ANEXO 15 SEGURIDAD DE LA INFORMACIÓN.

El proyecto propuesto y el proponente deberán cumplir con todos los requerimientos exigidos en el presente Anexo. A su vez el proponente deberá indicar en su propuesta la metodología y modalidad de cumplimiento de cada uno de los requerimientos indicados a continuación.

* 1. **Políticas del SGSI[[1]](#footnote-1):** Para efectos del control de acceso nos referiremos en este documento a Clientes, Usuarios y Funcionarios. El proponente deberá cumplir con los siguientes requerimientos:
* El sistema debe contar con un módulo de administración y control de acceso sincronizado.
* El control de acceso debe funcionar en el esquema de roles y responsabilidades y poseer control dual para las operaciones críticas si las hay.
* La solución debe contar con un mecanismo de autenticación, administración y monitoreo para el control de acceso desde los equipos.
* El sistema debe contar con facilidades implementadas para el control por parte de los administradores de acceso, tales como consultas y listados para circularizar opciones y privilegios.
* El sistema debe contar con un histórico de quienes han tenido acceso al sistema junto con sus atributos, inclusive después de la desvinculación para el caso de funcionarios.
	1. **Habeas Data:** Para el cumplimiento de esta Ley, es necesario que la solución permita tener segmentada la información de Clientes porque está sujeta a Reserva Bancaria y se debe tratar como información confidencial. Igualmente, si llegara a almacenar información de proveedores, este segmento debe tener un tratamiento propio de reserva comercial.
	2. **Circular externa 042 de 2012.** El proponente debe cumplir con la normativa vigente para las entidades vigiladas por la Superintendencia Financiera de Colombia -SFC, que se encuentran específicas en la **Circular externa 042 de 2012**, y sus modificaciones y demás reglamentación vigente y futura sobre la materia. En especial el proponente deberá cumplir con:
* **Numeral 3.1.4 C.E. 042 de 2012:** Dotar de seguridad la información confidencial de los clientes que se maneja en los equipos y redes de la entidad.

El sistema preferiblemente debe permitir marcar la información sensible para facilitar el manejo seguro de la misma de acuerdo con definiciones del SGSI de cada una de las tres entidades.

* **Numeral 3.1.12 C.E. 042 de 2012:** Establecer procedimientos para el bloqueo de canales o de instrumentos para la realización de operaciones, cuando existan situaciones o hechos que lo ameriten o después de un número de intentos de accesos fallidos por parte de un cliente, así como las medidas operativas y de seguridad para la reactivación de los mismos
* **Numeral 3.1.13 C.E. 042 de 2012:** Elaborar el perfil de las costumbres transaccionales de cada uno de sus clientes
* **Numeral 3.1.17 C.E. 042 de 2012:** Tener en operación sólo los protocolos, servicios, aplicaciones, usuarios, equipos, entre otros, necesarios para el desarrollo de su actividad.

La solución debe permitir el bloqueo de opciones que no sean necesarias. De igual forma deberían poderse activar cuando así se requiera.

* **Numeral 3.2.3 C.E. 042 de 2012:** Exigir que los terceros contratados dispongan de planes de contingencia y continuidad debidamente documentados. Las entidades deberán verificar que los planes, en lo que corresponde a los servicios convenidos, funcionen en las condiciones pactadas

La disponibilidad del sistema debe atender los requerimientos que en tal sentido haga Bancóldex y contar con planes de contingencia probados, actualizados, documentados y certificados por lo menos una (1) vez por año. Bancóldex podrá participar en los ejercicios de pruebas cuando así lo decida.

Los planes de contingencia de la solución deben estar sincronizados con otros terceros que participen en la misma y además deben ser de conocimiento del Banco.

* **Numeral 3.2.5 C.E. 042 de 2012:** Implementar mecanismos de cifrado fuerte para el envío y recepción de información confidencial con los terceros contratados.
* **Numeral 3.3.6 C.E. 042 de 2012:** Llevar un registro de las consultas realizadas por los funcionarios de la entidad 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 deberán 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.

El sistema debe generar logs a que se refiere la norma, los cuales deben ser de fácil lectura y deben poder exportarse a archivos Excel. Este requerimiento preferiblemente debe tener alcance a los cambios que se hagan en los registros de información y la dirección IP del responsable del cambio. Preferiblemente el log debe contener la información antes y después del cambio.

