CORPORACIÓN FINANCIERA NACIONAL B.P.

TERMINOS DE REFERENCIA PARA LA CONTRATACIÓN DE LA CONSULTORÍA PARA LA ELABORACIÓN DEL DISEÑO E IMPLEMENTACIÓN DEL SISTEMA DE ADMINISTRACIÓN DEL RIESGO OPERATIVO Y DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DE LA CFN B.P.

Marzo, 2020

Matriz Guayaquil: Av. 9 de Octubre #200 y Pichincha, Centro Financiero Público.
Oficina Principal Quito: Edificio Platinum G, Calle Iñaquito entre Corea y Av. Naciones Unidas, Torre A.
Oficinas: Ambato / Cuenca / Esmeraldas / Ibarra / Latacunga / Loja / Machala / Manta / Riobamba / Salinas.
www.cfn.fin.ec

Contenido

Matriz Guayaquil: Av. 9 de Octubre #200 y Pichincha, Centro Financiero Público.
Oficina Principal Quito: Edificio Platinum G, Calle Iñaquito entre Corea y Av. Naciones Unidas, Torre A.
Oficinas: Ambato / Cuenca / Esmeraldas / Ibarra / Latacunga / Loja / Machala / Manta / Riobamba / Salinas.
www.cfn.fin.ec

TÉRMINOS DE REFERENCIA PARA LA CONTRATACIÓN DE LA CONSULTORÍA PARA LA ELABORACIÓN DEL DISEÑO E IMPLEMENTACIÓN DEL SISTEMA DE ADMINISTRACIÓN DEL RIESGO OPERATIVO Y DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DE LA CFN B.P.

1. ANTECEDENTES Y JUSTIFICACIÓN DE LA CONTRATACIÓN

En función a la detección de las necesidades en la Administración de Riesgo Operativo, la Corporación Financiera Nacional B.P., debe fortalecer su metodología de gestión para registrar, ordenar, clasificar y disponer de información sobre los eventos de Riesgo Operativo y de Seguridad de la Información, fallas o insuficiencias incluidas las de orden legal; y, factores de riesgo operativo clasificados por línea de negocio, determinando la frecuencia con que se repite cada evento, el efecto cuantitativo de pérdida producida y otra información que la CFN B.P. considere necesaria y oportuna, para que a futuro se puedan estimar las pérdidas esperadas e inesperadas atribuibles a Riesgo Operativo.

La Resolución de la Superintendencia de Bancos, Capítulo sustituido por la Resolución N°. SB-2018-771 de 30 de julio de 2018; reformado por Resolución N°. SB-2018-814 de 13 de agosto de 2018 y por la Resolución N°. SB-2019-497 de 29 de abril de 2019, indica que las instituciones del sistema financiero controladas por ésta, deberán establecer esquemas eficientes y efectivos de administración y control de todos los riesgos a los que se encuentran expuestas en el desarrollo del negocio, por ende es de suma importancia que las mismas desarrollen manuales de operatividad, y normativos que contemplen estrategias, políticas, procesos y procedimientos de administración de riesgos que permitan identificar, medir, controlar y monitorear las exposiciones de riegos que están asumiendo, para lo cual se debe tener como referencia las mejores prácticas contempladas en el estándar ISO 31000:2018 Gestión del Riesgo y Modelo COSO ERM 2017 Enterprise Risk Management para la gestión de riesgos.

Seguidamente, con el objetivo de gestionar la Seguridad de la Información contra el uso, revelación y modificación no autorizados, así como daños y pérdidas, se debe tener como referencia la serie de estándares ISO/IEC 27001:2013 – Sistema de Gestión de Seguridad de la Información, ISO/IEC 27002:2013 Tecnología de la Información, Técnicas de Seguridad, Código de Prácticas para los controles de Seguridad de la Información, ISO/IEC 27005:2018 - Gestión de Riesgos de Seguridad de la Información y considerando lo dispuesto en el artículo 3 del Acuerdo Ministerial N° 025-2019 (publicado en el registro oficial el 10 de enero del 2020), en el cual se recomienda a las instituciones de la administración pública central y que dependen de la función ejecutiva, actualizar o implementar el Esquema Gubernamental de Seguridad de la Información EGSI basado en la familia ISO 27000, es necesario contar con un proyecto de consultoría, que permita fortalecer institucionalmente a la CFN B.P. en la administración del riesgo operativo y la gestión de seguridad de la información.

A continuación, se detalla la normativa aplicable a la presente contratación:

La normativa de la Superintendencia de Bancos, LIBRO I.- NORMAS DE CONTROL PARA LAS ENTIDADES DE LOS SECTORES FINANCIEROS PÚBLICO Y PRIVADO,
TITULO IX.- DE LA GESTIÓN Y ADMINISTRACIÓN DE RIESGOS, CAPÍTULO V.- NORMA DE CONTROL PARA LA GESTIÓN DEL RIESGO OPERATIVO (Capítulo sustituido por la Resolución No. SB-2018-771 de 30 de julio de 2018; reformado por Resolución No. SB-2018-814 de 13 de agosto de 2018; reformado por Resolución No. SB-2019-497 de 29 de abril de 2019) indica:

"ARTÍCULO 4.- En el marco de la administración integral de riesgos, las entidades controladas definirán políticas, procesos, procedimientos y metodologías para la administración del riesgo operativo como un riesgo específico, considerando su objeto social, tamaño, naturaleza, complejidad de sus operaciones y demás características propias.
La administración del riesgo operativo deberá permitir a las entidades controladas identificar, medir, controlar, mitigar y monitorear su exposición a este riesgo en el desarrollo de sus negocios y operaciones".

"ARTÍCULO 7.- Aspecto importante de la administración del riesgo operativo es el control, el cual requerirá que las entidades controladas cuenten con planes de mitigación formalmente establecidos y validados periódicamente, mediante la revisión de estrategias y políticas; actualización o modificación de procesos y procedimientos establecidos; implementación o modificación de límites de riesgo;

Matriz Guayaquil: Av. 9 de Octubre #200 y Pichincha, Centro Financiero Público.
Oficina Principal Quito: Edificio Platinum G, Calle Iñaquito entre Corea y Av. Naciones Unidas, Torre A.
Oficinas: Ambato / Cuenca / Esmeraldas / Ibarra / Latacunga / Loja / Machala / Manta / Riobamba / Salinas.
www.cfn.fin.ec

implementación, o modificación de controles; plan de continuidad del negocio; revisión de términos de pólizas de seguro contratadas; contratación de servicios provistos por terceros; u otros, según corresponda. Los controles deben formar parte integral de las actividades regulares de la entidad para generar respuestas oportunas ante diversos eventos de riesgo operativo y las fallas o insuficiencias que los ocasionaron.

ARTÍCULO 8.- Las entidades controladas deben realizar un monitoreo permanente de las actividades y contar con un esquema organizado de reportes que permita tener información suficiente, pertinente y oportuna para la toma de decisiones, el cual debe incluir como mínimo:

a. Reporte de indicadores claves de riesgo operativo que permitan evaluar la eficiencia y eficacia de las políticas, procesos, procedimientos y metodologías aplicadas;

b. Reporte del grado de cumplimiento de los planes de mitigación;

c. Reporte de la matriz y mapas de riesgos operativos, que incluya como mínimo: línea de negocio, proceso, subproceso, tipo de evento, riesgo / evento de riesgo, factor de riesgo operativo, fallas o insuficiencias, impacto inicial, probabilidad inicial, frecuencia, riesgo inherente/ inicial, controles existentes/ planes de mitigación, impacto final, probabilidad final y riesgo residual.

La Superintendencia de Bancos a través de circular determinará el formato de reporte de la matriz de riesgos operativos.

Además, la entidad controlada en los informes trimestrales dirigidos al comité de administración integral de riesgos, debe incluir los niveles de exposición al riesgo operativo, la evolución de los riesgos reflejados en sus respectivos indicadores clave de riesgos; la eficiencia y eficacia de las políticas, procesos, procedimientos y metodologías aplicadas; el grado de cumplimiento de los planes de mitigación; y, conclusiones y recomendaciones; de manera que puedan ser analizados con una perspectiva de mejora constante del desempeño en la administración del riesgo operativo; así como para establecer o modificar políticas, procesos, procedimientos, y metodologías, entre otros.

