un dispositivo de matriz.
- Las capturas y alarmas de SNMP se enrutan desde un administrador de matriz la red de administración a través del administrador de matriz.

# Apéndices

## Apéndice A: Asistencia técnica

### A.1 Restablecimiento de una rPDU Vertiv™ PowerIT

Si una rPDU de Vertiv™ PowerIT pierde la comunicación, el procesador puede reiniciarse manualmente sin afectar a la alimentación de las salidas. Si se pulsa el botón de reinicio en la parte frontal del IMD, se reiniciará el procesador. La interfaz web permanecerá desconectada durante el arranque. Para obtener más información, consulte [Dispositivo de monitorización intercambiable](#) en la página 27.

### A.2 Servicio y mantenimiento

No se necesita servicio ni mantenimiento. La apertura de la rPDU de Vertiv™ PowerIT puede anular la garantía. En el interior de la rPDU de Vertiv™ PowerIT no hay piezas que pueda reparar el usuario, salvo el dispositivo de supervisión intercambiable (IMD) que se puede sustituir sobre el terreno. Vertiv™ PowerIT recomienda desconectar la alimentación de la unidad antes de instalar o quitar cualquier equipo.

El IMD está diseñado para que su sustitución sobre el terreno la realice únicamente personal de servicio debidamente capacitado y cualificado. El IMD está diseñado para sustituirlo mientras la rPDU de Vertiv™ PowerIT sigue conectada a la alimentación eléctrica. Para obtener más información, consulte la rPDU de Vertiv™ PowerIT IMD Modules Replacement Guide (Guía de sustitución de módulos IMD de la rPDU de Vertiv™ PowerIT).

### A.3 Más asistencia técnica

Para obtener asistencia técnica, visite [www.Vertiv.com/support](http://www.Vertiv.com/support).

#### América

- Sitio web: [www.Vertiv.com/geist](http://www.Vertiv.com/geist)
- Correo electrónico: [geistsupport@vertiv.com](mailto:geistsupport@vertiv.com)
- Teléfono: 1-888-630-4445

#### Europa y Oriente Medio

- Asistencia técnica: [www.Vertiv.com/en-emea/support](http://www.Vertiv.com/en-emea/support)
- Correo electrónico: [eoc@Vertiv.com](mailto:eoc@Vertiv.com)
- Teléfono: 44 1823 275100

#### Asia

- Teléfono (inglés): 1-888-630-4445 (número de EE. UU.)
- Teléfono (chino): +86 755 23546462

## A.4 Uso de Microsoft Exchange como servidor SMTP

Si su centro utiliza un servidor de correo electrónico de Microsoft Exchange, el IMD de la rPDU de Vertiv™ PowerIT puede utilizarlo para enviar correos electrónicos de notificación de alarma y advertencia. Sin embargo, puede ser necesario configurar el servidor de Exchange para permitir primero las conexiones SMTP de la unidad, ya que las versiones posteriores del servidor de Exchange suelen tener los servicios SMTP o la autenticación básica deshabilitados de forma predeterminada. Si tiene dificultades para que el IMD de la rPDU de Vertiv™ PowerIT envíe correos electrónicos a través de su servidor de Exchange, las siguientes notas pueden ser de utilidad.

**NOTA: Estas sugerencias solo son válidas si utiliza su propio servidor físico de Exchange. El servicio de Office 365 hospedado de Microsoft no es compatible con el IMD de la rPDU Vertiv™ PowerIT que utilice versiones de firmware anteriores a la v3.0.0, ya que Office 365 requiere una conexión StartTLS. Las versiones de firmware 3.0.0 y posteriores tienen soporte para StartTLS y son compatibles con Office 365.**

En primer lugar, dado que el IMD de la rPDU de Vertiv™ PowerIT no puede utilizar IMAP ni los protocolos propietarios de Microsoft MAPI/RPC Exchange/Outlook para enviar mensajes, debe habilitar SMTP configurando un conector de envío SMTP en el servidor de Exchange. Si desea obtener más información sobre la configuración de un conector de envío SMTP en Exchange, consulte este artículo de Microsoft TechNet: <http://technet.microsoft.com/en-us/library/aa997285.aspx>

En segundo lugar, es posible que necesite configurar su servidor de Exchange para permitir la retransmisión de mensajes desde la unidad de monitorización. Habitualmente, esto implicará activar la opción *Reroute incoming SMTP mail* en las propiedades de enrutamiento del servidor de Exchange y luego añadir la dirección IP del IMD de la rPDU de Vertiv™ PowerIT como un dominio al que se permite retransmitir el correo a través del servidor de Exchange. Si desea obtener más información sobre la habilitación y configuración de la retransmisión SMTP en Exchange, consulte este artículo de Microsoft TechNet: <http://technet.microsoft.com/en-us/library/dd277329.aspx>

Los métodos de autenticación SMTP AUTH PLAIN y AUTH LOGIN para iniciar sesión en el servidor ya no suelen estar habilitados de forma predeterminada en el servidor de Exchange; solo está habilitado el método de autenticación NTLM propietario de Microsoft.

### Para volver a habilitar el método AUTH LOGIN:

1. En la consola de Exchange, seleccione *Server Configuration - Hub Transport*.
2. Haga clic con el botón derecho del ratón en *Client Server* y seleccione *Properties*.
3. Seleccione la pestaña *Authentication* y active la casilla *Basic Authentication*.
4. Anule la selección de la casilla *Offer Basic only after TLS*.
5. Haga clic en *Apply* o *Save* y, a continuación, en *Exit*.

**NOTA: Es posible que tenga que reiniciar el servidor de Exchange después de hacer estos cambios.**

Por último, una vez que haya activado el SMTP, la retransmisión y el método de autenticación básica AUTH LOGIN, es posible que también tenga que crear una cuenta de usuario específicamente para que se conecte el IMD de la rPDU de Vertiv™ PowerIT. Si creó una cuenta antes de habilitar el conector de envío SMTP o si intenta utilizar una cuenta creada para otro usuario y el IMD de la rPDU de Vertiv™ PowerIT aún no puede conectarse al servidor de Exchange, es probable que la cuenta no haya heredado correctamente los nuevos permisos al habilitarlos como se ha indicado anteriormente. Esto tiende a ser más frecuente en los servidores de Exchange que se han actualizado desde que se crearon las cuentas que intenta utilizar, pero a veces puede suceder con las cuentas cuando se añaden nuevos conectores y complementos, independientemente de la versión de Exchange. Elimine las cuentas de usuario y, a continuación, cree una nueva para que la utilice la unidad de monitorización; la nueva cuenta debería heredar correctamente la autenticación SMTP y los permisos de retransmisión de correo.

Si ninguna de las sugerencias anteriores logra que el IMD de la rPDU de Vertiv™ PowerIT envíe correo a través del servidor de Exchange, es posible que tenga que ponerse en contacto con el soporte técnico de Microsoft, a fin de que le ayude a configurar el servidor de Exchange para permitir el envío de correos electrónicos SMTP desde un dispositivo de terceros, que no sea de Windows, a través de su red.

Esta página se ha dejado en blanco intencionadamente.

## Apéndice B: Sensores disponibles

### B.1 Sensores remotos

- SRT: temperatura remoto inoxidable.
- GTHD: temperatura/humedad/punto de condensación.
- GT3HD: temperatura/humedad/punto de condensación con dos sensores SRT.
- RTAFHD3: Temperatura/caudal de aire/humedad/punto de condensación.
- A2D: convierte los sensores de E/S analógicos en sensores digitales remotos.

### B.2 Sensores de E/S analógicos

- FS-15: sensor de inundación (agua).
- PFS-100 US / PFS-100 UN: sensor de fallo de alimentación.
- RPDS: kit de conmutador de puerta.

