ANEXO – ESPECIFICACIONES DE REQUERIMIENTOS DE SEGURIDAD

	Requerimiento / Funcionalidad
1	Los trabajos que se realicen para el servicio deberán brindarse sin problemas en un entorno seguro para software (que contenga al menos antivirus) y hardware (en servidores con puertos y servicios limitados)
2	El proveedor debe presentar documentación técnica, en cuanto al procesamiento de los datos (lugar donde se almacenan, métodos de cifrado, diagramas entidad relación, interrelación del software con otros sistemas, proceso de respaldo y restauración -si existiera esa funcionalidad en el sistema, puede considerarse a la importación/exportación como parte del proceso de respaldos); tanto en la implementación como los desarrollos a realizarse.
3	El proveedor deberá presentar los parámetros técnicos que garanticen la capacidad de funcionamiento de la arquitectura y metodología a implementarse. Adicionalmente la documentación sobre los planes de ejecución, mantenimiento y pruebas para asegurar la continuidad de la operación de los aplicativos/funcionalidades implementadas.
4	El proveedor debe entregará documentación para el manejo de incidentes, que pueden presentarse durante el tiempo de ejecución de las aplicaciones implantadas en el servicio y se deberá establecer reuniones para su revisión. Adicionalmente los parámetros sobre los cuales se debe realizar el monitoreo del desempeño del software.
5	El proveedor deberá incluir documentación técnica sobre los registros de auditoría y registros de uso, que forman parte del sistema. Esta documentación deberá guardar completa relación con la versión y funcionalidades del software entragado a la Corporación. El proveedor deberá garantizar el acceso a los registros de auditoría y de uso del sistema/aplicación.
6	El proveedor deberá incluir metodología de gestión de cambios (de hardware, software) que se deberá utilizar para la arquitectura y metodología de trabajo implementado.
7	El proveedor deberá indicar en su oferta la metodología de análisis de capacidad futura e indicar el crecimiento en recursos aproximado que deberá ser contemplado por la corporación durante el primer año de operación.
8	El proveedor entregará toda la documentación necesaria para recuperarse, en el caso de un desastre (instación desde cero, instalación de parches, personalizaciones del caso, recuperar la información) de un desastre en la operatividad de hardware o software de la arquitectura y los desarrollos implementados)
9	El proveedor deberá incluir documentación técnica sobre el uso, administración y auditoría del software implementado.
10	Antes de la implementación se deberá contar con un informe de necesidades de capacidad y escalabilidad. Se deberá incluir en el mismo, proyecciones de capacidad futura (por lo menos para 5 años)
11	El proveedor deberá incluir instrucciones claras sobre la manera de dar tratamiento a errores o condiciones de excepción que se presenten en las aplicaciones implementadas por el servicio (se debe incluir mecanismo de contacto, preguntas frecuentes, base de conocimientos)
12	El proveedor entregará documentación técnica clara que contenga el procedimiento de reinicio y recuperación de los servicios implementados en caso de fallas. Los procedimientos de esta documentación deberán ser probados como parte de la recepción del servicio de implementación.
13	Las aplicaciones que se implementarán deberán permitir la segregación de funciones y contar con los roles y perfiles definidos, por funciones.
14	Las aplicaciones implementadas deberán permitir limitar el acceso de modificación de la información conforme a los perfiles definidos.

15	Las aplicaciones implementadas deberán contar con la funcionalidad para mantener registros de auditoría y registros de uso de todas sus funciones y registros por cada transacción ejecutada. Las mismas que podrán ser activadas o desactivadas acorde a las necesidades.
16	Las aplicaciones implementadas deberán permitir la activación de usuarios por jornadas de trabajo (es decir, permitir o no el acceso a usuarios conforme a un horario definido)
17	El software deberá ser implementado en, al menos, tres de los siguientes ambientes: capacitación, pruebas, desarrollo y producción.
18	El software deberá tener sistemas de autenticación independientes para cada ambiente de procesamiento.
19	El software deberá permitir la creación de perfiles de usuario, independientes para cada ambiente de procesamiento.
20	El proveedor tendrá acceso al ambiente de producción solamente durante la etapa de implementación y en la etapa de operación-mantenimiento, se otorgará acceso temporal controlado en caso de requerir soporte.
21	El proveedor entregará toda la documentación necesaria para implementar desde cero los aplicativos instalados los parches y personalizaciones del caso, recuperar la información y ponerlo en operación nuevamente en caso de un desastre.
22	El proveedor deberá garantizar el funcionamiento de las aplicaciones implementadas tomando en cuenta que CELEC EP mantendrá siempre operativo el antivirus y sus definiciones actualizadas. El servicio incluirá actualizaciones de las aplicaciones implementadas y parches.
23	Las aplicaciones implementadas deberán transmitir los datos usando protocolos seguros.
24	El proveedor deberá garantizar que la documentación de las aplicaciones implementadas esté expuesta en la red pública tiene una protección adecuada (control de accesos, controles de integridad de la información, asegurar su disponibilidad).
25	Los clientes de correos electrónicos usados en las aplicaciones implementadas, deberá permitir el uso de firmas electrónicas.
26	El proveedor deberá presentar como parte de los informes de implementación y entrega de aplicaciones implementadas un análisis de vulnerabilidades que garanticen que éste no tiene agujeros de seguridad conocidos. Adicionalmente el análisis de calidad del código fuente basado en modelos de la calidad de software
27	Las aplicaciones implementadas deberán permitir identificar las cuentas activas, inactivas, y bloqueadas.
28	Las transacciones de los aplicativos implementados deberán realizarse en un entorno fuera del acceso público.
29	Las aplicaciones implementadas deberán registrar los accesos autorizados y no autorizados, incluyendo: • Identificación del ID de usuario; • Fecha y hora de eventos clave; • Tipos de evento; • Acción realizada
30	Las aplicaciones implementadas deberán registrar y monitorear las operaciones privilegiadas, como: • Uso de cuentas privilegiadas; • Encendido y detección del sistema;
31	Las aplicaciones implementadas deberán registrar y monitorear intentos de acceso no autorizados, como: • Acciones de usuario fallidas o rechazadas;

32	Las aplicaciones implementadas deberán registrar y revisar alertas o fallas del sistema, como: • Alertas y/o mensajes de consola; • Excepciones de registro del sistema; • Alarmas del sistema de control de acceso;
33	Las aplicaciones implementadas deberán registrar cambios o intentos de cambio en la configuración y los controles de la seguridad que tenga.
34	Las aplicaciones implementadas deberán emitir alarmas con respecto al control de accesos (p.e. accesos no autorizados, intentos de acceso fallidos repetidos, entre otros) y enviar en tiempo real al adminsitrador, de ser posible tecnológicamente.
35	El software deberá permitir la configuración del formato de fecha y hora.
36	Las aplicaciones implementadas deberán integrarse al directorio activo de la Corporación para el manejo de usuarios
37	Las aplicaciones implementadas deberán garantizar que: - La identificación de usuario es única. - Las actividades de usuario regular no se hacen mediante cuentas privilegiadas - Se permite un máximo de intentos para inicio de sesión (máximo 3) - No existen contraseñas ni usuarios quemados en el código fuente. El proveedor del software deberá garantizar que se eliminan los usuarios ""por defecto"" cuando termine la implementación, para ello entregará documentación técnica donde consten esos usuarios por defecto y sus contraseñas. El software deberá bloquear una sesión cuando: - Se introduce más de 3 veces seguidas la contraseña erronea. - La cuenta no ha sido usada (inactiva) por más de 60 días sin justificación.
38	El software deberá manejar algoritmos de cifrado reconocidos.