

**SISTEMA PARA ANALISIS DE VULNERABILIDADES**

## INDICE

<b>1.</b>	<b>GENERALIDADES DE LA PROPUESTA .....</b>	<b>3</b>
1.1.	ANTECEDENTES .....	3
1.2.	ALCANCE DEL SERVICIO A CONTRATAR .....	3
1.3.	AMBIENTE INFORMATICO ACTUAL .....	3
1.4.	CONDICIONES PARA LA GESTIÓN DE LA PROPUESTA .....	4
1.4.1.	PRESENTACIÓN DE LA PROPUESTA .....	4
1.4.2.	CARTA DE PRESENTACIÓN DE LA PROPUESTA .....	4
1.4.3.	VALIDEZ DE LA PROPUESTA .....	4
1.4.4.	MONEDA DE LA PROPUESTA .....	4
1.4.5.	CLÁUSULA PROPIEDAD INTELECTUAL .....	4
1.4.6.	CONFIDENCIALIDAD DE LA INFORMACIÓN .....	5
1.4.7.	POLÍTICAS DE SEGURIDAD .....	5
1.4.8.	FECHA Y LUGAR DE ENTREGA DE PROPUESTAS .....	5
1.4.9.	ACLARACIONES DEL CONTENIDO DE LA PROPUESTA .....	5
<b>2.</b>	<b>REQUERIMIENTOS TECNICOS.....</b>	<b>7</b>
2.1.	INFORMACIÓN ESPECÍFICA DE LA SOLUCIÓN REQUERIDA.....	7
2.1.1.	HARDWARE DE PROPÓSITO ESPECIFICO.....	7
<b>3.</b>	<b>PRESENTACIÓN DEL PROPONENTE.....</b>	<b>9</b>
3.1.	PRESENTACIÓN DE LA EMPRESA.....	9
3.2.	EXPERIENCIA ESPECÍFICA DEL PROPONENTE.....	10
<b>4.</b>	<b>SERVICIOS DE LA SOLUCIÓN .....</b>	<b>11</b>
4.1.	SOPORTE TÉCNICO A LOS COMPONENTES DE LA SOLUCIÓN OFRECIDA .....	11
4.1.1.	SERVICIOS DE INSTALACIÓN Y CONFIGURACIÓN DEL ESCANEADOR. ....	11
4.1.2.	SOPORTE DE LA SOLUCIÓN .....	11
4.1.3.	MANTENIMIENTO .....	11

<b>4.1.4. CAPACITACIÓN .....</b>	<b>11</b>
<b>4.1.5. GARANTÍA .....</b>	<b>11</b>
<b>4.2. SERVICIOS DE CONSULTORIA.....</b>	<b>11</b>
<b>4.3. PLAN DE TRABAJO A EJECUTAR EN LA REALIZACIÓN DE LA SOLUCIÓN .....</b>	<b>12</b>
<b>4.4. ENTREGA DE LA SOLUCIÓN.....</b>	<b>12</b>
<b>4.4.1. LUGAR DE ENTREGA.....</b>	<b>12</b>
<b>4.4.2. TIEMPO DE ENTREGA.....</b>	<b>13</b>
<b>4.4.3. FORMALIZACIÓN.....</b>	<b>13</b>
<b>4.5. DOCUMENTACIÓN TÉCNICA .....</b>	<b>13</b>
<b>4.6. VALOR AGREGADO .....</b>	<b>13</b>
<b>5.1. CARTA DE PRESENTACIÓN.....</b>	<b>13</b>
<b>5.2. COSTOS .....</b>	<b>13</b>
<b>5.3. FORMA DE PAGO.....</b>	<b>13</b>

## **1. GENERALIDADES DE LA PROPUESTA**

### **1.1. ANTECEDENTES**

El Banco requiere implementar un sistema para análisis de vulnerabilidades que permita fortalecer los esquemas de seguridad informática de la entidad y a la vez dar cumplimiento a lo requerido en el numeral 7 de la circular 0052 de 2007 de la Superintendencia Financiera, que dice:

**Las entidades deberán implementar un sistema de análisis de vulnerabilidades informáticas que cumpla al menos con los siguientes requisitos:**

- ?? Estar basado en un hardware de propósito específico (appliance) totalmente separado e independiente de cualquier dispositivo de procesamiento de información, de comunicaciones y/o de seguridad informática.
- ?? Generar de manera automática por lo menos dos (2) veces al año un informe consolidado de las vulnerabilidades encontradas. Los informes de los últimos dos años deberán estar a disposición de la SFC.
- ?? Las entidades deberán tomar las medidas necesarias para remediar las vulnerabilidades detectadas en sus análisis.
- ?? Realizar un análisis diferencial de vulnerabilidades, comparando el informe actual con respecto al inmediatamente anterior.
- ?? Las herramientas usadas en el análisis de vulnerabilidades deberán estar homologadas por el CVE (Common Vulnerabilities and Exposures) y actualizadas a la fecha de su utilización.
- ?? Para la generación de los informes solicitados se deberá tomar como referencia la lista de nombres de vulnerabilidades CVE publicada por la corporación Mitre ([www.mitre.org](http://www.mitre.org)).

### **1.2. ALCANCE DEL SERVICIO A CONTRATAR**

- ?? El Banco requiere de un hardware de propósito específico para análisis de vulnerabilidades y de los servicios de instalación, configuración, soporte técnico y capacitación de la solución.
- ?? Adicionalmente se deben incluir los servicios de consultoría para el acompañamiento en la ejecución de dos (2) análisis de vulnerabilidades, análisis de reportes y acompañamiento en la remediación.

### **1.3. AMBIENTE INFORMATICO ACTUAL**

- ?? Actualmente el Banco requiere el análisis de 500 IP's para cubrir un estimado de 400 equipos de usuario (desktop y portátiles), 50 equipos de interconexión de red (switches, firewall, routers) y 50 servidores bajo diferentes plataformas.

#### **1.4. CONDICIONES PARA LA GESTIÓN DE LA PROPUESTA**

##### **1.4.1. Presentación de la propuesta**

La propuesta debe ser presentada en original impreso y una copia en medio electrónico, en el orden solicitado en el presente documento, debidamente numerada, las cuales deberán ser entregadas dentro del plazo fijado en sobres sellados, debidamente rotulados en su parte exterior con el nombre, dirección, teléfono y número de fax del proveedor, número de folios de que consta y la indicación del contenido del sobre según sea: Original impreso y la copia en medio electrónico. En caso de discrepancia entre el Original impreso y la copia en medio electrónico, se tendrá en cuenta la información contenida en el Original impreso.

Las propuestas técnicas y económicas deben presentarse en sobre separados en formato original, junto con el registro de proveedores del Banco debidamente diligenciado, con sus respectivos anexos, en sobres independientes. La presentación completa de los documentos exigidos es un factor de calificación dentro del proceso. Ver pagina <http://www.bancoldex.com/contratacion/contratacion.aspx>

No se aceptarán propuestas cuyos documentos presenten tachaduras o enmendaduras,

No se aceptarán propuestas complementarias o modificaciones que fueren presentadas con posterioridad a la fecha y hora de cierre del presente proceso de contratación.

##### **1.4.2. Carta de presentación de la propuesta**

La carta de presentación de la propuesta debe estar firmada por su representante legal o comercial o por el apoderado constituido para el efecto.

##### **1.4.3. Validez de la propuesta**

La propuesta debe tener una validez mínima de noventa (90) días, contados a partir de la fecha de cierre de la Invitación.

##### **1.4.4. Moneda de la propuesta**

La propuesta económica debe presentarse en pesos colombianos.

##### **1.4.5. Cláusula Propiedad Intelectual**

Tanto el Banco como los proveedores están obligados a responder por la confidencialidad de la información recibida y entregada durante el proceso de selección de proveedores. Bancóldex, de conformidad con el artículo 83 de la Constitución Política, presume que toda

la información que el proponente allegue a esta contratación es veraz, y corresponde a la realidad. No obstante, la entidad podrá verificar la información suministrada por el proponente.