### B.3 Sensores integrados y modulares de Liebert®

**NOTA:** Se requiere un adaptador para usar cualquiera de los sensores siguientes.

- SN-T: una sonda de temperatura.
- SN-TH: una sonda de temperatura y otra de humedad.
- SN-Z01: cable integrado con una sonda de temperatura.
- SN-Z02: cable integrado con tres sondas de temperatura.
- SN-Z03: cable integrado con cuatro sondas (tres de temperatura y una de humedad).
- SN-2D: sensor monitor del conmutador de dos puertas.

### B.4 Conexión de sensores remotos

Se pueden conectar hasta 16 sensores remotos "plug-and-play" a la unidad, en cualquier momento, a través de los conectores RJ-12 situados en la parte delantera de la unidad. En algunos casos, es posible que se necesiten divisores para añadir sensores adicionales. Cada sensor tiene un número de serie único y se detecta y añade automáticamente a la página web. El número de serie de los sensores determina su orden de visualización en la web. Los nombres de los sensores se pueden personalizar en la página de información general de los sensores.

**NOTA:** Los sensores utilizan Cat 5, cable CMP y conectores RJ-12. El cableado debe ser directo. La polaridad invertida desactiva temporalmente todos los sensores hasta que se corrige. Los sensores utilizan un protocolo de comunicaciones en serie y están sujetos a restricciones de señalización de la red que dependen del blindaje, el ruido ambiental y la longitud del cable. Las instalaciones típicas permiten distancias de hasta 600 ft. (180 m) de cable de sensor.

## Apéndice C: Adaptadores USB inalámbricos TP-Link

- Archer T2U Nano (adaptador USB inalámbrico AC600 Nano)
- Archer T2U Plus (adaptador USB inalámbrico de doble banda de alta ganancia AC600)
- Archer T2U v3 (adaptador USB inalámbrico de doble banda AC600)
- Archer T3U (adaptador USB inalámbrico mini MU-MIMO AC1300)
- Archer T3U Plus (adaptador USB inalámbrico de doble banda de alta ganancia AC1300)
- Archer T4U v3 (adaptador USB inalámbrico de doble banda AC1300)

**NOTA:** Estos dispositivos se pueden detectar automáticamente cuando están conectados y se pueden configurar como una interfaz de red adicional.

Esta página se ha dejado en blanco intencionadamente.

## Apéndice D: LED de salida

**NOTA:** este apéndice se aplica solamente a las rPDU de Vertiv™ PowerIT de salidas supervisadas/salidas conmutadas.

Los LED de salida proporcionan una indicación visual del estado de alimentación de salida (activado, desactivado o error). Los LED están numerados secuencialmente con números blancos fáciles de leer sobre un fondo negro. Dependiendo del estado de alimentación de salida, los LED se iluminan en colores sólidos o en colores intermitentes.

**Tabla D.1 Salidas LED**

LED	Descripción
Verde	El voltaje de salida está presente y por encima del límite de umbral mínimo
Rojo	El voltaje de salida no está presente
Ámbar	Se ha detectado una condición de error en la salida de alimentación

**Tabla D.2 Descripción del estado del LED**

Voltaje medido	Estado de relé	Estado	LED	
On	Activado o desconocido	Sólido	Verde	
Off	Desactivado o desconocido	Sólido	Rojo	
Off	On	Intermitente <sup>1</sup>	Ámbar	Rojo
On	Off	Intermitente <sup>2</sup>	Ámbar	Verde
<sup>1</sup> La salida se detecta como desactivada pero debería estar activada. <sup>2</sup> La salida se detecta como activada pero debería estar desactivada.				

### Código de error

Los LED se iluminan en ámbar sólido durante las siguientes situaciones:

- Fallo de alimentación (se fuerza la apertura de todos los relés en caso de fallo de alimentación para permitir la secuencia de encendido)
- Disyuntor abierto
- No se detecta voltaje de entrada

## Apéndice E: Códigos de pantalla del IMD

Tabla E.1 Códigos de pantalla del IMD

Pantalla	Tipo de IMD	Explicación
<i>Err1</i>	IMD-01 (solo medido)	El IMD no ha descubierto ninguna o más de una placa de entrada. Esto se puede deber a problemas de cableado interno o a una placa de entrada que no responde. Esto también se muestra si la placa de entrada comunica un error de medición.
<i>8888</i>	IMD-02, IMD-03, IMD-3	El IMD se está iniciando y aún no ha detectado la pantalla simple y muestra <i>boot</i> . Si se muestra durante más de unos segundos, hay un problema en la placa de la pantalla o con el cableado interno.
-- (dos guiones en la posición más a la derecha de la pantalla)	IMD-02, IMD-03, IMD-3	El IMD no puede comunicarse con la placa de entrada. Esto también se puede mostrar de forma intermitente para mediciones individuales. Hay un problema con la placa de entrada o con el cableado interno.
<i>boot</i>	IMD-01	El IMD se está iniciando y detectando la placa de entrada.
<i>boot</i>	IMD-02, IMD-03, IMD-3	El firmware se está inicializando. Se mostrará mientras se actualiza el firmware en las placas internas.
<i>updt</i>	IMD-02, IMD-03, IMD-3	Actualización del firmware en curso.
<i>rset dflt</i>	IMD-02, IMD-03, IMD-3	Después de la acción del usuario, aparecerá <i>rset</i> (Reset) durante una secuencia de restablecimiento de parámetros. Durante el restablecimiento de un parámetro, aparecerá brevemente <i>dflt</i> (Default).
<i>bcup</i>	IMD-02, IMD-03, IMD-3	<i>bcup</i> (Backup) aparecerá durante una copia de seguridad de la configuración.
<i>rest conf</i>	IMD-02, IMD-03, IMD-3	<i>rest</i> (Restore) y <i>Conf</i> (Configuration) aparecerán durante una restauración de la configuración.
____ (cuatro guiones bajos en la parte inferior de la pantalla)	IMD-03 IMD-3	La pantalla del IMD se ha configurado de modo que las opciones Total Power, Voltage y Current estén deshabilitadas.

**NOTA:** El IMD-5M no dispone de códigos de pantalla; la pantalla táctil muestra la información del estado.

Esta página se ha dejado en blanco intencionadamente.

## Apéndice F: Aprovevisionador: formato del archivo de ajustes de configuración

**NOTA:** A continuación se describe el formato del archivo de ajustes de configuración que ha usado el proveisionador. En los ejemplos se siguen, a grandes rasgos, los ajustes disponibles en la interfaz de usuario web de la rPDU Vertiv™ PowerIT.

1. En los ejemplos que aparecen a continuación, el texto en azul se puede copiar en un archivo de texto y actualizarse según sea necesario. A continuación, el archivo de texto se puede cargar en la herramienta de aprovisionamiento.
2. Cuando edite archivos de configuración, use un editor de texto como, por ejemplo, el Bloc de notas que pueda guardar archivos en formato .txt.
3. Las sangrías que se muestran en los ejemplos se pueden omitir.
4. Asegúrese de utilizar las comillas dobles correctas al editar la configuración.
5. Si se omite un ajuste en el archivo de configuración, el valor de ese ajuste permanecerá inalterado.
6. Cuando se configure una rPDU de Vertiv™ PowerIT no configurada anteriormente (nueva de fábrica), el primer ajuste de configuración debe ser la definición de un usuario administrador, consulte [Usuarios locales](#) abajo.
7. Para combinar varios ajustes (que no sean usuarios locales) en un solo archivo (consulte también el [Ejemplo 1](#) en la página 145 al final de este documento):
  - Combine los ajustes necesarios en un solo archivo.
  - Elimine todas las apariciones de `{"conf":{` excepto en la primera línea del archivo.
  - Reemplace todas las líneas que contengan solo `}}` por una `,` (coma) excepto en la última línea del archivo.
8. Si se combinan ajustes de usuario local con otros ajustes en un mismo archivo, consulte el [Ejemplo 2](#) en la página 146 al final de este documento.
9. Después de seleccionar *Provisioner>Discovery>Update*, introduzca el nombre de usuario y la contraseña solo cuando configure las rPDU de Vertiv™ PowerIT que se hayan configurado anteriormente (el nombre de usuario y la contraseña son los de las rPDU de Vertiv™ PowerIT que se están aprovisionando). No introduzca un usuario y una contraseña cuando configure unidades nuevas de fábrica (identificadas por el atributo Provisioned igual a False).

