**ANEXO No. 1**

**ESPECIFICACIONES TÉCNICAS**

El proponente acepta y garantiza, con la presentación de la propuesta, y la suscripción del anexo 2 – *carta de presentación de la propuesta*, que cumple, acepta y garantiza a la Cámara de Comercio de Bogotá, CCB, el cumplimiento de todas las características técnicas aquí descritas.

**Objeto:** Instalación, configuración, implementación, migración y conversión de imágenes, integración, capacitación, garantía, soporte y el licenciamiento de un software de gestión documental.

| Elemento | Descripción | Aclaraciones |
|---|---|---|
| Instancias | 3 instancias independientes:<br>1) Servicios Registrales<br>2) Centro de Arbitraje y Conciliación<br>3) Gestión Interna (Transversal a toda la Entidad) | |
| Ambientes | Para cada una de las instancias solicitadas se deben implementar 4 ambientes:<br>1) Desarrollo,<br>2) Pruebas<br>3) Preproducción<br>4) Producción. | |
| Despliegue y Licencias | Se debe cotizar 1 modelo obligatorio y 1 opcional:<br>• Licenciamiento a perpetuidad: Costo inicial y costo de mantenimiento anual, ó suscripción anual; para todos los ambientes (obligatorio). El mantenimiento debe incluir actualizaciones durante los tres (3) años siguientes a partir del despliegue de la solución.<br>• Servicio en la nube: Costo mensual de alquiler de la licencia y la plataforma para todos los ambientes. (opcional) | Para la calificación se tendrá en cuenta el costo total de propiedad a 3 años (TCO) de ambas opciones.<br><br>Para el modelo obligatorio se debe incluir dentro de la solución propuesta un presupuesto del costo de la infraestructura como servicio requerido para soportar los requerimientos incluidos en este pliego. |
| Número de Usuarios | La solución será utilizada por 500 usuarios para lectura/escritura, en donde la concurrencia oscila entre el 40% y 50%. La solución será utilizada por un número ilimitado de usuarios para consulta. | El número de usuarios para cada una de las instancias se encuentra distribuido de la siguiente forma:<br>• Servicios Registrales: 300 usuarios<br>• Centro de arbitraje y conciliación: 50 usuarios<br>• Gestión Interna: 150 usuarios |
| Almacenamiento | Actualmente se tienen almacenados 2TB de información en NAS y 5TB en EMC Centera | La solución debe integrarse con la plataforma EMC Centera y se debe incluir, dentro de la solución propuesta, el costo de almacenamiento en nube. |
| Características Básicas | Son de obligatorio cumplimiento las capacidades incluidas en el Anexo 1, en particular se deben cotizar los módulos que permitan:<br><br>1. Almacenamiento Documental<br>2. Captura e Indización | Deben ser cotizadas todas las capacidades descritas. Se deben tener en cuenta las capacidades de Gestión Documental según la ley general de archivo del Archivo General de la Nación y lo dispuesto por la |

| | | |
|---|---|---|
| | 3. OCR y alimentación automática de Metadatos<br>4. Visualización de documentos (incluyendo tipos de archivo de audio, video y planos en Autocad y Visio), con capacidades de marcado, subrayado y notas.<br>5. Mecanismos de Aprovisionamiento. Se deben proveer al menos dos mecanismos: aprovisionamiento en línea, y aprovisionamiento masivo (via batch)<br>6. Parametrización commercial off the shelf (COTS), "Funcionalidad Productizada incluida en la oferta básica", de la normativa del archivo general de la nación. | Superintendencia de Industria y Comercio en la resolución 8934 de 2014 y la resolución 723 de 2015. |
| Características Adicionales (módulos opcionales) | 7. Se requieren adicionalmente los siguientes módulos:<br>8. Digitalización / Digitalización Certificada<br>9. Conectores SAP<br>10. Herramienta para la implementación de flujos personalizados<br>11. Soporte BPMN 2.0<br>12. Mecanismos de Firma digital / Electrónica<br>13. Módulo de Correspondencia integrado a la solución | Estas características (módulos opcionales) deben estar soportadas pero NO deben ser incluidas en el precio ofertado (oferta básica). Sin embargo, se solicita explícitamente proveer costo referencial para estas características.<br><br>Se debe cotizar licenciamiento, despliegue (On-Premise y IaaS), integración, soporte, capacitación y todos los servicios requeridos en línea con los lineamientos de cotización estipulados dentro de la oferta básica. |
| Instalación | Se deben proveer servicios de instalación y configuración de la herramienta para la opción de licencias a perpetuidad o suscripción anual, para las tres instancias solicitadas. La configuración de Series Documentales solo aplica para Servicios Registrales y CAC. | Alcance de la configuración:<br>Se deben configurar hasta 40 series documentales, con hasta 5 sub-series conteniendo hasta 30 tipos documentales y hasta 40 metadatos por cada tipo documental. |
| Integración | En el anexo de integración se detalla la arquitectura propuesta, así como los protocolos de integración requeridos.<br><br>Se debe proveer servicios de integración para las tres instancias solicitadas. | Se debe proveer una interfaz CMIS 1.1 para la mayoría de interacciones, y se deben contemplar servicios de integración para los casos descritos en el anexo que no |

| | | |
|---|---|---|
| | | sean cubiertos por el estándar. |
| Conversión | Se deben convertir todos los documentos existentes TIFF IV a PDF/A 1ª hasta el momento de realizar la conversión (aproximadamente 117 millones de imágenes hasta Marzo/2015). Estas imágenes están almacenadas en EMC Centera. | Se deben cotizar los servicios y herramientas necesarios para esta actividad. |
| Migración | Se debe migrar/generar la metadata de cada documento en el momento de conversión. | Se debe presentar un plan de migración que contemple un crecimiento de 75000 páginas diarias.<br><br>Los metadatos deben ser autocontenidos. |
| Soporte y Garantía | Se debe proveer soporte y operación por 1 mes después de la salida a producción. Se solicita garantía de tres (3) años a partir de la entrada en producción de la primera instancia contra fallas del producto y las personalizaciones (parametrizaciones y configuraciones) implementadas. | Durante el primer mes se deberá realizar transferencia de conocimiento sobre todos los procesos necesarios para garantizar la disponibilidad de la solución y los procedimientos de reinicio en caso de fallas. |
| Capacitación | Se deben brindar servicios de capacitación a:<br>• 15 desarrolladores<br>• 45 usuarios de negocio/facilitadores<br>Se debe incluir el temario propuesto y la intensidad horaria.<br><br>Se debe incluir y proveer el material impreso y digital de capacitación para los participantes. | La capacitación a desarrolladores se enfoca en capacidades de integración y migración (APIs, carga masiva y en línea al ECM). La de usuarios de negocio en todos los casos de uso posibles sobre la herramienta. Se debe proveer herramientas multimedia en línea de autoaprendizaje. |
| Módulo de Correspondencia | Se debe implementar el módulo de Gestión de Correspondencia de la CCB de acuerdo con la especificación funcional hecha por la entidad. | |

**Estructura de Costos**

El proveedor debe diligenciar el Anexo PROPUESTA ECONÓMICA donde se detalla el costo total de la oferta.

El proveedor puede ofrecer un esquema de licenciamiento perpetuo con sus respectivos contratos de soporte para los años 2 y 3 (ítems 1, 2 y 3) o por suscripción (ítem 4), solo uno de los dos. En caso de ser por Suscripción, debe indicar el costo total de la suscripción por tres (3) años.

El proveedor debe incluir en su oferta la Infraestructura de hardware que soporta la solución On-Premise instalada y configurada. Opcionalmente puede ofrecer Infraestructura como

servicio (Iaas) en caso de estar en capacidad de proveerla e indicar el costo por tres (3) años.

A continuación se detallan los requerimientos descritos.

**a. Herramienta**

i. Requerimientos Funcionales

La herramienta debe cumplir con los requerimientos mínimos indicados en el Anexo Requerimientos Mínimos ECM que se adjunta, para lo cual el proveedor deberá responder a cada requerimiento el cumplimiento respectivo.

