

TÉRMINOS DE REFERENCIA PARA LA CONTRATACIÓN DE LA RENOVACIÓN DE LOS CERTIFICADOS DIGITALES EV SSL

1. ANTECEDES Y JUSTIFICACIÓN

La Corporación Financiera Nacional B.P., es una institución financiera pública, cuya misión es impulsar el desarrollo de los sectores productivos y estratégicos del Ecuador, a través de múltiples servicios financieros y no financieros alineados a las políticas públicas, servicios que se ofrecen a la ciudadanía a través de herramientas tecnológicas y sus aplicativos informáticos, ya sean contratadas o desarrolladas por CFN.

La CFN B.P. hace uso de los certificados digitales EV SSL los cuales hacen que la institución pueda ofrecer sus servicios de forma segura, garanticen la identidad y propiedad de la CFN B.P., reforzando la confiabilidad de la información para con sus clientes a través del internet. Con lo que aporta a consolidar con la visión de ser la banca múltiple de desarrollo, moderna, eficiente.

El objetivo primordial de disponer de certificados digitales SSL es brindar la seguridad necesaria a los aplicativos informáticos ya que son uno de los elementos vitales los aplicativos informáticos, debido a que en ellos se procesa la información fundamental de la institución y de sus transacciones de negocio. El objetivo primordial de disponer de certificados digitales, es brindar la seguridad necesaria a todos los aplicativos y así los clientes validen que se trata de un sitio seguro para realizar cualquier transacción.

Al respecto, la Corporación Financiera Nacional B.P. mediante orden de compra #RIMCB-CFNGYE-013-019 del 5 de julio de 2019, realizó la renovación y adquisición de los certificados digitales EV SSL con los cuales cuenta la institución y que se encuentran vigentes hasta el 31 de julio del 2020:

ÍTEM	DESCRIPCIÓN	CANT.
1	<u>Certificado EV simples</u> <ul style="list-style-type: none"> • cfntaveler.cfn.fin.ec • correoseguro.cfn.fin.ec • correoseguroalterno.cfn.fin.ec • bi.cfn.fin.ec • webmailuio.cfn.fin.ec • ive.cfn.fin.ec • webmailgye.cfn.fin.ec • canales.cfn.fin.ec • www.cfn.fin.ec • elearning.cfn.fin.ec • webfile.cfn.fin.ec • ibanking.cfn.fin.ec 	12
2	<u>Certificado Multidominio EV</u> <ul style="list-style-type: none"> • Dominio 1 <ul style="list-style-type: none"> - Obanking.cfn.fin.ec - Fondogarantia.cfn.fin.ec - Serviciosintegracion.cfn.fin.ec 	1
3	<u>Certificado Wildcard Organization Validation</u>	1

Base Legal

El numeral 6 de la sección 410-09: "Mantenimiento y control de la infraestructura tecnológica", subgrupo 410: "TECNOLOGÍA DE LA INFORMACIÓN", grupo 400: "ACTIVIDADES DE CONTROL" de las "Normas de Control Interno para las Entidades, Organismos del Sector Público", de la Contraloría General del Estado, establece textualmente "Se elaborará un plan de mantenimiento preventivo y/o correctivo de la infraestructura tecnológica sustentado en revisiones periódicas y monitoreo en función de las necesidades

organizacionales (principalmente en las aplicaciones críticas de la organización), estrategias de actualización de hardware y software, riesgos, evaluación de vulnerabilidades y requerimientos de seguridad", por lo cual la unidad de tecnología de información de cada organización es la responsable de definir y regular los procedimientos que garanticen el mantenimiento y uso adecuado de la infraestructura tecnológica de las entidades.

