ANEXO 4.

REQUISITOS DE SEGURIDAD Y CONFIDENCIALIDAD

Objeto contractual: Prestación de servicios de un Contact Center especializado, para la atención de usuarios, afiliados servicios de seguimiento comercial, asistencia procedimental, así como las demás actividades relacionadas con los productos y servicios ofrecidos por el Fondo Nacional del Ahorro a nivel nacional e internacional.

NOMBRE CORTO PROYECTO: UNIFICACIÓN CALL Y CONTACT CENTER

Los siguientes puntos presentan los requerimientos mínimos requeridos para cumplir los requisitos de seguridad y confidencialidad, que El oferente seleccionado deberá cumplir en el/los canales(es) de comunicación dedicado(s) con los correspondientes esquemas de seguridad, entrega y manejo de usuarios, seguridad en los equipos garantizando únicamente acceso a las aplicaciones que se requieran para la operación de los servicios requeridos por el FNA.

CUMPLIMIENTO LEGAL Y MARCO REGULATORIO SEÑALADO POR LA SUPERINTENDENCIA FINANCIERA.

NORMATIVA

Concernientes a los requisitos legales establecidos en la ley de protección de datos personales 1581 de 2012 y el decreto reglamentario 1377 de 2013, los requisitos enunciados en la Circular Básica Jurídica (C.E. 029/14) emitida por la Superintendencia Financiera de Colombia, respecto a Canales, medios, seguridad y calidad en el manejo de información en la prestación de servicios financieros, Requerimientos mínimos para la gestión de la seguridad de la información y la ciberseguridad y Reglas relativas al uso de servicios de computación en la nube, y el Manual de Políticas de Seguridad de la información de la Entidad, aprobado mediante acuerdo 2246 de 2019.

EN MATERIA DE DOCUMENTACIÓN

1. El oferente seleccionado deberá dejar constancia de todas las operaciones que se realicen a través de los distintos canales, la cual debe contener cuando menos lo siguiente: fecha, hora, código del dispositivo (para operaciones realizadas a través de IVR: el número del teléfono desde el cual se hizo la llamada; para operaciones por Internet: la dirección IP desde la cual se hizo la misma; para operaciones con dispositivos móviles, el número desde el cual se hizo la conexión), cuenta(s), número de la operación y costo de la misma para el cliente o usuario.
2. El oferente seleccionado deberá generar informes trimestrales sobre la disponibilidad y número de operaciones realizadas en cada uno de los canales de distribución.

3. El oferente seleccionado deberá conservar todos los soportes y documentos donde se hayan establecido los compromisos, tanto de las entidades como de sus clientes y las condiciones bajo las cuales éstas prestan sus servicios. Se debe dejar evidencia documentada de que los clientes las han conocido y aceptado.

4. El oferente seleccionado deberá llevar un registro de las consultas realizadas por los colaboradores sobre la información confidencial de los clientes, que contenga al menos lo

siguiente: identificación del funcionario que realizó la consulta, canal utilizado identificación del equipo, fecha y hora. En desarrollo de lo anterior, se deben establecer mecanismos que restrinjan el acceso a dicha información, para que solo pueda ser usada por el personal que lo requiera en función de su trabajo.

5. El oferente seleccionado deberá llevar el registro de las actividades adelantadas sobre los dispositivos finales a cargo de la entidad, usados en los canales de distribución de servicios, cuando se realice su alistamiento, transporte, mantenimiento, instalación y activación.

6. El oferente seleccionado deberá dejar constancia del cumplimiento de la obligación de informar adecuadamente a los clientes respecto de las medidas de seguridad que deben tener en cuenta para la realización de operaciones por cada canal, así como los procedimientos para el bloqueo, inactivación, reactivación y cancelación de los productos y servicios ofrecidos.

7. El oferente seleccionado deberá grabar las llamadas realizadas por los clientes a los centros de atención telefónica cuando consulten o actualicen su información.

8. El oferente seleccionado deberá informar a la Entidad como está configurada la infraestructura tecnológica que será utilizada para la prestación de servicios para el FNA, en caso de contar con infraestructura de computación den la nube deberá dar cumplimiento a lo establecido en la Circular Externa 005 de 2019 de la Superintendencia Financiera de Colombia.