### Usuarios locales

```
{ "auth": {
  "username": {
    "password": "userpw",
    "enabled": true,
    "control": false,
    "admin": false,
    "language": "en"}
}}
```

<b>username</b>	El nombre de usuario que se debe crear (entre comillas)
<b>password</b>	Contraseña (entre comillas)
<b>enabled</b>	Las opciones true o false determinan si el usuario está habilitado
<b>control</b>	Las opciones true o false determinan si el usuario tendrá privilegios de control
<b>admin</b>	Las opciones true o false determinan si el usuario tendrá privilegios de administrador
<b>language</b>	Anula el idioma predeterminado para este usuario; las opciones válidas son "de", "en", "es", "fr", "ja", "ko", "pt" y "zh"

## LDAP

```

{"conf":{
  "remoteAuth": {
    "mode": "ldap",
    "ldap": {
      "host": "192.168.123.1",
      "port": 389,
      "mode": "activeDirectory",
      "securityType": "ssl",
      "bindDn": "",
      "password": null,
      "baseDn": "",
      "userFilter": "(objectClass=posixAccount)",
      "userId": "uid",
      "userIdNum": "uidNumber",
      "groupFilter": "(objectClass=posixGroup)",
      "groupId": "gidNumber",
      "groupMemberUid": "memberOf",
      "enabledGroup": "enabled",
      "controlGroup": "control",
      "adminGroup": "admin"}}
}}

```

<b>host</b>	URL de LDAP (ref. RFC4516 > RFC2255) (entre comillas); es necesario si el protocolo LDAP está habilitado.
<b>port</b>	Puerto para la comunicación del protocolo
<b>mode</b>	Determina la compatibilidad predeterminada entre los diferentes tipos de LDAP; las opciones son "openLdap o activeDirectory"
<b>securityType</b>	Cifrado que se debe usar en la conexión con el servidor LDAP; las opciones son "ssl" y "starttls"
<b>bindDn</b>	Nombre distintivo (entre comillas) (ref. RFC4514 > RFC2253); se usa como enlace al servidor de directorios y una cadena en blanco significa un enlace anónimo
<b>password</b>	Contraseña (entre comillas) utilizada como enlace al servidor de directorios

<b>baseDn</b>	Nombre distintivo (entre comillas) (ref. RFC4514 > RFC2253) que se usará para la base de búsqueda
<b>userFilter</b>	Filtro de búsqueda LDAP (entre comillas) (ref. RFC4515 > RFC2254), objectClass equivalente a posixAccount (ref. RFC2307)
<b>userId</b>	Equivalente al atributo "uid" (entre comillas) ref. (RFC2307)
<b>userIdNum</b>	Equivalente al atributo "uidNumber" (entre comillas) (ref. RFC2307)
<b>groupFilter</b>	Filtro de búsqueda LDAP (entre comillas) (ref. RFC4515 > RFC2254), objectClass equivalente a posixGroup (RFC2307)
<b>groupId</b>	Equivalente al atributo "gidNumber" (ref. RFC2307) (entre comillas)
<b>groupMemberUid</b>	Equivalente al atributo "memberUid" (ref. RFC2307) (entre comillas)
<b>enabledGroup</b>	El usuario (entre comillas) de este grupo tendrá el privilegio de "enabled"
<b>controlGroup</b>	El usuario (entre comillas) de este grupo tendrá el privilegio de "control"
<b>adminGroup</b>	El usuario (entre comillas) de este grupo tendrá el privilegio de "admin"

```

{"conf":{
  "remoteAuth": {
    "mode": "tacacs",
    "tacacs": {
      "authenticationServer1": "10.20.30.21",
      "authenticationServer2": "10.20.30.70",
      "accountingServer1": "10.20.30.21",
      "accountingServer2": "10.20.30.70",
      "sharedSecret": "secret",
      "service": "raccess",
      "adminAttribute": "admin=true",
      "controlAttribute": "control=true",
      "enabledAttribute": "enabled=true"}}
}}

```

<b>authenticationServer1</b>	Servidor de autenticación/autorización primario (entre comillas)
<b>authenticationServer2</b>	Servidor de autenticación/autorización alternativo (entre comillas)
<b>accountingServer1</b>	Servidor de contabilidad primario (entre comillas)
<b>accountingServer2</b>	Servidor de contabilidad alternativo (entre comillas)
<b>sharedSecret</b>	El secreto (entre comillas) compartido por el cliente y el servidor (con el valor null se elimina el secreto)
<b>service</b>	Valor que se debe utilizar para el campo de servicio en las solicitudes TACACS+. Las opciones válidas son "ppp" y "raccess"
<b>adminAttribute</b>	El usuario (entre comillas) con este par atributo-valor tendrá el privilegio de "admin"

- controlAttribute** El usuario (entre comillas) con este par atributo-valor tendrá el privilegio de "control"
- enabledAttribute** El usuario (entre comillas) con este par atributo-valor tendrá el privilegio "enabled"

## Radius

```
{ "conf": {  
  "remoteAuth": {  
    "mode": "radius",  
    "radius": {  
      "authenticationServer1": "",  
      "authenticationServer2": "",  
      "accountingServer1": "",  
      "accountingServer2": "",  
      "sharedSecret": "Secret",  
      "groupAttribute": "filter-id",  
      "adminGroup": "admin",  
      "controlGroup": "control",  
      "enabledGroup": "enabled" } }  
}}
```

- authenticationServer1** Servidor de autenticación primario (entre comillas)
- authenticationServer2** Servidor de autenticación alternativo (entre comillas)
- accountingServer1** Servidor de contabilidad primario (entre comillas)
- accountingServer2** Servidor de contabilidad alternativo (entre comillas)
- sharedSecret** Secreto compartido por el cliente y el servidor (entre comillas)
- groupAttribute** Identifica el AVP que indica a qué grupo de acceso pertenece el usuario; los valores válidos son "filter-id" y "management-privilege-level".
- adminGroup** El usuario (entre comillas) que pertenece a este grupo tiene el privilegio de "admin"
- controlGroup** El usuario (entre comillas) que pertenece a este grupo tiene el privilegio de "control"
- enabledGroup** El usuario (entre comillas) que pertenece a este grupo tendrá el privilegio de "enabled"

## Nombre de host de la red y direcciones IP

```
{ "conf": {  
  "system": {  
    "hostname": "rPDUhostname",  
    "ip6Enabled": true,  
    "network": {  
      "ethernet": {  
        "label": "Bridge 0",  
        "enabled": true,  

```

```
"dhcpOn": false,
"address": {
"0": {"address": "192.168.123.123", "prefix": 24},
"1": {"address": "10.20.30.43", "prefix": 24}}}}
}}
```

<b>Hostname</b>	Nombre (entre comillas) para identificar la unidad en una red
<b>ip6Enabled</b>	Las opciones son true o false para habilitar o deshabilitar la compatibilidad con IPV6
<b>label</b>	Etiqueta del puente (entre comillas)
<b>enabled</b>	Las opciones son true o false para habilitar o deshabilitar el puente de red
<b>dhcpOn</b>	Las opciones son true o false para habilitar o deshabilitar DHCP
<b>address</b>	Dirección IP (entre comillas) de la interfaz
<b>prefix</b>	Prefijo de la dirección IP de la interfaz

### Puertos de red

```
{"conf":{
"network": {
"port0": {
"label": "Port 0",
"enabled": true,
"stp": {"cost": 0}},
"port1": {
"label": "Port 1",
"enabled": true,
"stp": {"cost": 0}}}
}}
```

<b>label</b>	Etiqueta del puerto (entre comillas)
<b>enabled</b>	Las opciones son true o false para determinar si el puerto está habilitado
<b>cost</b>	Coste del árbol de expansión para este puerto

