Subsecretaría de Economía y Empresas de Menor Tamaño

Gobierno de Chile

160014318
1106777186
División Jurídica - DJVP

ORD. N°: 5007 27 JUN 2018

MAT.: Emite pronunciamiento a solicitud de BPO-Advisors SpA.

ANT: Carta de 15 de mayo de 2018, de don Marcelo Mora Saa, Gerente General BPO-Advisors.

ADJ.: Informe Custodia de Certificado Privado en HSM.

Santiago,

DE: IGNACIO GUERRERO TORO
SUBSECRETARIO DE ECONOMÍA Y EMPRESAS DE MENOR TAMAÑO

A: MARCELO MORA SAA
GERENTE GENERAL
BPO – ADVISORS SPA

Por medio de la presente, me permito dar respuesta al pronunciamiento solicitado por usted mediante carta de 15 de mayo de 2018.

En dicha comunicación solicitó un pronunciamiento de esta Subsecretaría, respecto a la implementación de un procedimiento de emisión de firma electrónica avanzada de los usuarios utilizando la tecnología de HSM, con uso de PIN bajo exclusivo control del suscriptor de los certificados electrónicos.

Sobre el particular, puedo informar a usted que dicha solicitud ha sido analizada por el Encargado de la Entidad Acreditadora, emitiendo un Informe de "Custodia de Certificado Privado en HSM", que adjunto a la presente comunicación.

En dicho informe, se analiza la solicitud de la empresa BPO – Advisors, concluyendo que la firma electrónica avanzada custodiada en un HSM cumple con las normas técnicas requeridas, siempre que se observen las siguientes recomendaciones:

1. Esta modalidad debe incluirse de manera explícita en la Política de Certificación (CP – requisito PO01).
2. Esta modalidad debe incluirse de manera explícita en la Declaración de Prácticas de Certificación (CPS – requisito PO02).
3. En el contrato que se suscriba con el firmante, debe incluirse una cláusula de custodia de la clave privada. Se requiere un PIN de acceso y un PIN para firmar, este último es similar al que se le solicita al firmante cuando hace uso de un eToken.

4. El enrolamiento debe ser presencial o con prueba de vida y lo debe realizar un enrolador capacitado por el PSCA.
5. El enlace entre el cliente intermedio (empresa u organismo estatal) que facilita la plataforma y/o aplicación al firmante (cliente final), debe contar con cifrado (tipo VPN).
6. Los flujos de información entre el cliente intermedio (empresa u organismo estatal) y el PSCA deben estar cifrados (HTTPS).
7. La comunicación y flujo de información entre el cliente intermedio (empresa u organismo estatal) y el cliente final (firmante) deben estar cifrados.
8. La capacitación de los enroladores debe realizarla el PSCA, debiendo actualizarla anualmente o en caso de actualización de la plataforma tecnológica. Debe realizar una auditoría anual del proceso de enrolamiento, guardando los medios de prueba para presentarlos en la Inspección Anual Ordinaria.

Sin otro particular, saluda atentamente a usted,

REPUBLICA DE CHILE
SUBSECRETARIA DE ECONOMIA Y EMPRESAS DE MENOR TAMAÑO
SUBSECRETARIO

IGNACIO GUERRERO TORO
SUBSECRETARIO DE ECONOMÍA Y EMPRESAS DE MENOR TAMAÑO

GABINETE SUBSECRETARIO ECONOMIA Y E.M.T.
JEFE DE GABINETE

DISTRIBUCIÓN:
- Destinatario (Kennedy N° 7100, oficina 610, Vitacura, Santiago)
- Gabinete Subsecretario
- Entidad Acreditadora
- División Jurídica
- Oficina de Partes

SUBSECRETARIA DE ECONOMIA CHILE
ENCARGADA ADMINISTRACION