

BANCO CENTRAL DE RESERVA DEL PERÚ

MEMORANDO N° 0066-2023-ADM110-N

A: Javier Ernesto Olivera Vega
Gerente Central de Administración

DE: César Oscar Delizzia Infante
Jefe de Departamento de Programación Logística

ASUNTO: Estandarización para la renovación del soporte técnico y mantenimiento del licenciamiento perpetuo de la plataforma RSA Authentication Manager brindada por el fabricante o representante de la marca RSA; y la adquisición de los componentes Token RSA

REFERENCIA: Informe N° 0036-2023-GTI230-N

FECHA: 27 de febrero de 2022

Por el presente solicito a usted se sirva aprobar el informe N° 0036-2023-GTI230-N, elaborado por el Departamento de Ciberseguridad y Redes, referido a la estandarización para la renovación del soporte técnico y mantenimiento del licenciamiento perpetuo de la plataforma RSA Authentication Manager brindada por el fabricante o representante de la marca RSA; y la adquisición de los componentes Token RSA.

De acuerdo con lo indicado en el informe, el BCRP adquirió la solución de doble factor de autenticación de la marca RSA (RSA Authentication Manager) con licenciamiento perpetuo, incluyendo sus respectivos tokens de la misma marca RSA. La arquitectura de la solución está conformada por dos componentes:

- Componente Software - licenciamiento: RSA Authentication Manager.
- Componente Hardware: Tokens RSA.

Por lo que, la renovación del soporte técnico y mantenimiento del licenciamiento perpetuo brindado por el fabricante o representante de la marca RSA, y la adquisición de los componentes Tokens RSA, son complementarios a la infraestructura existente. Por un lado, la renovación del soporte técnico y mantenimiento del licenciamiento perpetuo brindado por el fabricante o representante de la marca RSA, es imprescindible, porque con el mantenimiento se obtendrá nuevas versiones, parches (fixes), Upgrade y service packs, para las licencias; y el soporte técnico permitirá contar con asistencia técnica ante problemas que se presenten con el uso de las licencias perpetuas. Por otro lado, los componentes tokens RSA son imprescindibles al ser los únicos tokens en el mercado que se pueden complementar con las licencias perpetuas de la plataforma RSA y permitir la integración de la solución RSA que el BCRP dispone, lo cual garantizará la funcionalidad y operatividad de la infraestructura existente.

Por los motivos descritos en el informe de la referencia, se enmarca en el proceso de estandarización previsto en el numeral 29.4 del Artículo 29 del Reglamento de la Ley de Contrataciones y la Directiva N° 004-2016-OSCE/CD. La presente estandarización tendrá vigencia durante el procedimiento de selección que se lleve a cabo para la renovación del soporte técnico y mantenimiento del licenciamiento perpetuo brindado por el fabricante o representante de la marca RSA, y la adquisición de los componentes Tokens RSA.

BANCO CENTRAL DE RESERVA DEL PERÚ

FIRMADO POR:

Cesar Oscar DELIZZIA INFANTE
Jefe de Departamento de Programación Logística
Departamento de Programación Logística

VISADO POR:

Cesar Oscar DELIZZIA INFANTE
Subgerente de Logística Interino
Subgerencia de Logística
Firma como encargado.

Jose Arturo Alberto PASTOR PORRAS
Gerente de Compras y Servicios
Gerencia de Compras y Servicios

Javier Ernesto OLIVERA VEGA
Gerente Central de Administración
Gerencia Central de Administración

BANCO CENTRAL DE RESERVA DEL PERÚ

INFORME N° 0036-2023-GTI230-N

Informe - Estandarización del servicio de renovación de la solución de doble factor de autenticación RSA

1. NOMBRE DEL ÁREA:

Subgerencia de Servicios de Tecnologías de Información.

2. RESPONSABLE DE LA EVALUACIÓN Y SU CARGO:

Christian García Cerna, Especialista en Ciberseguridad y Redes.

Leandro Alvarez Figueroa, Jefe de Departamento de Ciberseguridad y Redes.

Miguel Tejada Malaspina, Subgerente de Servicios de Tecnología de Información.

3. DESCRIPCIÓN DEL EQUIPAMIENTO O INFRAESTRUCTURA PREEXISTENTE

En el año 2017, el BCRP adquirió la solución de doble factor de autenticación de la marca RSA (RSA Authentication Manager) con licenciamiento perpetuo, incluyendo sus respectivos tokens de la misma marca RSA.