REQUISITOS DE CONFIDENCIALIDAD

1. El oferente seleccionado se obliga a guardar confidencialidad y reserva sobre toda la información que llegue a conocer en desarrollo del contrato. En consecuencia, no podrá reproducir en todo o en parte, ni suministrar esta información a terceras personas, ni usarla con fines distintos al propósito de las actividades contratadas, obligación que se extiende a las personas que participen en el desarrollo del objeto aquí contratado, siendo responsable frente al FNA por los daños y perjuicios que se generen en caso de que la misma no sea respetada. Así mismo, se obliga a responder hasta por la culpa levísima en la conservación, cuidado y manejo de la información y sólo podrá exonerarse de su responsabilidad mediante la prueba del caso fortuito o de la fuerza mayor. En todo caso, el oferente seleccionado no expedirá certificación alguna sobre el contenido, características, autenticidad, originalidad o cualquier otra circunstancia propia de los documentos que se le entregan con ocasión de este Contrato, por cuanto carece de facultad legal para ello.

ANEXO 4.

REQUISITOS DE SEGURIDAD Y CONFIDENCIALIDAD

Objeto contractual: Prestación de servicios de un Contact Center especializado, para la atención de usuarios, afiliados servicios de seguimiento comercial, asistencia procedimental, así como las demás actividades relacionadas con los productos y servicios ofrecidos por el Fondo Nacional del Ahorro a nivel nacional e internacional.

Se entiende por información confidencial a toda información y Sistemas de información recibidos de una parte por la otra, antes o después de la suscripción del presente contrato, bien sea en forma oral o escrita, la cual comprende pero no se limita a: (i) información de clientes de LAS PARTES; (ii) información de contratos con terceros; (iii) planes de negocio y de desarrollo: (iv) información técnica y financiera; (v) planes de productos y servicios; (vi) información de costos; (vii) informes de mercadeo; (viii) análisis y proyecciones; (ix) especificaciones, diseños, dibujos, datos prototipos, secretos industriales y know how; (x) elementos relacionados con la red de telecomunicaciones y plataformas; (xi) información de sus clientes, empleados y accionistas, (xii) software y/o sistemas de información y se complementa con lo descrito en los numerales 18 y 19 de la Ley 1712 de 2014. No se complementa con la definición de “Confidencialidad” y “Uso de información confidencial” los requisitos descritos en el Anexo numero 4 Requisitos de Seguridad y confidencialidad.

2. El oferente seleccionado debe cumplir con lo establecido en la normatividad expedida por el Ministerio de Tecnologías de la Información y las Comunicaciones en lo referente a la protección de los derechos de los suscriptores y/o usuarios de los servicios de telecomunicaciones por el envío de mensajería de textos comerciales y publicitarios, desde teléfonos móviles.

3. El oferente seleccionado debe velar por la protección de la información confidencial adoptando las medidas necesarias para que sea accesible solo a las personas autorizadas y en cumplimiento con la normatividad vigente. En ese sentido, el personal vinculado por el oferente seleccionado para la ejecución del contrato deberá suscribir un acuerdo de confidencialidad que deberá aparecer en la hoja de vida de cada trabajador.

4. El oferente seleccionado deberá asegurar que todos sus colaboradores asignados a la campaña del FNA cuenten con acuerdos de confidencialidad debidamente firmado al inicio del contrato y antes de realizar la entrega de información de la Entidad. Así mismo deben firmar la declaración de responsabilidad frente al uso de los activos de información del FNA y cumplimiento de la normatividad, documento que deberá crear el oferente seleccionado y la supervisión del contrato validará y aprobará.

PROPIEDAD DE LA INFORMACIÓN.

5. Los derechos patrimoniales que surjan de la producción intelectual que el oferente seleccionado realice en cumplimiento de las actividades propias del contrato, o con ocasión de ellas, pertenecen al FNA y por tanto por este mismo acto se cedidos por el oferente seleccionado a favor del FNA.

6. Toda la información generada como producto del contrato celebrado debe ser almacenada en una ruta provista por el FNA, para ello el oferente seleccionado deberá solicitar a través del supervisor asignado por el FNA, la creación de una carpeta en el servidor de archivos a la mesa de servicio para este fin, indicando los nombres de las personas que accederán a la misma.

RESTRICCIONES SOBRE EL SOFTWARE EMPLEADO.

7. Para el manejo de la información y del software, el oferente seleccionado se obliga a acatar la normatividad legal existente y los reglamentos internos del FONDO, so pena de las sanciones penales y/o administrativas a que haya lugar.

8. Se deberá definir por parte del coordinador asignado o el supervisor según sea el caso los accesos requeridos a las aplicaciones y sistemas y deberán tramitarse a través del supervisor del contrato con el formato definido por el FNA para tal fin.