ARTÍCULO 9.- En razón que la administración del riesgo operativo constituye un proceso continuo y permanente; y, para una gestión efectiva del riesgo, las entidades controladas deben conformar bases de datos centralizadas, que permitan registrar, ordenar, clasificar y disponer de información sobre los riesgos y eventos de riesgo operativo incluidos los de orden legal, de seguridad de la información y de continuidad del negocio, el efecto cuantitativo de pérdida producida y estimada así como la frecuencia y probabilidad, y otra información que las entidades controladas consideren necesaria y oportuna, para que se pueda estimar las pérdidas atribuibles a este riesgo. La administración de la base de datos es responsabilidad de la unidad de riesgo operativo (Artículo reformado por Resolución No. SB-2019-497, de 29 de abril de 2019)"

Las Instituciones Financieras deben gestionar el Riesgo Operativo, como elemento fundamental de una administración preventiva que reduzca al mínimo posible la posibilidad de pérdidas e incremente su eficiencia, para lo cual deberá implantar mecanismos, procesos contar con recursos humanos calificados y experimentados, y tecnología de información que soporte las operaciones de las Instituciones a fin de mitigar este riesgo, tomando en cuenta la normativa de los Organismos de Control.

"ARTÍCULO 15.- Con el objeto de gestionar la seguridad de la información para satisfacer las necesidades de la entidad y salvaguardar la información contra el uso, revelación y modificación no autorizados, así como daños y pérdidas, las entidades controladas deben tener como referencia la serie de estándares ISO/IES 27000 o la que la sustituya y contar al menos con:

a. Funciones y responsables de la seguridad de la información que permitan cumplir con los criterios de confidencialidad, integridad y disponibilidad de la información, acorde al tamaño y complejidad de los procesos administrados por el negocio.

Las entidades controladas deben conformar un comité de seguridad de la información que se encargue de evaluar, y supervisar el sistema de gestión de seguridad de la información.

Matriz Guayaquil: Av. 9 de Octubre #200 y Pichincha, Centro Financiero Público.
Oficina Principal Quito: Edificio Platinum G, Calle Iñaquito entre Corea y Av. Naciones Unidas, Torre A.
Oficinas: Ambato / Cuenca / Esmeraldas / Ibarra / Latacunga / Loja / Machala / Manta / Riobamba / Salinas.
www.cfn.fin.ec

El comité debe estar conformado como mínimo por: el miembro del directorio quien lo presidirá, el representante legal de la entidad, los funcionarios responsables de las unidades de: riesgos y seguridad de la información. Mantendrá un reglamento en donde se establezcan sus funciones y responsabilidades. Las reuniones de este comité se realizarán al menos trimestralmente dejando evidencia de las decisiones adoptadas.

b. Un área independiente y especializada con personal capacitado y experiencia en gestión de seguridad de la información, acorde al tamaño y complejidad de sus operaciones, que lidere el establecimiento, implementación, operación, monitoreo, mantenimiento y mejora continua del sistema de gestión de seguridad de la información de la entidad que debe mantener la independencia funcional del: área de tecnología, riesgos, áreas del negocio y función de auditoría.

ARTÍCULO 16.- Las entidades controladas deben establecer, implementar, operar, monitorear, mantener y mejorar un sistema de gestión de seguridad de la información que incluya al menos lo siguiente:

a. Alcance del sistema de gestión de seguridad de la información;

b. Políticas, objetivos, procesos, procedimientos y metodologías de seguridad de la información definidos bajo estándares de general aceptación, alineados a los objetivos y actividades de la entidad, así como las consecuencias de su incumplimiento.

Las políticas, procesos, procedimientos y metodologías de seguridad de la información deben ser revisados y aceptados por el comité de seguridad de la información; y, propuestos para la posterior aprobación del directorio; así como ser difundidos y comunicados a todo el personal involucrado de tal forma que se asegure su cumplimiento;

c. Inventario de activos de información, con su clasificación en términos de: valor, requerimientos legales, sensibilidad y criticidad para la entidad, propietario, custodio y ubicación;

d. La designación de los propietarios de los activos de información, que deben tener como mínimo las siguientes responsabilidades:

i. Clasificar los activos de información y revisar periódicamente el inventario de activos de información, con la finalidad de mantenerlo actualizado;

ii. Definir y revisar periódicamente las restricciones y accesos a los activos de información, tomando en cuenta las políticas de control de acceso aplicables; y,

iii. Autorizar los cambios funcionales a las aplicaciones y modificaciones a la información a través de accesos directos a la base de datos.

e. Identificación y documentación de los requerimientos y controles mínimos de seguridad para cada activo de información, con base en una evaluación de los riesgos que enfrenta la entidad, aplicando la metodología de gestión de riesgo operativo;

f. Plan de seguridad de la información que permita la implementación de los controles identificados y acciones de mejora;

g. Información que permita verificar el cumplimiento de las políticas, procesos, procedimientos y controles definidos para gestionar la seguridad de la información;

h. Monitoreo con una frecuencia al menos semestral, del cumplimiento y efectividad de los controles establecidos y generar informes dirigidos al comité de seguridad de la información;

i. Evaluación al menos una vez al año, del desempeño del sistema de gestión de la seguridad de la información, considerando los resultados de: auditorias de seguridad, gestión de incidentes de seguridad, monitoreo de los controles, resultados de las evaluaciones de riesgos, sugerencias, retroalimentación de las partes interesadas, entre otros aspectos; a fin de tomar acciones orientadas a

Matriz Guayaquil: Av. 9 de Octubre #200 y Pichincha, Centro Financiero Público.
Oficina Principal Quito: Edificio Platinum G, Calle Iñaquito entre Corea y Av. Naciones Unidas, Torre A.
Oficinas: Ambato / Cuenca / Esmeraldas / Ibarra / Latacunga / Loja / Machala / Manta / Riobamba / Salinas.
www.cfn.fin.ec

mejorarlo. El resultado de estas evaluaciones, así como las acciones de mejora deben ser conocidas y aprobadas por el comité de seguridad de la información; y,

j. Para considerar la existencia de un apropiado ambiente de gestión de seguridad de la información, la unidad responsable de la seguridad de la información debe implementar:

i. Medidas para proteger la información contenida en: documentos, medios de almacenamiento u otros dispositivos externos e intercambio electrónico, contra: robo, utilización o divulgación no autorizada de información para fines contrarios a los intereses de la entidad, por parte de su personal o de terceros;

ii. Procedimientos de eliminación de la información crítica de la entidad, de manera segura y considerando los requerimientos legales y regulatorios;

iii. Procedimientos para el control de accesos a la información que considere la concesión; administración de usuarios y perfiles para el registro, eliminación y modificación de la información, que garanticen una adecuada segregación de funciones y reduzcan el riesgo de error o fraude; así como la revocación de usuarios, tanto de aplicativos, software base, red, dispositivos de seguridad perimetral, bases de datos, entre otros. También se deberá controlar el acceso de los proveedores a la información de la entidad;

iv. Procedimientos para el monitoreo periódico de accesos, operaciones privilegiadas e intentos de accesos no autorizados, para asegurar que los usuarios solo estén realizando actividades para las cuales han sido autorizados;

v. Procedimientos que permitan contar con pistas de auditoría a nivel de aplicativos y bases de datos que registren los cambios realizados a la información crítica de la entidad. Los administradores no deben tener permiso para borrar o desactivar las pistas de sus propias actividades;

vi. Procedimientos para el uso, protección y tiempo de vida de las llaves criptográficas utilizadas para cifrar la información;

vii. Técnicas de cifrado sobre la información que lo requiera como resultado del análisis de riesgos de seguridad;

viii. Políticas y controles para detectar y evitar la instalación de software no autorizado o sin la respectiva licencia; y, para instalar y actualizar periódicamente aplicaciones de detección y desinfección de virus informáticos y demás software malicioso;

ix. La realización de las auditorías de seguridad de la infraestructura tecnológica con base en el perfil de riesgo de la entidad, por lo menos una (1) vez al año, con el fin de identificar vulnerabilidades y mitigar los riesgos que podrían afectar a la seguridad de los servicios que se brindan. Los procedimientos de auditoría deben ser ejecutados por personal independiente a la entidad, capacitado y con experiencia, aplicando estándares vigentes y reconocidos a nivel internacional; estas auditorías deben incluir al menos pruebas de vulnerabilidad y penetración a los equipos, dispositivos y medios de comunicación. Las entidades deben definir y ejecutar planes de acción sobre las vulnerabilidades detectadas;

x. Con base en un análisis de riesgos, realizar la segmentación de la red de datos y la implementación de sistemas de control y autenticación tales como: sistemas de prevención de intrusos (IPS), firewalls, firewall de aplicaciones web (WAF), entre otros; para evitar accesos no autorizados inclusive de terceros y ataques externos especialmente a la información crítica;

xi. Procedimientos para la definición de requerimientos de seguridad de la información para nuevos sistemas o su mantenimiento;

xii. Escaneo automatizado de vulnerabilidades en código fuente para mitigar los riesgos de seguridad de las aplicaciones previo a su liberación, y de aquellas que se encuentran en producción;

Matriz Guayaquil: Av. 9 de Octubre #200 y Pichincha, Centro Financiero Público.
Oficina Principal Quito: Edificio Platinum G, Calle Iñaquito entre Corea y Av. Naciones Unidas, Torre A.
Oficinas: Ambato / Cuenca / Esmeraldas / Ibarra / Latacunga / Loja / Machala / Manta / Riobamba / Salinas.
www.cfn.fin.ec

xiii. Procedimientos de gestión de incidentes de seguridad de la información, en los que se considere al menos: reporte de eventos, su evaluación, registro de incidentes, comunicación, priorización, análisis, respuesta y recolección de evidencias; y,

xiv. Procedimientos de afectación directa a las bases de datos que permitan identificar los solicitantes, autorizadores, y motivo de la modificación a la información, así como el registro de pistas de auditoría que facilite la trazabilidad del cambio."