Adicionalmente, en el "LIBRO I: NORMATIVA SOBRE OPERACIONES, TITULO IV: ADMINISTRACIÓN DE RIESGOS, SUBTITULO V: SEGURIDAD DE INFORMACIÓN (DIR-032-2010), CAPÍTULO I: MANUAL DE SEGURIDAD DE LA INFORMACIÓN, SECCIÓN I: POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN", de la Normativa de la CFN B.P., Numeral "5. DE LA SEGURIDAD FÍSICA Y AMBIENTAL, D. POLITICAS GENERALES", Sección "Seguridad del equipamiento y documentación", se establece textualmente que: "d) *El equipamiento será provisto de mantenimiento adecuado para asegurar que su disponibilidad e integridad sean permanentes.*"

De acuerdo con lo expuesto anteriormente y para dar cumplimiento a lo dispuesto en las "Normas de Control Interno para las Entidades, Organismos del Sector Público" y en la "Normativa de la CFN B.P.", la Gerencia de Tecnologías de la Información ha previsto la necesidad de contar con la renovación de los certificados digitales EV SSL que soporta los aplicativos informáticos.

2. OBJETO DE LA CONTRATACIÓN

Renovación de los certificados digitales EV SSL

3. OBJETIVOS

- Brindar servicios financieros y no financieros seguros y confiables tanto a clientes internos como externos, que garanticen la identidad y propiedad de la CFN B.P.
- Renovar e implementar los certificados digitales para precautelar la seguridad de la información en su confidencialidad, integridad y disponibilidad.

4. ALCANCE

El proceso contempla la renovación e implementación de los certificados digitales de los sitios web que dispone la CFN B.P. con el propósito de precautelar la seguridad de la información en cuanto a su confidencialidad, integridad y disponibilidad.

5. METODOLOGÍA DE TRABAJO Y REQUERIMIENTOS POR GESTIÓN DE RIESGO OPERATIVO

5.1. Metodología de trabajo

Una vez suscrita la orden de compra, y de acuerdo al plazo definido, el proveedor deberá realizar la generación, instalación y configuración de los certificados digitales.

Los certificados deberán estar firmados por 1 sola empresa certificadora

Esta actividad se la realizará en las oficinas de Quito, deberán ser realizadas bajo la supervisión del Administrador de la Orden.

Dicho proceso será efectuado en los horarios establecidos por la CFN B.P., pudiendo ser estos en horarios no laborables, incluyendo fines de semana y días festivos.

5.2. Requerimientos por Gestión de Riesgo Operativo – SB:

De conformidad con los requerimientos por Gestión de Riesgos Operativo conforme a las disposiciones de la Superintendencia de Bancos, el contratista durante la ejecución del contrato deberá cumplir con lo establecido en los acuerdos que se detallan a continuación:

5.2.1. Acuerdo de nivel de servicio (SLA)

De conformidad con lo establecido en el Libro I.- NORMAS DE CONTROL PARA LAS ENTIDADES DE LOS SECTORES FINANCIEROS PÚBLICO Y PRIVADO, TITULO IX.- DE LA GESTIÓN Y ADMINISTRACIÓN DE RIESGOS, CAPITULO V.- NORMA DE CONTROL PARA LA GESTIÓN DEL RIESGO OPERATIVO, SECCIÓN VI.- SERVICIOS PROVISTOS POR TERCEROS, ARTICULO 14, numeral b., i: Niveles mínimos de calidad del servicio acordado, de la Codificación de Resoluciones de la Junta Bancaria y de la Superintendencia de Bancos, el contratista deberá cumplir con lo establecido en el “ACUERDO DE NIVEL DE SERVICIO”, cuyo formulario deberá ser presentado previa suscripción de la Orden de Compra.

Si por necesidad de la institución, durante el tiempo de vigencia de los certificados, se requiere volver a generarlos y colocarlos en el mismo u otro servidor, el proveedor deberá realizar dicha actividad sin costo adicional, en coordinación con los técnicos de CFN B.P.

Este requerimiento deberá ser atendido con una modalidad de 7x24x365 (todos los días y horas del año, con tiempo de atención en sitio o remoto de 4 horas), siendo el tiempo de solución de problemas al siguiente día.

