ANEXO 10 - REQUISITOS DE GESTIÓN DE RIESGOS

Conforme al alcance de la contratación se relacionan a continuación los requisitos de Gestión de Riesgos:

Riesgos Operacionales:

- Se cuente con un procedimiento para la gestión de riesgos operacionales materializados. En caso de presentarse un evento se deberá informar a la CCB por los canales que la CCB designe un tiempo no mayor a las 6 horas después detectado el suceso.

Seguridad de la Información:

Gobierno

- Para efectos de la prestación del servicio, el proponente debe gestionar la seguridad de la información aplicando las buenas prácticas de seguridad de la información basándose como mínimo en el estándar ISO27001 versión vigente.
- Contar con políticas y procedimientos de seguridad de la información aprobadas y divulgadas en toda la organización.
- Generar acuerdos de confidencialidad con todos los colaboradores que se encuentren designados para la prestación del servicio donde se especifique que la información que se obtenga y genere durante el contrato es exclusivamente para uso de las actividades definidas con la CCB.
- Permitir visitas periódicas en las instalaciones del proponente para verificar la implementación de gestión de seguridad de la información basado en buenas prácticas vigentes

Operación

El proveedor debe asegurar que:

- El licenciamiento del sistema operativo, así como de las aplicaciones que se encuentren dentro de la prestación del servicio.
- Los equipos designados para la prestación del servicio deben como mínimo contar con:
    - Puertos deshabilitados para el uso de dispositivos extraíbles,
    - No permitir el almacenamiento de información de manera local
    - Restricción para la instalación de software.
    - Asignación de usuario único.
    - Software de detección de malware, así como la actualización de firmas en línea
    - Actualización de parches.
    - Los equipos deberán tener usuarios estándar y no administrador.

El acceso a los sitios de operación de la prestación del servicio deberá ser restringido, así como el acceso de dispositivos personales y uso de elementos que puedan realizar copia o captura de información.

- Se cuente con alta disponibilidad en la conectividad a las aplicaciones que la CCB establezca.

Personal

- Dentro del proceso de selección de personal debe asegurase la idoneidad técnica o profesional y ética de su personal, mediante la verificación de antecedentes ante las páginas de instituciones de seguridad o vigilancia.
- Los colaboradores deben contar con formación, sensibilización y concientización en las políticas y procedimientos de seguridad de la información, así como de nuevas tendencias en amenazas cibernéticas.
- Ante cualquier eventualidad del personal se deberá contar con un plan de contingencia cuyo reemplazo o suplencia debe cumplir con las competencias de personal solicitadas. Los cambios deben informarse dentro de los tiempos establecidos por la CCB.

Seguridad de servidores y aplicaciones:

- Las aplicaciones que se utilizarán durante la prestación del servicio deberán ser desarrolladas con metodologías de desarrollo seguro. En aplicaciones web deberán tomar como mínimo de referencia el top de OWASP vigente.
- Las aplicaciones que el proveedor suministre para el cumplimiento del objeto del contrato deberán contar con protocolos de transferencia de información segura, como mínimo TLS 1.2 en adelante.
- Los ambientes de desarrollo, pruebas y producción deben estar separados. En ambientes no productivos no se debe utilizar datos productivos.
- El proveedor debe 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.
- Los sistemas de información cuenten con controles de acceso, como mínimo usuario y contraseña. Se deben tener políticas definidas para su creación, asignación y vigencia. La vigencia de la contraseña no deberá superar los 30 días calendario.
- En los sistemas de información del proveedor que estén dentro de la prestación del servicio a la CCB los registros de auditoria deberán estar activos, permitiendo la trazabilidad de un evento. Los registros de auditoría deberán tener como mínimo formato estándar syslog con la información de: quién, qué, hora, desde dónde, hacia y deberán estar disponibles cuando la CCB los requiera.
- Los sistemas de información deberán ser sincronizados con la hora legal colombiana.
- Se cuente con un procedimiento para la gestión de incidentes de seguridad de la información. En caso de presentarse un incidente se deberá informar a la CCB por los canales que la CCB designe un tiempo no mayor a las 6 horas después detectado el suceso.
- Se deberá contar con un procedimiento del borrado seguro y herramientas licenciadas especializadas para tal fin. Una vez finalice el contrato y previa coordinación con los funcionarios que la CCB designe, se debe realizar 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.
- Las redes LAN y WAN involucradas para la prestación del servicio deben ser protegidas de 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.
- El proveedor deberá contar procedimiento relacionado con los procesos de la toma de copias de respaldo, su periodicidad, entre otros.
- Los repositorios de información (bases de datos) de los diferentes canales deberán ser protegidos de acceso no autorizado, para ello deberá identificar los usuarios de acceso de acuerdo con lo que defina la CCB.

Los siguientes riesgos pueden materializarse durante la ejecución del contrato:

- Afectación a la confidencialidad de la información debido la utilización de la información de forma indebida.
- Afectación a la integridad de la información debido fallas en las aplicaciones o falla en la lógica para captura e integración en las aplicaciones.
- Afectación a la disponibilidad del servicio debido a fallas tecnológicas u operativas.
- Incumplimiento a las regulaciones establecidas en materia de seguridad por afectación a la confidencialidad y disponibilidad de la información.

CUMPLE ☐ NO CUMPLE ☐

Atentamente,

_____ _____

Nombre Representante Legal Firma del Representante Legal

C.C. No._____ Expedida en:_____