Las políticas de seguridad contenidas en este documento deben ser cumplidas por parte de proponentes y proveedores de Bancóldex S.A., en el evento que le resulten aplicables, para asegurar un adecuado nivel de confidencialidad, integridad y disponibilidad de la información del Banco y el cumplimiento normativo vigente aplicable al objeto de la propuesta y del contrato en el evento que el mismo resulte adjudicado.

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN Y DE CIBERSEGURIDAD

1. Contar con políticas de seguridad de la información que incorporen directrices y medidas para el control preventivo, detectivo y correctivo de posibles ataques del ciberespacio, incluyendo programas de concientización en tal sentido a toda la organización.

2. Contar con un procedimiento documentado y divulgado para la gestión de incidentes de seguridad, que contenga etapas de prevención, protección y detección, respuesta y comunicación y recuperación y aprendizaje.

3. Contar con programas de capacitación y sensibilización en materia de ciberseguridad a los funcionarios del proponente o proveedor del Banco.

4. Participar de manera activa con las organizaciones gremiales que corresponda, creadas para la defensa en ciberseguridad.

5. Contar con un programa periódico de fortalecimiento de la seguridad de la información y monitoreo de la ciberseguridad, liderado por personal competente en esa materia.

CUMPLIMIENTO DE LAS POLÍTICAS DEL BANCO

1. Dar a conocer y verificar el entendimiento de las políticas objeto de este documento a los funcionarios designados por el proveedor para la atención del proceso de oferta y desarrollo del objeto del contrato.

2. Verificar el cumplimiento de las políticas objeto de este documento, de parte de los funcionarios y terceros del proveedor vinculados al proceso de oferta y desarrollo del objeto del contrato.

CONECTIVIDAD CON LA RED DEL BANCO

1. Tramitar de manera previa la autorización del Banco para cualquier conexión e interacción con la red de Bancóldex y su información.

2. Aceptar el monitoreo de cualquier conexión e interacción con la red del Banco y su información cuando BANCOLDEX lo considere oportuno.

3. Utilizar mecanismos de encripción fuerte de la información cuando se transfiera o comparta información confidencial o sensible entre el proveedor y el Banco..

BUEN USO DE LA TECNOLOGÍA DEL BANCO

1. Utilizar los recursos tecnológicos que facilite el Banco, en forma exclusiva para la ejecución del contrato.

2. 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.

3. Reportar de manera inmediata al Banco, cuando se encuentre evidencia de alteración o manipulación de dispositivos o información

ACCESO FISICO A LAS INSTALACIONES DEL BANCO

1. No acceder las áreas del Banco sin el acompañamiento o bajo la responsabilidad de un funcionario autorizado y permitir el registro de la visita por el medio que se tenga destinado para tal fin.

2. Contar con un mecanismo sencillo que permita al Banco identificar los funcionarios designados por el proveedor para la ejecución del contrato.

3. Reportar de manera inmediata al Banco cualquier novedad que afecte el acceso de los funcionarios designados por el proveedor para la ejecución del contrato a las instalaciones del Banco.

CALIDAD DE LOS ENTREGABLES PARA EL BANCO

1. 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 Tecnología y por la Dirección del Departamento de Sistemas del Banco.

2. Comprometerse con el Banco a entregar propuestas y soluciones que preserven la confidencialidad, integridad y disponibilidad de la información en los términos previstos en el contrato que para el efecto se celebre.

PROPIEDAD INTELECTUAL DEL SOFTWARE EN USO AL INTERIOR DEL BANCO

1. Aportar certificación suscrita por el Representante Legal del oferente o del proveedor, sobre la propiedad del licenciamiento del software contenido en cualquier equipo de su propiedad, que ingrese al Banco. La certificación debe ser extensiva a cualquier software o herramienta tecnológica que se utilice para la ejecución del contrato que se celebre, para lo cual debe mediar el permiso o licencia suscrita por el fabricante.

2. Asegurar que, al término del contrato, toda información, software, y demás elementos tecnológicos de propiedad del Banco serán eliminados de manera segura de los equipos del proveedor, cumpliendo con la obligación de confidencialidad y/o atendiendo el acuerdo de confidencialidad que para el efecto se hubiese suscrito.