5.2.2. Acuerdo de confidencialidad de la información y datos

De conformidad con lo establecido en el Libro I.- NORMAS DE CONTROL PARA LAS ENTIDADES DE LOS SECTORES FINANCIEROS PÚBLICO Y PRIVADO, TITULO IX.- DE LA GESTIÓN Y ADMINISTRACIÓN DE RIESGOS, CAPITULO V.- NORMA DE CONTROL PARA LA GESTIÓN DEL RIESGOS OPERATIVO, SECCIÓN VI.- SERVICIOS PROVISTOS POR TERCEROS, ARTÍCULO 14, b., vi. “Confidencialidad de la información y datos”, de la Codificación de Resoluciones de la Junta Bancaria y de la Superintendencia de Bancos, el Contratista deberá cumplir con lo establecido en el “ACUERDO DE CONFIDENCIALIDAD DE INFORMACIÓN Y DATOS”, cuyo formulario deberá ser presentado como parte de su oferta.

En el acuerdo de confidencialidad de la información y datos se incluye como mínimo lo siguiente:

- Será responsabilidad del proveedor el guardar absoluta reserva sobre la información y las aplicaciones de propiedad de la CFN B.P. que acceda o le sean confiada en virtud de la ejecución, desarrollo o cumplimiento del contrato, inclusive la información que pueda ser expuesta debido a las vulnerabilidades en los sistemas de la CFN B.P.
- La inobservancia de lo manifestado dará lugar a que la Corporación Financiera Nacional B.P., ejerza las acciones legales, civiles y penales correspondientes en el Código Orgánico Integral Penal.
- La contratista será responsable del cumplimiento del acuerdo por parte del personal que el oferente empleare para la ejecución del presente contrato.

5.2.3. Acuerdo de derechos de propiedad intelectual del conocimiento, productos, datos e información

De conformidad con lo establecido en el Libro I.- NORMAS DE CONTROL PARA LAS ENTIDADES DE LOS SECTORES FINANCIEROS PÚBLICO Y PRIVADO, TITULO IX.- DE LA GESTIÓN Y ADMINISTRACIÓN DE RIESGOS, CAPITULO V.- NORMA DE CONTROL PARA LA GESTIÓN DEL RIESGO OPERATIVO, SECCIÓN VI.- SERVICIOS PROVISTOS POR TERCEROS, ARTICULO 14, numeral b., vii: Derechos de propiedad intelectual, productos, datos e información, cuando aplique” de la Codificación de Resoluciones de la Junta Bancaria y de la Superintendencia de Bancos, el Contratista

deberá cumplir con lo establecido en el “ACUERDO DE PROPIEDAD INTELECTUAL”, cuyo formulario deberá ser presentado como parte de su oferta.

En el acuerdo de propiedad intelectual se incluye como mínimo lo siguiente:

- Los informes, materiales didácticos, código fuente, conocimientos, productos, datos; e, información que, de ser el caso, resulten de la ejecución del contrato serán de propiedad exclusiva de la CFN B.P. y no podrán ser divulgados total o parcialmente por el profesional y/o por los profesionales que participen en la ejecución del contrato.
- La CFN B.P. podrá hacer uso que considere conveniente y sea aplicable, de los informes, materiales didácticos, código fuente, conocimientos, productos, datos; e, información que se generen durante la ejecución del contrato, de acuerdo con los intereses institucionales.
- La CFN B.P. podrá realizar el registro en el Servicio Nacional de Derechos Intelectuales (SENADI) cuando lo considere conveniente y sea aplicable, para los informes, materiales didácticos, código fuente, conocimientos, productos, datos; e, información que se generen durante la ejecución del contrato, de acuerdo con los intereses institucionales.

6. INFORMACIÓN QUE DISPONE LA ENTIDAD.

Detalle de los certificados que dispone actualmente la CFN B.P.

