

**INFORME TÉCNICO PREVIO DE EVALUACIÓN DE SOFTWARE**  
**No. 021-2009-GTI000**

**ADQUISICIÓN DE LICENCIAS CRIPTOGRÁFICAS PARA EQUIPOS HSM**

**1. NOMBRE DEL ÁREA:**

Dpto. de Redes, Telecomunicaciones y Bases de Datos

**2. RESPONSABLE DE LA EVALUACIÓN:**

Alexander Gamboa Inga

**3. CARGO:**

Especialista en Seguridad Informática en Redes

**4. FECHA:**

1 de julio de 2009.

**5. JUSTIFICACIÓN:**

A fines de 2008 el BCRP adquirió los equipos Thales HSM 8000, para su uso en la implementación de las funcionalidades criptográficas del nuevo Sistema LBTR.

El Software criptográfico, incluido con dichos equipos, proporciona las siguientes funcionalidades:

- Gestión de clave maestra (LMK – Local Master Key).
- Cifrado de clave asimétrica (RSA), empleado en la generación y verificación de firmas digitales.

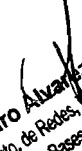
Con la finalidad de implementar las funciones de cifradodescifrado de datos, que son requeridas en la operación del nuevo Sistema LBTR (según consta en el informe de sustento del líder de dicho proyecto), se requiere adquirir licencias criptográficas que habiliten dichas funciones en los equipos HSM.

**6. ALTERNATIVAS:**

Considerando que el software criptográfico solicitado, de la marca Thales, se ejecuta en los equipos HSM 8000, de la misma marca, con el que ya cuenta el BCRP (equipamiento preexistente), se ha solicitado en este proceso la adquisición de licencias criptográficas que permitan a dichos equipos implementar el uso de funciones de cifradodescifrado de datos (Message Encryption).

**7. ANÁLISIS COMPARATIVO TÉCNICO:**

Debido a que es un sistema con el cual ya cuenta el BCRP y el cual ha sido solicitado sea estandarizado, lo que se desea es la adquisición de licencias criptográficas que

  
**Leandro Alvarez Figueroa**  
Jefe. Dpto. de Redes, Telecomunicaciones  
y Bases de Datos

  
**MIGUEL TEJADA MALASPINA**  
Sub-Gerente de Servicios de  
Tecnologías de Información

  
**ALEXANDER GAMBOA INGA**  
REB. 2002

permitan implementar las funcionalidades requeridas en los equipos HSM con que ya cuenta el BCRP, por lo que no cabe un análisis comparativo técnico.

## 8. ANÁLISIS COMPARATIVO DE COSTO – BENEFICIO:

### Beneficios:

- 9 Implementación de funciones de cifradoldescifrado de datos, requeridas para la operación del nuevo sistema LBTR.

### Costos:

- 9 Adquisición de licencias

Adquisición de licencias de software para cifradoldescifrado de datos en los equipos Thales HSM 8000 del BCRP.

Se obtuvo una cotización **referencial** por un monto de S/. 24 069,42 incluido IGV.

- 9 Hardware necesario para su funcionamiento

El software solicitado se ejecutará en dos appliances Thales HSM 8000, con los cuales ya cuenta el BCRP.

- 9 Mantenimiento y soporte técnico externo

El mantenimiento y soporte técnico se realizará por un treinta (30) meses, en el esquema 24x7x2, lo que comprende el soporte técnico del proveedor (con el correspondiente respaldo del fabricante), incluyendo el suministro de nuevas versiones (releases) y reparaciones (en general denominadas comercialmente como patches, temporaty *fixes*, etc.).

- 9 Tiempo de entrega de la solución, con las condiciones exigidas por el BCRP

El plazo de entrega será no mayor de 7 días calendario, contabilizados a partir de la suscripción de la orden de compra o contrato.

## 9. CONCLUSIONES:

Por lo expuesto anteriormente, se considera conveniente la adquisición de Licencias Criptográficas para los equipos Thales HSM 8000, incluyendo el mantenimiento de software y soporte técnico correspondientes, por el periodo de treinta (30) meses.

## 10. FIRMAS:

  
**Leandro Alvarez Figueroa**  
Jefe, Dpto. de Redes, Telecomunicaciones  
y Bases de Datos

  
**ALEXANDER GÁMBOA INGA**  
REG. 2002