



## SEGURIDAD DE DATOS DE ORANGE HRM

¡Tus datos están a salvo con nosotros!



Mantener la información de sus compañeros de trabajo segura y protegida es el nombre del juego. Con Orange HRM ya no tendrá que preocuparse por implementar medidas de seguridad. Por favor, lea nuestra documentación a continuación para ver todos los detalles que necesita.





## PROVEEDOR DE SERVICIO EN LA NUBE - RACKSPACE

Las soluciones híbridas y de múltiples nubes seguras de Rackspace nos ayudan a cumplir con las cambiantes expectativas tecnológicas, adoptar tecnologías emergentes y responder a los estrictos mandatos de seguridad y cumplimiento.

Rackspace brinda un soporte incomparable que nos ayuda a resolver los desafíos operativos de manera más rápida e inteligente. Rackspace garantiza:

- 100% de garantía de tiempo de actividad de la red.
- Cartera inigualable de aplicaciones, datos, seguridad e infraestructura.
- SLA líderes en la industria y puntajes de satisfacción del cliente.
- Soporte 24x7x365 de expertos certificados
- Auditorías y certificaciones de seguridad independientes (p. ej., ISO, SOC, PCI, FISMA)

## CONTROLES DE SEGURIDAD - RACKSPACE

### SEGURIDAD FÍSICA

- El acceso al centro de datos está limitado solo al personal autorizado.
- Credenciales y escaneo biométrico para acceso controlado al centro de datos.
- Monitoreo de cámaras de seguridad en todas las ubicaciones del centro de datos.
- Retención de logs de acceso y videovigilancia.
- El personal in situ disponible las 24 horas, los 7 días de la semana, los 365 días del año brinda protección adicional contra la entrada no autorizada.
- Instalaciones sin marcar para ayudar a mantener un perfil bajo.
- La seguridad física es auditada anualmente por firmas independientes.



## INFRAESTRUCTURA DE RED

- Ancho de banda de alto rendimiento proporcionado por múltiples proveedores de red.
- Eliminación de puntos únicos de falla en toda la infraestructura de red compartida.
- Cables debidamente canalizados y asegurados.
- La metodología proactiva de gestión de red supervisa la eficiencia de la ruta de la red.
- Mejoras de configuración y topología en tiempo real para ajustar las anomalías.
- Tiempo de actividad de la red respaldado por acuerdos de nivel de servicio.
- Gestión de red realizada por personal autorizado.

## INFRAESTRUCTURA DE RED

- Rutas de alimentación duales hacia las instalaciones.
- Sistemas de alimentación ininterrumpida (mínimo N+1).
- Generadores diésel (mínimo N+1).
- Acuerdos de servicio con proveedores de combustible vigentes.
- HVAC (mínimo N + 1 ).
- VESDA/supresión de incendios.
- Detección de inundaciones
- Supervisión continua de las instalaciones.

## INFRAESTRUCTURA DE RED

- Investigación de antecedentes realizada en empleados con acceso a cuentas de clientes.
- Los empleados deben firmar acuerdos de confidencialidad y no divulgación.
- Los empleados se someten a seguridad obligatoria formación de sensibilización
- en el momento del empleo y anualmente a partir de entonces.



Rackspace mantiene varias certificaciones para ayudarlo a verificar las políticas y los procesos de seguridad que Rackspace tiene implementados para el entorno de su servidor alojado. infraestructura.

Rackspace ha sido evaluado y tiene validación para los siguientes marcos de cumplimiento.

- ✓ ISO27001
- ✓ SSAE 16 and ISAE 3402 (previously SAS 70 Typell)
- ✓ PCI DSS
- ✓ Safe Harbour (export.gov)



## CUMPLIMIENTO DE RACKSPACE

### ISO 27001

El sistema de administración de seguridad de la información (ISMS) certificado por Rackspace ISO 27001 es un sistema de administración iterativo que ayuda a garantizar que las políticas y los procesos de seguridad sean efectivos para mitigar los riesgos identificados.