Además se requiere:

1. Cumplir con los requisitos definidos por las buenas prácticas para herramientas de gestión documental establecidos en la norma ISO 16175, el modelo de requisitos para gestión de documentos electrónicos (MoReq) y por los requisitos vigentes aplicables para aplicaciones de gestión documental definidos por el Archivo General de la Nación, el Ministerio de las Tecnologías de la Información y las Comunicaciones y la SIC.-

2. Los requerimientos funcionales se presentan detallados en el anexo técnico de esta solicitud y fundamentalmente están enfocados a soportar el siguiente modelo funcional de alto nivel: La creación o captura de documentos, el mantenimiento durante todas las fases del ciclo de vida de documentos, su difusión y consulta, la administración de la herramienta de gestión documental y la implementación de las políticas, procedimientos, codificación, cuadros de clasificación y tablas de retención documental.

3. Gestión ciclo de vida del documento

4. Captura o creación (Digitalización no incluida). Creación de documentos en los contextos definidos (Formatos, orígenes), con la estructura de acuerdo con las clasificaciones establecidas y con su contenido original.

5. Mantenimiento. Gestión para que los documentos sean fiables y auténticos, con la implementación de los controles y la seguridad definida. Debe permitir la implementación de la trazabilidad y audibilidad necesaria de acuerdo con la clasificación de los documentos.

6. Visualización. Proveer un conjunto de funcionalidades que permitan la búsqueda, la recuperación, presentación de un documento durante todo su ciclo de vida y reproducción por mecanismos de impresión.

7. Administración de usuarios y perfiles. Facilitar la Integración Directorio Activo, administrar los niveles de acceso, mantenimiento de grupos de usuarios.

8. Administración de Políticas: Implementar y configurar la metadata de los documentos, las políticas de mantenimiento por los tiempos establecidos, las clasificaciones y reclasificaciones de los documentos, los procedimientos de reasignación.

9. Gestión de Procesos (no incluido pero soportado). La solución debe tener integrada nativamente una herramienta de modelamiento de proceso y permitir su ejecución integrándose con las funcionalidades disponibles en el ciclo de vida de un documento.

Así mismo, debe permitir la integración con flujos de trabajo existentes en otras herramientas o soluciones.

ii. Requerimientos No Funcionales

1. La solución ofrecida debe proveer una arquitectura que permita operar con las características necesarias para un sistema de misión crítica como lo es la gestión documental para la entidad. En particular se deben cumplir los requerimientos de:

2. Escalabilidad: Capacidad de soportar un aumento de carga en pico y/o sostenido debido a condiciones coyunturales o de negocio (tanto en usuarios como en número y complejidad de transacciones), de manera que la adición de recursos necesarios como memoria, procesador o ancho de banda no sea un proceso traumático ni oneroso. La solución deberá garantizar escalabilidad en repositorios únicos de información, es decir, la escalabilidad de la solución no debe depender del volumen de datos o del tamaño del almacenamiento físico.

3. Disponibilidad: Capacidad de mantener la operación y acceso de los servicios ofrecidos por la plataforma con periodos de indisponibilidad no programada iniciales de 0,1 y hasta 0,001 % (de 99,9% a 99,999% de disponibilidad)

4. Seguridad: La solución debe proveer niveles de seguridad acordes con estándares internacionales que permitan la protección de la información, su confidencialidad e integridad, así como impedir los ataques conocidos tanto internos como externos. La solución debe ofrecer la posibilidad de administrar las claves de cifrado por parte del usuario.

5. Interoperabilidad (Integración): Al convertirse en la herramienta transversal de soporte documental, la solución debe estar en capacidad de integrarse al core del negocio mediante estándares de interoperabilidad como Web Services y RESTful services. Se tendrá en cuenta también el conjunto de conectores a herramientas conocidas de uso en la entidad, como SAP. El estándar CMIS 1.1 será la base de integración.

6. Despliegue (Nube, On-Premise): Es fundamental que la herramienta permita ser instalada On-Premise y en nube (IaaS), así como opcionalmente poseer ofertas de plataforma como servicio (PaaS). En este sentido, la solución debe estar optimizada para garantizar una integración, con el core del negocio, flexible y eficiente en consumo de recursos de red, así como tolerante a la latencia.

7. Usabilidad: El sistema debe estar en capacidad de presentar al usuario una interfaz probada, consistente y que siga estándares de facilidad de uso.

8. Extensibilidad: La solución debe poder adaptarse a los cambios en los requerimientos funcionales que sean necesarios por las definiciones de negocio, ya sea a través de parametrización o extensión de funcionalidad mediante servicios y APIs.

9. Capacidad – Dimensionamiento: Inicialmente la solución debe proveerse para un estimado de 400 usuarios, y sin embargo es importante considerar una oferta competitiva de licenciamiento que permita el acceso masivo de usuarios públicos, con potencial en los ciudadanos Colombianos.

10. Rendimiento – La CCB podrá solicitar una prueba de concepto para medir la capacidad de rendimiento y estabilidad de la solución en caso de ser necesario antes de realizar la contratación.

11. El cumplimiento de normatividad archivística se validará con una visita a un cliente que tenga el producto ofrecido en producción.

**b. Servicios**

**TODOS LOS SERVICIOS PROFESIONALES DEBEN SER OFRECIDOS DIRECTAMENTE POR EL FABRICANTE DE LA SOLUCION O TRAVES DE UN CANAL CERTIFICADO QUE GARANTICE EXPERIENCIA COMPROBADA EN LA ENTREGA DE SERVICIOS.**

Instalación. –La solución a contratar deberá ser debidamente instalada por el fabricante. La CCB dispondrá de la Infraestructura necesaria para la instalación de la solución en los diferentes ambientes.

Parametrización y Configuración. –El proceso de parametrización y configuración de la solución deberá obedecer a las mejores prácticas que garanticen el buen desempeño, pero además al cumplimiento normativo que la Cámara dispondrá a través de su política y directrices definidas más adelante. Se deberá incluir en este ítem además, todos los procesos para respaldar y restaurar la información en caso de ser necesario. La solución deberá ser configurada para que además de guardar documentos electrónicos en nube, también permita guardar dichos documentos electrónicos On-Premise, inclusive en soluciones de almacenamiento de contenido fijo, EMC CENTERA. Se deben parametrizar y configurar las TRD de Servicios Registrales y el CAC, cada una de ellas con entre 15 y 20 series documentales, cada serie puede tener de 2 a 5 sub-series y cada sub-serie puede tener de 20 a 30 tipos documentales. El número de metadatos por tipo documental oscila entre 30 y 40.

Operación y Mantenimiento (1 mes). –El proveedor deberá realizar la operación y el mantenimiento de la solución durante el período de un (1) mes contado a partir de la entrada en el ambiente Productivo de la primera instancia (Registros Públicos). Durante este período deberá realizar transferencia de conocimiento sobre todos los procesos necesarios para garantizar la disponibilidad de la solución y los procedimientos de reinicio en caso de fallas que conlleven a la salida de Producción.

Esfuerzos de integración. Se anexa el documento de integraciones en donde se detallan las diferentes funcionalidades a integrar así como los protocolos que deben soportarse. Se solicitará certificación del proveedor indenova sobre la integración con la plataforma eSigna, para todos los servicios implementados actualmente sobre la herramienta.

Conversión y Migración - El proveedor seleccionado deberá realizar todo el proceso de conversión del archivo (imágenes en formato .TIFF IV) que hoy se encuentra almacenado en el sistema EMC CENTERA, junto con su metada la cual se encuentra en las bases de datos DB2 y Microsoft SQL SERVER, al formato PDF/A 1a. A continuación se presentan las cifras de la información que debe ser migrada, teniendo en cuenta que esta información tiene un crecimiento diario. En la migración se debe diagnosticar y garantizar la integridad de las imágenes origen y presentar un reporte.

