

# HPE Device Entitlement Gateway (DEG) como Servicio

## Apéndice II: Descripción del procesamiento

1. Descripción del procesamiento	Como parte de la prestación de servicios profesionales y soporte de mantenimiento de software, el Procesador podría tener acceso a los datos almacenados en la plataforma Device Entitlement Gateway (DEG) del Procesador (incluidos los metadatos). Estos datos pueden incluir información personal del Controlador.
2. Tipo de datos personales procesados	El tipo de datos que se procesa dependerá de los datos que el Controlador haya almacenado en las aplicaciones empresariales (incluidos los metadatos), la TI y la infraestructura de red, e incluye los siguientes datos personales: IMSI, MSISDN, ID del dispositivo (IMEI, EID, ICCID), Dirección IP, Cookie.
3. Categorías de datos personales procesados	Cualquier sujeto de datos cuyos datos personales almacene el Controlador en las aplicaciones empresariales (incluidos los metadatos), la TI y la infraestructura de red, entre ellos, los datos de identificación del dispositivo, los metadatos de las comunicaciones electrónicas y los datos de autenticación.
4. Duración del procesamiento	El Procesador deberá procesar los datos personales del Controlador durante el periodo del Acuerdo y/o cualquier documento de la transacción aplicable. Todos los datos personales se almacenarán en la plataforma de DEG durante un máximo de 6 meses.
5. Medidas técnicas y organizacionales	El Procesador deberá mantener el programa de seguridad física y de la información para proteger los datos personales del Controlador como se detalla en el Apéndice III a continuación.

## HPE Device Entitlement Gateway (DEG) como Servicio

### Apéndice III: Medidas técnicas y organizacionales, incluidas las medidas que garantizan la seguridad de los datos

1. Como parte del programa de seguridad física y de la información usado por el Procesador para proteger los datos personales del Controlador (“Programa de Seguridad”), HPE conduce revisiones periódicas de las prácticas de seguridad comparándolas con estándares del sector como NIST, ISO 27001 y SOC. El Procesador reevalúa con regularidad y actualiza el Programa de Seguridad del Procesador a medida que el sector evoluciona, aparecen nuevas tecnologías o se identifican nuevas amenazas.
2. El Programa de Seguridad del Procesador consiste (como mínimo) en lo siguiente:
  - a. El Procesador mantiene los estándares de seguridad física diseñados para prohibir que personas no autorizadas tengan acceso físico a las instalaciones y el equipo del Procesador, mediante las siguientes prácticas:
    - i. El acceso físico a las instalaciones se limita a los empleados, subcontratistas y visitantes autorizados del Procesador

- ii. A los empleados, subcontratistas y visitantes autorizados del Procesador se les brindan tarjetas de identificación que deben usar mientras permanezcan en las instalaciones
  - iii. Se monitorea el acceso a las instalaciones del Procesador y eso incluye las áreas y el equipo restringidos
  - iv. El acceso al centro de datos donde se alojan los datos personales del Controlador se registra, monitorea y rastrea; y
  - v. Los centros de datos están protegidos con sistemas de alarma y cámaras de video.
- b. El Procesador mantiene control del acceso al entorno de TI relevante, de acuerdo con las mejores prácticas del sector. Estos controles incluyen, entre otros, los requisitos relacionados con principios de privilegios mínimos, complejidad y uso de contraseña.
- c. La infraestructura del Procesador tiene versiones del software de seguridad del sistema razonablemente actualizadas, que pueden incluir un firewall host, protección antivirus, y parches y definiciones de virus actualizados. El Procesador mantiene registros de los eventos relacionados con la infraestructura, incluidos los sistemas de detección de intrusiones para monitorear, detectar e informar patrones de uso inadecuado, actividades sospechosas, usuarios no autorizados y otros riesgos de seguridad.
3. Si se solicita, el Procesador revisará con el Controlador un resumen de las evaluaciones de vulnerabilidad. Las evaluaciones de vulnerabilidad no le dan derecho al Controlador de ver o acceder de ningún modo a los registros y/o procesos: (a) que no se relacionen directamente con el servicio; (b) de modo que infrinja leyes aplicables y/o (c) de modo que infrinja las obligaciones de confidencialidad y seguridad del Procesador con terceros.
4. Los empleados y contratistas reciben capacitación sobre las políticas de privacidad y seguridad del Procesador y se les informa acerca de sus responsabilidades con relación a las prácticas de privacidad y seguridad. Los empleados y contratistas del Procesador están obligados contractualmente a mantener la confidencialidad de los datos personales del Controlador y a cumplir las políticas, estándares o requisitos del Procesador con relación al procesamiento de los datos personales del Controlador. El incumplimiento de estas políticas, estándares o requisitos estará sujeto a investigación, lo que podría generar una acción disciplinaria, incluidos el despido o la rescisión del contrato de parte del Procesador.
5. En caso de que el Procesador confirme una infracción de seguridad que, de modo accidental o ilegal, lleve a la destrucción, pérdida, modificación o divulgación o acceso no autorizado a los datos personales del Controlador ("Incidente de seguridad"), el Procesador hará lo siguiente:
- a. Sin una demora indebida, le notificará al Controlador sobre el Incidente de seguridad. El Procesador proporcionará al Controlador actualizaciones sobre el estado del Incidente de seguridad hasta que se haya resuelto el problema. Los informes incluirán, entre otros, una descripción del Incidente de seguridad, las acciones tomadas y los planes de solución. Si el Controlador se entera de un Incidente de seguridad que afecta los servicios, deberá notificarlo inmediatamente al Procesador, e informarle el alcance del Incidente de seguridad.
  - b. A petición y expensas del Controlador, (I) le proporcionará al Controlador asistencia razonable para notificar una infracción de seguridad a la autoridad competente según las leyes de privacidad aplicables al Controlador y (II) le proporcionará al Controlador asistencia razonable para comunicar una fuga de datos a las partes interesadas, en los casos en que la fuga pueda representar un alto riesgo para los derechos y libertades de las personas.

Visite [HPE.com](https://www.hpe.com)

### [Chatee ahora](#)

© Copyright 2026 Hewlett Packard Enterprise Development LP. La información contenida en el presente documento está sujeta a cambios sin previo aviso. Las únicas garantías para los productos y servicios de Hewlett Packard Enterprise se establecen en las declaraciones de garantía expresas que acompañan a dichos productos y servicios. Ninguna información contenida en este documento debe interpretarse como una garantía adicional. Hewlett Packard Enterprise no se responsabiliza de los errores técnicos o editoriales ni por las omisiones que pueda contener este documento.

a50000032SPL - Apéndice a50009392SPL

HEWLETT PACKARD ENTERPRISE

[hpe.com](https://www.hpe.com)

