ANEXO - 9 - SEGURIDAD DE LA INFORMACIÓN

SEGURIDAD DEL RECURSO HUMANO (cada SI vale 25 puntos)		
Cuenta con una clara definición de los roles y responsabilidades en Seguridad de la Información para los funcionarios	Si No	Justificación y/o comentarios:
Cuenta con procesos disciplinarios aplicables por Incidentes de Seguridad de la Información, si fuera del caso.	Si No	Justificación y/o comentarios:
Posee Acuerdos de Confidencialidad con funcionarios y terceros que forman parte de la cadena de suministro.	Si No	Justificación y/o comentarios:
Realiza charlas de concientización en Seguridad de la Información y Ciberseguridad a funcionarios y terceros de la cadena de suministro.	Si No	Justificación y/o comentarios:
SEGURIDAD FISICA Y AMBIENTAL (cada SI vale 33,33)		
Cuenta con control de acceso restringido a áreas sensibles.	Si No	Justificación y/o comentarios:
Tiene mecanismos para control de temperatura y humedad de los sitios que lo requieren	Si No	Justificación y/o comentarios:
Existen programas de mantenimiento preventivo para los equipos críticos.	Si No	Justificación y/o comentarios:
GESTION DE OPERACIONES Y COMUNICACIONES (cada SI vale 14,2)		
Están documentados los procesos operativos que soportan la solución ofrecida	Si No	Justificación y/o comentarios:
Cuenta con procedimientos definidos para la planeación de capacidad de los sistemas de información que comercializa	Si No	Justificación y/o comentarios:
Tiene implementados segmentos de la red interna para la segregación a partir de criterios de seguridad de la información.	Si No	Justificación y/o comentarios:
Cuenta con procedimientos para el manejo de medios externos de almacenamiento. (Cintas, CD, USB, entre otros).	Si No	Justificación y/o comentarios:
Cuenta con herramientas de encripción para la información clasificada como confidencial en reposo y en tránsito que brinden la seguridad ofrecida por AES,RSA,o 3DES.	Si No	Justificación y/o comentarios:
Los logs implementados en la solución son monitoreados.	Si No	Justificación y/o comentarios:
Si cuenta con redes inalámbricas, éstas tienen una clara definición de la arquitectura de seguridad que evite generación de brechas de seguridad en el resto de la red.	Si No	Justificación y/o comentarios:
CONTROL DE ACCESO (cada SI vale 16,66)		
Tiene asignados privilegios de acceso a los sistemas de información	Si No	Justificación y/o comentarios:
Los funcionarios conocen claramente las responsabilidades respecto al manejo de usuarios y contraseñas.	Si No	Justificación y/o comentarios:
Se tienen definidas las políticas y controles generales de uso y manejo de herramientas como internet, correo electrónico, dispositivos de almacenamiento y recursos de red.	Si No	Justificación y/o comentarios:
Monitorea la actividad de los usuarios privilegiados	Si No	Justificación y/o comentarios:
La plataforma permite la autenticación con el directorio activo de los funcionarios del Fiduciaria	Si No	Justificación y/o comentarios:
El sistema permite parametrizar el tiempo con el cual los usuarios deben hacer el cambio de su contraseña	Si No	Justificación y/o comentarios:

GESTION DE ACTIVOS DE INFORMACIÓN (cada SI vale 50)		
Se tienen identificados los activos de información e implementadas las medidas de protección de acuerdo con políticas establecidas	Si No	Justificación y/o comentarios:
Se tienen identificados los responsables de los activos y los controles mínimos dependiendo de su clasificación	Si No	Justificación y/o comentarios:
ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACION (Cada SI vale 33,33)		
Cuando se adquieren o desarrollan aplicaciones se consideran mecanismos de desarrollo seguro.	Si No	Justificación y/o comentarios:
Existen procedimientos de Control de Cambios para aplicaciones y sistemas operativos.	Si No	Justificación y/o comentarios:
Se efectúan periódicamente pruebas de Ethical Hacking con el fin de identificar y corregir vulnerabilidades.	Si No	Justificación y/o comentarios:
GESTIÓN DE INCIDENTES (cada SI vale 33,33)		
Existe un procedimiento formal para el reporte y gestión de los incidentes de Seguridad de la Información dentro de la organización	Si No	Justificación y/o comentarios:
Existen procedimientos para el reporte de Incidentes relacionadas con Terceras partes. (Clientes – Proveedores)	Si No	Justificación y/o comentarios:
La plataforma cuenta con mecanismos de control para la fuga de información.	Si No	Justificación y/o comentarios:
CUMPLIMIENTO (cada SI vale 25)		
Se cumplen las regulaciones existentes sobre derechos de autor.	Si No	Justificación y/o comentarios:
Cuenta con un responsable del cumplimiento regulatorio que aplica a la empresa.	Si No	Justificación y/o comentarios:
La plataforma proporciona un esquema de logs con los cuales se puede conocer la trazabilidad de las acciones que un usuario hizo en el sistema	Si No	Justificación y/o comentarios:
La información de los ambientes de producción, pruebas o desarrollo son ambientes independientes y se encuentran en Colombia o en países equivalentes en cuanto a protección de Datos de acuerdo con lo estipulado por la SIC	Si No	Justificación y/o comentarios:
CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACION (cada SI vale 20)		
Cuenta con planes de contingencia y continuidad documentados para los servicios contratados y con los niveles de seguridad de la información del ambiente de producción.	Si No	Justificación y/o comentarios:
Cuenta con un protocolo para la comunicación oportuna de eventos de interrupción del servicio contratado	Si No	Justificación y/o comentarios:
Sus planes de continuidad se integran con el procedimiento de gestión de incidentes de seguridad de la información.	Si No	Justificación y/o comentarios:
Realiza pruebas de sus planes de continuidad de Negocio incluidos ataques cibernéticos y los hace conocer de sus clientes.	Si No	Justificación y/o comentarios:
Comunica el resultado de las pruebas de continuidad a sus clientes y les permite participar en ellas en caso que lo consideren adecuado	Si No	Justificación y/o comentarios:
OTRAS OBLIGACIONES (cada SI vale 50)		
Posee una póliza vigente que cubra los riesgos daño o pérdida en los equipos del proveedor instalados en el Fiduciaria para el desarrollo del contrato, cuando aplique.	Si No	Justificación y/o comentarios:
La infraestructura utilizada para la prestación del servicio a sus clientes convive con protocolo IPv4 / IPv6	Si No	Justificación y/o comentarios:

Declaro que toda la información proporcionada con este formulario es verdadera y completa, correcta, y puede ser verificada, para ello firmo en constancia:

Nombre de la Empresa	
Nit:	
Nombre del Representante Legal	
Firma del Representante Legal	
Identificación: cc.	