Distribución porcentual del crecimiento de 75.000 páginas diarias

Volumetría de cantidad de páginas por instancia:

| Instancia | Cantidad de Paginas Abril 2015 | Cantidad de Documentos Abril 2015 | Cantidad de Paginas Junio 2015 | Cantidad de Documentos Junio 2015 | Crecimiento Bimensual Paginas (Abril a junio de 2015) | Crecimiento Bimensual Documentos (Abril a junio de 2015) |
|---|---|---|---|---|---|---|
| **CAC** | 5.416.006 | 322.997 | 5.589.317 | 326.118 | 3% | 1% |
| **G. Interna** | 2.513.149 | 880.440 | 2.682.940 | 1.005.555 | 6% | 12% |
| **Registros** | 112.621.780 | 16.445.383 | 116.079.621 | 16.875.452 | 3% | 3% |
| **Total** | **120.550.935** | **17.648.820** | **124.351.878** | **18.207.125** | **3%** | **3%** |

Soporte (ANS: Acuerdos de Nivel de Servicio).- El proveedor deberá prestar servicio de soporte técnico ante eventuales fallas en la modalidad 7x24. Para tal efecto deberá especificar una línea telefónica a la cual la CCB se comunicará para reportar el incidente. Así mismo es necesario presentar las modalidades de prestación de este servicio con sus correspondientes ANS, y la categorización de las fallas. El proveedor deberá estar en disposición de prestar el soporte de forma remota o en sitio, dependiendo de la severidad lo cual deberá especificar en la propuesta.
La solución debe contar con soporte local en Bogotá.

**ESQUEMA DE SOPORTE**

Categorización de incidencias:

- **Trivial:** Problema de visualización.
- **Leve**: Mínima pérdida de funcionalidad.
- **Grave:** Gran pérdida de funcionalidad que no implica afectación a usuarios externos.
- **Crítico:** Caídas, pérdidas de datos o comportamiento anormal grave de la aplicación, que impliquen la imposibilidad de atender un proceso que afecte a usuarios externos de la Cámara de Comercio.

Estado de los incidentes:

- **Abierta:** Cuando la incidencia es reportada por la CCB.
- **Asignada**: Cuando la incidencia es tomada por un funcionario del proveedor para su gestión.
- **En Resolución**: Cuando ha sido diagnosticada la causa de la incidencia y se procede a su corrección.

- **Resuelta**: Cuando se ha corregido la incidencia.
- **Cerrada**: Cuando la CCB ha validado que la incidencia se corrigió satisfactoriamente.

Acuerdo de Nivel de Servicio:

- **Entre Abierta y Asignada**:
  - Crítica: 30 minutos
  - Otros: 2 horas
- **Entre Asignada y En Resolución**
  - Crítica: 30 minutos
  - Otros: 12 horas
- **Entre En Resolución y Resuelta**
  - Crítica: 1 hora[1]
  - Otros: 36 horas

Garantía.- Se solicita garantía de tres (3) años contra fallas del producto y las personalizaciones (parametrizaciones y configuraciones) implementadas.

Capacitación.- El proveedor deberá realizar transferencia de conocimiento así:

i. Para el grupo de Desarrolladores.- Se indicarán las prácticas para abordar nuevas integraciones

ii. Para el grupo de usuarios finales.- Se enseñará la utilización de todas las opciones asociadas al ciclo de vida del documento desde el momento en que pasa del papel al medio electrónico hasta la fase de archivo y conservación.

[1] Para estas incidencias, se entiende que la solución que se dará permitirá desbloquear el trabajo que no se pueda ejecutar, aunque la resolución definitiva pueda llegar a requerir actuaciones de la plataforma.

**CUMPLIMIENTO DE REQUISITOS PARA LA SELECCIÓN DE SOFTWARE DE GESTION DOCUMENTAL**

| | REQUISITO | Descripción-El sistema permite… |
|---|---|---|
| 1 | ESTRUCTURA DE CLASIFICACION | Permite el uso de una estructura de clasificación de la información |
| 2 | | Permite la definición de una estructura de clasificación de la información en el que los documentos se puedan representar en jerarquías como mínimo en tres niveles |
| 3 | | Permite restringir el número de niveles de la estructura de clasificación de la información |
| 4 | | Permite definir mecanismos de asignación de nombres a los diferentes niveles de la estructura de clasificación de la información |
| 5 | | Permite que los usuarios administradores o quienes tengan asignados los permisos correspondientes, puedan crear nuevos niveles dentro de la estructura de clasificación |
| 6 | | Posee una interfaz gráfica que permita la navegación de los documentos y de la estructura de clasificación de la información |
| 7 | | Posee una interfaz gráfica que permita la selección, recuperación y presentación de los documentos y sus contenidos por medio del mecanismo descrito |
| 8 | | Permite la definición y uso simultáneo de varios sistemas de clasificación de la información (estructura de carpetas, estructura de categorias, thesauros, navegación por palabras clave, entre otros) |
| 9 | | Permite la reubicación de una carpeta (o conjunto de carpetas) o documento, a un lugar distinto dentro de la estructura de clasificación |
| 10 | | Permite luego de la reubicación garantizar que se mantegan los metadatos y demás atributos (permisos) |
| 11 | | Permite a los usuarios administradores, trasladar partes de la estructura de clasificación |
| 12 | | Permite registrarse en la pista de auditoría, cuando se realice la reubicación de una carpeta (o conjunto de carpetas) o documento |
| 13 | | Permite el registro de las razones por las que se realiza la reubicación de cualquier elemento de la estructura de clasificación y almacenarlo como una propiedad o metadato |
| 14 | | Permite evitar la eliminación de carpetas o documentos, a menos que se trate del creador del mismo o del usuario administrador |
| 15 | | Permite que un documento pueda estar ubicado en diferentes partes de la estructura de clasificación, sin que esto signifique la duplicación del documento |
| 16 | Requerimientos de Metadatos | Permite imponer limitación sobre el número de metadatos estimados sobre los documentos, carpetas o subcarpetas |

| | | |
|---|---|---|
| **17** | | Permite en la configuración del sistema que se definan varios conjuntos de elementos de metadatos adecuados para los distintos niveles dentro de la estructura de clasificación |
| **18** | | Permite que el administrador en el momento de la configuración, decida, cuáles de los elementos de los metadatos son obligatorios y cuáles opcionales, así como los que podrán ser objeto de búsqueda |
| **19** | | Permite el formato Alfabético de elementos de metadatos |
| **20** | | Permite el formato Alfanumérico de elementos de metadatos |
| **21** | | Permite el formato Numérico de elementos de metadatos |
| **22** | | Permite el formato de Fecha de elementos de metadatos |
| **23** | | Permite el formato Lógico (Si/No, Verdadero/falso) de elementos de metadatos |
| **24** | | Permite estructuras de metadatos normalizados para la Gestión de Información/Gestión Documental tales como Dublin Core[1] |
| **25** | | Permite estructuras de metadatos normalizados para la Gestión de Información/Gestión Documental tales como ISAD (G)[2] |
| **26** | | Permite estructuras de metadatos normalizados para la Gestión de Información/Gestión Documental tales como ISDIAH[3] |
| **27** | | Permite la extracción automática de metadatos de los documentos al momento de la captura o cargue al sistema |
| **28** | | Permite que el administrador defina qué elementos de los metadatos se pueden introducir y mantener mediante la entrada de datos desde el teclado y cuáles se escogerán de una lista desplegable |
| **29** | | Permite que los metadatos se asignen o hereden automáticamente a los niveles inferiores de una determinada carpeta y/o subcarpeta .Esta funcionalidad podrá ser activada/desactivada por el administrador en caso de ser necesario. |
| **30** | | Permite obtener los valores de los metadatos a partir de tablas de referencias y/o de llamadas a otras aplicaciones de software |
| **31** | | Permite la validación de los elementos de los metadatos mediante algoritmos de verificación de dígitos |
| **32** | | Permite que cualquier elemento de metadatos se pueda utilizar como campo en una búsqueda no estructurada (por ejemplo, una búsqueda de texto libre) |
| **33** | | Siempre que un elemento de un metadato se almacene en formato de fecha, el sistema permite realizar búsquedas que reconozcan el valor de la fecha |
| **34** | | Siempre que un elemento de un metadato se almacene en formato numérico, el sistema permite realizar búsquedas que reconozcan el valor del número |
| **35** | | Siempre que un elemento de un metadato se almacene en formato alfanumérico, el sistema permite realizar búsquedas que reconozcan el valor alfanumérico |