El Acuerdo Ministerial N°. 025-2019 (publicado en el registro oficial el 10 de enero del 2020) indica:

"Articulo 1.- Expedir el Esquema Gubernamental de Seguridad de la Información EGSI, el cual es de implementación obligatoria en la Instituciones de la Administración Pública Central, Institucional y que dependen de la Función Ejecutiva".

A lo largo de los planteamientos hechos, la CFN B.P. requiere contar con una consultoría mediante la cual se realice el diseño e implementación del Sistema de Administración de Riesgo Operativo y el Sistema de Gestión de Seguridad de la Información que permitirá la identificación, análisis y evaluación de riesgos operativos y de seguridad de la Información para los 13 procesos críticos del negocio y el diseño de una base de datos de riesgos centralizada, en la cual se integren temas asociados al riesgo operacional y de seguridad de la información, garantizando que sean identificados, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan, el entorno y las tecnologías. Todo esto permitirá el cumplimiento del Acuerdo Ministerial del Mintel No 025-2019 y de la normativa vigente de la Superintendencia de Bancos LIBRO I.- NORMAS DE CONTROL PARA LAS ENTIDADES DE LOS SECTORES FINANCIEROS PÚBLICO Y PRIVADO TITULO IX.- DE LA GESTIÓN Y ADMINISTRACIÓN DE RIESGOS CAPÍTULO V.- NORMA DE CONTROL PARA LA GESTIÓN DEL RIESGO OPERATIVO (Capítulo sustituido por la Resolución No. SB-2018-771 de 30 de julio de 2018; reformado por Resolución No. SB-2018-814 de 13 de agosto de 2018; reformado por Resolución No. SB-2019-497 de 29 de abril de 2019), optimizando la labor del personal responsable de esta gestión.

Por lo expuesto, la Gerencia de Riesgos ha determinado la necesidad de contratar la **CONSULTORÍA PARA LA ELABORACIÓN DEL DISEÑO E IMPLEMENTACIÓN DEL SISTEMA DE ADMINISTRACIÓN DEL RIESGO OPERATIVO Y DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DE LA CFN B.P.**

2. OBJETO DE LA CONTRATACIÓN

CONSULTORÍA PARA LA ELABORACIÓN DEL DISEÑO E IMPLEMENTACIÓN DEL SISTEMA DE ADMINISTRACIÓN DEL RIESGO OPERATIVO Y DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DE LA CFN B.P.

3. OBJETIVO GENERAL

Contar con la CONSULTORÍA PARA LA ELABORACIÓN DEL DISEÑO E IMPLEMENTACIÓN DEL SISTEMA DE ADMINISTRACIÓN DEL RIESGO OPERATIVO Y DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DE LA CFN B.P., mediante el análisis de los procesos críticos del negocio, para facilitar la Gestión de Riesgos Operacionales y riesgos en Seguridad de la Información, a fin de descentralizar las actividades correspondientes a la identificación, medición, control y monitoreo de los eventos relacionados con este tipo de riesgo, para emprender acciones de gestión adecuadas que minimicen el impacto económico en la Institución.

4. OBJETIVOS ESPECÍFICOS

- Establecer un Sistema de Administración del Riesgo Operativo y un Sistema de Gestión de Seguridad de la Información en todos los niveles, que incluya metodologías, políticas y

Matriz Guayaquil: Av. 9 de Octubre #200 y Pichincha, Centro Financiero Público.
Oficina Principal Quito: Edificio Platinum G, Calle Iñaquito entre Corea y Av. Naciones Unidas, Torre A.
Oficinas: Ambato / Cuenca / Esmeraldas / Ibarra / Latacunga / Loja / Machala / Manta / Riobamba / Salinas.
www.cfn.fin.ec

procedimientos, orientado a los procesos críticos del negocio identificados en el Plan de Continuidad Institucional.

- Disminuir la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o, por la ocurrencia de acontecimientos externos, incluyendo aquellas situaciones relacionadas con asuntos legales y reputacionales.
- Cuantificar la pérdida real y esperada de los eventos de Riesgo Operativo y de Seguridad de la Información.
- Medir los Riesgos identificados (operativos y de seguridad de la información) de acuerdo con los parámetros establecidos por la Gerencia de Riesgos y la Gerencia General.
- Diseñar e implementar los controles que permitan tratar adecuada y eficientemente los riesgos (operativos y de seguridad de la información) y disminuir la probabilidad de incurrir en pérdidas generadas por eventos de riesgo.
- Establecer las actividades que serán requeridas para adoptar las oportunidades de mejora existentes entre las prácticas actuales y las mejores prácticas del mercado en la materia.
- Establecer los indicadores de riesgo descriptivo y/o prospectivo, así como retrospectivos que son requeridos en cada uno de los sistemas de administración de riesgos operativos y de gestión de seguridad de la información.
- Proteger los activos de Información de la CFN B.P., en base a los criterios de confidencialidad, integridad y disponibilidad de la información.
- Administrar los Riesgos de Seguridad de la Información para mantenerlos en niveles de aceptación tolerables.
- Sensibilizar y capacitar a los servidores públicos y partes interesadas acerca del Sistema de Gestión de Seguridad de la Información, fortaleciendo el nivel de conciencia de los mismos en cuanto a la necesidad de salvaguardar los activos de información institucionales.
- Implementar acciones correctivas y de mejora para el Sistema de Gestión de Seguridad de la Información.
- Mantener el adecuado uso de los recursos y de la gestión del riesgo, con el fin de asegurar la disponibilidad, integridad y confidencialidad de la información que administra.

5. ALCANCE

El alcance de la presente contratación contempla desde el desarrollo e implementación de la metodología para al Sistema de Administración de Riesgo Operativo y el Sistema de Gestión de Seguridad de la Información basado en las mejores prácticas ISO 31000:2018 - Gestión de Riesgos; modelo COSO ERM 2017 - Enterprise Risk Management para la gestión de riesgos; Norma ISO IEC/27001, el Acuerdo Ministerial N° 025-2019 del Ministerio de Telecomunicaciones y de la Sociedad de la Información, la normativa de la Superintendencia de Bancos - Resolución No. SB-2018-771, y derivados de la misma, hasta el análisis, identificación y evaluación de los Riesgos Operativos y de Seguridad de la Información de los procesos críticos de CFN B.P, detallados a continuación:

- 5.1 Concesión de Crédito
  - Análisis y aprobación de crédito de primer piso
  - Instrumentación y desembolso de créditos de primer piso
- 5.2 Administración del Crédito
  - Seguimiento del crédito y desembolsos parciales de primer piso
  - Seguimiento del crédito de segundo piso
  - Administración y supervisión de las operaciones de venta de CPG.
  - Custodia y archivo de documentos, títulos y especies
  - Liberación de garantías
  - Abonos y pre cancelación de créditos
- 5.3 Recuperación y Cobranza del Crédito
  - Gestión de cobranzas
  - Novación, refinanciamiento y reestructuración del crédito
  - Asignación de cartera judicial
  - Recuperación mediante el ejercicio de la potestad coactiva.
- 5.4 Medición del Riesgo de Lavado de Activos y Financiamiento de Delitos

Matriz Guayaquil: Av. 9 de Octubre #200 y Pichincha, Centro Financiero Público.
Oficina Principal Quito: Edificio Platinum G, Calle Iñaquito entre Corea y Av. Naciones Unidas, Torre A.
Oficinas: Ambato / Cuenca / Esmeraldas / Ibarra / Latacunga / Loja / Machala / Manta / Riobamba / Salinas.
www.cfn.fin.ec