#### **1.4.6. Confidencialidad de la información**

El contrato será desarrollado por el proveedor bajo parámetros de absoluta reserva y no podrá utilizar total o parcialmente la información que reciba directa o indirectamente del Banco, o aquella a la cual tenga acceso en cumplimiento del proceso de contratación o por cualquier otro motivo, adoptando las medidas necesarias para mantener la confidencialidad de los datos suministrados.

La información que conozca el proponente durante el proceso debe ser entendida como confidencial y dará un adecuado tratamiento.

#### **1.4.7. Políticas de seguridad**

El proponente deberá dar lectura al documento titulado "Políticas de la información" y deberá diligenciar la carta sobre la aceptación de dichas políticas. Estos documentos se encuentran en el anexo1.

#### **1.4.8. Fecha y lugar de entrega de Propuestas**

Las propuestas técnicas y económicas deberán ser entregadas debidamente firmadas, junto con los documentos exigidos en la Calle 28 #13A-15 Piso 40 Bogotá - Oficina de correspondencia dirigida al Departamento de Sistemas hasta el día **3 de Junio de 2009 a las 04:00 PM**. Las propuestas técnicas no deben incluir costos de ninguna naturaleza, pero si cantidades y especificaciones necesarias para calificar el diseño de la misma. La propuesta económica debe clarificar costos unitarios y globales de la solución. Las cantidades deben coincidir puntualmente en la propuesta técnica y económica.

Las propuestas deberán ser entregadas en sobres cerrados, con su respectiva carta remisoría, la cual debe indicar con claridad el número de la invitación a cotizar a la cual hace referencia y si la propuesta es técnica o económica.

BANCOLDEX S.A se reserva el derecho de rechazar cualquiera o todas las propuestas que se presenten, si así lo conviene a sus intereses, sin necesidad de dar explicación alguna a los proponentes.

#### **1.4.9. Aclaraciones del contenido de la propuesta**

El Banco solicitará por medio de la Dirección de Sistemas, mediante comunicación escrita de ser necesario, ampliar el contenido de su oferta o aclarar temas sobre la propuesta. El tiempo de ajuste de propuesta es de 3 días hábiles una vez el Banco informe los ajustes a realizar. Si la propuesta no es ajustada y devuelta dentro de este periodo de tiempo, será retirada del proceso.



**INVITACIÓN A COTIZAR**

Fecha de elaboración  
15 de mayo de 2009  
Este documento incluye 15 páginas.

Para consultas favor enviar correos a [byron.arciniegas@bancoldex.com](mailto:byron.arciniegas@bancoldex.com)

## 2. REQUERIMIENTOS TECNICOS

### 2.1. INFORMACIÓN ESPECÍFICA DE LA SOLUCIÓN REQUERIDA

#### 2.1.1. Hardware de propósito específico

**Favor responder a cada uno de los requerimientos punto a punto, con la respectiva argumentación. La argumentación debe incluir la característica técnica o la conceptualización que garantice que se cumple con la condición.**

Item	Requerimientos de la herramienta	Si/No	Argumentación
1	Estar certificada por el MITRE.		
2	La solución debe estar basada en un hardware de propósito específico (appliance).		
3	Descubrimiento de activos: tener la capacidad de descubrir los activos informáticos de la organización (Firewall, Router, Switches, Access Point, PC's, etc...)		
4	Actualizarse de las bases de datos de vulnerabilidades del CVE's de MITRE.		
5	Se debe poder crear manualmente activos como direcciones IP.		
6	Permitir hacer escaneo para 500 activos. Especificar capacidad de crecimiento del equipo.		
7	Análisis de Vulnerabilidades: Permitir realizar un escaneo de vulnerabilidades inmediatas o programadas sobre los activos.		
8	Permitir observar en tiempo real si los activos están conectados vía ICMP.		
9	La solución NO debe exigir el uso de agentes de software o clientes instalados en los PCs de la red. Es decir, debe ser Clientless.		
10	Hacer actualización de las bases de datos de vulnerabilidades usando un protocolo seguro https.		
11	La solución debe clasificar las vulnerabilidades en Críticas, Altas, Medias y bajas.		
12	Generar reportes técnicos con detalles de vulnerabilidades encontradas con el formato CVE.		