### Rutas de red

```
{"conf":{
"network": {
"ethernet": {
"route": {
"0": {
"gateway": "10.20.30.254",
"prefix": 0,
"destination": "0.0.0.0"}}}}
}}
```

<b>gateway</b>	Dirección de la puerta de enlace (entre comillas) para la ruta
<b>prefixDestination</b>	Prefijo de red; 0 para la puerta de enlace predeterminada
<b>destination</b>	Dirección de red de destino (entre comillas); "0.0.0.0" para la red predeterminada

### DNS de red

```

{"conf":{
  "network": {
    "ethernet": {
      "dns": {
        "0": {"address": "8.8.8.8"},
        "1": {"address": "8.8.4.4"}}}}
}}

```

**address** La dirección del servidor DNS (entre comillas). La segunda ocurrencia es para el servidor DNS alternativo.

### RSTP de red

```

{"conf":{
  "network": {
    "ethernet": {
      "stp": {
        "enabled": false,
        "mode": "rstp",
        "bridgePriority": 24576,
        "helloTime": 2,
        "maxAge": 40,
        "maxHops": 40,
        "forwardDelay": 21}}}
}}

```

<b>enabled</b>	Las opciones son true o false; determina si el protocolo de árbol de expansión está habilitado
<b>mode</b>	Las opciones son "stp" o "rstp"; el modo RSTP permite volver a STP cuando sea necesario
<b>bridgePriority</b>	La prioridad del puente del árbol de expansión de esta interfaz
<b>helloTime</b>	Intervalo en segundos entre las transmisiones periódicas del mensaje de configuración
<b>maxAge</b>	Antigüedad máxima de la información transmitida por esta interfaz cuando sirve como puente de raíz. Se usa cuando "mode" está configurado como "stp". Debe ser al menos $2 * (\text{helloTime} + 1)$
<b>maxHops</b>	Número máximo de cruces del puente de la información transmitida por esta interfaz cuando sirve como puente raíz; se usa cuando "mode" está configurado como "rstp"
<b>forwardDelay</b>	El retardo utilizado por los puentes para la transición del puente raíz y los puertos designados al modo de reenvío; debe ser como mínimo $(\text{maxAge} / 2) + 1$

## Servidor web

```

{"conf":{
  "http": {
    "httpEnabled": true,
    "httpPort": 80,
    "httpsPort": 443}
}}
```

**httpEnabled** Las opciones son true o false para permitir las comunicaciones no cifradas

**httpPort** Número de puerto para la comunicación HTTP

**httpsPort** Número de puerto para la comunicación HTTPS

## Informes

```

{"conf":{
  "report": {
    "0": {
      "start": "00:00",
      "days": "MTWTFSS",
      "targets": ["1", "2"],
      "interval": 1},
    "1": {
      "start": "00:00",
      "days": "MT-----",
      "targets": ["1"],
      "interval": 1}}
}}
```

**start** Hora del día a partir de la cual se aplica el intervalo. El formato es "(00-23):(00-59)", configurable en incrementos de 15 minutos

**days** Primera letra de los días seleccionados (entre comillas) en orden de lunes a domingo. Se usa un '-' para representar destinos de días no seleccionados

Lista de claves que hacen referencia a los destinos de correo electrónico (entre comillas)

**interval** Número de horas entre informes; el valor puede ser 1, 2, 3, 4, 6, 8, 12 y 24

## Pantalla

```

{"conf":{
  "display": {
    "gmsd": {
      "mode": "currentAndTotalPower",
      "inverted": false,
      "vlc": {"enabled": false}}}
}}
```

- mode** Selecciona un conjunto de datos para presentar en la pantalla; las opciones son "current", "totalPower" y "currentAndTotalPower"
- inverted** Las opciones son true o false para describir la orientación actual de la pantalla
- enabled** Las opciones son true o false para determinar el modo de pantalla de VLC de la rPDU

## Time

```
{"conf":{  
  "time": {  
    "mode": "ntp",  
    "datetime": "2021-03-09 12:05:36",  
    "zone": "UTC",  
    "ntpServer1": "0.pool.ntp.org",  
    "ntpServer2": "1.pool.ntp.org"}  
  }  
}
```

- mode** El modo; las opciones válidas son "ntp" y "manual"
- datetime** Fecha y hora. El formato es "AAAA-MM-DD HH:MM:SS". Las horas van de 0 a 23 (este campo se muestra en hora local). Solo debe usarse con mode = "manual"
- zone** Debe ser un nombre válido (entre comillas) de la base de datos tz
- ntpServer1** Dirección del servidor NTP primario (entre comillas); solo debe utilizarse con mode = "ntp"
- ntpServer2** Dirección del servidor NTP de reserva (entre comillas); solo debe utilizarse con mode = "ntp"

## SSH

```
{"conf":{  
  "ssh": {  
    "enabled": true,  
    "port": 22}  
  }  
}
```

- enabled** Las opciones son true o false para habilitar o deshabilitar SSH
- port** Número de puerto para la comunicación SSH

## USB

```
{"conf":{  
  "usb": {"enabled": true}  
}
```

- enabled** Las opciones son true o false y habilita o deshabilita el puerto USB

## Serial Port

```

{"conf":{
  "serial": {
    "baudRate": 115200,
    "dataBits": 8,
    "enabled": true,
    "parity": "none",
    "stopBits": 1}
}}
```

<b>baudRate</b>	Velocidad en baudios; las opciones son 1200, 2400, 4800, 9600, 19200, 38400, 57600 y 115200
<b>dataBits</b>	Número de bits de datos en una trama; las opciones son 7 y 8
<b>enabled</b>	Las opciones son true o false; habilita o deshabilita la CLI serie en un dispositivo
<b>parity</b>	Tipo de bit de paridad utilizado en la trama; las opciones son "none", "even" y "odd"
<b>stopBits</b>	Número de bits de parada usados para terminar cada trama; las opciones son 1 y 2

## Email

```

{"conf":{
  "email": {
    "server": "Example-server",
    "port": 25,
    "sender": "From email address",
    "username": "username",
    "password": "password",
    "target": {
      "0": {"name": "email1@domain.com"},
      "1": {"name": "email2@domain.com"}}}
}}
```

<b>server</b>	Dirección del servidor SMTP (entre comillas)
<b>port</b>	Número de puerto SMTP
<b>sender</b>	Dirección de correo electrónico del remitente (entre comillas)
<b>username</b>	Nombre de usuario SMTP (entre comillas)
<b>password</b>	Contraseña SMTP (entre comillas)
<b>name</b>	Dirección de correo electrónico de destino (entre comillas)

## SNMP v1 o v2c

```

{"conf":{
```

```

"snmp": {
  "v1v2cEnabled": true,
  "port": 161,
  "readCommunity": "public",
  "writeCommunity": "private",
  "trapCommunity": "private",
  "target": {
    "0": {
      "port": 162,
      "name": "10.20.30.10",
      "trapVersion": "1"},
    "1": {
      "port": 162,
      "name": "10.20.30.11",
      "trapVersion": "1"},
    "2": {
      "port": 162,
      "name": "10.20.30.12",
      "trapVersion": "2c"}}}
  }}

```

<b>v1v2cEnabled</b>	Las opciones son true o false; habilita o deshabilita SNMP (versión 1 y 2c)
<b>port</b>	Número de puerto para la comunicación SNMP
<b>readCommunity</b>	Nombre de la comunidad de lectura (entre comillas); debe ser diferente de writeCommunity
<b>writeCommunity</b>	Nombre de la comunidad de escritura (entre comillas); debe ser diferente de readCommunity
<b>trapCommunity</b>	Nombre de comunidad de captura (entre comillas)
<b>port</b>	Número de puerto para las capturas de SNMP
<b>name</b>	Dirección (entre comillas) para el destino de las capturas de SNMP
<b>trapVersion</b>	Versión de captura de SNMP, "1" o "2c"