- Análisis del riesgo
- Evaluación del riesgo

➢ 5.5 Tratamiento del Riesgo de Lavado de Activos y Financiamiento de Delitos
- Controlar el cumplimiento de las políticas de prevención de lavado de activos y financiamiento de delitos

➢ 5.6 Control/Mitigación del Riesgo
- Evaluación de riesgos por operaciones individuales

➢ 5.7 Administración de la Liquidez Institucional
- Proyección del flujo de caja
- Movimiento de recursos
- Seguimiento y control del encaje bancario

➢ 5.8 Negocios Fiduciarios
- Administrar el negocio fiduciario

➢ 5.9 Permanencia del Talento Humano
- Movimientos de personal
- Administración de remuneraciones y beneficios de Ley

➢ 5.10 Entregar Servicios de TI
- Gestionar la disponibilidad y capacidad
- Gestionar la configuración
- Gestionar operaciones
- Gestionar la continuidad

➢ 5.11 Operar Servicios de TI
- Gestionar los activos
- Gestionar incidentes
- Gestionar problemas
- Gestionar servicios de seguridad

➢ 5.12 Gestión de la Contratación Pública
- Contratación de obras, bienes, servicios y consultoría

➢ 5.13 Gestión de la Asesoría Legal.
- Constitución de garantías
- Elaboración de pronunciamientos y criterios jurídicos,
- Revisión de productos contingentes
- Elaboración de contratos y convenios
- Elaboración de informes legales

6. METODOLOGÍA Y CRONOGRAMA

Dentro del presente proceso de contratación se deberá considerar la metodología detallada a continuación:

Se deberá trabajar en base a la siguiente normativa:

- La normativa de la Superintendencia de Bancos LIBRO I.- NORMAS DE CONTROL PARA LAS ENTIDADES DE LOS SECTORES FINANCIEROS PÚBLICO Y PRIVADO TITULO IX.- DE LA GESTIÓN Y ADMINISTRACIÓN DE RIESGOS CAPÍTULO V.- NORMA DE CONTROL PARA LA GESTIÓN DEL RIESGO OPERATIVO (Capítulo sustituido por la Resolución No. SB-2018-771 de 30 de julio de 2018; reformado por Resolución No. SB-2018-814 de 13 de agosto de 2018; reformado por Resolución No. SB-2019-497 de 29 de abril de 2019).
- Recomendaciones del Comité de Supervisión Bancaria de Basilea, acuerdos consisten en recomendaciones sobre la legislación y regulación bancaria, emitidos por el Comité de supervisión bancaria de Basilea.
- Norma ISO 31000 y demás normas aplicables de la familia ISO 31000, COSO ERM 2017.
- Normas ISO sobre la Seguridad de la Información ISO 27001:2013, Norma ISO 27004:2016 para la evaluación del SGSI, Norma ISO 27005:2018 sobre la evaluación de riesgos de seguridad de la información, ITIL Information Technology Infraestructure Library.
- Acuerdo Ministerial No 025-2019, Ministerio de Telecomunicaciones y de la Sociedad de la Información.

Matriz Guayaquil: Av. 9 de Octubre #200 y Pichincha, Centro Financiero Público.
Oficina Principal Quito: Edificio Platinum G, Calle Iñaquito entre Corea y Av. Naciones Unidas, Torre A.
Oficinas: Ambato / Cuenca / Esmeraldas / Ibarra / Latacunga / Loja / Machala / Manta / Riobamba / Salinas.
www.cfn.fin.ec

Para el desarrollo e implementación del Sistema de Administración del Riesgo Operativo en adelante S.A.R.O. y del Sistema de Gestión de Seguridad de la Información en adelante S.G.S.I, se deberán considerar las actividades detalladas a continuación:

ACTIVIDADES	SEMANA					
	5	16	27	38	49	56
FASE I						
Planificación del proyecto	X					
Desarrollar el cronograma del proyecto	X					
Actualizar el alcance y objetivos del S.G.S.I. en términos del negocio que mostrará la organización, su localización, activos y tecnologías, incluyendo detalles y justificación de cualquier exclusión Elaborar el alcance y objetivos del S.A.R.O. en términos del negocio por cada proceso crítico definido en la fase donde realizará la identificación, medición y control de los riesgos operativos identificados.	X					
Definir roles y responsabilidades del S.A.R.O y del S.G.S.I de la CFN B.P	X					
Desarrollar el modelo de gestión de riesgo operativo y el modelo del sistema de gestión de seguridad de la información de la CFN B.P	X					
Levantar información para identificar los activos de información de la CFN B.P.	X					
Definir roles y responsabilidades para el S.G.S.I Y S.A.R.O.	X					
Desarrollar la estructura documental para el S.G.S.I. y S.A.R.O.	X					
FASE II						
Desarrollo de las actividades de esta fase de acuerdo a los los siguientes procesos críticos del negocio: • 5.4 Medición del Riesgo de Lavado Activos y Financiamiento de Delitos • 5.5. Tratamiento del Riesgo de Lavado de Activos y Financiamiento de Delitos. • 5.13 Gestión de la Asesoría Legal.		X				
Definición y desarrollo de políticas, procedimientos y metodologías de riesgo operativo que identifiquen, midan, controlen, mitiguen y monitoreen el riesgo.		X				
Definición y desarrollo de políticas, procedimientos y metodologías del sistema de gestión de seguridad de la información.		X				
Identificación de los riesgos operativos por: Línea de Negocio, Tipo de Evento, Factor de Riesgo Operativo, fallas o insuficiencias.		X				
Desarrollo de Talleres de Riesgo Operativo respecto a los siguientes temas: • Matriz de eventos de riesgo • Riesgo Inherente • Riesgo Residual • Mapa de Calor		X				

Matriz Guayaquil: Av. 9 de Octubre #200 y Pichincha, Centro Financiero Público.
Oficina Principal Quito: Edificio Platinum G, Calle Iñaquito entre Corea y Av. Naciones Unidas, Torre A.
Oficinas: Ambato / Cuenca / Esmeraldas / Ibarra / Latacunga / Loja / Machala / Manta / Riobamba / Salinas.
www.cfn.fin.ec

ACTIVIDADES	SEMANA					
	5	16	27	38	49	56
Desarrollo del informe de resultados B.I.A. (Bussines Impact Analysis) por cada proceso crítico de esta fase.		X				
FASE III						
Desarrollo de las actividades de esta fase de acuerdo a los siguientes procesos críticos del negocio: • 5.1Concesión del Crédito • 5.2 Administración del Crédito • 5.3 Recuperación y Cobranza del Crédito			X			
Definición y desarrollo de políticas, procedimientos y metodologías de riesgo operativo que identifiquen, midan, controlen, mitiguen y monitoreen el riesgo			X			
Definición y desarrollo de políticas, procedimientos y metodologías del sistema de gestión de seguridad de la información			X			
Identificación de los riesgos operativos por: Línea de Negocio, Tipo de Evento, Factor de Riesgo Operativo, fallas o insuficiencias			X			
Desarrollo los Talleres de Riesgo Operativo donde se consideren los siguientes temas: • Matriz de eventos de riesgo • Riesgo Inherente • Riesgo Residual • Mapa de Calor			X			
Desarrollo del informe de resultados B.I.A. (Bussines Impact Analysis) por cada proceso crítico de esta fase.			X			
FASE IV						
Desarrollo de las actividades de esta fase de acuerdo a los siguientes procesos críticos del negocio: • 5.12 Gestión de la Contratación Pública • 5.10 Entregar Servicios de TI • 5.11 Operar Servicios de TI.				X		
Definición y desarrollo de políticas, procedimientos y metodologías de riesgo operativo que identifiquen, midan, controlen, mitiguen y monitoreen el riesgo				X		
Definición y desarrollo de políticas, procedimientos y metodologías del sistema de gestión de seguridad de la información				X		
Identificación de los riesgos operativos por: Línea de Negocio, Tipo de Evento, Factor de Riesgo Operativo, fallas o insuficiencias.				X		
Desarrollo de los Talleres de Riesgo Operativo donde se consideren los siguientes temas: • Matriz de eventos de riesgo • Riesgo Inherente • Riesgo Residual • Mapa de Calor				X		
Desarrollo del informe de resultados B.I.A. (Bussines Impact Analysis) por cada proceso crítico de esta fase.				X		
FASE V						