13	Explicar si es posible exportar los reportes en otros formatos		
15	Generar informes gerenciales con resumen de las vulnerabilidades encontradas.		
16	Generar reportes diferenciales con referencia a análisis previos.		
17	Remediación: Debe proveer la información necesaria para la remediación de las vulnerabilidades encontradas.		
18	Indicadores de gestión: Generar reportes globales o parciales y análisis de GAP o brechas de cumplimiento respecto a estándar internacional de seguridad ISO 27001/17799.		
19	Desempeño: Explicar como hace uso eficiente del ancho de banda de la red y especificar que no afecta el desempeño de la misma mientras envía y recibe mensajes.		
20	Permitir el envío de notificaciones mediante protocolo SMTP.		
21	Permitir la creación de políticas de mejores prácticas de seguridad desde el appliance.		
22	Permitir medir o determinar el nivel de cumplimiento respecto a normativas internacionales, regulaciones o a mejores prácticas.		
23	Describir los estándares o las mejores prácticas que pueden ser utilizadas para medir el cumplimiento.		
24	Únicamente debe permitir el GUI y conexión directa.		
25	La solución debe permitir la actualización de service packs desde el GUI para el dispositivo.		
26	Utilizar métodos de autenticación en el dispositivo para el control de acceso de los administradores y usuarios.		
27	Explicar patrones de escaneo que permite la solución.		
28	Permite la configuración de backups y el posterior envío de este a un servidor FTP		
29	Describir que tipos de reportes pueden generarse desde la solución.		
30	Permitir gestión por protocolo SNMP y envío de logs a otros sistemas. Explicar.		

31	La solución debe tener mínimo procesador Pentium 4 de 3.0 Ghz, 80 GB de Disco Duro y 1 GB de memoria RAM.		
32	Especificar dimensiones del equipo.		
33	Especificar consumo de energía.		
34	Especificar interfaces de red.		
35	Permitir gestionar los recursos de hardware de la máquina.		

**Opcionales**

1	Facilitar la gestión de procesos de remediación mediante la generación y seguimiento de "ticket".		
2	Incluir un modulo NAC (Network Admission Control) – Clientless. Permitir la integración con Firewall y Switches, especificar funcionalidad con Checkpoint y CISCO.		
3	Especificar si la herramienta esta certificada por otras organizaciones especializadas en vulnerabilidades		

**3. PRESENTACIÓN DEL PROPONENTE****3.1. PRESENTACIÓN DE LA EMPRESA**

Los interesados deben (a título individual u oferente plural) realizar una presentación general de su empresa, en la cual se puede conocer el objeto de su negocio, su estructura organizacional y operacional para desarrollar el objeto de este proceso en diferentes ciudades del país, el talento humano con que cuenta a nivel interno y los instrumentos que dispone para contratar profesionales y técnicos, su capacidad de asociación, trayectoria en el mercado.

En lo relativo con la estructura organizacional, es de especial interés conocer si la empresa cuenta con los siguientes documentos, los cuales debe adjuntar a la propuesta:

- a. Misión, visión, objetivos
- b. Personal vinculado y/o asociado con experiencia en proyectos similares
- c. Sucursales en algunas de las ciudades en las que se va a desarrollar el contrato, si aplica
- d. Estados financieros que permitan acreditar el estado económico en el que se encuentra la empresa; en caso de tener estados financieros negativos, explicar por qué y cómo soportarán la participación en la contratación.
- e. Presentar el certificado de inscripción en el registro único de proponentes – RUP en el que se clasifique como proponente. Si aplica.

