Corporación Viva la Ciudadanía
Términos de Referencia
Plan informático

1. Presentación de la organización

La Corporación Viva La Ciudadanía es un acuerdo programático de ocho ONG que realiza actividades tendientes a la incidencia política, la profundización de la democracia, la construcción del Estado Social y Democrático de Derecho, la construcción de una ciudadanía de "alta intensidad" y la defensa de derechos. Se destaca por:

- La defensa de los derechos de las víctimas del conflicto armado interno y la incidencia para incorporar el Enfoque Basado en Derechos Humanos en las políticas públicas.
- El desarrollo de metodologías de comunicación pública que logran la movilización social frente a diversos temas como la paz, los derechos humanos y la democracia.
- Las Escuelas de Liderazgo Democrático que es un proceso pedagógico de líderes y lideresas para conducir procesos de participación y empoderamiento ciudadano.
- La incidencia y deliberación sobre participación política y ciudadana, democracia local, planeación y presupuestación participativa.
- La participación en diversos procesos locales, regionales y nacionales de construcción de paz.

Infraestructura tecnológica

Actualmente la Corporación cuenta con 35 usuarios: 27 en Bogotá y 8 en Medellín. La modalidad de trabajo es híbrida: los equipos van algunos días a la oficina y otros días trabajan en casa. El área financiera y contable si va todos los días a la oficina.

En la sede de Bogotá hay 40 computadores y 10 en la sede de Medellín, aproximadamente, entre portátiles, equipos de escritorio y todo en uno. En Medellín hay 2 impresoras y en Bogotá también, pero estas últimas son alquiladas. Tenemos licencias Office 365 y antivirus. Contamos con un servidor en el cual está instalado el software contable.

2. Descripción del servicio

Objetivo

Diseñar, implementar y hacer seguimiento al Plan informático de la Corporación Viva La Ciudadanía con el fin de administrar y dirigir todos los recursos y la infraestructura tecnológica.

Alcance

El Plan informático estará alineado con el plan estratégico institucional e incluirá un análisis de la situación actual y las propuestas de mejora considerando: la estructura interna, procesos, infraestructura, requerimientos legales, comunicaciones, aplicaciones y servicios a brindar, así como la definición de estrategias, riesgos, cronograma y presupuesto.

El plan debe considerar aspectos como la calidad, seguridad, confidencialidad, controles internos, propiedad intelectual, mensajería de datos, legalidad del software, entre otros, los cuales además estarán alineados con la legislación colombiana y estándares de tecnología de información.

3. Mantenimiento y control de la infraestructura tecnológica

Mantenimiento y uso adecuado de la infraestructura tecnológica de la Corporación. Los puntos para considerar son:

a) Definición de procedimientos para mantenimiento, actualizaciones o mejora de software de aplicación por planeación, por cambios a las disposiciones legales y normativas, por corrección y mejoramiento de estos o por requerimientos de los usuarios.
b) Los cambios que se realicen en los sistemas serán registrados e informados a todos los actores y usuarios finales relacionados, adjuntando las respectivas evidencias. Así mismo, se actualizarán los manuales técnicos y de usuario por cada cambio o mantenimiento que se realice, los mismos que estarán en constante difusión y publicación.
c) Se elaborará un plan de mantenimiento preventivo y/o correctivo de la infraestructura tecnológica sustentado en revisiones periódicas y monitoreo en función de las necesidades de la Corporación, estrategias de actualización de hardware y software, riesgos, evaluación de vulnerabilidades y requerimientos de seguridad.
d) Se mantendrá el control de los bienes informáticos a través de un inventario totalmente automatizado y actualizado con el detalle de las características y responsables a cargo, conciliado con los registros contables.
e) El mantenimiento de los bienes que se encuentren en garantía será proporcionado por el proveedor, sin costo adicional para la entidad.