9. No se crearán cuentas genéricas, cada asesor contará con un usuario y clave para el ingreso de manera personal e intransferible únicamente a las aplicaciones autorizadas por el supervisor del contrato, el oferente seleccionado deberá reportar en forma inmediata cualquier escenario que requiera de la aplicación del control de retiro o ajuste de los derechos de acceso a las aplicaciones de la Entidad.

10. Habilitar correo certificado o seguro del FNA (cuenta suministrada por el FNA) para los puestos de los Back office, (cumpliendo lo especificado en el anexo 3 requerimientos mínimo de personal) que tendrá como objetivo enviar al Consumidor Financiero (CF) los requisitos o condiciones para un trámite específico, o los que apliquen para dar respuesta al usuario, (antes de enviar cualquier información se debe solicitar autorización del CF y envió de información al correo electrónico, según las normas aplicables), la información enviada desde esta cuenta de correo contará con cifrado.

11. Toda máquina que se conecte a la red corporativa del FNA debe contar con un sistema operativo debidamente licenciado, con soporte técnico por parte del fabricante y con un proceso definido e implementado para la actualización de parches de seguridad, de tal manera que:

- se vigile el estado de actualización de todos los dispositivos y aplicaciones.
- permita elegir la opción de actualizaciones automáticas siempre que esté disponible
- instalar las actualizaciones tan pronto como se publiquen, especialmente las de los sistemas operativos y navegadores.

12. Toda máquina que se conecte a la red corporativa del FNA debe contar con una herramienta de protección de malware, de tal manera que:
    - se realicen controles automáticos y periódicos;
    - se realicen comprobaciones automáticas de ficheros adjuntos al correo o de aquellos que se descarguen de cualquier página web;
    - se bloquee el acceso a aplicaciones basándose en una política de listas negras, y que permita el acceso a aquellas que se encuentren en listas blancas;
    - se permitan analizar páginas web para detectar posibles amenazas.
    - se actualice periódicamente, se recomienda automáticamente, así como contar con una periodicidad de búsqueda de actualizaciones diaria.

13. En caso de ser requerido por parte de la Entidad se deberá instalar la herramineta de prevención de fuga de información, Forcepoint DLP, en todas las maquinas del oferente seleccionado que sean utilizadas para la campaña de la Entidad, cuyo agente deberá permanecer instalado durante la vigencia del acuerdo contractual, sus prorrogas y/o adiciones.

14. Los dueños del servicio contratado deberán definir los mecanismos de control y protección de las operaciones realizadas en los sistemas, identificando las necesidades de control dependiendo (del) el riesgo de las operaciones e informarlas a la oficina de informática a través del supervisor con el fin de validar si se requiere algún cambio sobre los sistemas o se programan las alertas correspondientes sobre acciones indebidas que se ejecuten.

NORMAS DE SEGURIDAD INFORMÁTICA Y FÍSICA

A fin de garantizar la integridad, confidencialidad y disponibilidad de la información que sea enviada o recibida entre las partes (CONTRATISTA y FNA) se deberá garantizar como mínimo los siguientes requerimientos:

15. El oferente seleccionado deberá configurar un enlace dedicado, Reusó 1:1, seguro hacia la red del FNA, con un ancho de banda que permita la redirección o recepción de contactos hacia otros proveedores de centro de atención telefónica de modo tal que permita cumplir con los ANS establecidos, el oferente seleccionado deberá asumir los costos de los servicios

que se requieran para atender la totalidad de los servicios requeridos, deberá disponer de los canales adicionales para atender la totalidad del tráfico, especialmente en temporadas con mayor tráfico como el recaudo de cesantías.

16. El oferente seleccionado debe disponer de las herramientas para la operación del servicio y asumir todos los costos generados por la instalación del Canal dedicado, entre los que se encuentra el costo de cross conexión.

17. La conexión establecida entre el Fondo Nacional y el sitio de atención del oferente seleccionado deberá cumplir con la normatividad emitida por la Superintendencia Financiera, en el caso particular de los equipos de interconexión se deberá encriptar el tráfico LAN to LAN a través de algoritmos de cifrado fuerte empleando un dispositivo (hardware) exclusivo para el cifrado el cual se deberá integrar con el concentrador de encripción CISCO FIREPOWER 2140 que posee el FNA.