- f. Certificado de existencia y representación legal, o sus documentos equivalentes en caso de personas jurídicas, expedidos dentro del mes anterior a la fecha señalada para la presentación de las manifestaciones de interés.
- g. Tiempo de permanencia en el mercado.
- h. Experiencia en implementaciones o servicios similares al solicitado en este documento.  
Diligenciar el formato de Vinculación, Actualización de clientes, naturales o jurídicos, con todos los documentos anexos correspondientes.
- i. Actualización de los documentos, en el caso de las empresas que tienen contrato vigente con el Banco. Si aplica.
- j. Diligenciamiento del formato SARLAFT exigido por el gobierno para procesos de contratación.
- k. Incluir resumen ejecutivo de la propuesta

**Nota: En caso de que los resultados de los estados financieros presentados sean negativos, se deberá explicar las razones de dicho estado y explicar como se soportará la participación en la contratación.**

Deberá adjuntarse fotocopia del documento de identificación del representante legal de la persona jurídica cuyas facultades deberán constar en los documentos antes mencionados y ser suficientes para presentar la propuesta y celebrar y ejecutar el contrato. En caso de resultar necesario, deberán adjuntar las autorizaciones adicionales que se requieran.

Como complemento de este documento, la empresa podrá adjuntar el catálogo de presentación o portafolio de servicios de la empresa, así como la dirección de la página Web si dispone de ella.

### **3.2. EXPERIENCIA ESPECÍFICA DEL PROPONENTE**

- 1. El proponente deberá presentar una certificación actualizada, emitida por el fabricante, que le acredite como distribuidor autorizado de los equipos ofertados y de la prestación de servicios de soporte sobre la solución.
- 2. Se deberán presentar al menos tres (3) certificaciones de provisión de la herramienta ofertada, emitidas por clientes, en las que se especifique la solución adquirida y el nivel de cumplimiento del proponente.
- 3. Se deberán presentar al menos tres (3) certificaciones de prestación de servicios de consultoría de seguridad, preferiblemente sobre análisis de vulnerabilidades, emitidas por clientes, en las que se especifique el tipo de consultoría y el nivel de satisfacción del cliente frente al servicio.
- 4. El proponente debe certificar la práctica de prestación de servicios de soporte en informática, con especialización en las áreas afines al alcance de esta solicitud bajo la norma internacional ISO 9001:2000. Adicionalmente en la práctica de ejecución de "Gestión de Servicios de TI", bajo la norma internacional ISO 27001 e ITIL (IT Information Library) que garanticen la calidad en la prestación del servicio.

#### **4. SOPORTE DEL SERVICIO A LA SOLUCIÓN OFRECIDA**

##### **4.1. SOPORTE TÉCNICO A LOS COMPONENTES DE LA SOLUCIÓN OFRECIDA**

###### **4.1.1. Servicios de Instalación y configuración del escaneador.**

Se deberá ofrecer la entrega de la solución “llave en mano”, instalación y configuración de la herramienta lista para funcionar con el ambiente informático actual del Banco. Culminada la instalación y configuración deberá entregarse la documentación técnica correspondiente.

###### **4.1.2. Soporte de la solución**

Se deberá incluir los servicios de soporte para la solución por un periodo de dos (2) años en horario 5X8, con tiempos de respuesta no mayor a 4 horas y de solución máximo de 72 horas. Describir el esquema de soporte ofrecido para la solución. El proveedor deberá especificar cuál es el procedimiento a seguir en caso de fallas en los elementos de hardware y software de la solución.

###### **4.1.3. Mantenimiento**

?? Todo el software dentro de la solución deberán incluir la suscripción a actualizaciones y últimas versiones por dos años a partir de la entrega.

?? Se deberá incluir dos (2) visitas de mantenimiento por año para evaluar el estado de la solución y realizar las recomendaciones que sean del caso.

###### **4.1.4. Capacitación**

La solución deberá incluir capacitación básica de operación y mantenimiento de la herramienta ofertada para análisis de vulnerabilidades.