La arquitectura de la solución está conformada por dos componentes:

- Componente Software - licenciamiento: RSA Authentication Manager.
- Componente Hardware: Tokens RSA.

Por un lado, el componente software RSA Authentication Manager, tiene licenciamiento perpetuo de acuerdo lo indicado por el fabricante y como se muestra en la siguiente imagen:

Part Number	Part Description	Quantity
AUT0000025B8	SID Access Base Perp from 10 - 25u	1
# of Users - 10		
License Duration - Perpetual		
License Type Selection - Base Server License		
Sales Type - Upgrade		
Version - VERSION 8.2.1		
Serial/License Number: 81370633		

Por otro lado, el componente hardware Token RSA, genera un código de un solo uso (OTP - One Time Password) que se utiliza en conjunto con un nombre de usuario y una contraseña para proporcionar una capa adicional de seguridad en el inicio de sesión de las PC del Departamento de Mensajes Financieros con acceso a la red de Swift. Los Tokens RSA por seguridad cuentan con un tiempo de vida útil limitado y son los únicos que se pueden integrar con el componente software RSA Authentication Manager, confirmado por el área de soporte de la solución RSA.

BANCO CENTRAL DE RESERVA DEL PERÚ

El sistema internacional de pago Swift, dentro de las exigencias de controles, requiere que sus clientes Swift (dentro de ellos el BCRP) cumplan con su política de controles de seguridad del cliente (SWIFT Customer Security Controls Framework v2022), siendo la solución de doble factor de autenticación un control obligatorio como exigencia del marco de cumplimiento.

4. DESCRIPCIÓN DEL BIEN O SERVICIO REQUERIDO

El servicio requerido comprende la renovación del soporte técnico y mantenimiento del licenciamiento perpetuo de la plataforma RSA Authentication Manager brindada por el fabricante o representante de la marca RSA; y la adquisición de los componentes Token RSA.

El servicio requerido permitirá mantener vigente la solución de doble factor de autenticación RSA, la cual es crucial para evitar un acceso no autorizado a un sistema crítico como es el caso de SWIFT, además de ser obligatorio para cumplir la política de controles de seguridad del cliente de SWIFT (SWIFT Customer Security Controls Framework v2022).

5. USO O APLICACIÓN QUE SE DARÁ AL BIEN O SERVICIO REQUERIDO

La renovación del soporte técnico y mantenimiento del licenciamiento perpetuo comprende la atención a problemas o fallas en el firmware de la solución, escalamiento con el fabricante, actualizaciones a nuevas versiones y reparaciones (denominadas comercialmente como patches, temporary fixes y updates).

Asimismo, se requiere la adquisición de los componentes Token RSA (hardware), debido a que son los únicos en el mercado que se pueden complementar con las licencias perpetuas de la plataforma RSA Authentication Manager y cumplir con el segundo factor de autenticación.

El servicio de renovación de la solución de doble factor de autenticación RSA brindará y asegurará la atención temprana del fabricante a problemas o fallas en el firmware, así como el soporte contra fallas del hardware en los Tokens RSA (RMA).

6. JUSTIFICACIÓN

A continuación, se sustentan los requisitos para proceder con la estandarización:

6.1 Aspectos Técnicos:

La solución RSA se encuentra integrada a las PC autorizadas de la red Swift del Banco, siendo indispensable la renovación del soporte técnico y mantenimiento del licenciamiento perpetuo de la plataforma RSA Authentication Manager brindada por el fabricante o representante de la marca RSA; y la adquisición de los componentes Token RSA, por lo siguiente:

- Seguridad: Las amenazas de ciberseguridad están en constante evolución, por lo que es importante mantener la solución actualizada para protegerse contra nuevas vulnerabilidades que expongan la continuidad operativa.

BANCO CENTRAL DE RESERVA DEL PERÚ

- Vida útil: Los tokens RSA tienen una vida útil limitada, después de la cual ya no funcionan por seguridad, por lo que es imprescindible renovarlos antes de que alcancen su fin de vida útil el 30 de Julio del 2023.
- Cumplimiento: Es requisito obligatorio disponer de la solución de doble factor de autenticación para cumplir la política de controles de seguridad del sistema internacional de pago Swift (SWIFT Customer Security Controls Framework v2022).

