Colpensiones	**ANEXO N 3**

ANEXO SEGURIDAD DE LA INFORMACION y CIBERSEGURIDAD	
1.	El CONTRATISTA debe contar con una política de ciberseguridad establecida y comunicada al interior de la organización.
2.	El CONTRATISTA debe ejecutar pruebas de escenarios en casos de incidentes de ciberseguridad y las acciones para soportar recuperar la operación en la prestación del servicio los cuales deben ser documentados y entregados a COLPENSIONES.
3.	El CONTRATISTA debe priorizar y generar respuesta junto con los planes de acción acerca de riesgos de seguridad de la información que sean identificados por COLPENSIONES.
4.	El CONTRATISTA debe asegurar controles físicos y/o lógicos el acceso no autorizado a los equipos de información asignados a la prestación de sus servicios, es decir todos aquellos dispositivos que interactúan con las plataformas informáticas de COLPENSIONES.
5.	El CONTRATISTA debe implementar mecanismos para la adecuada autenticación y segregar las funciones y responsabilidades de los usuarios con privilegios administrador o que brindan soporte remoto, para mitigar los riesgos de seguridad de la información.
6.	El CONTRATISTA debe mantener el inventario actualizado de los dispositivos físicos, aplicaciones y sistemas de información que prestan el servicio a COLPENSIONES.
7.	El CONTRATISTA debe establecer los roles y responsabilidades del equipo de trabajo encargado de la ciberseguridad en la prestación del servicio a COLPENSIONES.
8.	El CONTRATISTA debe garantizar que los equipos de cómputo cuentan con el soporte, mantenimiento, licenciamiento de programas y sistema operativo durante la ejecución de contrato.
9.	EL CONTRATISTA debe enviar la información objeto del contrato únicamente por los canales y mecanismos definidos por Colpensiones.
10.	EL CONTRATISTA debe implementar controles para mitigar los riesgos que pudieran afectar la seguridad de información confidencial, en reposo o tránsito que es procesada, almacenada o transmitida para el desarrollo del contrato con COLPENSIONES.
11.	EL CONTRATISTA debe dotar sus terminales, equipos de cómputo y redes locales de los elementos necesarios que permitan prevenir incidentes de seguridad informática.
12.	El CONTRATISTA deberá reportar todas las novedades (ingresos, vacaciones, licencias, retiros) del personal que disponga para la ejecución del contrato, con el fin de mantener únicamente los accesos requeridos para cumplir con el objeto del contrato; contar con mecanismos de control para evitar que su personal preste sus usuarios y claves de acceso o utilice usuarios de funcionarios retirados.

13.	El CONTRATISTA deberá realizar campañas de concientización al personal que disponga para la ejecución del contrato, sobre las responsabilidades adquiridas en el mantenimiento de la eficacia de las medidas de control de acceso, con respecto al uso de contraseñas y a la seguridad de la información puesta a su disposición.
14.	El CONTRATISTA debe contar con procedimientos para la gestión de incidentes en seguridad de la información y Ciberseguridad, que permitan la detección, contención, tratamiento y cierre, gestionando lecciones aprendidas.
15.	El CONTRATISTA informará a COLPENSIONES incidentes de ciberseguridad que afecten de manera significativa la confidencialidad, integridad y disponibilidad de la información de la entidad, haciendo una breve descripción del incidente, su impacto y las medidas adoptadas para gestionarlo.
16.	El CONTRATISTA debe establecer procedimientos para la retención y destrucción final de la información entregada por COLPENSIONES y ejecutar las acciones respectivas al finalizar la prestación del Servicio.
17.	El CONTRATISTA debe alinearse y cumplir las políticas de seguridad de la información y Ciberseguridad de COLPENSIONES.
Documento Generado por el Grupo de Seguridad Informática de COLPENSIONES	