| | | |
|---|---|---|
| **36** | | Siempre que un elemento de un metadato se almacene en formato alfabético, el sistema permite realizar búsquedas que reconozcan el valor alfabético |
| **37** | | Permite restringir la capacidad de realizar modificaciones en los valores de los metadatos |
| **38** | | Permite adquirir metadatos, creados por el software que crea el documento |
| **39** | | Permite adquirir metadatos, creados por el usuario, en el momento del cargue del documento al sistema |
| **40** | | Permite adquirir metadatos, creados por otros sistemas o aplicaciones con las que el documento esté ligado |
| **41** | | El sistema debe permitir la creación de metadatos por agrupaciones exigidas por la ISO 23081 y la Guía de expediente electrónico de Gobierno en Línea para su diligenciamiento a nivel de expediente y tipo documental. |
| **42** | | El sistema debe permitir la creación, al menos, los siguientes formatos de elementos de metadatos: alfabético; alfanumérico; numérico; de fecha; lógico (esto es, SÍ/NO, VERDADERO/FALSO). |
| **43** | | Debe permitir agregar dinámicamente a cada expediente electrónico, metadatos personalizados propios del negocio. |
| **44** | | El sistema debe validar y controlar la entrada de los metadatos mínimos obligatorios. |
| **45** | Carpetas y Documentos | Permite soportar metadatos para las carpetas y los documentos organizados en la estructura de clasificación |
| **46** | | Permite la asignación de un número de referencia, numérico o alfanúmerico para las carpetas y/o documentos y que sea el identificador único de la carpeta o documento dentro del sistema |
| **47** | | Permite manejar un mecanismo que asigne texto como título a las carpetas y/o documentos |
| **48** | | Permite grabar la fecha de creación de una carpeta o documento (en cualquier parte de la estructura de clasificación) e incluirla en los metadatos del mismo. |
| **49** | | Siempre que se cree una carpeta o documento, Permite incluir de forma automática en los metadatos los atributos relacionados con la posición de la carpeta o documento dentro de la estructura de clasificación |
| **50** | | Debe permitir al administrador o usuarios con privilegios en el sistema crear expedientes en el sistema. |
| **51** | | Los expedientes electrónicos deben crearse vinculando la TRD de la dependencia que lo va a gestionar. La TRD debe establecer la disposición final del expediente. |
| **52** | | El expediente electrónico debe permitir elegir un usuario responsable de su gestión y un título del mismo. |
| **53** | | Los expedientes del sistema deben tener vinculado tipos documentales obligatorios y opcionales para cargar. |
| **54** | | El sistema debe asignar un número de identificación único para el expediente, cuyo número debe ser parametrizable por el administrador del sistema. |

| | | | |
|---|---|---|---|
| 55 | | | El sistema debe permitir parametrizar el tiempo de vencimiento de los préstamos documentales. |
| 56 | | | El sistema debe ofrecer una funcionalidad que permita solicitar el préstamo de expedientes. |
| 57 | | | El sistema debe permitir aceptar o rechazar el préstamo. |
| 58 | | | E sistema debe controlar la devolución del préstamo. |
| 59 | | | El sistema debe registrar en el histórico del expediente el registro de la operación en torno al proceso de préstamo documental. |
| 60 | | | Permite controlar las ubicaciones fisicas de los expedientes, con metadatos tales como estante, cara, entrepaño etc |
| 61 | Controles y Seguridad | Acceso | Permite que el administrador restrinja el acceso a carpetas, documentos y metadatos a determinados usuarios del sistema |
| 62 | | | Permite asociar el perfil del usuario con ciertos atributos que determinan las características, los campos de metadatos y los documentos a los que el usuario tendrá acceso |
| 63 | | | Permite vetar el acceso al sistema cuando no se aplique un mecanismo de autenticación aceptado y atribuido al perfil del usuario |
| 64 | | | Permite vetar el acceso a carpetas y/o documentos |
| 65 | | | Permite restringir el acceso a funciones como la lectura, modificación y eliminación de documentos y/o metadatos |
| 66 | | | Permite vetar el acceso después de una fecha concreta |
| 67 | | | Permite proporcionar las mismas funciones de control tanto para perfiles como para usuarios |
| 68 | | | Permite definir grupos de usuarios asociados a un conjunto de carpetas y documentos |
| 69 | | | Permite la creación de grupos de usuarios |
| 70 | | | Permite que un usuario pertenezca a más de un grupo |
| 71 | | | Permite que sólo los usuarios administradores creen usuarios, establezcan perfiles de usuario, permisos y asignar usuarios a grupos |
| 72 | | | Si un usuario lleva a cabo una búsqueda de texto completo, el sistema jamás deberá incluir en los resultados carpetas o documentos a los que el usuario no tenga derecho a acceder. El sistema permite realizar este bloqueo |
| 73 | | | Registrar todos los accesos. |
| 74 | | Pista de auditoría | Permite mantener una pista de auditoría inalterable, capaz de capturar y almacenar de forma automática los datos sobre todas las acciones relacionadas con los documentos y la estructura de clasificación |
| 75 | | | Permite mantener una pista de auditoría inalterable, capaz de capturar y almacenar de forma automática los datos sobre los usuarios que inician o realizan la acción |
| 76 | | | Permite mantener una pista de auditoría inalterable, capaz de capturar y almacenar de forma automática los datos sobre la fecha y hora de la acción |

| | | | |
|---|---|---|---|
| **77** | | | Permite rastrear de forma automática y sin ninguna intervención manual todas las acciones realizadas en el sistema, y almacenar los datos sobre estas en la pista de auditoría |
| **78** | | | Permite mantener la pista de auditoría durante el tiempo necesario, que cubrirá al menos el ciclo de vida de los documentos a los que hace referencia |
| **79** | | | Permite incluir en la pista de auditoría, todas las acciones que afecten a grupos de documentos, documentos individuales, carpetas y subcarpetas, estructura de clasificación y metadatos de cualquiera de los elementos anteriores |
| **80** | | | Permite capturar y almacenar en la pista de auditoría datos sobre fecha y hora del cargue del documento |
| **81** | | | Permite capturar y almacenar en la pista de auditoría datos sobre la reclasificación de los documentos en otro nivel de la estructura de clasificación |
| **82** | | | Permite capturar y almacenar en la pista de auditoría datos sobre cualquier modificación a los metadatos de la estructura de clasificación, carpetas, subcarpetas y documentos |
| **83** | | | Permite capturar y almacenar en la pista de auditoría datos sobre la fecha y la hora de creación, modificación y eliminación de metadatos |
| **84** | | | Permite capturar y almacenar en la pista de auditoría datos sobre los cambios realizados en los privilegios y permisos que se le asignan a los usuarios sobre la estructura de clasificación y los documento |
| **85** | | | Permite capturar y almacenar en la pista de auditoría datos sobre la eliminación de carpetas o documentos. |
| **86** | | | Permite exportar la pista de auditoría a medios externos al sistema, sin que esto repercuta en la pista almacenada en el sistema |
| **87** | | | Permite hacer reportes e informes de las acciones sobre la estructura documental, carpetas y documentos |
| **88** | | | Permite hacer los reportes e informes mencionados en el item anterior permitiendo su organización por fechas o secuencias cronológicas, usuarios y elemento sobre el que se realizó la acción |
| **89** | | Copias de Seguridad y Recuperación | Permite contar con procedimientos automáticos para copias de seguridad y restauración encaminados a realizar copias periódicas de seguridad de todos elementos dentro del sistema (carpetas, documentos, metadatos, usuarios, roles, permisos, configuraciones específicas) |
| **90** | | | Permite programar rutinas de copias de seguridad en las que pueda especificar con qué frecuencia se realizará la copia de seguridad |
| **91** | | | Permite programar rutinas de copias de seguridad en las que pueda escoger los elementos o espacios específicos sobre los que se hará la copia de seguridad |
| **92** | | | Permite programar rutinas de copias de seguridad en las que pueda seleccionar un medio de almacenamiento al que se destinará la copía de seguridad. |