18. Se requiere también durante esta etapa la elaboración del documento correspondiente a controles de cambio, en el cual se especificará IPs de origen y destino para la conexión y puertos TCP o UDP que deberán ser configurados en los Firewalls del FNA para tener acceso a los servidores requeridos para la ejecución del Contrato; esta labor se efectuará con apoyo de funcionarios del FNA.

19. El oferente seleccionado deberá contar con la infraestructura que permita la redirección de llamadas o contactos por diversos canales a otro Centro de Contacto en caso que la Entidad requiera que su Centro de Contacto además de recibir sus contactos, pueda también ser un punto inicial de contacto y pueda redireccionar los contactos a otro Centro de Contacto que preste servicios a la Entidad, la infraestructura y constes asociados deberá ser asumida en su totalidad por el oferente seleccionado.

20. El oferente seleccionado deberá implementar mecanismos de cifrado fuerte para el envío y recepción de información clasificada con la Entidad.

21. El oferente seleccionado deberá garantizar que el envío de información confidencial y los instrumentos utilizados para la realización de operaciones a los clientes, debe hacerse en condiciones de seguridad. Cuando dicha información se envíe como parte de, o adjunta a un correo electrónico, ésta deberá estar cifrada.

22. El oferente seleccionado deberá cifrar mediante algoritmos de cifrado fuerte la Información que sea suministrada por parte del FNA, mientras que se encuentre en reposo o en tránsito en su infraestructura.

23. La información que viaja hacia la Entidad deberá estar cifrada usando hardware de propósito específico, o software, o una combinación de los anteriores, el hardware o software empleados deberán ser totalmente separados e independientes de cualquier otro dispositivo o elemento de procesamiento de información, de seguridad informática, de transmisión y/o recepción de datos, de comunicaciones, de conmutación, de enrutamiento, de gateways, servidores de acceso remoto (RAS) y/o de concentradores. En cualquiera de los casos anteriores se deberá emplear cifrado fuerte.

24. El oferente seleccionado deberá establecer, mantener y documentar los controles de acceso (lógicos, físicos y procedimentales) y gestión de identidades bajo la premisa que las personas solo pueden disponer de los recursos que demande su trabajo, durante el tiempo que ello sea necesario, dentro de los alcances del servicio y/o solución ofrecida.

25. El oferente seleccionado deberá gestionar y documentar la seguridad de las plataformas que soporten los servicios contratados por el FNA.

26. El oferente seleccionado deberá identificar, y en la medida de lo posible, medir, los riesgos cibernéticos emergentes que puedan llegar a afectar a la entidad, y establecer controles para su mitigación.

27. El oferente seleccionado deberá reportar al supervisor del contrato cualquier incidente de Seguridad de la Información o Ciberseguridad que afecte la confidencialidad, integridad o disponibilidad de la información de la entidad, haciendo una breve descripción del incidente, su impacto y las medidas adoptadas para gestionarlo, el reporte se debe hacer una vez se conozca el incidente.

28. El oferente seleccionado deberá adoptar procedimientos y mecanismos para identificar, analizar y gestionar incidentes de Seguridad de la Información o ciberseguridad que se presenten sobre la infraestructura que soporta el servicio contratado por el FNA y afecte que afecte la confidencialidad, integridad o disponibilidad de la información de la entidad.

29. El oferente seleccionado deberá realizar un monitoreo continuo a su plataforma tecnológica con el propósito de identificar comportamientos inusuales que puedan evidenciar amenazas que pudieran afectar a la información de la Entidad.

30. El oferente seleccionado en su calidad de custodio o usuario de los activos de la información, se compromete a acatar las normas de seguridad de la información que el FNA tiene establecidas en el acuerdo 2246 de 2019 "Manual Políticas de Seguridad de la Información" y del que lo adicione, modifique o sustituya; por lo tanto, debe asumir las responsabilidades establecidas en el citado Manual, brindando la protección y cuidado necesarios a la

infraestructura computacional, dispositivos de almacenamiento, bases de datos, programas e información confidencial que deba manejar durante la ejecución del contrato, evitando que usuarios externos y no autorizados puedan acceder a estos. El oferente seleccionado deberá dar cumplimiento al Manual de Políticas en cuanto a la cadena de suministro de productos y servicios de tecnología y comunicación, transfiriendo la responsabilidad sobre la información que se encuentre a su cargo en las calidades antes descritas, a los subcontratistas y demás personal que contrate por su cuenta y que tengan acceso al procesamiento, almacenamiento, comunicación o suministro de los componentes de infraestructura de TI para la información de la organización. La Entidad se reservará el derecho de realizar seguimiento, revisión y auditoria de la prestación del servicio.