Matriz Guayaquil: Av. 9 de Octubre #200 y Pichincha, Centro Financiero Público.
Oficina Principal Quito: Edificio Platinum G, Calle Iñaquito entre Corea y Av. Naciones Unidas, Torre A.
Oficinas: Ambato / Cuenca / Esmeraldas / Ibarra / Latacunga / Loja / Machala / Manta / Riobamba / Salinas.
www.cfn.fin.ec

ACTIVIDADES	SEMANA					
	5	16	27	38	49	56
Desarrollo de las actividades de esta fase de acuerdo a los siguientes procesos críticos del negocio: • 5.6 Control/Mitigación del Riesgo • 5.7 Administración de la Liquidez Institucional • 5.8 Negocios Fiduciarios • 5.9 Permanencia del Talento Humano					X	
Definición y desarrollo de políticas, procedimientos y metodologías de riesgo operativo que identifiquen, midan, controlen, mitiguen y monitoreen el riesgo					X	
Definición y desarrollo de políticas, procedimientos y metodologías del sistema de gestión de seguridad de la información					X	
Identificación de los riesgos operativos por: Línea de Negocio, Tipo de Evento, Factor de Riesgo Operativo, fallas o insuficiencias.					X	
Desarrollo Talleres de Riesgo Operativo: • Matriz de eventos de riesgo • Riesgo Inherente • Riesgo Residual • Mapa de Calor					X	
Desarrollo del informe de resultados B.I.A. (Bussines Impact Analysis) por cada proceso crítico de esta fase.					X	
FASE VI						
Capacitación al personal de Riesgo Operativo en un taller práctico relacionado con la administración del riesgo operativo ISO 31000						X
Capacitación al personal de Seguridad de la Información en un taller práctico relacionado con la gestión de seguridad de la información ISO 27001						X
Desarrollo e Implementación la Vista Analytics para integrar y correlacionar los datos de los riesgos identificados (SARO, SGSI, BCP) con el formato establecido por la Superintendencia de Bancos, visualización y cálculos de KPI's (Key Performance Indicator) y KRI´s (Key Risk Indicator). Desarrollo de formato de reportes e informes para presentar a C.A.I.R. de manera mensual.						X
Desarrollo de la información sobre los eventos de riesgos de Seguridad de la Información y del Riesgo Operativo de los procesos críticos del negocio						X

El contratista entregará reportes mensuales donde se mencionen los avances de cada fase, se realizarán reuniones de avance cada dos semanas con el administrador de contrato donde se detallen las definiciones realizadas, las decisiones tomadas, las excepciones administradas, y los eventuales incumplimientos de las partes involucradas.

Así mismo entregará la información correspondiente a cada fase en formatos y medios de comunicación seguros, por ejemplo: disco de duro cifrado, USB con contraseña y cifrado, información en cd/dvd encriptados.

Adicionalmente el consultor en su oferta deberá presentar el respectivo cronograma de trabajo, mismo que durante la ejecución del contrato podrá ser modificado por las partes, previa aprobación del Administrador del contrato y de justificarse su necesidad.

Matriz Guayaquil: Av. 9 de Octubre #200 y Pichincha, Centro Financiero Público.
Oficina Principal Quito: Edificio Platinum G, Calle Iñaquito entre Corea y Av. Naciones Unidas, Torre A.
Oficinas: Ambato / Cuenca / Esmeraldas / Ibarra / Latacunga / Loja / Machala / Manta / Riobamba / Salinas.
www.cfn.fin.ec

7. INFORMACIÓN QUE DISPONE LA ENTIDAD

Para el presente proceso de contratación, la CFN B.P. dispone de la siguiente información,

- Políticas y procedimientos para:
  - Concesión de Crédito
  - Administración del Crédito
  - Recuperación y Cobranza del Crédito
  - Medición del Riesgo de Lavado de Activos y Financiamiento de Delitos
  - Tratamiento del Riesgo de Lavado de Activos y Financiamiento de Delitos
  - Control/Mitigación del Riesgo
  - Administración de la Liquidez Institucional
  - Negocios Fiduciarios
  - Permanencia del Talento Humano
  - Entregar Servicios de TI
  - Operar Servicios de TI
  - Gestión de la Contratación Pública
  - Gestión de la Asesoría Legal.
- Inventario de Procesos
- Raking de procesos
- Organigrama Institucional
- Metodología de Calificación de Procesos Críticos
- Plan de continuidad del negocio Institucional
- BIAs de los procesos críticos del negocio
- Documentación vital por cada proceso crítico

8. PRODUCTOS / SERVICIOS ESPERADOS

La CONSULTORÍA PARA LA ELABORACIÓN DEL DISEÑO E IMPLEMENTACIÓN DEL SISTEMA DE ADMINISTRACIÓN DEL RIESGO OPERATIVO Y DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DE LA CFN B.P., debe contar con los siguientes entregables, los mismos que deben cumplir con los estándares y plantillas de la metodología de proyectos de la Corporación Financiera Nacional B.P. definidas Por la Superintendencia de Bancos y por el área de Calidad.

El resultado del análisis deberá de presentarse en una base de datos de riesgo centralizada respetando la estructura definida en la normativa de la Superintendencia de Bancos, LIBRO I.- NORMAS DE CONTROL PARA LAS ENTIDADES DE LOS SECTORES FINANCIEROS PÚBLICO Y PRIVADO, TITULO IX.- DE LA GESTIÓN Y ADMINISTRACIÓN DE RIESGOS, CAPÍTULO V.- NORMA DE CONTROL PARA LA GESTIÓN DEL RIESGO OPERATIVO (Capítulo sustituido por la Resolución No. SB-2018-771 de 30 de julio de 2018; reformado por Resolución No. SB-2018-814 de 13 de agosto de 2018; reformado por Resolución No. SB-2019-497 de 29 de abril de 2019).

FASE	ENTREGABLES
1	• Análisis GAP – Brechas S.B. - Acuerdo Ministerial N° 025-2019. • Alcance del Sistema de Gestión de Seguridad de la Información (SGSI) y Administración de Riesgo Operativo (SARO). • Cronograma de trabajo de la Consultoría (SGSI y SARO). • Estructura Organizacional (SGSI y SARO). • Plan de Entrenamiento y Sensibilización (SGSI y SARO). • Cronograma de talleres de Seguridad de la Información y talleres de Riesgo Operativo. • Inventario de activos de Información con su clasificación en términos de valor, requerimientos legales, sensibilidad y criticidad para la entidad, propietario, custodio y ubicación. • Estructura organizacional para distribuir los roles y responsabilidades del Sistema de Gestión de Seguridad de la Información y del Sistema de

<table>
<tr><td></td><td>Administración del Riesgo Operativo.
• Definición de roles y responsabilidades.
• Estructura documental SGSI y SARO.</td></tr>
<tr><td>2</td><td>S.A.R.O.
• Metodología para la identificación de las Líneas de Negocio de la Corporación Financiera Nacional B.P.
• Manual de metodologías, políticas y procedimientos de riesgo operativo para identificar, medir, controlar, mitigar y monitorear el riesgo.
• Identificación de los riesgos operativos por línea de negocio, tipo de evento, factor de riesgo operativo y las fallas o insuficiencias, que incluya al menos:
o Establecimiento de evaluación de impacto (Matriz de eventos)
o Definición del plan de tratamiento de riesgos.
o Definición del modelo de estimación capital por RO

S.G.S.I.

• Manual de metodologías, políticas y procedimientos de seguridad de la información (incluye las políticas de seguridad de la información en la relación con proveedores), que incluyan al menos lo siguiente:
o Política/Procedimiento de traer su propio dispositivo.
o Política/Procedimiento de teletrabajo.
o Política/Procedimiento de clasificación, valoración y etiquetado de la información.
o Política de contraseñas.
o Metodología para la administración de la Gestión de Seguridad de la Información.
o Metodologías para la Administración de Riesgo de Seguridad con enfoque para identificar, medir, controlar, mitigar y monitorear los riesgos.
o Metodología para clasificar y controlar los activos de información.
o Política/Procedimiento para realizar la segmentación de la red de datos y selección/ajustes de sistemas, controles y autenticación, para evitar accesos no autorizados inclusive de terceros y ataques externos especialmente a la información crítica.
o Política/Procedimiento para la identificación y documentación de los requerimientos y controles mínimos de seguridad para cada activo de información, con base en una evaluación de los riesgos.
o Políticas de seguridad de la información en la relación con proveedores, concerniente a la prestación de servicios asociados al tratamiento de información, en situaciones en las que se requiere contratar servicios de tratamiento o resguardo de activos de información.
o Definición del plan de tratamiento de riesgos.