| | | | |
|---|---|---|---|
| **93** | | | Dado que la integridad de los datos no debe verse afectada en modo alguno por la restauración de la copia de seguridad, el sistema permite restringir al administrador la restauración de las copias de seguridad |
| **94** | | | Permite restringir al administrador la actualización de las copias de seguridad, manteniendo la plena integridad de los datos |
| **95** | | | En caso de presentarse fallas durante la restauración de las copias de seguridad, el sistema permite notificar sobre el fallo y los detalles del mismo, para que el administrador tome las decisiones necesarias para subsanar los errores |
| **96** | | | El sistema permite identificar los documentos vitales[4] |
| **97** | | | Permite la restauración de los documentos vitales y los demás en operaciones separadas |
| **98** | | Autenticidad | Permite restringir el acceso a las funciones del sistema según el perfil del usuario |
| **99** | | | Permite impedir que los usuarios o los administradores modifiquen el contenido de los documentos, excepto cuando los cambios sean completamente necesarios en desarrollo del proceso |
| **100** | TRD (Tabla de Retención Documental) | | Permite la parametrización de las TRD |
| **101** | | | Permite la actualización de las TRD |
| **102** | | | Permite la almacenar las versiones de las TRD |
| **103** | | | Permite ajustar los tiempos de retención |
| **104** | | | Permite generar alertas al aproximarse la finalización del tiempo de retención |
| **105** | | | Permite la impresión de las TRD en el formato AGN |
| **106** | | | Permite que los campos de fecha final de los registros del inventario se crucen con los tiempos de retención |
| **107** | | | Permite realizar el cálculo de los tiempos de retención por expediente y no por carpeta |
| **108** | | | Permite generar el reporte e impresión del "formato de transferencia" de documentos al archivo central |
| **109** | | | Permite generar el reporte e impresión del "acta de eliminación" de los documentos a eliminar según la TRD |
| **110** | | | Permite la interoperabilidad mencionada en el Articulo No 18 del Acuerdo 004 de 2013 del AGN |
| **111** | | | Permite la carga de diversas TRDs En linea y por lotes Permite importar y exportar TRDs |
| **112** | | | El sistema debe permitir crear tipos documentales y a estos se puedan vincular metadatos creados, tomándolos de una matriz de metadatos ordenados por categorías. |
| **113** | | | La vinculación de metadatos para un tipo documental debe ser una acción altamente usable y fácil de gestionar. |
| **114** | | | Debe permitir vincular a un tipo documental plantillas que se puedan utilizar para generar documentos en la plataforma. |
| **115** | | | Debe permitir al usuario administrador crear las relaciones para configurar la TRD a nivel se sección, subsección, serie |

| | | | |
|---|---|---|---|
| | | | subserie, tipos documentales y a estos asignar tiempos de retención. |
| **116** | | | Debe permitir al administrador del sistema generar un reporte de las secciones que se encuentran pendiente por configurar TRD. |
| **117** | | | El sistema no debe restringir la cantidad de niveles de jerarquías para crear las TRD. |
| **118** | | | El sistema debe garantizar que los documentos electrónicos de archivo que se capturen se asocien a una TRD configurada en el sistema. |
| **119** | CAPTURA | Búsqueda | Permite incluir una gama de funciones aplicables a los metadatos asociados a los diferentes niveles de la estructura de clasificación y al contenido de los documentos por medio de parámetros definidos por el usuario, a partir de los cuales se localizarán y recuperarán los documentos y/o sus metadatos, y se accederá a ellos, de forma individual o en grupo |
| **120** | | | El sistema permite la búsqueda en todos los niveles de la estructura de clasificación, a los que se tenga permiso, de documentos y sus metadatos asociados . |
| **121** | | | Permite la búsqueda de texto completo sobre los documentos almacenados en el sistema |
| **122** | | | Permite que el usuario especifique la búsqueda con combinaciones de metadatos y/o contenidos del documento buscado |
| **123** | | | Permite la búsqueda de texto libre y metadatos de forma integrada y coherente |
| **124** | | | Permite la búsqueda de metadatos usando "comodines" que permitan la expansión hacia atrás, hacia adelante e interna Por ejemplo, al buscar "proy*" el sistema debería arrojar como resultado los documentos que contegan "proyecto". Y al buscar "c*n" se obtendría "comisión" |
| **125** | | | Permite la búsqueda por proximidad, con lo cual se puede precisar la distancia entre dos palabras |
| **126** | | | Permite la búsqueda dentro de un documento, independientemente del nivel de la estructura de clasificación en el que se encuentre |
| **127** | | | Permitir la búsqueda a partir del nombre o título del documento |
| **128** | | | Permitir la búsqueda a partir del número de documento |
| **129** | | | Permite mostrar el número total de resultados de una búsqueda en la pantalla del usuario y permite que éste visualice dichos resultados o bien refine sus criterios de búsqueda y realice otra solucitud de búsqueda |
| **130** | | | Permite que en los resultados de búsqueda se presenten únicamente las carpetas y documentos a los que el usuario tiene acceso de acuerdo a los niveles de permisos definidos |
| **131** | | | Permite que las carpetas y documentos mostrados en la lista de resultados, puedan ser seleccionados y abiertos, con un clic o bien pulsando una tecla |

| | | | |
|---|---|---|---|
| 132 | | | Permitir que el usuario grabe y reutilice las búsquedas |
| 133 | | | Permite a los usuarios refinar (restringir) sus búsquedas Por ejemplo, un usuario podría iniciar una nueva búsqueda a partir de la lista de resultados de una de las búsquedas guardadas. |
| 134 | | | Permite restringir los resultados de búsqueda por intervalos de tiempo |
| 135 | | | Permite a los usuarios y administradores configurar los formatos de presentación de los resultados de las búsquedas, incluyendo características y funciones como la elección del orden en que se muestran los resultados de la búsqueda |
| 136 | | | Permite a los usuarios y administradores configurar los formatos de presentación de los resultados de las búsquedas, incluyendo características y funciones como la definición del número del resultados que se muestran en pantalla en la visualización de la búsqueda |
| 137 | | | Permite a los usuarios y administradores configurar los formatos de presentación de los resultados de las búsquedas, incluyendo características y funciones como la determinación del número máximo de resultados de una búsqueda |
| 138 | | | Permite a los usuarios y administradores configurar los formatos de presentación de los resultados de las búsquedas, incluyendo características y funciones como la grabación de los resultados de la búsqueda |
| 139 | | | Permite a los usuarios y administradores configurar los formatos de presentación de los resultados de las búsquedas, incluyendo características y funciones como la selección de los campos de metadatos que se muestran en la lista de resultados de la búsqueda |
| 140 | | | Permite ofrecer una clasificación de los resultados de la búsqueda, según su pertinencia, relevancia, fechas, nombre, autor, creador, modificador, tipo de documento, tamaño, entre otros |
| 141 | | | Permite que ninguna función de búsqueda revele jamás al usuario información como contenido o metadatos, que se le tengan restringidos por permisos de acceso |
| 142 | | | Permite búsqueda de texto completo sobre los documentos almacenados en el sistema |
| 143 | | | Permite contar con una barra de búsqueda que ubique documentos a partir de palabras o términos que se encuentren en los documentos, sus metadatos o su contenido |
| 144 | | Visualización de documentos. | Permite mostrar los documentos recuperados mediante una búsqueda, con independencia de la aplicación de software que ha generado el documento, al menos para los formatos comúnes |
| 145 | | | Permite mostrar los metadatos asociados a los documentos recuperados mediante una búsqueda |
| 146 | | | Permite la privisualización de documentos del expediente, sin que eso implique la descarga del documento |
| 147 | DIGITALIZACION | | Escanear por bandeja |