### SNMP v3

```

{"conf":{
  "snmp": {
    "v3Enabled": true,
    "port": 161,
    "user": {
      "0": {
        "privPassword": "password",
        "type": "read",
        "username": "name",
        "privType": "aes",
        "authPassword": "password",
        "authType": "sha1"},
      "1": {
        "privPassword": "password",

```

```

"type": "write",
"username": "name",
"privType": "none",
"authPassword": "password",
"authType": "none"},
"2": {
"privPassword": "password",
"type": "trap",
"username": "name",
"privType": "none",
"authPassword": "password",
"authType": "none"}}}
}}
```

<b>v3Enabled</b>	Las opciones son true o false; habilita o deshabilita SNMP (versión 1 y 2c)
<b>port</b>	Número de puerto para la comunicación SNMP
<b>type</b>	Tipo de permiso: los valores posibles son "read", "write" o "trap"
<b>username</b>	Nombre de usuario de SNMPv3 (entre comillas)
<b>privPassword</b>	Contraseña de privacidad (entre comillas)
<b>privType</b>	Tipo de cifrado de privacidad; los valores son "aes", "des" o "none"
<b>authPassword</b>	Contraseña de autenticación (entre comillas)
<b>authType</b>	Tipo de autenticación; los valores son "sha1", "md5" o "none"

### Syslog

```

{"conf":{
"syslog": {
"enabled": true,
"target": "10.20.30.40",
"port": 514}
}}
```

<b>enabled</b>	Las opciones son true o false; permite habilitar la transmisión de mensajes de syslog a un destino remoto
<b>target</b>	Dirección (entre comillas) del destino remoto de los mensajes de syslog
<b>port</b>	Número de puerto de destino para los mensajes

### Admin

```

{"conf":{
"contact": {
"description": " Geist GU PDU ",
"location": "Example Location",
```

```
"contactName": "Example Contact",  
"contactEmail": "email@example.com",  
"contactPhone": "123 456 789"},  
"system": {"label": "System Label"}  
}}
```

<b>description</b>	Descripción de la unidad (entre comillas)
<b>location</b>	Ubicación de la unidad (entre comillas)
<b>contactName</b>	Nombre de contacto de la unidad (entre comillas)
<b>contactEmail</b>	Correo electrónico de contacto de la unidad (entre comillas)
<b>contactPhone</b>	Número de teléfono de contacto de la unidad (entre comillas)
<b>label</b>	Etiqueta del sistema de la unidad (entre comillas)

### Locale

```
{"conf":{  
  "locale": {  
    "defaultLang": "en",  
    "units": "metric"}  
  }  
}}
```

<b>defaultLang</b>	Idioma; las opciones válidas son "de", "en", "es", "fr", "ja", "ko", "pt" y "zh"
<b>units</b>	Unidades; las opciones válidas son "metric" e "imperial"

### Intervalo de registro de datos

```
{"conf":{  
  "datalog": {"interval": 15}  
}}
```

<b>interval</b>	Intervalo en minutos para el registro de datos
-----------------	--

### Agregación

```
{"conf":{  
  "oneview": {  
    "enabled": true,  
    "username": "x",  
    "password": "pass"}  
  }  
}}
```

<b>enabled</b>	Las opciones son true o false; determina si la agregación está habilitada
<b>username</b>	Nombre de usuario (entre comillas) para establecer dispositivos de matriz
<b>password</b>	Contraseña (entre comillas) a establecer para los dispositivos de matriz (con un valor nulo se elimina la contraseña)

### Ejemplo 1

Archivo para configurar un nombre de host, la dirección IP, la puerta de enlace, los nombres de comunidad de SNMP v1 y la configuración regional:

```

{"conf":{
  "system": {
    "hostname": "hostname1"},
  "network": {
    "ethernet": {
      "dhcpOn": false,
      "address": {
        "0": {"address": "10.20.30.40", "prefix": 24}}}}
  },
  "network": {
    "ethernet": {
      "route": {
        "0": {
          "gateway": "10.20.30.254",
          "prefix": 0,
          "destination": "0.0.0.0"}}}}
  },
  "network": {
    "ethernet": {
      "dns": {
        "0": {"address": "8.8.8.8"},
        "1": {"address": "8.8.4.4"}}}}
  },
  "snmp": {
    "v1v2cEnabled": true,
    "port": 161,
    "readCommunity": "public",
    "writeCommunity": "private",
    "trapCommunity": "private",
    "target": {
      "0": {
        "port": 162,
        "name": "10.20.30.60",
        "trapVersion": "1"}}}
  },
  "locale": {
    "defaultLang": "en",
    "units": "metric"}
}}
```

## Ejemplo 2

Archivo para configurar un usuario administrador, deshabilitar HTTP y configurar un servidor NTP:

```
{ "auth": {
  "username": {
    "password": "userpw",
    "enabled": true,
    "control": false,
    "admin": false,
    "language": "en"
  },
  "conf": {
    "http": {
      "httpEnabled": false
    },
    "time": {
      "mode": "ntp",
      "zone": "UTC",
      "ntpServer1": "0.pool.ntp.org", "ntpServer2": "1.pool.ntp.org" } } }
```

## Ajustes del sensor y alarmas

```
{ "dev": {
  "0000000000000000": {
    "label": "PDU 22A",
    "type": "i03",
    "conf": {"outletControlEnabled": true},
    "outlet": {
      "0": {
        "poaAction": "last",
        "rebootHoldDelay": 10,
        "rebootDelay": 5,
        "poaDelay": 1.25,
        "onDelay": 5,
        "mode": "manual",
        "offDelay": 5,
        "label": "Outlet 1"
      },
      "1": {
        "poaAction": "last",
        "rebootHoldDelay": 10,
        "rebootDelay": 5,
        "poaDelay": 1.50,
        "onDelay": 5,
        "mode": "manual",
        "offDelay": 5,
        "label": "Outlet 2"
      }
    },
    "entity": {
```

```

        "total0": {"label": "Total"},
        "breaker0": {"label": "Circuit 1"},
        "breaker1": {"label": "Circuit 2"},
        "phase0": {"label": "Phase A"},
        "phase1": {"label": "Phase B"},
        "phase2": {"label": "Phase C"},
        "line3": {"label": "Neutral Line"}
    }
},
"alarm": {
    "action": {
        "0": {
            "target": "trap0",
            "delay": 0,
            "repeat": 0
        },
        "1": {
            "target": "email0",
            "delay": 0,
            "repeat": 0
        }
    }
},
"trigger": {
    "0": {
        "path": "0000000000000000/entity/phase0/measurement/0",
        "severity": "alarm",
        "type": "high",
        "threshold": 222.0,
        "tripDelay": 0,
        "clearDelay": 1,
        "latching": false,
        "selectedActions": ["0","1"]
    },
    "1": {
        "path": "0000000000000000/outlet/0/measurement/0",
        "severity": "alarm",
        "type": "low",
        "threshold": 55.0,
        "tripDelay": 2,
        "clearDelay": 0,
        "latching": false,
        "selectedActions": ["0"]
    },
    "2": {
        "path": "0000000000000000/entity/breaker0/measurement/4",
        "severity": "alarm",
        "type": "high",
        "threshold": 12.0,
        "tripDelay": 0,
        "clearDelay": 0,
        "latching": false,
        "selectedActions": ["0"]
    },
    "3": {
        "path": "0000000000000000/entity/total0/measurement/0",
        "severity": "alarm",
        "type": "high",

```

```

        "threshold": 7200.0,
        "tripDelay": 0,
        "clearDelay": 0,
        "latching": false,
        "selectedActions": ["0"]
    }
}
}}
```

- 000000000000000000** El ID del dispositivo (que se encuentra en la página Sensors>Overview) de la rPDU que se va a configurar. Se aprovisionarán todos los dispositivos seleccionados si este ID del dispositivo no coincide con ninguno de los dispositivos seleccionados que se están aprovisionando. Al establecer el ID del dispositivo en 000000000000000000 se garantiza que todos los dispositivos seleccionados estén configurados.
- label** La etiqueta de la rPDU (que se muestra en la página Sensors>Overview)
- type** Para la configuración de las alarmas en las mediciones de la PDU internas, el valor "type" debe coincidir con el IMD que se esté utilizando con la PDU; por consiguiente, debe ser "i03" para las PDU que utilicen cualquier IMD-03x o IMD-3x, e "i05" para las PDU que utilicen el IMD-5M.