Procesos críticos de la fase

• Evaluación de los siguientes procesos críticos del negocio:
o Medición del riesgo de lavado de activos y financiamiento de delitos.
o Tratamiento del riesgo de lavado de activos y financiamiento de delitos.
o Gestión de la asesoría legal
• Establecimiento de evaluación de procesos (matriz de identificación).
• Establecimiento de los riesgos operativos y de seguridad de la información</td></tr>
</table>

Matriz Guayaquil: Av. 9 de Octubre #200 y Pichincha, Centro Financiero Público.
Oficina Principal Quito: Edificio Platinum G, Calle Iñaquito entre Corea y Av. Naciones Unidas, Torre A.
Oficinas: Ambato / Cuenca / Esmeraldas / Ibarra / Latacunga / Loja / Machala / Manta / Riobamba / Salinas.
www.cfn.fin.ec

<table>
<tr><td></td><td>que se encuentren asociados a los procesos críticos de esta fase.
• Determinación del tipo de riesgo asociado, incluido el Riesgo Legal.
• Cuantificación de la identificación de la probabilidad de ocurrencia, el impacto y el riesgo inherente.
• Descripción de los controles y su grado de efectividad.
• Establecimiento del riesgo residual por procesos.
• Niveles de Exposición de cada uno de los riesgos identificados.
• Sistemas de indicadores de alerta temprana de cada uno de los riesgos, basado en reportes objetivos y oportunos.
• Seguimiento al riesgo neto o residual para su mitigación.
• S.G.S.I.: Declaración de aplicabilidad de acuerdo a los procesos críticos que corresponden a esta fase.
• Identificación de KRI’s (Key Risk Indicator) (mínimo 3 indicadores), por cada proceso crítico del monitoreo.
• Matriz de Identificación y Matriz de Eventos de Riesgos.
• Matriz de Riesgo Inherente.
• Matriz de Riesgo Residual.
• Mapa de Calor.
• Actas de Reunión.
• Listados de asistencia.
• Informe de Resultados de los talleres para identificar control y mitigación de riesgos operativos y seguridad de la información para los procesos críticos que corresponden a esta fase.
• Manuales de metodología, políticas y procedimiento para establecer las líneas del Negocio.</td></tr>
<tr><td>3</td><td>S.A.R.O.
• Manual de metodologías, políticas y procedimientos de riesgo operativo para identificar, medir, controlar, mitigar y monitorear el riesgo, identificar los riesgos operativos por línea de negocio, tipo de evento, factor de riesgo operativo y las fallas o insuficiencias, que incluya al menos:
o Riesgos de contratos de servicios a terceros.
o Metodología y procedimientos para la cuantificación del riesgo operativo.
o Actualización del Manual de Administración de Riesgo Operativo (vigente).
o Metodología para la verificación de vinculados.

S.G.S.I.

• Manual de metodologías, políticas y procedimientos de seguridad de la información (incluye las políticas de seguridad de la información en la relación con proveedores), que incluyan al menos los siguientes documentos:
o Política/Procedimiento de eliminación de la información crítica de la entidad, de manera segura y considerando los requerimientos legales y regulatorios.
o Política/Procedimiento para determinar información sensible y/o crítica considerando los requerimientos legales y regulatorios.
o Política/Procedimiento para el monitoreo periódico de accesos, operaciones privilegiadas e intentos de accesos no autorizados.
o Política/Procedimiento de administración de cambios.
o Política/Procedimiento de Gestión de Incidentes de Seguridad de la Información.
o Política/Procedimiento que impida que funcionarios de la entidad que no estén debidamente autorizados tengan acceso a consultar información confidencial de los clientes en ambiente de producción, mediante los aplicativos y bases de datos,</td></tr>
</table>

Matriz Guayaquil: Av. 9 de Octubre #200 y Pichincha, Centro Financiero Público.
Oficina Principal Quito: Edificio Platinum G, Calle Iñaquito entre Corea y Av. Naciones Unidas, Torre A.
Oficinas: Ambato / Cuenca / Esmeraldas / Ibarra / Latacunga / Loja / Machala / Manta / Riobamba / Salinas.
www.cfn.fin.ec

<table>
<tr><td></td><td>incluyendo el ambiente de desarrollo, considerando mantener y monitorear un log de auditoría sobre las consultas realizadas por los funcionarios a la información confidencial de los clientes, la cual debe contener como mínimo: identificación del funcionario, sistema utilizado, identificación del equipo (IP), fecha, hora, e información consultada.
o Definición de estatutos del Comité de Administración Integral de Riesgos, Comité de Seguridad de la Información

Procesos críticos de la fase

• Evaluación de los siguientes procesos críticos del negocio:
o Concesión del Crédito
o Administración del Crédito
o Recuperación y Cobranza del Crédito
• Establecimiento de evaluación de procesos (matriz de identificación).
• Establecimiento de los riesgos operativos y de seguridad de la información que se encuentren asociados a los procesos.
• Determinación del tipo de riesgo asociado, incluido el riesgo legal.
• Cuantificación de la identificación de la probabilidad de ocurrencia, el impacto y el riesgo inherente.
• Descripción de los controles y su grado de efectividad.
• Establecimiento del riesgo residual por procesos.
• Niveles de exposición de cada uno de los riesgos identificados.
• Sistemas de indicadores de alerta temprana de cada uno de los riesgos basado en reportes objetivos y oportunos.
• Seguimiento al riesgo neto o residual para su mitigación.
• S.G.S.I.: Declaración de aplicabilidad de acuerdo a los procesos críticos que corresponden a esta fase.
• Identificación de KRI’s (Key Risk Indicator) por cada proceso crítico del monitoreo.
• Matriz de Identificación y Matriz de Eventos de Riesgos.
• Matriz de Riesgo Inherente.
• Matriz de Riesgo Residual.
• Mapa de Calor.
• Actas de Reunión.
• Listados de asistencia.
• Informe de Resultados de los talleres para identificar riesgos y controles operativos para los procesos críticos que corresponden a esta fase.</td></tr>
<tr><td>4</td><td>S.A.R.O.
• Manual de metodologías, políticas y procedimientos de riesgo operativo para identificar, medir, controlar, mitigar y monitorear el riesgo, identificar los riesgos operativos por línea de negocio, tipo de evento, factor de riesgo operativo y las fallas o insuficiencias, que incluya al menos:
o Metodología para la determinación de factores de riesgo por línea de negocio y perfil de riesgo.
o Metodología para la elaboración del mapa de riesgo inherente y residual.
o Metodología para la evaluación del riesgo en nuevos productos y servicios.

S.G.S.I.
• Manual de metodologías, políticas y procedimientos de Seguridad de la Información (incluye las políticas de seguridad de la información en la relación con proveedores), que incluyan al menos los siguientes documentos:</td></tr>
</table>

Matriz Guayaquil: Av. 9 de Octubre #200 y Pichincha, Centro Financiero Público.
Oficina Principal Quito: Edificio Platinum G, Calle Iñaquito entre Corea y Av. Naciones Unidas, Torre A.
Oficinas: Ambato / Cuenca / Esmeraldas / Ibarra / Latacunga / Loja / Machala / Manta / Riobamba / Salinas.
www.cfn.fin.ec

	○ Política/Procedimiento de intercambio de información interna y con terceros. ○ Política/Procedimiento para proteger la información contenida en: documentos, medios de almacenamiento u otros dispositivos externos e intercambio electrónico, contra: robo, utilización o divulgación no autorizada de información. ○ Procedimientos para el control de accesos a la información que considere la concesión; administración de usuarios y perfiles para el registro, eliminación y modificación de la información, que garanticen una adecuada segregación de funciones. ○ Procedimiento para el uso, protección y tiempo de vida de las llaves criptográficas utilizadas para cifrar la información. ○ Política/Procedimiento para cifrar la información que lo requiera como resultado del análisis de riesgos de seguridad. ○ Política/Procedimiento para la definición y verificación de requerimientos de seguridad de la información para nuevos sistemas o su mantenimiento. ○ Política/Procedimiento para monitorear, controlar y emitir alarmas en línea que informen oportunamente sobre el estado de los canales electrónicos, con el fin de identificar eventos inusuales, fraudulentos o corregir las fallas. ○ Procedimiento de elaboración, evaluación y mantenimiento de inventario de activos de información. ○ Procedimiento para gestionar la auditoría externa de seguridad de la infraestructura tecnológica. ○ Procedimiento de gestión y monitoreo de usuarios y súper usuarios (usuarios administradores). ○ Procedimiento para escaneo automatizado de vulnerabilidades en código fuente para mitigar los riesgos de seguridad de las aplicaciones previo a su liberación, y de aquellas que se encuentran en producción. **Procesos críticos de la fase** • Evaluación de los siguientes procesos críticos del negocio: ○ Gestión de la Contratación Pública ○ Entregar Servicios de TI ○ Operar Servicios de TI • Establecimiento de evaluación de procesos (matriz de identificación). • Establecimiento de los riesgos operativos y de seguridad de la información que se encuentren asociados a los procesos críticos del negocio. • Determinación del tipo de riesgo asociado, incluido el riesgo legal. • Cuantificación de la identificación de la probabilidad de ocurrencia, el impacto y el riesgo inherente. • Descripción de los controles y su grado de efectividad. • Establecimiento del riesgo residual por procesos • Niveles de exposición de cada uno de los riesgos identificados. • Sistemas de indicadores de alerta temprana de cada uno de los riesgos, basado en reportes objetivos y oportunos. • Seguimiento al riesgo neto o residual para su mitigación. • **S.G.S.I.:** Declaración de Aplicabilidad de acuerdo a los procesos críticos que corresponden a esta fase. • Identificación de KRI's (Key Risk Indicator) por cada proceso crítico del monitoreo. • Matriz de Identificación y Matriz de Eventos de Riesgos. • Matriz de Riesgo Inherente. • Matriz de Riesgo Residual. • Mapa de Calor. • Actas de Reunión.

