|  |  |
| --- | --- |
| Tipo de Trámite: | **Autorización de sistema informático principal CORE.** |
| Subsistema a que aplica: | **Sociedades de Seguros** |
| Fecha de creación: | **16/09/2014** |
| Fecha de última modificación: | **20/07/2016** |

**Base legal:**

* **Manual de Contabilidad de Sociedades de Seguros**

Deberá presentarse a la Superintendencia del Sistema Financiero la información completa que se detalla a continuación:

1. Descripción general del sistema y de cada módulo que lo conforma, especificando los procesos que comprende, la integración entre los mismos, así como la interacción con otros aplicativos informáticos, incluir tipo de licenciamiento y propiedad del software.
2. Manuales de usuario y documentación técnica del sistema, diseño relacional de archivos (Diagrama Entidad-Relación), Diccionario de Datos; preferentemente en formato digital.
3. Listado de usuarios que tendrán acceso al sistema, indicando el nivel jerárquico y de acceso, perfiles de usuarios.
4. Procedimiento para el manejo de claves de acceso
5. Detalle de los reportes que genera el sistema, especificando por cada uno la frecuencia con que se genera, el número de copias y como se distribuyen.
6. Si los sistemas están siendo desarrollados, describir el procedimiento para probar y aprobar los programas; así como las responsabilidades de estas actividades.
7. Política y/o procedimiento para el mantenimiento o desarrollo de nuevas funcionalidades del sistema.
8. Inventario y características de la plataforma de tecnología sobre la cual opera el sistema. (Hardware y Software).
9. Procedimiento para realizar respaldos.
10. Plan de migración de datos.
11. Copia del contrato de garantía o mantenimiento del equipo central y periféricos
12. Copia el contrato de adquisición/implementación, garantía, licencia de uso y mantenimiento del sistema.
13. Diagrama de Red/ Comunicaciones.
14. Documentación relativa a los procesos de continuidad de operaciones
    1. Análisis de Impacto en el Negocio (BIA);
    2. Plan de continuidad del Negocio (BCP); y
    3. Plan de recuperación ante Desastres (DRP).
    4. Plan de Gestión de Incidentes.
15. Descripción de servicios informáticos tercerizados que incluya información del proveedor.
16. Análisis de riesgos y el sistema de gestión de seguridad de la información implementado.
17. Listado de los reportes que se generarán con el nuevo sistema, incluyendo los reportes y alertas relacionados con prevención de LA/FT.
18. Documentación de las pruebas efectuadas, así como las actas o certificación de usuario y los informes de revisión por parte de auditoría interna.
19. Ambiente de pruebas debidamente configurado.