ÍTEM	DESCRIPCIÓN	CANT.
1	<u>Certificado EV simples</u> <ul style="list-style-type: none"> • cfntaveler.cfn.fin.ec • correoseguro.cfn.fin.ec • correoseguroalterno.cfn.fin.ec • bi.cfn.fin.ec • webmailuio.cfn.fin.ec • ive.cfn.fin.ec • webmailgye.cfn.fin.ec • canales.cfn.fin.ec • www.cfn.fin.ec • elearning.cfn.fin.ec • webfile.cfn.fin.ec • ibanking.cfn.fin.ec 	12
2	<u>Certificado Multidominio EV</u> <ul style="list-style-type: none"> • Dominio 1 <ul style="list-style-type: none"> - Obanking.cfn.fin.ec - Fondogarantia.cfn.fin.ec - Serviciosintegracion.cfn.fin.ec 	1
3	<u>Certificado Wildcard Organization Validation</u> <ul style="list-style-type: none"> • *.cfn.fin.ec 	1

7. PRODUCTOS O SERVICIOS ESPERADOS

7.1. Renovación certificados

- Renovación de los certificados digitales EV SSL que dispone la institución:

ÍTEM	DESCRIPCIÓN	CANT.
1	<u>Certificado EV simples</u> <ul style="list-style-type: none"> • cfntaveler.cfn.fin.ec • correoseguro.cfn.fin.ec 	12

	<ul style="list-style-type: none"> • correoseguroalterno.cfn.fin.ec • bi.cfn.fin.ec • webmailuio.cfn.fin.ec • ive.cfn.fin.ec • webmailgye.cfn.fin.ec • canales.cfn.fin.ec • www.cfn.fin.ec • elearning.cfn.fin.ec • webfile.cfn.fin.ec • ibanking.cfn.fin.ec 	
2	<p><u>Certificado Multidominio EV</u></p> <ul style="list-style-type: none"> • Dominio 1 <ul style="list-style-type: none"> - Obanking.cfn.fin.ec - Fondogarantia.cfn.fin.ec - Serviciosintegracion.cfn.fin.ec 	1
3	<p><u>Certificado Wildcard Organization Validation</u></p> <ul style="list-style-type: none"> • *.cfn.fin.ec 	1

Las especificaciones técnicas de los certificados deberán contemplar lo siguiente:

- Cumplir con el estándar X.509 de la UIT-T
 - Cifrado de información con los algoritmos SSL SHA-256, SHA-2, SHA256withRSA
 - Cifrado de 256 bits SSL Encryption como mínimo
 - Soporte para algoritmo SHA-1 y SHA-2
 - Llave de 2k o más
 - Los certificados simples y multidominio deben cumplir con validación extendida (barra de direcciones del navegador verde).
 - Compatibilidad con navegadores de Internet comúnmente usados (Mozilla Firefox, Google Chrome, Microsoft Edge, Microsoft Internet Explorer, Apple Safari)
 - Renovación, revocación y sustitución del certificado en línea
 - Todos los certificados solicitados deben ser firmados por una misma entidad certificadora (CA).
 - Sello de seguridad y autenticidad para el sitio.
 - Soporte sobre el protocolo criptográfico mínimo SSL v2.
- La instalación de los certificados comprende de las siguientes actividades:
 - El proveedor deberá generar el request (requerimiento) de los certificados y enviar para la firma de la entidad certificadora (CA).
 - Activación del logo de la entidad certificadora (CA), en los aplicativosweb que la CFN B.P. defina, de acuerdo a los certificados del presente proceso.
 - El proveedor deberá realizar la instalación, activación y configuración de los certificados firmados por la entidad certificadora (CA) en los servidores correspondientes que tiene disponible la CFN B.P.
 - La instalación deberá ser realizado directamente por técnicos del oferente.
 - La instalación debe cubrir todo lo referente a instalaciones y configuraciones de los certificados ofertados, para que su funcionamiento sea el requerido por la CFN B.P.