En concreto, el SGSI de Rackspace certifica la gestión de la seguridad de la información en las operaciones de sus instalaciones de centros de datos.

### SSAE 16 AND ISAE 3402

El informe global de Rackspace Tipo II a SOC 1 se puede utilizar para satisfacer los requisitos de las normas SSAE 16 e ISAE 3402. Este informe contiene una descripción de los controles implementados y la opinión informada de los auditores sobre cuán efectivos fueron los controles durante el período de auditoría. El período



## PCI DSS

Un asesor de seguridad calificado (QSA) valida a Rackspace como proveedor de servicios de nivel 1 de PCI DSS. La validación QSA de nuestro cumplimiento con PCI DSS cubre:

- Seguridad física para centros de datos de Rackspace ubicados en:
  - ✓ Reino Unido
  - ✓ Hong Kong
  - ✓ Estados Unidos.
- Infraestructura de red (routers y switches).
- Acceso de los empleados de Rackspace a los dispositivos de red.

## EVALUACIONES DE SEGURIDAD DE RACKSPACE

### SEGURIDAD DE LA ORGANIZACIÓN

- Responsabilidades de gestión de seguridad asignadas a Global Security Services.
- La supervisión del director de seguridad de las operaciones de seguridad y las actividades de gobierno, riesgo y cumplimiento.
- Participación directa con la gestión de incidentes, la gestión del cambio y la continuidad del negocio

### SEGURIDAD DE LA OPERACIÓN

- Políticas basadas en ISO 27001/2 revisadas al menos una vez al año.
- Procedimientos documentados de gestión de cambios de infraestructura.
- Destrucción segura de documentos y medios.
- Función de gestión de incidencias.
- Un plan de Continuidad de Negocio enfocado en la disponibilidad de infraestructura.
- Revisiones independientes realizadas por terceros
- Monitoreo continuo y mejoras de los programas de seguridad.



# CUMPLIMIENTO DE ORANGEHRM

## SERVICIOS CERTIFICADOS DE ISO 27001:2013

La certificación ISO 27001:2013 establece los requisitos para implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información (SGSI) dentro del entorno de la organización junto con los requisitos para evaluar y tratar los riesgos de seguridad de la información.

Nuestros servicios para clientes certificados incluyen:

- Operaciones Técnicas.
- Servicios de Soporte Técnico.
- Entrega del producto.
- Éxito del cliente.



## CUMPLIMIENTO GDPR

El RGPD, también conocido como el Reglamento General de Protección de Datos, requiere que las organizaciones que tratan con datos personales de ciudadanos de la UE cumplan con esta ley de privacidad y seguridad aprobada por el Parlamento Europeo el 25 de mayo de 2018.

Según lo exigen las regulaciones GDPR, nos aseguramos de que los datos personales de los residentes de la UE estén protegidos a través de una variedad de protocolos y funciones de seguridad, como la capacidad de depurar la información de los empleados, el consentimiento para conservar la información de candidatos y empleados, registros de auditoría y registros de cambios, y estrictos protocolos de manejo de datos.

Siga el enlace para obtener más información sobre cómo OrangeHRM cumple con GDPR



<https://www.orangehrm.com/resources/news/gdpr-readines/>



## SEGURIDAD DE LA APLICACIÓN

- Copias de seguridad diarias de la base de datos en el sitio.
- Retención de copia de seguridad continua de 4 semanas (ampliada a pedido).
  - ✓ Lenguaje de marcado de aserción de seguridad 2.0 (SAML 2.0). Habilitar caducidad
  - ✓ Contraseña segura forzada.
  - ✓ CAPTCHA y bloqueo de acceso por intentos fallidos
  - ✓ Contraseña Secundaria
  - ✓ Evaluaciones regulares de OWASP.
- Niveles de acceso configurables basados en roles
- Para más información contacte con nuestro Delegado de Protección de Datos (DPO) en **dpo@orangehrm.com**



# ¡GRACIAS!

[www.orangehrm.com](http://www.orangehrm.com)