Matriz Guayaquil: Av. 9 de Octubre #200 y Pichincha, Centro Financiero Público.
Oficina Principal Quito: Edificio Platinum G, Calle Iñaquito entre Corea y Av. Naciones Unidas, Torre A.
Oficinas: Ambato / Cuenca / Esmeraldas / Ibarra / Latacunga / Loja / Machala / Manta / Riobamba / Salinas.
www.cfn.fin.ec

	• Listados de asistencia. • Informe de Resultados de los talleres para identificar riesgos y controles operativos para los procesos críticos que corresponden a esta fase.
5	**<u>Contra entrega fase 5</u>** **S.A.R.O.** • Manual de metodologías, políticas y procedimientos de riesgo operativo para identificar, medir, controlar, mitigar y monitorear el riesgo. • Identificar los riesgos operativos por línea de negocio, tipo de evento, factor de riesgo operativo y las fallas o insuficiencias, que incluya al menos: o Metodología para la Administración de los KRI´s (Key Risk Indicator), donde se incluya la definición, monitoreo, límites y potenciales medidas de acción. o Elaborar el análisis sobre los efectos en la posición de riesgos operativos en la entidad sobre los factores de riesgo institucionales, así como las pérdidas potenciales que podría sufrir ante una situación adversa en los segmentos en os que opera. o Límites de exposición de los riesgos identificados con sustento técnico. o Metodología para elaborar el informe trimestral para la administración integral del riesgo operativo. **S.G.S.I.:** • Manual de metodologías, políticas y procedimientos de seguridad de la información (incluye las políticas de seguridad de la información en la relación con proveedores), que incluyan al menos los siguientes documentos: o Políticas, procesos, procedimientos y metodologías para la gestión de la seguridad de la información. o Cronograma de Implementación de la continuidad de seguridad de la información. o Políticas/Procedimiento para detectar y evitar la instalación de software no autorizado o sin la respectiva licencia; y, para instalar y actualizar periódicamente aplicaciones de detección y desinfección de virus informáticos y demás software. o Política/Procedimiento para el control del escaneo automatizado de vulnerabilidades en código fuente. o Política/Procedimiento que permitan diseñar, monitorear y contar con pistas de auditoría a nivel de aplicativos y bases de datos. o Política/Procedimiento para monitorear la efectividad de los niveles de seguridad implementados en hardware, software, redes y comunicaciones. o Procedimiento de verificación y establecimiento de Controles y Medidas de Seguridad Aplicadas en canales electrónicos. o Procedimiento de Seguridad Física y Ambiental. o Sistema de Administración de la Seguridad de la Información a través de la ISO 27014 Gobernanza de Seguridad de la Información. o Uso aceptable de los activos. **Procesos críticos de la fase** • Evaluación de los siguientes procesos críticos del negocio. o Control/Mitigación del Riesgo o Administración de la Liquidez Institucional o Negocios Fiduciarios o Permanencia del Talento Humano • Establecimiento de evaluación de procesos (matriz de identificación).

Matriz Guayaquil: Av. 9 de Octubre #200 y Pichincha, Centro Financiero Público.
Oficina Principal Quito: Edificio Platinum G, Calle Iñaquito entre Corea y Av. Naciones Unidas, Torre A.
Oficinas: Ambato / Cuenca / Esmeraldas / Ibarra / Latacunga / Loja / Machala / Manta / Riobamba / Salinas.
www.cfn.fin.ec

	• Establecimiento de los riesgos operativos y de seguridad de la información que se encuentren asociados a los procesos. • Determinación del tipo de riesgo asociado, incluido el riesgo legal. • Cuantificación de la identificación de la probabilidad de ocurrencia, el impacto y el riesgo inherente. • Descripción de los controles y su grado de efectividad. • Establecimiento del riesgo residual por procesos. • Niveles de Exposición de cada uno de los riesgos identificados. • Sistemas de indicadores de alerta temprana de cada uno de los riesgos, basado en reportes objetivos y oportunos. • Seguimiento al riesgo neto o residual para su mitigación. • **S.G.S.I.:** Declaración de Aplicabilidad de acuerdo a los procesos críticos que corresponden a esta fase. • Identificación de KRI's (Key Risk Indicator) por cada proceso crítico del monitoreo. • Matriz de Identificación y Matriz de Eventos de Riesgos. • Matriz de Riesgo Inherente. • Matriz de Riesgo Residual. • Mapa de Calor. • Actas de Reunión • Listados de asistencia. • Informe de Resultados de los talleres para identificar riesgos y controles operativos para los procesos críticos que corresponden a esta fase.
6	**<u>Contra entrega fase 6</u>** • Transferencia de Conocimientos (Anexo 2) • Material para capacitación en S.G.S.I. y S.A.R.O. • Declaración de Aplicabilidad Consolidada. • Matrices consolidadas en una base de datos centralizada de los riesgos identificados (SGSI, SARO y BCP)., donde se pueda visualizar el mapa de riesgo, eventos de riesgo, riesgo inherente y el riesgo residual, que cumpla al menos con la estructura establecida por la Superintendencia de Bancos. • Inventario de Activos de la Información. • Metodología para la Evaluación del riesgo operativo en nuevos productos y servicios. • Desarrollo de Vistas para Analytics (Power BI deseado). • Implementación de Vistas para Analytics (Power BI deseado). o Alcance: Integrar y correlacionar con facilidad grandes cantidades de información provenientes de múltiples fuentes, con el formato establecido por el organismo de control S.B. o Analizar continuamente sus KPI (Key Performance Indicator) y colaborar con el monitoreo constante de los datos que se arrojan de cada actividad de la entidad. o Migración de datos del riesgo factor eventos externos a la base de datos centralizada de riesgos. • Diseño y formatos de tableros de control, operativos, de gestión y de gobierno de seguridad de la información. • Elaboración de presupuesto para el año 2021, para proveer los recursos necesarios para implementar y mantener de forma efectiva y eficiente el S.A.R.O. y el S.G.S.I. • Procedimiento/formato de reportes al Comité de Seguridad de la Información y Comité de Administración Integral de Riesgos. • Evaluación de riesgos y Metodología de tratamiento al riesgo. • Plan de tratamiento del riesgo. • Informe de evaluación de riesgos.

Matriz Guayaquil: Av. 9 de Octubre #200 y Pichincha, Centro Financiero Público.
Oficina Principal Quito: Edificio Platinum G, Calle Iñaquito entre Corea y Av. Naciones Unidas, Torre A.
Oficinas: Ambato / Cuenca / Esmeraldas / Ibarra / Latacunga / Loja / Machala / Manta / Riobamba / Salinas.
www.cfn.fin.ec

	• Definición de responsabilidades y roles de seguridad. • Revisión del procedimiento de afectaciones a la base de datos. • Procedimientos operativos para la gestión del sistema de seguridad de la información. • Principio de ingeniería en sistemas seguros 27002 referencias ISO 27002, mismo que detalla que la seguridad debe de ser diseñada en todas las capas de arquitectura (de negocios, datos, aplicaciones y tecnología), con la necesidad de accesibilidad. • Identificación de la legislación aplicable y de los requisitos contractuales respecto a Seguridad de la Información. • Procedimiento de trabajo en áreas seguras. • Política/Procedimiento para evaluar el desempeño del sistema de gestión de la seguridad de la información, considerando los resultados de auditorías de seguridad, gestión de incidentes de seguridad, monitoreo de los controles, resultados de las evaluaciones de riesgos, sugerencias, retroalimentación de las partes interesadas, entre otros aspectos. • Políticas y procedimientos para la gestión de los reportes del monitoreo emitido por el Security Operation Center (SOC) y de las alarmas del Software antimalware, antivirus y antiphising, incluyendo las actividades que debe de realizar le personal técnico autorizado ante eventos inusuales o falla de los servicios.