* **Numeral 4.9 C.E. 042 de 2012:** Dado que la solución debe poder ser accedida por los funcionarios que autorice Bancóldex usando el canal de Internet, se solicita al proveedor el cumplimiento de los siguientes numerales a que se refiere la norma específicamente para ese canal:
* **Numeral 4.9.1 C.E. 042 de 2012:** Implementar los algoritmos y protocolos necesarios para brindar una comunicación segura.
* **Numeral 4.9.2 C.E. 042 de 2012:** Realizar como mínimo dos (2) veces al año una prueba de vulnerabilidad y penetración a los equipos, dispositivos y medios de comunicación usados en la realización de operaciones por este canal. Sin embargo, cuando se realicen cambios en la plataforma que afecten la seguridad del canal, deberá realizarse una prueba adicional (si aplica).
* **Numeral 4.9.3 C.E. 042 de 2012:** Promover y poner a disposición mecanismos que reduzcan la posibilidad de que la información pueda ser capturada por personal no autorizado.
* **Numeral 4.9.4 C.E. 042 de 2012:** Establecer el tiempo máximo de inactividad, después del cual se deberá dar por cancelada la sesión, exigiendo una nueva conexión.
* **Numeral 4.9.5 C.E. 042 de 2012:** Informar al funcionario al inicio de cada sesión, la fecha y hora del último acceso.
* **Numeral 4.9.6 C.E. 042 de 2012:** Implementar mecanismos que permitan a la entidad financiera verificar constantemente que no sean modificados los enlaces (links) de su sitio Web, ni suplantados sus certificados digitales, ni modificada indebidamente la resolución de sus DNS.
* **Numeral 4.9.7 C.E. 042 de 2012:** Contar con mecanismos para incrementar la seguridad de los portales, protegiéndolos de ataques de negación de servicio, inyección de código malicioso u objetos maliciosos, que afecten la seguridad de la operación o su conclusión exitosa.
* **Numeral 5 C.E. 042 de 2012:** Mantener tres ambientes independientes: uno para el desarrollo de software, otro para la realización de pruebas, y un tercer ambiente para los sistemas en producción. En todo caso, el desempeño y la seguridad de un ambiente no podrá influir en los demás.

Por tratarse de una solución adquirida, el esquema de ambientes será el que posea el proveedor, sin perjuicio que la esencia del control que busca la norma, se preserve.

* **Numeral 5.5 C.E. 042 de 2012:** Contar con interfaces que cumplan con los criterios de seguridad y calidad, de tal manera que los funcionarios y otros servicios puedan hacer uso de ellas de una forma simple e intuitiva.
	+ **Numeral 5.6 C.E. 042 de 2012:** Mantener documentada y actualizada, al menos, la siguiente información: parámetros de los sistemas donde operan las aplicaciones en producción, incluido el ambiente de comunicaciones; versión de los programas y aplicativos en uso; soportes de las pruebas realizadas a los sistemas de información; y procedimientos de instalación del software.
	+ Preferiblemente el sistema debe contar con consultas que faciliten el cumplimiento de lo descrito en el anterior numeral y especialmente las opciones activas que no son utilizadas por los funcionarios.
* **Numeral 7 C.E. 042 de 2012:** 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.
* 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)).

## **1.4 CONSIDERACIONES ADICIONALES**

* El proponente deberá describir claramente el esquema de seguridad que maneja la solución o servicio; dando a conocer las características de acceso, roles, perfiles, permisos, auditoría, actualizaciones de seguridad, antivirus y análisis de vulnerabilidades utilizados en los servidores dedicados para la solución, entre otros aspectos mencionados en la circular (042) de la Superintendencia Financiera de Colombia.
* Toda la información que se maneje en virtud del desarrollo del contrato es de propiedad de Bancóldex y el proponente o proveedor debe describir claramente los mecanismos para la destrucción de la misma, cuando ya no sea necesaria, o cuando el contrato finalice, así como para devolverla a Bancóldex en un formato estándar.
* El proponente deberá tener en cuenta los requerimientos de información y de disponibilidad de los servicios para clientes y usuarios, a que se refiere la **circular externa 028 de 2016**.
* Implementación de CCM 3.0.1 (The Cloud Security Alliance Cloud Controls Matrix (CCM)).
* La propuesta debe garantizar que el proponente será el responsable exclusivo de la calidad, oportunidad y cumplimiento de las diferentes componentes del proceso.
* El proveedor debe documentar todas las actividades descritas y anexar los procedimientos operativos propuestos.
* El proveedor debe notificar a Bancóldex en caso de una solicitud de divulgación y los casos de violación de datos.
* El proveedor debe divulgar a Bancóldex la información sobre todos los subcontratistas utilizados para el desarrollo del proyecto.
* El proveedor debe establecer acuerdos de confidencialidad para las personas (funcionarios) que pueden acceder a datos personales dentro de la cadena de abastecimiento.
* El proveedor debe especificar a Bancóldex el procedimiento para la recuperación y restauración de datos o contenidos cargados.
* Si la solución está implementada sobre nube, adicionalmente se debe tener en cuenta lo siguiente:
* Presentar la información de los Terceros que participan en la solución de la nube (cadena de valor de la nube).
* Detallar la modalidad de nube que se está ofreciendo (privada, híbrida, publica), ventajas y beneficios.
* Detallar cómo funciona la administración de copias de seguridad durante la ejecución del contrato. Si Bancóldex recibirá durante el contrato copias de respaldo periódicas que minimicen la dependencia total del proveedor en tal sentido. Especificar: periodicidad y disponibilidad de custodia de forma que se garantice la plena disponibilidad e integridad de los datos almacenados.
* Describir los Acuerdos de nivel de servicio tanto para disponibilidad como para desempeño del sistema.
* Tratamiento transfronterizo de datos. En este caso, dónde estarán los datos tanto en ambiente de producción como en ambiente de contingencia.
1. [↑](#footnote-ref-1)