

## Requisitos de seguridad de la información

### Especificaciones Generales:

Para efectos de la prestación del servicio, el contratista deberá acogerse a la Política y los Lineamientos y prácticas Gestión de Seguridad de la Información que la CCB tiene definidas.

El proponente debe cumplir con todos los derechos de autor sobre el software que se encuentre en los equipos conectados a la red de la CCB. Deberá entregar la relación de equipos, software y licencia a los funcionarios que la CCB designe.

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.
- Establecer mecanismos de autenticación en las estaciones de trabajo, como mínimo usuarios y contraseñas. Las contraseñas deberán cumplir como mínimo con lo establecido en los Lineamientos y Prácticas de Seguridad de la Información de la CCB.
- Asignar usuarios únicos para el ingreso de las estaciones de trabajo, así como un procedimiento para la gestión de usuarios (creación, eliminación, bloqueo).
- 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.