###### **4.1.5. Garantía**

Los equipos deberán contar con una garantía mínima de 2 años.

##### **4.2. SERVICIOS DE CONSULTORIA**

?? La solución deberá incluir la consultoría para la ejecución de dos (2) análisis de vulnerabilidades con la herramienta provista, con escaneos generales, con entrega de informes de evaluación y la adecuada interpretación de las vulnerabilidades encontradas, con recomendaciones sobre esquemas de remediación y seguimiento.

?? El proveedor deberá especificar el esquema del servicio y los entregables.

- ?? El personal asignado a la consultoría deberá contar con experiencia certificada de al menos 3 años como consultor en los servicios requeridos. Adjuntar las hojas de vida.

#### **4.3. PLAN DE TRABAJO A EJECUTAR EN LA REALIZACIÓN DE LA SOLUCIÓN**

El Proponente deberá presentar con la propuesta un cronograma o plan de trabajo en el cual describa los procesos/actividades requeridos para alcanzar el objeto de la solución requerida, explicando claramente el número de días de la actividad y profesionales dedicados para desarrollar cada actividad relacionada en el cronograma.

El cronograma debe cumplir con las siguientes condiciones:

- ?? Explicar claramente la relación entre las distintas actividades, especificando la ruta crítica.
- ?? Indicar los productos específicos a ser presentados y su oportunidad (informes, reportes, etc.).
- ?? Indicar el personal empleado en cada actividad, de manera que garantice el adecuado cumplimiento del objeto del presente proceso según los términos de referencia.
- ?? El cronograma general debe presentarse respecto de las actividades a ejecutar, Identificar entregables, plan de pago y secuencia prevista para las actividades detalladas en esta contratación.
- ?? Identificando: Actividades, fecha de inicio, fecha de terminación, hitos, ruta crítica. La secuencia y duración de cada una de las actividades debe estar discriminada en semanas.

Si la propuesta llegara a ser seleccionada, al momento de la firma del acta de inicio, se deberá entregar a Bancóldex el cronograma detallado y ajustado, teniendo en cuenta el presentado inicialmente.

Bancóldex a través del Supervisor del contrato verificará el desarrollo del cronograma presentado, la dedicación del personal ofrecido, los resultados esperados y en general el cumplimiento de los compromisos adquiridos. En caso de que exista inconformidad en los resultados Bancoldex podrá solicitar realizar nuevamente el análisis o el cambio del personal asignado.

#### **4.4. ENTREGA DE LA SOLUCIÓN.**

##### **4.4.1. Lugar de entrega**

Todos los equipos de cómputo solicitados deberán ser entregados en las oficinas del Departamento de Sistemas de Bancoldex ubicadas en el piso 40 del edificio CCI- Centro de Comercio Internacional- Calle 28 #13A -15.

#### **4.4.2. Tiempo de entrega**

El tiempo de entrega de los equipos no debe exceder cuarenta y cinco (45) días a partir de la emisión de la carta de aceptación de la propuesta por parte del Banco.

#### **4.4.3. Formalización**

La recepción de los componentes de la solución por parte de Bancoldex será formalizado mediante la correspondiente acta de entrega.

#### **4.5. DOCUMENTACIÓN TÉCNICA**

Se deberán integrar a la propuesta técnica todos los documentos de especificaciones técnicas de los componentes ofertados.

#### **4.6. VALOR AGREGADO**

El proponente deberá especificar, si es el caso, los valores agregados como parte de su propuesta.

### **5. CONTENIDO DE LA PROPUESTA ECONOMICA**

#### **5.1. CARTA DE PRESENTACIÓN**

El proveedor presentará por separado su propuesta económica, con carta dirigida a la Dirección del departamento de Sistemas de Bancoldex. Todos los valores que se estimen en la propuesta deben presentarse en pesos colombianos.

#### **5.2. COSTOS**

La propuesta debe indicar claramente los precios unitarios de los componentes y total de la solución discriminando IVA y descuentos.

