ANEXO No. 4 SEGURIDAD INFORMÁTICA

A continuación, se relacionan los requerimientos de seguridad informática que deben cumplir los CONTRATISTAS que ofrezcan servicios para COLPENSIONES y que contengan elementos tecnológicos de hardware y/o software. Dichos requerimientos serán verificados por COLPENSIONES anualmente y/o cuando el Supervisor del Contrato lo disponga. En caso de identificarse incumplimiento EL CONTRATISTA debe corregir el hallazgo acorde a los ANS establecidos. En la prestación del servicio ofrecido a COLPENSIONES, EL CONTRATISTA debe cumplir con los siguientes requisitos:

Ítem	DESCRIPCION
1	El contratista debe cumplir con las circulares externas de la Superintendencia Financiera: (007 y 008 de 2018 - CE042 de 2012) o las que se encuentren vigentes durante el tiempo de duración del contrato.
2	El contratista debe entregar la Arquitectura de Seguridad de la plataforma tecnológica que soporta el servicio durante la fase de planeación de acuerdo al Anexo Técnico No. 6 Protocolo de Transición mesa
3	Identificar y medir los riesgos cibernéticos emergentes que puedan afectar la operación del servicio y establecer controles para su mitigación.
4	Establecer los procedimientos para reportar cuando se considere pertinente al grupo de respuestas al grupo de emergencias Cibernéticas de Colombia COLCERT o quien haga sus veces directamente o a través de CSIRT sectoriales los ataques cibernéticos presentados.
5	Adoptar los mecanismos necesarios para recuperar los sistemas de información, al estado al que se encontraban antes del ataque cibernético.
6	En la medida de lo posible, preservar las evidencias digitales, para que las áreas de seguridad de Colpensiones, o las autoridades puedan realizar las investigaciones correspondientes.
7	Ajustar sus sistemas de gestión de riesgo y de seguridad de la información, como consecuencia de los incidentes presentados, adoptando los controles que resulten pertinentes.
8	Garantizar que todos los equipos de cómputo destinados a la prestación de servicio a COLPENSIONES serán de uso exclusivo.
9	Considerar y ejecutar dentro del plan de continuidad del negocio la respuesta recuperación, reanudación de la operación, contingencia y restauración ante la materialización de ataques cibernéticos.
10	Adelantar la atención de la gestión de las vulnerabilidades que presenten las plataformas destinadas a la prestación del servicio, con el objetivo de mantener asegurados, todos los componentes tecnológicos del servicio.
11	Realizar un monitoreo continuo a su plataforma tecnológica, con el propósito de identificar comportamientos inusuales que puedan evidenciar ciberataques contra el servicio.

ANEXO No. 4 SEGURIDAD INFORMÁTICA

12	Establecer procedimientos de respuesta a incidentes cibernéticos, tales como desconexión automática de equipos, cambio de contraseñas, actualización de base de firmas de antivirus, bloqueo de direcciones IP o cualquier otro que sea necesario para proteger el servicio.
13	EL CONTRATISTA debe proteger las claves de acceso a recursos que hacen parte del objeto contractual. En desarrollo de esta obligación, EL CONTRATISTA deberá evitar el uso de claves compartidas, genéricas o para grupos. La identificación y autenticación en los recursos debe ser única y personalizada. Por lo anterior, EL CONTRATISTA debe contar con estándares para la definición y asignación de cuentas de acceso a los recursos informáticos y políticas de contraseñas.

14	EL CONTRATISTA debe elaborar, conservar y revisar regularmente los registros y/o Logs acerca de actividades, excepciones, fallas y eventos de seguridad de la información e informar periódicamente a Colpensiones.
15	El CONTRATISTA debe documentar un procedimiento que garantice la retención de información de logs, archivos de configuración e históricos de configuraciones sobre los componentes objeto del contrato por la duración del mismo, facilitar a su vez los procedimientos de uso, consulta de esta información y generación de reportes. A si mismo del suministro de los mismos a solicitud de Colpensiones y al finalizar el contrato.
16	EL CONTRATISTA debe garantizar que los equipos que usa para la prestación del servicio cuenten con las actualizaciones de software y control de instalación de aplicaciones que se realice de forma automatizada. Para el Sistema Operativo Sistema operativo a) Licencia del sistema operativo. b) Actualizaciones del sistema operativo al día (Windows Update). c) Tarea Programada de actualización 1 vez a la semana como mínimo. d) La cuenta de acceso debe contar con contraseña
17	EL CONTRATISTA debe permitir el desarrollo de análisis de vulnerabilidades a los componentes que hacen parte del objeto contractual por parte de Colpensiones, con el fin de validar las amenazas que pueden vulnerar la información procesada en los recursos objeto del contrato. Colpensiones se reserva el derecho de ejecutar dichas pruebas, de la misma manera deberá presentar un plan de mejoramiento en caso de encontrar vulnerabilidades.