| | | | |
|---|---|---|---|
| 148 | | | Escanear por automático |
| 149 | | | Escanear cara siempre y guardar |
| 150 | | | Escanear cara doble y guardar |
| 151 | | | Herramientas de visualización (paginar, atrás, adelante, zoom…) |
| 152 | | | Eliminar paginas antes de guardar |
| 153 | | | Duplicar documentos para otros registros |
| 154 | | | No doble digitación de numero de caja |
| 155 | | | Opciones de zoom |
| 156 | | | Asociación de documentos ya digitalizados |
| 157 | | | Digitalización masiva |
| 158 | | | Importación de documentos (texto, HTML) |
| 159 | | | Importación de documentos desde carpetas compartidas |
| 160 | | | Aplicación tome funcionalidades del escáner (VRS) |
| 161 | | | Ajuste de tamaño de papel automático (La aplicación debe tomar todas las características técnicas del escáner para mejorar la digitalización) |
| 162 | | | Evidencia de digitalización(debe permitir realizar captura en serie y luego indexar para mejor tiempos de alistamiento) |
| 163 | | | El sistema debe permitir el escaneo distribuido: permitir que los usuarios remotos puedan importar documentos al sistema por escaneo directo mediante la web a través de un escáner de escritorio compatible para bajos volúmenes. |
| 164 | | | El sistema debe permitir a usuarios con privilegios el reemplazo de documentos digitalizados, que por error humano así lo requiera. Esta acción exige la debida observación. |
| 165 | ADMINISTRACION | Admón General | Permite que los administradores de forma controlada y sin ningún esfuerzo innecesario, recuperen, visualicen y reconfiguren parámetros del sistema y opciones escogidas en el momento de la configuración, como los elementos que se indexan, así como la asignación de usuarios y funciones a otros perfiles de usuarios |
| 166 | | | Permite incluir instrumentos de seguridad y características que permitan restaurar el sistema a partir de dichas copias y de la pista de auditoría, sin menoscabo de la integridad del sistema |
| 167 | | | En caso de presentarse errores del sistema, permite a los administradores "deshacer" transacciones hasta llegar a un estado en que la integridad de la base de datos quede garantizada |
| 168 | | | Permite supervisar el espacio de almacenamiento disponible y avisar a los administradores cuando convenga intervenir, ya sea por escasez de espacio, o porque sea necesario alguna otra medida de tipo administrativo |

| | | | |
|---|---|---|---|
| **169** | | | Permite que los administradores realicen cambios masivos en la estructura de clasificación, incluyendo la completa manipulación de todos los metadatos y dejando la respectiva pista de auditoría, de forma que sea posible realizar en la estructura de clasificación la división de niveles de carpetas en dos o más |
| **170** | | | Permite que los administradores realicen cambios masivos en la estructura de clasificación, incluyendo la completa manipulación de todos los metadatos y dejando la respectiva pista de auditoría, de forma que sea posible realizar en la estructura de clasificación la combinación de dos o más carpetas en una sola |
| **171** | | | Permite que los administradores realicen cambios masivos en la estructura de clasificación, incluyendo la completa manipulación de todos los metadatos y dejando la respectiva pista de auditoría, de forma que sea posible realizar en la estructura de clasificación el traslado o redenominación de una carpeta |
| **172** | | | La solución debe proveer un componente destinado a la gestión de todos los componentes del ECM. Al menos debe incluir: Gestión de Configuración (Administración del Servicio, de los Usuarios, etc), Gestión de Fallas, Gestión del Desempeño (Administración de Indicadores de Desempéño), Gestión de Seguridad. |
| **173** | | | La solución debe proveer al menos dos intefaces para la Gestión del ECM y sus componentes:<br>* Interface de comandos<br>* Interface gráfica de usuario |
| **174** | | | El módulo de Gestión del ECM debe permitir ser integrado a sistemas de gestión de orden superior (HP Open View, IBM Tivoli, Infovista, etc). La integración del módulo de gestión ECM y los sistemas de gestión de orden superior debe garantizarse a través de mecanismos de interoperabilidad estándar como SNMP, XML SOAP - REST, etc. |
| **175** | | | Permite que se definan perfiles de usuarios y que a cada perfil se le asignen varios usuarios |
| **176** | | Informes | Permite incluir instrumentos de elaboración de informes a los que pueda recurrir el administrador como la capacidad de informar sobre el número de documentos y carpetas |
| **177** | | | Permite incluir instrumentos de elaboración de informes a los que pueda recurrir el administrador como la capacidad de informar sobre las estadísticas de las transacciones con documentos y carpetas |
| **178** | | | Permite incluir instrumentos de elaboración de informes a los que pueda recurrir el administrador como la capacidad de informar sobre las actividades de cada usuario |
| **179** | | | Permite que los administradores realicen consultas y generen informes de determinadas carpetas basados en la pista de auditoría |
| **180** | | | Permite que los administradores realicen consultas y generen informes de determinados documentos basados en la pista de auditoría |

| | | | |
|---|---|---|---|
| 181 | | | Permite que los administradores realicen consultas y generen informes de determinados usuarios basados en la pista de auditoría |
| 182 | | | Permite que los administradores realicen consultas y generen informes de determinados intervalos de tiempo basados en la pista de auditoría |
| 183 | | | Permite a los administradores realizar consultas y elaborar informes sobre la pista de auditoría basados en determinadas categorías de seguridad |
| 184 | | | Permite a los administradores realizar consultas y elaborar informes sobre la pista de auditoría basados en determinados grupos de usuarios |
| 185 | | | Permite a los administradores realizar consultas y elaborar informes sobre la pista de auditoría basados en otros metadatos |
| 186 | | | Permiten clasificar y seleccionar datos de los informes |
| 187 | | | Permite que el administrador restrinja el acceso a los usuarios a determinados informes |
| 188 | | | Permite parametrizar indicadores y metas de productividad de cada proceso |
| 189 | | | Permite visualizar por gráficos tipo tacometro el cumplimiento de indicadores y sus metas en productividad en cierto momento |
| 190 | | | Permite indicar por rangos para que gráficamente muestre en qué rango se encuentra un proceso en cierto momento |
| 191 | | | Permite generar alertas cuando los indicadores esten fuera de rango de metas, enviando mensajes de correo electrónico a responsables de la gestión del proceso |
| 192 | | | permite tener un tablero de control que presenta estado del proceso, frente a indicadores y metas |
| 193 | | | Permite el registro de costo presupuestado de cada actividad de cada proceso y/o por unidad de medida (documento, imagen, recorridos) |
| 194 | | | permite el registro del costo real de cada actividad de cada proceso y/o por unidad de medida (documento, imagen, recorridos) |
| 195 | | | permite generar informe de costo acumulado presupuestado de un proceso en un periodo de tiempo |
| 196 | | | permite generar informe de costo acumulado real de un proceso en un periodo de tiempo |
| 197 | | | Permite registrar el valor cobrado a cliente de un proceso bien sea por el proceso total o por unidad de medida (documento, imagen, recorridos) |
| 198 | | | permite genera informes de comparación costo real versus costo presupuestado y/o cobrado a un cliente para cada proceso o por unidad de medida (documento, imagen, recorridos) |
| 199 | | | Permite para cada proceso configurar fecha inicio y final de los procesos |
| 200 | Otras Funcionalidades | Documentos no electrónicos | Permite configurar la productividad esperada diaria por cada proceso |
| 201 | | | Permitir visualizar en una línea de tiempo y saber el avance de los procesos programados |

