ANEXO 10 - SEGURIDAD DE LA INFORMACIÓN

INVITACIÓN PÚBLICA No. 3000000685 - PRESTAR LOS SERVICIOS PARA GESTIONAR EXPERIENCIAS DE APRENDIZAJE A TRAVÉS DE UNA PLATAFORMA OMNICANAL EN LA NUBE, CON HERRAMIENTAS QUE FACILITEN Y ASEGUREN PROCESOS DE APRENDIZAJE EXITOSOS, CON SERVICIO DE SOPORTE, ADMINISTRACIÓN Y ACOMPAÑAMIENTO ESTRATÉGICO; CON EL FIN DE OFRECER HERRAMIENTAS PARA EL EMPRESARIO FORTALECIENDO SU EXPERIENCIA Y AUMENTANDO LA COBERTURA.

Especificaciones Generales:
Para efectos de la prestación del servicio, el contratista deberá acogerse a la Política de Seguridad de la Información que la CCB tiene definidas.

Cumplir, con los parámetros y condiciones establecidos en la Ley 1581 de 2012 Protección de datos personales, así como cualquier otra que la modifique, adicione o sustituya.

Permitir visita en las instalaciones del proponente para verificar la implementación de gestión de seguridad de la información basado en buenas prácticas vigentes.

Conforme al alcance de la contratación se relaciona a continuación los requisitos de seguridad de la información:

El proponente debe:

- Gestionar la seguridad de la información durante la ejecución del contrato aplicando las buenas prácticas de seguridad de la información basándose como mínimo en el estándar ISO27001 versión vigente.
- Asegurar a la CCB acuerdos de confidencialidad y no revelación de información con los colaboradores que sean asignados para la prestación del servicio.
- Contar con políticas, procedimientos y mecanismos para evitar la fuga de datos e información.
- Contar con un procedimiento para la atención y la gestión de incidentes de seguridad de la información e informar todos los incidentes que se presenten durante la ejecución del contrato a los funcionarios la CCB designe.
- Contar con un procedimiento para la identificación y gestión de remediación de vulnerabilidades técnicas, para los equipos, dispositivos y medios de comunicación involucrados en la prestación del servicio, así como pruebas adicionales cuando se realicen cambios en la plataforma, el proveedor debe asegurar a la CCB que la plataforma no cuenta con vulnerabilidades no remediadas antes de puesta a producción y durante el tiempo de la ejecución del contrato. En caso de que la CCB identifique vulnerabilidades técnicas en la aplicación el proveedor deberá remediar durante los tiempos que la CCB lo indique.
- Acordar los tiempos de entrega de la información una vez finalice el contrato y en las condiciones que establezca la CCB.
- Asegurar que una vez finalizado el contrato y previa coordinación con los funcionarios que la CCB designe, el borrado de manera segura de toda la información derivada de las actividades

desarrolladas durante la ejecución del contrato, en sus sistemas de información incluidas bases de datos, copias de respaldo (en cualquier medio), estaciones de trabajo y/o cualquier dispositivo utilizado en la prestación del servicio, para ello debe contar con procedimiento de borrado seguro de la información y herramientas especializadas las cuales deben ser previamente aprobadas por la CCB.

- Mantener y controlar adecuadamente sus redes para protegerlas de las amenazas cibernéticas (interceptación, copiado, modificación enrutamiento inadecuado y destrucción) y mantener la seguridad de los sistemas y aplicaciones que usan la red, incluyendo la información en tránsito.
- Contar con controles de seguridad física para proteger la información entregada por la CCB y las operaciones en las instalaciones del proponente.
- Asegurar que los colaboradores cuenten con formación, sensibilización y concientización en las políticas y procedimientos organizacionales, en temas la seguridad de la información.
- Informar a la CCB los procedimientos relacionado con los procesos de la toma de copias de respaldo, su periodicidad, entre otros.
- Asegurar la continuidad del servicio ante posibles inconvenientes presentados en: logística, fluido eléctrico, software, hardware y telecomunicaciones, personal, imposibilidad de acceso a sus instalaciones, entre otros.
- Cuando cada uno de los distintos actores (roles) inicie deberá incluir de forma visible los términos y condiciones de protección de datos CCB y tener herramientas para la protección y el cuidado de los contenidos y derechos de autor de cada uno de los temas.
- Se debe almacenar la evidencia de la aceptación de los términos y condiciones al momento de la inscripción en la plataforma.
- Asegurar que los enlaces o link, cuenten con derechos de autor y estos sean de páginas que no estén tipificadas como phishing o malware.
- La plataforma deberá generar registros de auditoría con la finalidad en caso de existir un incidente se pueda establecer que, quien, desde donde, cuando y que cambio se realizó.
- Cumplir con los demás ítems de Seguridad que estén relacionados en el Anexo 2. Especificaciones Técnicas.

CUMPLE ☐ NO CUMPLE ☐

Atentamente,

_____
Nombre y firma del Representante Legal
C.C. No. ……. Expedida en……..