ANEXO No. 4 SEGURIDAD INFORMÁTICA

18	EL CONTRATISTA debe asegurar que todos los componentes de la solución ofrecida, sin importar si la conexión se realiza desde una red externa o una red interna, cuenten con controles como motores de antivirus, Anti Spam y se actualice de forma periódica. Se debe garantizar que los equipos de cómputo que utiliza el contratista para la prestación del servicio de mes de ayuda cuenten con la última versión estable publicada por el fabricante, como mínimo para el Software antivirus a) Contar con Licenciamiento. (No se aceptan antivirus de Windows Defender ni Essentials, ni versiones Free de antivirus de dudosa reputación) b) Antivirus activo. c) Tener configurada la tarea programa de escaneo diario y protección en tiempo real. d) Tener activo el firewall de aplicación de Windows. e) Base de datos de firmas de virus actualizada.
19	EL CONTRATISTA debe realizar una adecuada segregación de funciones del personal que administre, opere, mantenga y en general, tenga la posibilidad de acceder a los recursos del servicio.
20	EL CONTRATISTA debe velar porque los niveles de seguridad de los elementos que hacen parte del objeto del contrato, no se vean disminuidos durante la duración del contrato. EL CONTRATISTA debe notificar a COLPENSIONES cuando estos se vean disminuidos y se puedan comprometer los niveles de seguridad usados.
21	EL CONTRATISTA debe garantizar el uso de protocolos seguros para acceso a los servicios, gestión o administración del mismo objeto de este estudio de mercado, en su última versión. (TLS/SSL, SSH, SMTPS, IMAPS, POP3S. entre otros). versiones actualizadas.
22	EL CONTRATISTA debe implementar un procedimiento de gestión de usuarios y privilegios en los sistemas o equipos que disponga para el servicio.
23	EL CONTRATISTA deberá presentar a COLPENSIONES, el procedimiento para la gestión de incidentes de seguridad informática y las estrategias para la documentación, contención y mitigación de incidentes.
24	El CONTRATISTA debe establecer procedimientos y controles para la entrega de la información y la destrucción de la misma, una vez finalizada la prestación del servicio: EL CONTRATISTA, sin perjuicio de la normatividad nacional sobre la conservación de la documentación relevante para efectos contables y legales, debe definir un procedimiento de saneamiento de medios, basado en buenas prácticas y en la ley colombiana, el cual debe ser entregado para su revisión por parte de COLPENSIONES y que posteriormente será aceptado como suficiente para todos los efectos de su interés. El contratista deberá garantizar el borrado y destrucción de la información a través de una carta de certificación de un tercero avalado para tal fin.
25	EL CONTRATISTA debe contar con políticas, normas y procedimientos de seguridad de la información oficializadas y divulgadas hacia sus empleados, terceros y PROVEEDORES

ANEXO No. 4 SEGURIDAD INFORMÁTICA

26	A través de los recursos informáticos del CONTRATISTA no se podrán efectuar modificaciones a la información de COLPENSIONES directamente en ninguna plataforma informática sin la aprobación previa del Supervisor del Contrato o dueño de la información por parte de COLPENSIONES.
27	Toda integración tecnológica entre plataformas de información de COLPENSIONES y/o del CONTRATISTA, debe considerar procedimientos de autenticación para las comunicaciones entre los módulos de software de integración que se hayan definido. Para esta labor es necesario contar con un profesional dedicado 100% a este proceso con los módulos ya definidos en la etapa de la oferta y que se implementará lo que se alcance durante el desarrollo del contrato (bolsa de horas -300 horas)
28	El CONTRATISTA debe garantizar que los inicios de sesión en los equipos y en el acceso a el software de mesa de servicio se realicen de forma presencial y no permita accesos remotos, salvo previa autorización del área de seguridad informática.
29	El CONTRATISTA deberá dotar a los equipos de cómputo dispuestos para el servicio, de los elementos necesarios que impidan el uso de dispositivos de almacenamiento no autorizados por la entidad. Igualmente, se deberá bloquear cualquier tipo de conexión a red distinta a la usada para la prestación del servicio y que solo sean utilizados para los servicios de Colpensiones.
30	El CONTRATISTA deberá garantizar que, en los equipos de cómputo destinados para el servicio, no se permita la navegación por Internet a sitios diferentes a los necesarios para la prestación del servicio, que permita el intercambio de información, garantizar con políticas de navegación segura.
31	El CONTRATISTA deberá cumplir con la protección de datos personales ley 1581 de 2012