| | | | |
|---|---|---|---|
| **202** | | | Permite generar alertas cuando un proceso esta incumpliendo las metas programadas |
| **203** | | | Permite definir carpetas y subcarpetas en el sistema de clasificación |
| **204** | | | Permite que la presencia de registros de documentos físicos, se refleje y se gestione del mismo modo que los documentos electrónicos |
| **205** | | | Permite que en el sistema de clasificación las carpetas y subcarpetas contengan tanto documentos electrónicos, como físicos mediante el registro de su información |
| **206** | | | Permite la administración integrada de carpetas fisicas y electrónicas de documentos Esto es carpetas o expedientes híbridos. |
| **207** | | Expedientes híbridos | Permite que los registros de los documentos físicos contengan el mismo título y código de referencia numérica que el documento electrónico, pero con la indicación de que se trata de un registro del documento físico |
| **208** | | | Permite registrar información básica de identificación de los documentos físicos, como sus fechas y ubicación física |
| **209** | | | Permite que los registros de los documentos físicos hagan parte integral de los resultados de búsquedas |
| **210** | | | Permite controlar los documentos fisicos que se han incluido a traves del ECM en expedientes electronicos |
| **211** | | | El sistema debe permitir parametrizar el tiempo de vencimiento de los préstamos documentales. |
| **212** | | | El sistema debe ofrecer una funcionalidad que permita solicitar el préstamo de expedientes. |
| **213** | | | El sistema debe permitir aceptar o rechazar el préstamo. |
| **214** | | Flujos de trabajo | El sistema debe controlar la devolución del préstamo. |
| **215** | | | El sistema debe registrar en el histórico del expediente el registro de la operación en torno al proceso de préstamo documental. |
| **216** | | | Permite controlar las ubicaciones fisicas de los expedientes, con metadatos tales como estante, cara, entrepaño etc |
| **217** | | | Permite limitar el número de pasos que componen una tarea o flujo de trabajo |
| **218** | | | El flujo de trabajo permite el uso de correo electrónico como medio de notificación de las acciones que se realizan en el flujo |
| **219** | | | Permite que los flujos de trabajo inicien o no con un documento |
| **220** | | | Permite que en los flujos de trabajo se agreguen más documentos de ser necesario |
| **221** | | | Permite que el administrador pueda definir qué usuarios podrán reasignar tareas o acciones de un flujo de trabajo y remitirlas a otros usuarios o grupos de usuarios |
| **222** | | | La función de flujos de trabajo permite consignar en la pista de auditoría todas las modificaciones realizadas sobre los documentos que se adjuntan al flujo |
| **223** | | | La función de flujos de trabajo permite consignar en la pista de auditoría todas las acciones propias del desarrollo del flujo |

| | | | |
|---|---|---|---|
| **224** | | | La función de flujos de trabajo permite incluir una función de recordatorio que avise a los usuarios las fechas de vencimiento y los detalles de cada flujo, según corresponda |
| **225** | | | La función de flujos de trabajo permite reconocer como "participantes" tanto a los individuos como a los grupos de trabajo |
| **226** | | | La funcion de flujos de trabajo permite hacer ruteo de contenido y de tareas |
| **227** | | | El acceso a los contenidos es permitido a traves de todo el sistema de flujos, no restringido a repositorios o actividades especificas excepto cuando asi sea configurado por seguridad |
| **228** | | | Permite hacer ruteo basado en un motor de reglas de negocio |
| **229** | | | Permite definir los flujos de trabajo basado en plantillas |
| **230** | | | Permite la administracion de los flujos creados en una consola unificada |
| **231** | | | Permite hacer encadenamiento e integracion de flujos |
| **232** | | | Permite el ruteo y asignacion de tareas ad hoc |
| **233** | | | Permite la creacion grafica de flujos |
| **234** | | | Permite incluir scripts para logica avanzada |
| **235** | | | Permite ruteo paralelo |
| **236** | | | Permite asignar precedencia y prioridad a las tareas del flujo |
| **237** | | | Permite cambiar la precedencia y prioridad a las tareas del flujo en ejecución |
| **238** | | | Realiza manejo de excepciones y errores |
| **239** | | | Permite detener un flujo |
| **240** | | | Permite definir limites de tiempo, escalamiento y reasignacion basado en timers |
| **241** | | | Notificacion automatica de los estados de las tareas configurable |
| **242** | | | Ejecucion del flujo programada y/o iniciada por eventos |
| **243** | | | Permite manejar grupos de flujos |
| **244** | | | Maneja una cola de trabajo de los usuarios y una lista de tareas |
| **245** | | | Monitoreo de flujos |
| **246** | | | Reportes de flujos |
| **247** | | | Soporte a firmas electronicas dentro del flujo |
| **248** | | Firmas Electrónicas y Estampado Cronológico | La función de flujos de trabajo permite asociar fechas límite a pasos o procesos individuales de cada flujo |
| **249** | | | La función de flujos de trabajo permite informar de los elementos atrasados conforme a los límites |
| **250** | | | Permite incluir instrumentos de informes exhaustivos que permitan a los gestores controlar el volúmen, los resultados y las excepciones del proceso |
| **251** | | | Permite que se incluyan metodos que garanticen la integridad de la información, como las firmas electrónicas |
| **252** | | | Permite que se incluyan metodos que garanticen la integridad de la información, como el estampado cronológico |

| | | | |
|---|---|---|---|
| 253 | | | Permite presentar una estructura que facilite la introducción de distintas tecnologías de firma electrónica |
| 254 | | | Permite verificar la validez de una firma electrónica |
| 255 | | | Permite conservar y mantener como metadatos ciertos detalles relacionados con el proceso de verificación de una firma electrónicia, tales como la prueba de verificación de la validez de la firma |
| 256 | | | Permite conservar y mantener como metadatos ciertos detalles relacionados con el proceso de verificación de una firma electrónicia, tales como la autoridad de certificación que ha validado la firma |
| 257 | | | Permite conservar y mantener como metadatos ciertos detalles relacionados con el proceso de verificación de una firma electrónicia, tales como la fecha y la hora en que se realizó la verificación |
| 258 | | | Permite contar con funciones que mantengan la integridad de los documentos dotados de firmas electrónicas (y demostrar ese mantenimiento), aun cuando un administrador haya modificado algunos de sus metadatos, pero no el contenido del documento, con posteriorirdad a la aplicación de la firma electrónica al documento en cuestión |
| 259 | | Encripción | Permite almacenar junto con los documentos electrónicos la firma o firmas asociadas a tal documento |
| 260 | | | Permite almacenar junto con los documentos electrónicos el certificado o certificados digitales que validan la firma |
| 261 | | | Permite almacenar junto con los documentos electrónicos cualquier refrendo de verificación añadido por la autoridad de certificación, de tal forma que pueda recuperarse con el registro, y sin menoscabo de la integridad de la una clave privada |
| 262 | | Inter-operabilidad | Permite encriptar los documentos y hacer imposible su consulta por fuera del sistema |
| 263 | | | Permite garantizar la captura de documentos encriptados directamente desde la aplicación de software que posea tal capacidad |
| 264 | | otros | Permite presentar una estructura que introduzca fácilmente distintas tecnologías de encripción |
| 265 | | | Permite interactuar en doble vía con otros sistemas de información de la empresa |
| 266 | | Integracion con otras aplicacines | Permite procesar transacciones en tiempo real, que sean generadas por otros sistemas externos de aplicaciones |
| 267 | | | Permite la gestión de procesos para multiples empresas |
| 268 | | | Permite modelar reportes propios según la necesidad del proceso y sin nuevos desarrollos |
| 269 | | | Se debe permitir la gestión de documentos en las diferentes aplicaciones (traslado de documentos entre aplicaciones, cambios de índices, anexo o eliminación de paginas, ..etc.) |
| 270 | | | Debe permitir la visualización y navegación sobre los diferentes aplicaciones y documentos a través de un navegador de internet. |