Para la configuración de alarmas en los sensores externos, el valor "type" debe ser el tipo de sensor externo. Los valores válidos son "remotetemp", "afht3", "thd", "t3hd", "a2d", "snt", "snh" y "snd".

Al omitirse, se evita que se configuren las rPDU seleccionadas cuando el ID del dispositivo no coincida con el de ninguna rPDU.
- outletControlEnabled** Se aplica solo a las rPDU de salida conmutada y determina si es posible controlar las salidas en una rPDU de salida conmutada. El valor true permite controlar las salidas, el valor false evita que se controlen las salidas.
- outlet** La sección outlet se aplica solo a las rPDU de salida conmutada y define los ajustes para cada salida de la rPDU. Observe que la numeración de las salidas comienza con 0 (número de salida de la rPDU 1). Se pueden omitir las salidas individuales (o toda la sección Outlet) si no es necesario cambiar este ajuste.
- poaAction** Define el estado en que se iniciará la salida cuando se encienda ("on", "off" o "last").

<b>rebootHoldDelay</b>	El tiempo, en segundos, que la unidad espera después de apagar la salida antes de volver a encenderla durante un reinicio. Puede ser cualquier número entero entre 0 y 14.400.
<b>rebootDelay</b>	El tiempo, en segundos, que la unidad espera antes de reiniciar una salida. Puede ser cualquier número entero entre 0 y 14.400.
<b>poaDelay</b>	El tiempo, en segundos, que la unidad espera después del encendido antes de activar una salida. Puede ser cualquier número entero entre 0 y 14.400.
<b>onDelay</b>	El tiempo, en segundos, que la unidad espera antes de activar una salida. Puede ser cualquier número entero entre 0 y 14.400.
<b>mode</b>	Debe tener el valor "manual" para las salidas controladas por el usuario.
<b>offDelay</b>	El tiempo, en segundos, que la unidad espera antes de desactivar una salida. Puede ser cualquier número entero entre 0 y 14.400.
<b>label</b>	La etiqueta de la salida.
<b>entity</b>	La sección entity se usa para etiquetar mediciones sin salida en la página Sensors>Overview.
<b>total0 label</b>	La etiqueta para el total de rPDU en la página Sensors>Overview
<b>breaker0 label</b>	Etiqueta para el primer circuito (si está presente). Los circuitos posteriores, si están presentes, se pueden etiquetar como breaker1, breaker2, etc.
<b>phase0 label</b>	Etiqueta para la primera fase. Las fases posteriores, si están presentes, se pueden etiquetar como phase1 y phase2.
<b>line3 label</b>	Etiqueta para la línea neutra.
<b>alarm</b>	La sección alarm define los métodos que se pueden utilizar para enviar alarmas. Cada método está numerado a partir de 0 y define:  Para el envío de alarmas de SNMP, el objetivo puede tener los valores "trap0", "trap1" etc., que hacen referencia a las capturas de SNMP primera, segunda, etc., definidas en la página System>SNMP.
<b>target</b>	Para el envío de alarmas de correo electrónico, el objetivo puede tener los valores "email0", "email1" etc., que hacen referencia al primer, segundo, etc. correo electrónico de destino definido en la página System>Email.  Observe que el destino no debe especificar capturas SNMP ni destinos de correo electrónico que no se hayan configurado.
<b>delay</b>	Determina el tiempo durante el que este suceso debe permanecer activado antes de que se envíe la primera notificación vertical de esta acción.
<b>repeat</b>	Determina si se enviarán varias notificaciones para esta acción de suceso.
<b>trigger</b>	Esta sección define qué alarmas se han configurado, comenzando con la primera alarma que está numerada como 0.
<b>Path</b>	Define la medida en la que se activará la alarma. El formato de este campo es:

"0000000000000000/entity/phase0/measurement/0" define alarmas para mediciones de fase de entrada de la rPDU, donde phase0 se refiere a la primera fase de entrada de la rPDU, phase1 se refiere a la segunda fase (si está presente), etc. El número que sigue inmediatamente a la medición indica el tipo de medición para activar la alarma como se define a continuación:

- 0: Voltaje
- 4: corriente
- 8: alimentación real
- 9: alimentación aparente
- 10: Factor de alimentación
- 11: energía
- 14: factor de cresta actual

"0000000000000000/outlet/0/measurement/0" define las alarmas de salida para las rPDU con supervisión de salida, donde el número que sigue inmediatamente a la salida especifica el número de salida (a partir de cero). El número que sigue inmediatamente a la medición indica el tipo de medición para activar la alarma como se define a continuación:

- 0: Voltaje
- 4: corriente
- 8: alimentación real
- 9: alimentación aparente
- 10: Factor de alimentación
- 11: energía
- 12: equilibrio
- 14: factor de cresta actual

"0000000000000000/entity/total0/measurement/0" define alarmas para mediciones de entrada total de fase de la rPDU. El número que sigue inmediatamente a la medición indica el tipo de medición para activar la alarma como se define a continuación:

- 0: alimentación real
- 1: alimentación aparente
- 2: Factor de alimentación
- 3: energía

"0000000000000000/entity/breaker0/measurement/4" define alarmas para las alarmas del circuito de la rPDU, donde el primer circuito está indicado mediante breaker0, el segundo mediante breaker1, etc. El número que sigue inmediatamente a la medición indica el tipo de medición para activar la alarma como se define a continuación:

4: corriente

"0000000000000000/entity/line3/measurement/4" define las alarmas para las alarmas de corriente neutra de la rPDU. El número que sigue inmediatamente a la medición indica el tipo de medición para activar la alarma como se define a continuación:

0: corriente

<b>severity</b>	Puede ser "warning" o "alarm" y describe la gravedad de la alarma generada.
<b>type</b>	Puede ser "high" o "low" y define si se trata de un umbral alto o bajo.
<b>threshold</b>	El valor de umbral puede ser cualquier número entre -999,0 y 999,0. La corriente de la línea neutra se puede especificar hasta con dos decimales.
<b>tripDelay</b>	La medición debe superar el umbral durante este número de segundos antes de que el suceso se active. Puede ser cualquier número entero entre 0 y 14.400.
<b>clearDelay</b>	La medición debe volver a la normalidad durante este número de segundos antes de que el suceso se borre y se restablezca. Puede ser cualquier número entero entre 0 y 14.400.
<b>latching</b>	Puede ser true o false. Si está configurado en true, este suceso y sus acciones asociadas permanecen activos hasta que se confirme el suceso, incluso si la medición vuelve posteriormente a la normalidad.
<b>selectedActions</b>	Especifica cuáles de las acciones definidas anteriormente se pueden usar para enviar la alarma. Como ["0","1"] que indican las acciones 0 y 1, que se definen como acciones, y usan los valores trap0 y email0 en el ejemplo anterior.

Esta página se ha dejado en blanco intencionadamente.