31. En caso de incidentes de Seguridad de la Información el oferente seleccionado deberá preservar las evidencias digitales, en la medida de lo posible, para que las áreas de seguridad del FNA o las autoridades puedan realizar las investigaciones correspondientes.

32. La información, equipos y software empleados en desarrollo del contrato, están protegidos con las limitaciones, regulaciones y políticas del FNA, de conformidad con lo dispuesto en el acuerdo 2246 de 2019 “Manual Políticas de Seguridad de la Información”, por lo que si se llegaren a encontrar evidencias de alteración o manipulación de éstos, el oferente seleccionado deberá responder contractualmente por estas conductas, sin perjuicio de las acciones disciplinarias, penales, civiles, fiscales y demás que llegaren a producirse.

33. El oferente seleccionado deberá establecer el tiempo máximo de inactividad, después del cual debe darse por cancelada la sesión, exigiendo un nuevo proceso de autenticación para realizar otras operaciones.

34. El oferente seleccionado deberá implementar mecanismos que permitan verificar constantemente que no sean modificados los enlaces (links) del servicio en el sitio web, ni suplantados los certificados digitales, ni modificada indebidamente la resolución de los DNS.

35. El oferente seleccionado deberá contar con mecanismos para incrementar la seguridad de los portales, protegiéndolos de ataques de negación de servicio, inyección de código u objetos maliciosos, que afecten la seguridad de la operación o su conclusión exitosa.

36. El oferente seleccionado deberá dotar a sus terminales, equipos de cómputo y redes locales de los elementos necesarios que eviten la instalación de programas o dispositivos que capturen la información de los clientes y de sus operaciones.

37. El oferente seleccionado deberá establecer los mecanismos necesarios para que el mantenimiento y la instalación o desinstalación de programas o dispositivos en las terminales o equipos de cómputo sólo pueda ser realizado por personal debidamente autorizado.

ENTREGA DE LA INFORMACIÓN MANEJADA Y LA DESTRUCCIÓN DE ESTA POR PARTE DEL TERCERO UNA VEZ FINALIZADO EL SERVICIO

38. El oferente seleccionado deberá contar con procedimientos controlados para la devolución de información que le haya sido entregada o que se haya consolidado durante la ejecución del contrato, de ser el caso, la destrucción de esta una vez finalizado el acuerdo contractual o cuando así lo requiera la Entidad, esta información debe ser devuelta en su totalidad y en las condiciones de Seguridad que establezca la entidad, se deben aplicar procedimientos de borrado de bajo nivel a cualquier medio que pudiera contener información de la Entidad, una vez se termine el acuerdo contractual o así lo considere la Entidad.

PLANES DE CONTINGENCIA Y CONTINUIDAD

39. El oferente seleccionado deberá disponer de planes de contingencia y continuidad debidamente documentados y probados, los cuales deberán ser suministrados a la Entidad al momento de suscripción del contrato. El FNA podrá verificar en cualquier momento durante la ejecución del contrato que los planes, en lo que corresponde a los servicios convenidos, funcionen en las condiciones pactadas.

40. El oferente seleccionado deberá considerar dentro del plan de continuidad del negocio la respuesta, recuperación, reanudación de la operación en contingencia y restauración ante la materialización de ataques cibernéticos.

El oferente seleccionado deberá considerar dentro del plan de continuidad del negocio la respuesta, recuperación, reanudación de la operación en contingencia y restauración ante un escenario que requiera de Teletrabajo, o cualquier mecanismo que implique trabajo remoto. Únicamente durante el tiempo que permanezcan las condiciones de aislamiento decretados por el gobierno nacional como consecuencia de la emergencia sanitaria; sin embargo, una vez se actualicen las regulaciones respecto al distanciamiento social se debe migrar a modalidad de trabajo en instalaciones físicas, dando cumplimiento a la

normativa emitida por la superintendencia financiera y las obligaciones contractuales establecidas.

41. El oferente seleccionado deberá considerar dentro del plan de continuidad del negocio la respuesta, recuperación, reanudación de la operación en contingencia ante posibles fallas de la planta telefónica y permitir el reenvío de tráfico en caso de fallas con la planta principal.