9. PLAZO DE LA CONTRATACIÓN

El plazo total de ejecución será de 392 días (56 semanas) contados a partir de la notificación de inicio del servicio por parte del administrador del contrato.

El plazo se divide en las siguientes fases:

	SEMANAS					
	1 a la 5	**6 a la 16**	**17 a la 27**	**28 a la 38**	**39 a la 49**	**50 a la 56**
FASE I	x					
FASE II		X				
FASE III			x			
FASE IV				x		
FASE V					x	
FASE VI						X

10. PERSONAL TÉCNICO / EQUIPO DE TRABAJO / RECURSOS

10.1. PERSONAL TÉCNICO MÍNIMO

Para la presente contratación se requiere del siguiente personal técnico:

NRO.	FUNCIÓN	NIVEL DE EDUCACIÓN	TITULACIÓN ACADÉMICA	CANT.
1	Gerente de Proyecto	Tercer nivel con título	Sistemas e informática/ Seguridad de la Información/ Administración de empresas/ Sistemas de Información/ Sistemas o Telecomunicaciones	1

11. EQUIPO MÍNIMO

Matriz Guayaquil: Av. 9 de Octubre #200 y Pichincha, Centro Financiero Público.
Oficina Principal Quito: Edificio Platinum G, Calle Iñaquito entre Corea y Av. Naciones Unidas, Torre A.
Oficinas: Ambato / Cuenca / Esmeraldas / Ibarra / Latacunga / Loja / Machala / Manta / Riobamba / Salinas.
www.cfn.fin.ec

Dentro de la presente contratación se requiere del equipo detallado a continuación:

NRO.	DETALLE	CARACTERÍSTICAS	CANT.
1	Computador (laptop)	○ Procesador Core i3 o Core i5 (preferible séptima generación) ○ Memoria RAM de 4 GB a 8 GB ○ Disco duro de 500 GB o superior ○ Pantalla de entre 13″ a 15″. ○ Batería con duración de 8 horas (en el caso de una laptop) ○ Entradas USB 3.0, multilector de tarjetas, USB-C o Thunderbolt	1

En caso de que el equipo sea propiedad del consultor se deberá incluir los soportes respectivos (factura o carta de venta); si dicho equipo va a ser adquirido se deberá adjuntar carta de intención de venta del proveedor; y, si el equipo se alquilará, se deberá presentar la carta de compromiso de alquiler.

12. FORMA Y CONDICIONES DE PAGO

La CFN B.P. cancelará el valor total del contrato de acuerdo con el siguiente detalle:

- El primer pago correspondiente al veinte por ciento (20%) del valor del contrato, se cancelará contra recepción a satisfacción del Administrador del Contrato de los entregables inherentes a la fase 1, presentación de la factura correspondiente e informe de conformidad del administrador del contrato.
- El segundo pago correspondiente al quince por ciento (15%) del valor del contrato, se cancelará contra recepción a satisfacción del Administrador del Contrato de los entregables inherentes a la fase 2, presentación de la factura correspondiente e informe de conformidad del administrador del contrato.
- El tercer pago, correspondiente al quince por ciento (15%) del valor del contrato, se cancelará contra recepción a satisfacción del Administrador del Contrato de los entregables inherentes a la fase 3, factura correspondiente e informe de conformidad del administrador del contrato.
- El cuarto pago, correspondiente al quince por ciento (15%) del valor del contrato, se cancelará contra recepción a satisfacción del Administrador del Contrato de los entregables inherentes a la fase 4, factura correspondiente e informe de conformidad del administrador del contrato.
- El quinto pago, correspondiente al quince por ciento (15%) del valor del contrato, se cancelará contra recepción a satisfacción del Administrador del Contrato de los entregables inherentes a la fase 5, factura correspondiente e informe de conformidad del administrador del contrato.
- El sexto pago, correspondiente al quince por ciento (15%) del valor del contrato, se cancelará contra recepción a satisfacción del Administrador del Contrato de los entregables inherentes a la fase 6, factura correspondiente, informe favorable del administrador del contrato, y suscripción del acta de entrega recepción provisional.
- El último pago correspondiente al 5%, se cancelará contra entrega del Informe Final Definitivo y la suscripción del Acta Entrega Recepción Definitiva acorde a lo establecido en el art 124 de Reglamento General a la Ley Orgánica del Sistema Nacional de Contratación Pública.

Nota: para la presentación de las facturas, en el caso de que corresponda a un comprobante electrónico, se deberá adjuntar la respectiva constancia en los catastros del SRI.
Pagos indebidos: La 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 el contratista a satisfacer las reclamaciones que por este motivo llegare a plantear la contratante, reconociéndose el interés calculado a la tasa máxima del interés convencional, establecido por el Banco Central del Ecuador.

13. MULTAS

Por cada día de retraso en la entrega de la información solicitada dentro del tiempo establecido en cada fase, se aplicará una multa de 1x1000 sobre el porcentaje de las obligaciones que se encuentren pendientes de ejecutarse conforme lo establecido en el contrato, excepto en el evento de caso fortuito o fuerza mayor, conforme lo dispuesto en el artículo 30 del Código Civil, debidamente comprobado y aceptado por el contratante, para lo cual se notificará dentro 48 horas subsiguientes de ocurridos los hechos. Una vez transcurrido este plazo, de no mediar dicha notificación, se entenderá como no ocurridos los hechos que alegue la contratista como causa para la no ejecución de la provisión del servicio y se le impondrá la multa prevista anteriormente.

14. OTRO(S) PARÁMETRO(S) RESUELTO POR LA ENTIDAD CONTRATANTE

El consultor en su oferta deberá adjuntar debidamente suscritos los siguientes acuerdos:

- Acuerdo de Confidencialidad de la Información (Anexo 1).
- Acuerdo de Transferencia de Conocimientos (Anexo 2).

15. OBLIGACIÓN DE LAS PARTES

15.1. OBLIGACIONES DEL CONTRATISTA

- Durante la ejecución del contrato el consultor deberá entregar toda la información y documentación que la CFN B.P. solicite, en relación al objeto de la contratación, según los entregables definidos.
- Dar solución a los problemas que se presenten en la ejecución del contrato.
- Cumplir con todas las obligaciones establecidas en el presente documento y en el contrato.
- Para el cumplimiento de los servicios de consultoría, contará durante la vigencia del contrato, con el personal técnico clave señalado en su oferta, conforme al cronograma de actividades aprobado.
- Para sustituir personal técnico clave, asignado al proyecto, solicitará la previa autorización, por escrito, del administrador del contrato.
- A solicitud de la entidad, fundamentada en la ineficiencia comprobada del personal, a su costo, deberá sustituir uno o más de los profesionales, empleados o trabajadores asignados al proyecto.
- Solicitará a la entidad la aprobación correspondiente en caso de que requiera personal adicional al indicado en su oferta.

15.2. OBLIGACIONES DE LA CFN B.P.

- Designar al administrador del contrato.
- Velar por el cabal cumplimiento del contrato.
- Dar solución a las peticiones y problemas que se presentaren en la ejecución del contrato.
- De ser necesario, previo el trámite legal y administrativo respectivo, celebrar contratos complementarios.
- Suscribir las actas de entrega recepción de los trabajos recibidos, siempre que se haya cumplido con lo previsto en la ley para la entrega recepción; y, en general, cumplir con las obligaciones derivadas del contrato.

Elaborado por:	Revisado por:	Autorizado por:
MIsia. Ilse Ycaza Especialista de Riesgo Operativo	Msc. Ma. Cristina Aguirre Subgerente Riesgo Operativo	Econ. Guido González Gerente de Riesgos

Matriz Guayaquil: Av. 9 de Octubre #200 y Pichincha, Centro Financiero Público.
Oficina Principal Quito: Edificio Platinum G, Calle Iñaquito entre Corea y Av. Naciones Unidas, Torre A.
Oficinas: Ambato / Cuenca / Esmeraldas / Ibarra / Latacunga / Loja / Machala / Manta / Riobamba / Salinas.
www.cfn.fin.ec