3. Responsabilizarse del tratamiento de los riesgos de equipos, información y demás elementos de propiedad del proveedor, puestos a disposición del Banco durante la ejecución del contrato.

PLANES DE CONTINGENCIA Y DE CONTINUIDAD DEL PROPONENTE O DEL PROVEEDOR

1. Disponer de un plan de contingencia y continuidad documentado y probado que permita mantener disponible la prestación del servicio contratado por el Banco, en el evento que se presenten situaciones de interrupción.
2. Contar con protocolos para la comunicación inmediata al Banco de interrupciones del servicio contratado ya sean programadas o sorpresivas.
3. Reportar de manera periódica al Banco, las interrupciones que ha tenido el servicio ofrecido por el proveedor.

4. Reportar de manera periódica al Banco los resultados de las pruebas efectuadas a los planes de contingencia y de continuidad en cuanto a los servicios ofrecidos o contratados por el Banco.

5. En calidad de observador, permitir al Banco la participación en las pruebas de continuidad que se ejecuten, en caso que este lo considere adecuado.

PROPIEDAD Y MANEJO DE LA INFORMACIÓN DEL BANCO POR PARTE DEL CONTRATISTA

1. Conocer y cumplir con la política de protección de datos personales del Banco, publicada en su página WEB.

2. Cumplir con el rol de Responsable o de Encargado conforme lo establece la Ley en el tema de Protección de Datos Personales.

3. Verificar que la información sometida a tratamiento de datos personales que el Banco autorice para fines del contrato se encuentre alojada en países que cuenten con un nivel adecuado de protección de datos personales de acuerdo con la Circular Externa No- 02 del 23 de marzo de 2018 publicada por la SIC o de ser necesario remitir a consulta previa para autorización la SIC.

4. Cuando la información de propiedad del Banco sea almacenada por el proveedor, entregar de manera periódica copia de la información para su custodia, durante la ejecución del contrato.

5. Contar con un procedimiento y con controles para la devolución de la información de propiedad del Banco en un formato estándar y para la destrucción segura de la misma, una vez terminado el proceso de oferta o desarrollo del contrato.

6. Diseñar y ejecutar planes de concienciación y cultura al interior de la empresa para el personal en materia de protección de datos personales y de la información de sus clientes.

7. Contar con protocolos de comunicación que permitan el reporte inmediato al Banco de cualquier incidente que pueda comprometer la disponibilidad, integridad o confidencialidad de la información del Banco.

SOLUCIONES DE NUBE DE PROPIEDAD DEL PROPONENTE O CONTRATISTA

1. Mantener informado al Banco sobre la cadena de proveedores que participan en la solución ofrecida o contratada por el Banco. Esta obligación incluye el reporte inmediato de cualquier novedad que se presente en este tema durante el desarrollo del contrato.

2. Cumplir con las políticas de administración de usuarios que se encuentran en el Sistema de Gestión de Seguridad de la Información (SGSI) del Banco.

3. Identificar la modalidad de nube que utilizar la solución ofrecida o contratada por el Banco. (Pública, mixta o privada), así como el sitio donde estará almacenada la información propiedad del Banco.

4. Especificar el esquema de copias de seguridad que se ofrece o se contrata, incluyendo los procedimientos de devolución de información al Banco y los mecanismos de destrucción de la misma una vez finaliza el contrato.

5. Cumplir con el rol de Responsable o de Encargado conforme lo establece la Ley en el tema de Protección de Datos Personales.

6. Disponer de un plan de continuidad para los servicios de nube ofertados o contratados.

7. Especificar los acuerdos de nivel de servicio que incorporen desempeño y disponibilidad de la solución.

ADQUISICIONES DE SOFTWARE, HARDWARE Y ELEMENTOS DE COMUNICACIONES PARA EL BANCO

Garantizar al Banco que los componentes tecnológicos entregados para su uso en cualquiera de las modalidades comerciales, esto es compra, arriendo, leasing etc, se ajustan al protocolo de internet versión 6 o IPV6 nativo y además que admiten la transición desde el Protocolo de Internet versión 4 o IPV4, para el cumplimiento de las exigencias formuladas por el Ministerio de las Tecnologías de la Información y las Comunicaciones MINTIC.