42. El oferente seleccionado deberá considerar dentro del plan de continuidad del negocio la respuesta, recuperación, reanudación de la operación en contingencia de modo tal que se garanticen el 100% de los recursos o puestos de trabajo asignados a la campaña de la Entidad y atender la totalidad de solicitudes o contactos de los consumidores financieros durante este escenario.

43. El FNA, podrá realizar la verificación del cumplimiento de los puntos anteriormente expuestos y hacer parte de las pruebas cuando lo considere necesario, previa comunicación escrita al contratista seleccionado en donde se especifiquen las actividades a realizar. Si el resultado de dicha visita genera acciones de tipo correctivo, preventivo y planes de mejoramiento, para lo cual el proveedor establecerá los correspondientes planes de acción e informará al FNA para su respectiva revisión y cierre.

ANÁLISIS DE VULNERABILIDADES

44. El oferente seleccionado deberá implementar un sistema de análisis y gestión de vulnerabilidades informáticas en las plataformas que soporten los servicios contratados por el FNA. El FNA podrá realizar análisis de vulnerabilidades sobre las plataformas que soporten los servicios contratados con el fin de identificar posibles brechas de seguridad que puedan comprometer la seguridad de la información de la Entidad, el proveedor deberá gestionar la corrección oportuna y eficaz de dichas vulnerabilidades.

    a. Las herramientas usadas en el análisis de vulnerabilidades deben estar homologadas por el CVE (Common Vulnerabilities and Exposures) y actualizadas a la fecha de su utilización.
    b. Para la generación de los informes se debe tomar como referencia la lista de nombres de vulnerabilidades CVE publicada por la corporación Mitre.

REQUERIMIENTOS ESPECIALES

ANEXO 4.

REQUISITOS DE SEGURIDAD Y CONFIDENCIALIDAD

Objeto contractual: Prestación de servicios de un Contact Center especializado, para la atención de usuarios, afiliados servicios de seguimiento comercial, asistencia procedimental, así como las demás actividades relacionadas con los productos y servicios ofrecidos por el Fondo Nacional del Ahorro a nivel nacional e internacional.

45. El oferente seleccionado deberá destinar un área dedicada exclusivamente para la operación de los recursos necesarios en la prestación del servicio a la campaña del FNA, la cual debe contar con los controles físicos y lógicos que impidan el ingreso de personas no autorizadas, así como la extracción de la información manejada.

46. El oferente seleccionado deberá impedir el ingreso de dispositivos que permitan almacenar o copiar cualquier tipo de información, o medios de comunicación, que no sean suministrados por la entidad.

47. El oferente seleccionado deberá dotar a los equipos de cómputo que operan en la campaña del FNA los elementos necesarios que impidan el uso de dispositivos de almacenamiento no autorizados por la entidad. Igualmente, se debe bloquear cualquier tipo de conexión a red distinta a la usada para la prestación del servicio.

48. El oferente seleccionado deberá garantizar que los equipos de cómputo destinados a la campaña del FNA sean utilizados exclusivamente en la prestación de servicios del Centro de Atención Telefónica para esta campaña.

49. El oferente seleccionado deberá asegurar que en los equipos de cómputo asignados y utilizados en la campaña del FNA no se permita la navegación por internet, el envío o recepción de correo electrónico, la mensajería instantánea, ni ningún otro servicio que permita el intercambio de información.

50. El oferente seleccionado deberá asegurar que en el Sistema de Audio Respuesta IVR se permita transferir la llamada a un operador, al menos en los horarios hábiles de atención al público.

51. El oferente seleccionado deberá gestionar el licenciamiento requerido para la prestación del servicio de chat a través de la herramienta de WhatsApp Bussines, el servicio deberá ser prestado en la sede del oferente seleccionado. (incluir requisitos de los números de la Entidad).

52. El oferente seleccionado deberá asumir los costos de los servicios que se requieran para atender la totalidad de los servicios requeridos, deberá disponer de los canales adicionales para atender la totalidad del tráfico, especialmente en temporadas con mayor tráfico como el recaudo de cesantías.

ANEXO 4.

REQUISITOS DE SEGURIDAD Y CONFIDENCIALIDAD

Objeto contractual: Prestación de servicios de un Contact Center especializado, para la atención de usuarios, afiliados servicios de seguimiento comercial, asistencia procedimental, así como las demás actividades relacionadas con los productos y servicios ofrecidos por el Fondo Nacional del Ahorro a nivel nacional e internacional.

Aprobó: Jaime Eduardo Martinez –VR
Revisó: Andres Ricardo Garzón – VR