Seguridad, integridad, confiabilidad y disponibilidad de los recursos y datos, tanto como la oportunidad de los servicios tecnológicos. Los aspectos para considerar son:

a) Revisiones periódicas para determinar si la capacidad y desempeño actual y futura de los recursos tecnológicos son suficientes para cubrir los niveles de servicio acordados con los usuarios.
b) Estandarización de la identificación, autenticación y autorización de los usuarios, así como la administración de sus cuentas.
c) Revisiones regulares de todas las cuentas de usuarios.
d) Medidas de prevención, detección y corrección que protejan a los sistemas de información y a la tecnología de la institución de software malicioso y virus informáticos. Ejecución de pruebas para encontrar vulnerabilidades en los equipos.
e) Administración de los incidentes reportados, requerimientos de servicio y solicitudes de información y de cambios que demandan los usuarios, a través de mecanismos efectivos y oportunos.
f) Administración adecuada de la información, librerías de software, respaldos y recuperación de datos y creación de inventario de activos de información.
g) Incorporación de mecanismos de seguridad aplicables a la recepción, procesamiento, almacenamiento físico y entrega de información y de mensajes sensitivos.

4. Seguridad de tecnología de información

Mecanismos de protección y salvaguarda contra pérdidas y fugas los medios físicos y la información que se procesa mediante sistemas informáticos, para ello se aplicarán al menos las siguientes medidas:

a) Ubicación adecuada y control de acceso físico en especial a las áreas de: servidores, desarrollo y bibliotecas.
b) Definición de procedimientos de obtención periódica de respaldos en función a un cronograma definido y aprobado;
c) En los casos de actualización de tecnologías de soporte se migrará la información a los medios físicos adecuados y con estándares abiertos para garantizar la perpetuidad de los datos y su recuperación;
d) Almacenamiento de respaldos con información crítica y/o sensible en lugares externos a la organización;
e) Implementación y administración de seguridades a nivel de software y hardware, que se realizará con monitoreo de seguridad, pruebas periódicas y acciones correctivas sobre las vulnerabilidades o incidentes de seguridad identificados.
f) Instalaciones físicas adecuadas que incluyan mecanismos, dispositivos y equipo especializado para monitorear y controlar fuego, mantener ambiente con temperatura y humedad controlado, energía estabilizada, control de acceso, entre otros.

5. Requisitos

- Ser persona natural o jurídica.
- Experiencia relacionada mínima de dos (2) años.
- Persona o equipo de trabajo profesional o tecnólogo en ingeniería de sistemas, telemática, informática, etc.

6. Propuesta

La propuesta deberá incluir como mínimo:

- Presentación de la empresa natural o jurídica y experiencia
- Metodología, criterios y enfoque propuesto
- Perfil detallado del equipo de trabajo
- Cronograma de trabajo previsto
- Honorarios propuestos incluido IVA
- Información de contacto

Se recibirán propuestas hasta el 25 de marzo de 2022 a los siguientes correos: maisabel.contento@viva.org.co y asistenteadministrativa@viva.org.co

7. Contratación y forma de pago

Se realizará un contrato por prestación de servicios cuyo valor incluye los respectivos descuentos de ley. Los pagos serán acordados entre las partes.

La contratación se realizará teniendo en cuenta la selección de la mejor propuesta bajo los siguientes criterios: experiencia, conocimiento, precio y cumplimiento.

8. Plazo

El contrato de prestación del servicio se realizará por un año, prorrogable a consideración de las partes.

9. Cláusulas especiales

- **Compromiso de buen uso de la información**: Todos los datos, informes, productos, incluyendo los borradores, a que tengan acceso, son propiedad exclusiva de la Corporación
  Se prohíbe la reproducción o publicación total o parcial

- **Confidencialidad**: Las Partes se comprometen a proteger la confidencialidad y a no divulgar, revelar o utilizar cualquier documento, dato, información, proceso, material a que tenga acceso durante la vigencia de este contrato o por el período que consideren prudente las organizaciones contratantes, después de terminado el contrato.

- **Fraude**: Las partes acuerdan, que en caso de que en la oferta o ejecución del contrato una de las partes comete dolo, fraude o engaño referente a lo procurado o pactado, dicha acción dará lugar a la rescisión del contrato con la sola responsabilidad de la parte que induce, comete o ejecuta la acción dolosa o fraudulenta.