#### **5.3. FORMA DE PAGO**

Los pagos se realizarán contra entregables, de manera independiente sobre los siguientes ítems:


- ?? Herramienta de análisis de vulnerabilidades con los servicios de instalación, configuración y puesta en funcionamiento de la solución.
- ?? Capacitación.
- ?? Servicios de consultoría.

- ?? Los servicios de soporte de los numerales 4.1.2 y 4.1.3 podrán ser facturados en pagos parciales o mediante un único pago.

**ANEXO 1. POLÍTICAS CORPORATIVAS**

Las políticas de seguridad contenidas en este documento deben ser cumplidas por parte de los proveedores de Bancóldex S.A., para asegurar un adecuado nivel de confidencialidad, integridad y disponibilidad en su información.

1. Aportar certificación suscrita por el Representante Legal, sobre la propiedad del licenciamiento del software contenido en cualquier equipo de su propiedad, que ingrese al Banco. Igualmente, la certificación debe ser extensiva a cualquier software o herramienta tecnológica que se utilice para el desarrollo del objeto del contrato, para lo cual debe mediar el permiso o licencia suscrita por el fabricante.
2. Tramitar la autorización previa del Banco para cualquier conexión e interacción con la red de Bancóldex y su información.
3. Aceptar el monitoreo de cualquier conexión e interacción con la red del Banco y su información cuando BANCOLDEX lo considere oportuno.
4. Comprometerse a no acceder las áreas de Centro de Cómputo, Cintoteca o cualquier otro sitio declarado como de acceso restringido en el Banco, sin un acompañante o con la debida autorización, para lo cual se compromete a dejar registro en las bitácoras dispuestas para tal fin.
5. Garantizar que toda actualización y modificación a la infraestructura tecnológica del Banco será validada y aprobada en forma previa por la Vicepresidencia de Operaciones y la Dirección del Departamento de Sistemas.
6. Utilizar los recursos tecnológicos que le entregue el Banco, en forma exclusiva para el desarrollo de la labor para la cual fue contratado.
7. Cumplir con especial cuidado, el principio de buen uso y confidencialidad de los medios de acceso que ha entregado el Banco para el desarrollo del objeto del contrato.
8. Asegurar que al término del contrato, toda información, software, dispositivos y demás elementos tecnológicos de propiedad del Banco serán eliminados de los equipos del proveedor, atendiendo los acuerdos de confidencialidad
9. Asegurar que como producto de este contrato, entregará al Banco una solución que garantice confidencialidad, integridad y disponibilidad de la información relacionada con el objeto del mismo.
10. Garantizar al Banco que el personal asignado por el proveedor a la atención del contrato, conoce y cumple las políticas contenidas en este documento y responde por cualquier inobservancia de las mismas.
11. Disponer de un plan de contingencia y continuidad que permita mantener disponible la prestación del servicio contratado por el Banco, en el evento que se presenten situaciones de interrupción. Dicho plan se mantendrá documentado y disponible en el momento que el Banco lo requiera para verificar su adecuado funcionamiento.

		VERSIÓN: 1
		CÓDIGO: VUL-1
SISTEMA DE ANALISIS DE VULNERABILIDADES		FECHA: ABRIL DE 2009

Bogotá D.C.,

Señores  
 BANCO DE COMERCIO EXTERIOR  
 DE COLOMBIA S.A.  
 Ciudad

Estimados Señores:

Actuando en mi calidad de Representante Legal de \_\_\_\_\_, y de acuerdo a su solicitud, con la presente me permito certificar que conozco y acepto las políticas de seguridad corporativa adoptadas por el Banco. Así mismo, me permito certificar que el software relacionado en nuestra propuesta de la invitación No. \_\_\_\_\_ se encuentra debidamente licenciado. En consecuencia, la sociedad que represento se obliga a dar cumplimiento a dichas políticas y a divulgarlas entre los funcionarios designados para la ejecución de dicho contrato.

Cordialmente,

Nombre: \_\_\_\_\_  
 C.C: \_\_\_\_\_

\_\_\_\_\_ Firma