8. PLAZO TOTAL DE LA CONTRATACIÓN

El plazo total de la contratación será de 20 días calendario contados a partir de la notificación de suscripción de la Orden de Compra.

Consideraciones:

- En el plazo indicado el proveedor deberá realizar la entrega e instalación de los certificados digitales.
- El plazo de vigencia de los certificados digitales es de 365 días calendarios contados a partir del 31 de julio de 2020.

9. FORMA DE PAGO

La CFN B.P. pagará al proveedor el valor total de la Orden de Compra contra entrega de todos los certificados digitales, una vez que los mismos se hayan generado, instalado y configurado en los servidores de las CFN B.P., se hayan realizado las pruebas de funcionamiento, posterior al informe de conformidad del Administrador de la Orden de Compra, la suscripción del acta entrega recepción definitiva, y la entrega de la factura correspondiente.

Pagos indebidos: El CONTRATANTE se reserva el derecho de reclamar al CONTRATISTA, en cualquier tiempo, antes o después de la prestación del servicio, sobre cualquier pago indebido por error de cálculo o por cualquier otra razón, debidamente justificada, obligándose la contratista a satisfacer las reclamaciones que por este motivo llegare a plantear EL CONTRATANTE, reconociéndose el interés calculado a la tasa máxima del interés convencional, establecido por el Banco Central del Ecuador.

10. LOCALIDAD

En la siguiente tabla se indica el detalle de la localidad donde están instalados los certificados digitales:

Oficina - Localidad	Dirección
Quito	Calle Ñaquito 36 A, entre Corea y Naciones Unidas, Edificio Platinum G, 6to piso

11. OBLIGACIONES DEL CONTRATISTA

- Cumplir con las obligaciones establecidas en la Orden de Compra, y en el presente documento.
- Entregar los certificados digitales a entera satisfacción de la CFN B.P.
- Suscribir acta de entrega de recepción definitiva, siempre que se haya cumplido con lo previsto en la ley para la entrega recepción; y, en general, cumplir con las demás obligaciones que establezca la normativa legal vigente.

12. OBLIGACIONES DEL CONTRATANTE

- Designar al Administrador de la Orden de Compra.
- Hacer cumplir las obligaciones derivadas de la Orden de Compra.
- Suscribir acta de entrega de recepción definitiva, siempre que se haya cumplido con lo previsto en la ley para la entrega recepción; y, en general, cumplir con las demás obligaciones que establezca la normativa legal vigente

13. GARANTÍAS

El proveedor adjudicado deberá entregar una Garantía Técnica, en la que se avale el buen funcionamiento de los certificados durante su vigencia, que es de 365 días calendarios contados a partir del 31 de julio de 2020.

Esta garantía también debe considerar que, si por necesidad de la institución, durante el tiempo de vigencia de los certificados, se requiere volver a generarlos y colocarlos en el mismo u otro servidor, el proveedor deberá realizar dicha actividad sin costo adicional, en coordinación con los técnicos de CFN B.P.

Este requerimiento deberá ser atendido con una modalidad de 7x24x365 (todos los días y horas del año, con tiempo de atención en sitio o remoto de 4 horas), siendo el tiempo de solución de problemas al siguiente día.

14. MULTAS

Por cada día de retraso en la entrega e instalación de los certificados, se aplicará una multa de 1x1000 (uno por mil) respecto a las obligaciones que se encuentren pendientes de ejecutar. El contratista autoriza expresamente a la CFN B.P. para que descuente el valor correspondiente a las multas de la o las planillas que se presenten para el pago cuando apliquen.

Elaborado por:	Revisado por:
<hr/> <p>Ing. Diana Chávez Especialista Gestión de Proyectos Informáticos</p>	<hr/> <p>Ing. José Játiva U. Gerente de Tecnologías de la Información</p>