## Apéndice G: Códigos de error API / CLI

### G.1 Success

Código	Explicación
Success	La operación se ha realizado correctamente

### Errores de autenticación

Código	Explicación
No Admin user configured	Debe configurarse por lo menos un usuario administrador en el sistema
Not Authorized	El usuario actual no está autorizado
Not Authorized: Session expired	El token utilizado ya no es válido
Not Authorized: Not enough permissions	El usuario actual no tiene permisos suficientes para realizar la operación
Invalid credential combination	Se proporcionaron tanto el nombre de usuario/contraseña como el token o solo se proporcionó el nombre de usuario o la contraseña
Must have at least one admin user	Debe configurarse por lo menos un usuario administrador en el sistema

### Errores de formato JSON

Código	Explicación
Malformed JSON	El JSON recibido no es válido o está dañado
Missing field	No se ha encontrado un campo esperado en la estructura JSON
Duplicate fields	El mismo campo se ha establecido varias veces, por ejemplo en el cuerpo HTTP y en la cadena de consulta

### Errores en la ruta

Código	Explicación
Invalid path	La ruta indicada no cumple los requisitos del sistema
Path not found	La ruta indicada no se ha encontrado
Identifier not found	Uno de los campos de la estructura JSON recibida no existe
Field not applicable	Un campo de la estructura JSON existe pero no se debería haber enviado

### Errores de validación de datos

Código	Explicación
Invalid input	Un campo de entrada no es válido pero no se ajusta a otras categorías de validación de datos
Input too long	Un campo de entrada supera la longitud máxima permitida
Invalid characters	Un campo de entrada contiene caracteres no válidos para el campo
Invalid serial	Un campo de entrada es un número de serie no válido
Invalid Boolean	Un campo de entrada es un valor booleano no válido
Out of range	Un campo de entrada está fuera del intervalo válido para el campo
Invalid integer	Un campo de entrada no es un entero cuando se espera uno
Invalid number	Un campo de entrada no es un número cuando se espera uno
Invalid URL	Un campo de entrada no es una URL válida cuando se espera una
Invalid IP	Un campo de entrada no es una dirección IP válida cuando se espera una
Paths not allowed	Un campo de entrada contiene una ruta de acceso cuando no se espera una
Invalid username	Un campo de entrada es un nombre de usuario no admisible
Invalid email address	Un campo de entrada no es una dirección de correo electrónico válida cuando se espera una
Invalid option	Un campo de entrada contiene una selección de opción no válida
Invalid datetime	Un campo de entrada no es una fecha u hora válida cuando se espera una
Out of bounds	Un campo de entrada está fuera de los límites permitidos para el campo
Invalid week	Un campo de entrada representa una selección de días de la semana no válida
Duplicate entry	Un campo de entrada crearía un duplicado cuando no se permite uno
Invalid Route	Una ruta de red se ha configurado de forma incorrecta

### Otros errores

Código	Explicación
Unknown error	Se ha producido un error del sistema para el que no es aplicable ningún otro código de error
Command not allowed	El comando recibido no está permitido en la ruta de acceso especificada
System busy	La acción que se ha intentado realizar no se puede ejecutar en este momento y se debe volver a intentar posteriormente

### Errores de coherencia de datos

Código	Explicación
Inconsistent state	El comando dejará el sistema en un estado incoherente, por lo que se ha rechazado
Syslog enabled requires target	La activación de syslog remoto requiere que se especifique un host de destino
NTP mode requires servers	La activación de NTP requiere servidores para consultas

Código	Explicación
Start time must come before end time	Se ha recibido una hora para la que el final llegó antes del inicio
Invalid SNMPv3 auth/priv combination	La privacidad de SNMPv3 no se puede usar sin autenticación
Port not available	Se ha intentado establecer un número de puerto que ya está en uso
Vertiv Intelligence Director missing credentials	Para activar Vertiv Intelligence Director es necesario configurar un nombre de usuario y contraseña
Time not settable	Para poder ajustar la fecha y la hora se necesita el modo de hora manual

### Errores de carga

Código	Explicación
Invalid firmware package	El paquete tiene un formato incorrecto o está dañado
Invalid file key	El paquete especifica una clave OEM incorrecta y no se puede usar con esta unidad
Invalid version	La versión es demasiado antigua o no es compatible
Invalid product	El paquete se ha diseñado para una arquitectura de hardware diferente
Invalid certificate file	El certificado SSL proporcionado no se ha podido analizar
Invalid certificate password	La contraseña no ha funcionado con el certificado SSL proporcionado

Esta página se ha dejado en blanco intencionadamente.

## Apéndice H: Un ejemplo de configuración de LDAP para las credenciales de Active Directory

### H.1 Información general

La integración de Active Directory con el dispositivo de monitorización intercambiable (IMD) de la marca PowerIT permite la autenticación y autorización de los usuarios en la interfaz CLI y en la web del IMD mediante el uso de sus credenciales empresariales de Active Directory. También se autorizará al usuario en uno de los tres roles del IMD basados en un grupo de seguridad de Active Directory del que el usuario es miembro. Estos roles son:

- **Admin:** derechos de configuración completos, incluidos los permisos de rol de control.
- **Control:** capacidad para controlar el estado de la salida, si corresponde, cambiar los nombres de los dispositivos y los ajustes de alarmas/sucesos.
- **Enabled:** la opción Read-only de los ajustes de configuración y sin derechos de control de salida.

### H.2 Requisitos generales y notas

- Para este procedimiento se puede utilizar IMD v5.3.3 o un nuevo firmware.
- Los ejemplos se representan en verde.

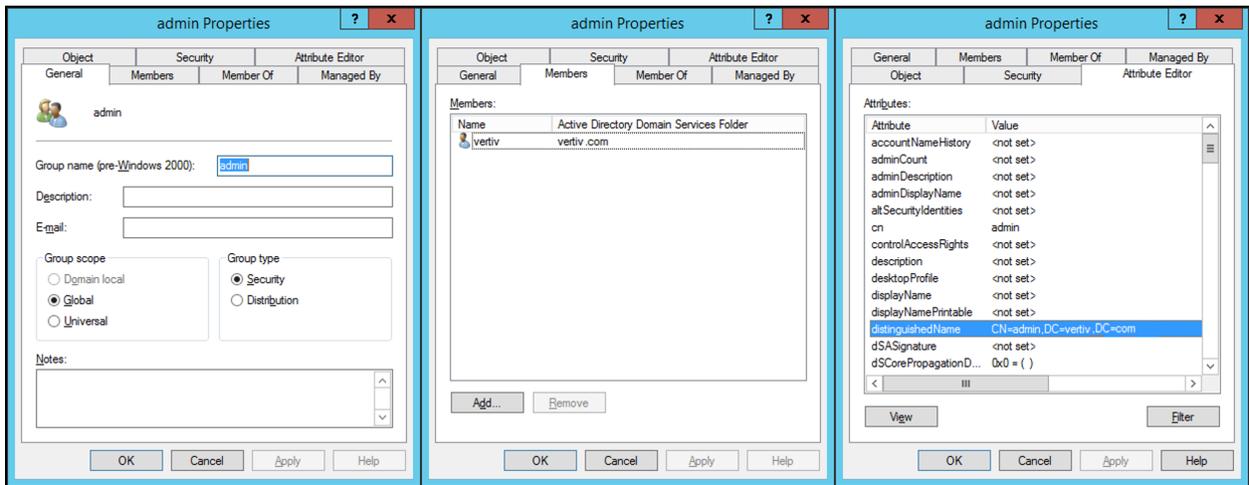
### H.3 Procedimiento de configuración de Active Directory

- Cree o utilice una cuenta de enlace de AD para el IMD. El IMD utilizará esta cuenta para buscar el dominio de AD y autenticar a los usuarios. La contraseña de esta cuenta debe configurarse de modo que nunca caduque.
- Cree uno o más grupos de seguridad de AD para representar los roles del IMD: Admin, Control y Enabled.
- Incluya al usuario de AD como miembro del grupo de seguridad correspondiente.
  - En el ejemplo que se muestra a continuación, a la cuenta de AD "vertiv" se le ha asignado un miembro del grupo de seguridad "admin". Como resultado, la cuenta de usuario de AD "vertiv" asumirá el rol Admin del IMD al iniciar sesión.

**NOTA:** El nombre del grupo de seguridad queda a su elección. El nombre del grupo de seguridad y el DN deben coincidir con lo que se define en la sección "Group" de LDAP del IMD.

**NOTA:** Un usuario de AD que pertenezca a más de uno de estos grupos de seguridad asignados a los roles del IMD, heredará los privilegios de rol más elevados.