6.2 Verificación de los presupuestos:

a. La Entidad posee determinado equipamiento o infraestructura pudiendo ser maquinarias, equipos, vehículos, u otro tipo de bienes, así como ciertos servicios especializados.

El BCRP cuenta la solución de doble factor de autenticación de la marca RSA detalladas en el numeral 3, la misma que se encuentra integrada para el acceso a las PC autorizadas a la red Swift, brindando una capa adicional de protección contra cualquiera que busque obtener acceso no autorizado.

b. Los bienes o servicios que se requiere contratar son accesorios o complementarios al equipamiento o infraestructura preexistente, e imprescindibles para garantizar la funcionalidad, operatividad o valor económico de dicho equipamiento o infraestructura.

La renovación del soporte técnico y mantenimiento del licenciamiento perpetuo brindado por el fabricante o representante de la marca RSA, y la adquisición de los componentes Tokens RSA, son complementarios a la infraestructura existente detallada en el numeral 3.

Por un lado, la renovación del soporte técnico y mantenimiento del licenciamiento perpetuo **brindado por el fabricante o representante de la marca RSA, es imprescindible, porque con el mantenimiento se obtendrá nuevas versiones, parches (fixes), Upgrade y service packs, para las licencias; y el soporte técnico permitirá contar con asistencia técnica ante problemas que se presenten con el uso de las licencias perpetuas. Por otro lado, los componentes tokens RSA son imprescindibles al ser los únicos tokens en el mercado que se pueden complementar con las licencias perpetuas de la plataforma RSA Authentication Manager y permitir la integración de la solución RSA que el BCRP dispone, lo cual garantizará la funcionalidad y operatividad de la infraestructura existente.**

El correcto funcionamiento de la solución de doble factor de autenticación RSA garantizará la continuidad operativa y el cumplimiento de la política de controles de seguridad del sistema internacional de pago Swift (SWIFT Customer Security Controls Framework v2022).

6.3 Incidencia Económica de la Contratación

El disponer del soporte técnico y mantenimiento de las licencias perpetuas reduce la posibilidad de obsolescencia tecnológica debido a que permite mantener actualizada la solución RSA, preservando de esta manera el valor

BANCO CENTRAL DE RESERVA DEL PERÚ

económico de la inversión realizada en la adquisición de esta y tener la disponibilidad en caso de una emergencia o ante un evento de seguridad.

Además, la adquisición de los Token RSA asegura la operatividad de la solución RSA puesto que solo esta se puede complementar con las licencias perpetuas de la plataforma RSA. La implementación de cualquier otro similar implicaría un nuevo proyecto de solución de largo alcance que impactaría en términos de tiempo y costos de nuevas licencias, tokens e implementación del desarrollo para elaborar las funcionalidades que se tienen actualmente. Por ello lo que se desea es el servicio de renovación de la solución de doble factor de autenticación RSA.

7. CONCLUSIONES

En cumplimiento con lo establecido en la Directiva N°004-2016-OSCE/CD que norma la estandarización, se solicita se apruebe la estandarización de la solución de doble factor de autenticación RSA, el cual comprende la renovación del soporte técnico y mantenimiento del licenciamiento perpetuo brindado por el fabricante o representante de la marca RSA, y la adquisición de los componentes Tokens RSA.

8. FECHA DE ELABORACIÓN DEL INFORME:

Lima, 23 de febrero de 2023

cc. Departamento de Programación Logística - Mayra Andrea Quispe Huancahuari

BANCO CENTRAL DE RESERVA DEL PERÚ

FIRMADO POR:

Christian Manuel GARCIA CERNA
Especialista en Ciberseguridad y Redes
Departamento de Ciberseguridad y Redes

Leandro Manuel ALVAREZ FIGUEROA
Jefe de Departamento de Ciberseguridad y Redes
Departamento de Ciberseguridad y Redes

VISADO POR:

Miguel Angel TEJADA MALASPINA
Subgerente de Servicios de Tecnologías de
Información
Subgerencia de Servicios de Tecnologías de
Información

Silvia Elizabeth MEDINA MORENO
Gerente de Tecnologías de Información
Gerencia de Tecnologías de Información