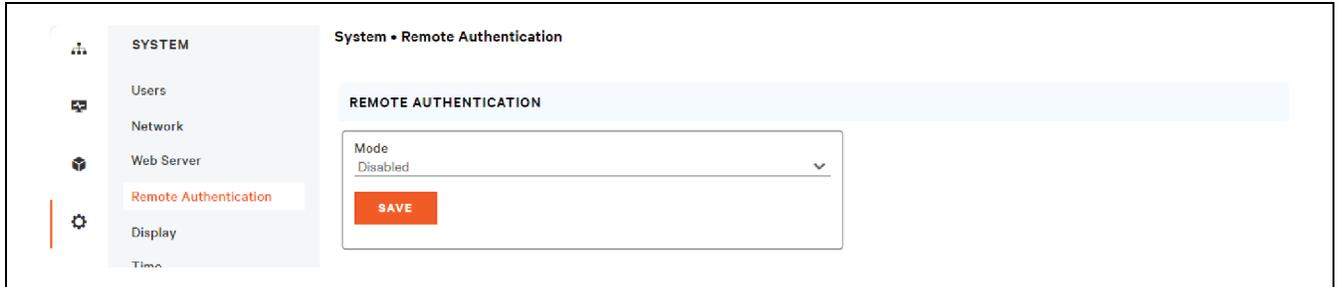
Figura H.1 Ajustes de Admin Properties



### H.4 Procedimiento de configuración del IMD (interfaz web)

- Abra un navegador web con la IP o el nombre DNS del IMD e inicie sesión como cuenta de admin local.
- Vaya a *System >Remote Authentication*.
- Establezca la opción Remote Authentication Mode en LDAP y guarde la selección.

Figura H.2 Remote Authentication



- Consulte la siguiente ilustración para obtener descripciones de los ajustes de la sección LDAP.

Figura H.3 Ajustes de LDAP

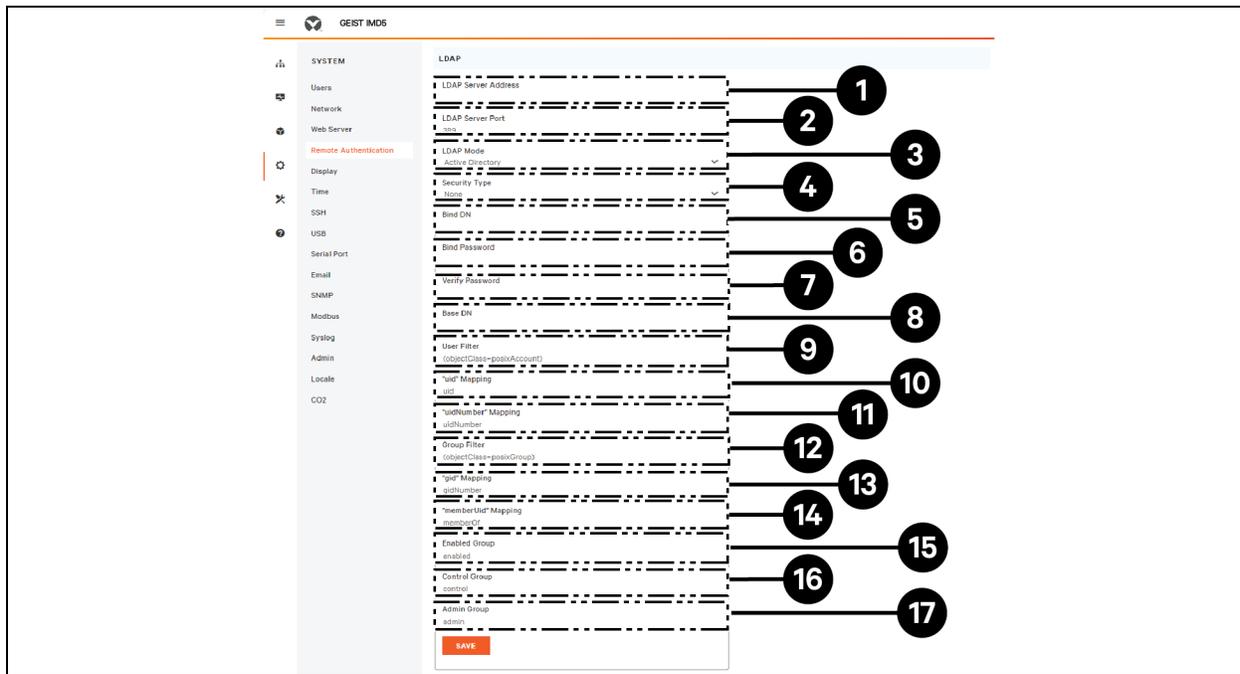


Tabla H.1 Ajustes de LDAP

Elemento	Descripción
1	Dirección IP del servidor de Active Directory
2	Puerto TCP de Active Directory <sup>2</sup> 389 - Non SSL 636 - SSL
3	Modo LDAP OpenLDAP - Active Directory
4	Seguridad de Active Directory <sup>2</sup> None - SSL - StartTLS
5	Cuenta de AD utilizada para enlazar con el servidor de AD Debe estar en notación de ruta de DN completo CN=adbindacct,CN=Users,DC=vertiv,DC=com La contraseña de la cuenta no debe caducar
6	Establecer la contraseña de la cuenta de enlace de AD
7	Verificar contraseña
8	Ruta de dominio base para buscar usuarios de AD <sup>1</sup> Debe estar en notación de ruta de DN completo DC=vertiv, DC=com
9	Filtro de atributo ObjectClass de usuario de AD

**Tabla H.1 Ajustes de LDAP (continuación)**

Elemento	Descripción
	(objectClass=user)
10	Filtro de nombre de cuenta de usuario de AD samaccountname
11	"uidNumber" Mapping uidNumber
12	Filtro de atributo ObjectClass de grupo de AD (objectClass=group)
13	"gid" Mapping gidNumber
14	Ajuste necesario memberOf
15	Asignación de grupo de seguridad de AD a rol de Enabled Debe estar en notación de ruta de DN completo CN=enabled, DC=vertiv, DC=com
16	Asignación de grupo de seguridad de AD a rol de Control Debe estar en notación de ruta de DN completo CN=control, DC=vertiv, DC=com
17	Asignación de grupo de seguridad de AD a rol de Admin Debe estar en notación de ruta de DN completo CN=admin, DC=vertiv, DC=com
<p><b>NOTA: <sup>1</sup>La mejor práctica es reducir el ámbito de cruce de dominios de AD para buscar usuarios autenticados. Intente evitar especificar solo el dominio base si hay un esquema de AD grande y anidado.</b></p> <ul style="list-style-type: none"> <li>• Ideal: OU=Enabled Users, OU=User Accounts, DC=vertiv, DC=com</li> <li>• No ideal: DC=vertiv, DC=com</li> </ul>	
<p><b>NOTA: <sup>2</sup>StartTLS utiliza el puerto TCP 389. Inicialmente establece la sesión sin cifrar pero la cifrará a partir de ese momento si el servidor de Active Directory acepta la solicitud LDAP_START_TLS_OID.</b></p>	

## Conectar con Vertiv en las redes sociales



<https://www.facebook.com/vertiv/>



<https://www.instagram.com/vertiv/>



<https://www.linkedin.com/company/vertiv/>



<https://www.x.com/Vertiv/>



---

Vertiv.com | Vertiv Headquarters, 505 N Cleveland Ave, Westerville, OH 43082 EE. UU.

©2025 Vertiv Group Corp. Todos los derechos reservados. Vertiv™ y el logotipo de Vertiv son marcas comerciales o marcas comerciales registradas de Vertiv Group Corp. Todos los demás nombres y logotipos a los que se hace referencia son nombres comerciales, marcas comerciales o marcas comerciales registradas de sus respectivos propietarios. Si bien se han tomado todas las precauciones para garantizar la exactitud e integridad de la información incluida en el presente documento, Vertiv Group Corp. no asume ninguna responsabilidad y rechaza toda responsabilidad legal por los daños y perjuicios resultantes del uso de esta información o por cualquier error u omisión cometidos.

SL-71211\_REVB\_05-25