| | | | |
|---|---|---|---|
| **271** | Requerimientos No Funcionales | Facilidad de uso | Recuperacion de información de los índices de documentos, numero de paginas, retornar documento. |
| **272** | | | Se debe permitir realización de OCR sobre los documentos con marcaciones identificadas. |
| **273** | | | Debe permitir la marcación y categorización de las marcaciones sobre los documentos. |
| **274** | | | Tiene asistencia en línea al usuario 7/24 |
| **275** | | | Permite contar con mensajes de error claros, de forma que el usuario pueda identificar la falla y darle solución |
| **276** | | | Permite proporcionar al usuario final y al administrador en todo momento, funciones de uso fácil e intuitivo |
| **277** | | | Siempre que el sistema comprenda el uso de ventanas, permite que los usuarios las muevan y que modifiquen su tamaño y apariencia y que se guarden estas especificaciones en un perfil de usuario |
| **278** | | | Permite integrarse estrechamente con el sistema de correo electrónico de la entidad, de forma que los usuarios puedan enviar y recibir correos sin necesidad de salir del sistema |
| **279** | | | Siempre que se lleve a cabo la función anterior, permite que el sistema envíe, en lugar de copias, referencias a tales elementos de correo |
| **280** | | Rendimiento y Escalabilidad | Permite que los usuarios modifiquen o configuren la interfaz gráfica a su gusto. Con elementos de personalización sencillos, que abarquen, al menos las siguientes opciones, sin limitarse necesariamente a estas:<br>- Contenidos de los menús,<br>- Disposición de las pantallas,<br>- Uso de teclas de funciones y atajos de teclado,<br>- Colores y tamaño de las fuentes que se muestran en pantalla |
| **281** | | | Permite contar con un esquema de clasificación de la información que se presente en forma gráfica y que permita a los usuarios navegar por este de forma natural y sencilla |
| **282** | | | Incluye alguna función de ayuda sobre el uso del sistema de clasificación |
| **283** | | | Debe ofrecer tiempos de respuesta adecuados para la realización de las funciones habituales en ciertas condiciones normalizadas, como:<br>- Con el 10% de la totalidad de la población prevista de usuarios conectada y activa,<br>- Con el 100% del volúmen total previsto de documentos gestionados por el sistema,<br>- Con usuarios realizando una combinación de tipos de transacción a distintas velocidades.<br>En estas condiciones, el rendimiento se deberá mantener estable durante un mínimo de diez intentos de transacción. |
| **284** | | | Debe ser capaz de realizar una búsqueda sencilla en **3** segundos y una búsqueda compleja (combinando criterios) en máximo **5** segundos, con independencia de la capacidad de almacenamietno y el número de documentos en el sistema |

| | | | |
|---|---|---|---|
| 285 | | Disponibilidad del sistema | Permitir que una sola implementación del sistema disponga de un almacén de documentos electrónicos de al menos 15 teras o de 200 millones de documentos y que preste servicio al menos a 500 usuarios de forma simultanea. |
| 286 | | | Debe permitir la expansión controlada del sistema hasta al menos 5000 usuarios sin perjudicar la continuidad y eficacia del servicio |
| 287 | | | Debe ser escalable y no permitir ninguna característica que impida su uso en organización de pequeño o gran tamaño, con un número variable de unidades de distinto tamaño. |
| 288 | | | El sistema deberá estar disponible las 24 horas del día, 7 días de la semana, 365 días del año. |
| 289 | | | El período de inactividad previsto del sistema, no debe superar las 40 horas al año |
| 290 | | Flexibilidad | El tiempo de inactividad no prevista del sistema, no debe superar las 10 horas al trimestre. |
| 291 | | Despliegue | La disponibilidad debe ser flexible para ofertas de servicio en nube |
| 292 | | | Cuando se produzca un fallo del software o del hardware, debe resultar posible devolver el sistema a un estado conocido (más reciente que la copia de seguridad del día anterior) en menos de 02 horas de trabajo con el hardware disponible. |
| 293 | | Arquitectura | El sistema debe ser diseñado y construido con los mayores niveles de flexibilidad en cuanto a la parametrización de los tipos de datos, de tal manera que la administración del sistema sea realizada por un administrador funcional del sistema. |
| 294 | | | El sistema debe ser fácil de instalar en todas las plataformas de hardware y software de base requeridas, así como permitir su instalación en diferentes tamaños de configuracion. |
| 295 | | | Los plugins y desarrollos personalizados, deben permitir su fácil instalación y despliegue. |
| 296 | | | Debe ser 100% web y su administración y parametrización debe realizarse desde el navegador. Se deben proveer interfaces de escritorio opcionales. |
| 297 | | | Integracion con almacenamiento secundario (para documentos con acceso infrecuente) en nube y onPremises |
| 298 | | | Soporte a multiples repositorios |
| 299 | | | Soporte completo al estandar CMIS 1.1 |
| 300 | | | Funcionalidades publicadas como servicios que soporten al menos Web Services (SOAP) y REST |
| 301 | | | Cache de contenidos para acceso frecuente |
| 302 | | | Almacenamiento y administracion nativas de tipos BLOB |
| 303 | | | Soporte para NAS |
| 304 | | | Soporte para SANs |
| 305 | | | Soporte para DAS |

| | | | |
|---|---|---|---|
| **306** | | | Certificacion JEE |
| **307** | SEGURIDAD DE LA INFORMACIÓN | | La solución debe proveer un componente destinado a la gestión de todos los componentes del ECM. Al menos debe incluir: Gestión de Configuración (Administración del Servicio, de los Usuarios, etc), Gestión de Fallas, Gestión del Desempeño (Administración de Indicadores de Desempéño), Gestión de Seguridad. |
| **308** | | | La solución debe proveer al menos dos intefaces para la Gestión del ECM y sus componentes:<br>* Interface de comandos<br>* Interface gráfica de usuario |
| **309** | | | El módulo de Gestión del ECM debe permitir ser integrado a sistemas de gestión de orden superior (HP Open View, IBM Tivoli, Infovista, etc). La integración del módulo de gestión ECM y los sistemas de gestión de orden superior debe garantizarse a través de mecanismos de interoperabilidad estándar como SNMP, XML SOAP - REST, etc. |
| **310** | | | Se deben incluir avisos de derechos de propiedad intelectual en todo el código fuente y en la presentación de la aplicación. |
| **311** | | | La aplicación debe permitir generar reportes a partir del estado de los usuarios de manera que sea posible obtener reportes de usuarios por rangos de fecha de creación, rangos de fecha de cambio de estado y estados (habilitado, deshabilitado y bloqueado). |
| **312** | | | La aplicación debe disponer de un módulo para manejo de eventos y alertas de seguridad. |
| **313** | | | Los registros de seguridad deberían contener como mínimo la siguiente información: Tipo de evento (acierto y error), fecha y hora de generación del evento, origen (Programa que motivó el registro de seguridad), código de evento, descripción del evento, código de usuario, nombre del equipo y dirección IP. Estos campos deben poder ser activados o desactivados por parámetros. Los tipos de evento se describen a continuación: |
| **314** | | | **Acierto:** Cualquier evento que no represente una violación a las políticas o controles de seguridad definidos para la operación de la aplicación. Por ejemplo: ingresos válidos al sistema, |
| **315** | | | **Error:** Cualquier evento que represente un intento de violación a las políticas o controles de seguridad definidos para la aplicación. |
| **316** | | | Los archivos que contienen los registros de seguridad deberían tener un tamaño mínimo y máximo definido por parámetro de acuerdo con los requerimientos de seguridad establecidos para el aplicativo. |

| | | |
|---|---|---|
| **317** | | La aplicación debe contar con un módulo de consulta de los registros de seguridad. Este módulo debe facilitar la visualización por pantalla y la generación de reportes impresos mediante la aplicación de filtros por cada uno de los campos que componen dichos registros. |
| **318** | | Se debe facilitar la administración de los archivos que contienen los registros de seguridad permitiendo hacer depuración (borrado de registros o de los archivos), hacer copias de seguridad y definir su rotación por parámetros de tiempo de generación y tamaño. Se debe permitir hacer corte de los archivos de manera programada para generar uno nuevo de acuerdo con el día específico del mes y de la semana y a una hora determinada. |
| **319** | | Los archivos que almacenan los registros de seguridad de la aplicación deben poder ser exportados a un archivo plano, separando los campos con un carácter específico. |
| **320** | | Se deben generar registros de control o hashes que permitan validar la integridad de los registros de seguridad generados. |
| **321** | | Se debe permitir definir y controlar por parámetro las siguientes acciones a realizar con los archivos que contienen los registros de seguridad: |
| **322** | | **Sobrescribir registros cuando sea necesario**: Se seguirán escribiendo los nuevos registros cuando el archivo alcance el tamaño máximo definido por parámetro. Cada nuevo suceso reemplazará al suceso más antiguo del registro. |
| **323** | | **Sobrescribir registros de hace más de [x] días**: Conserva el archivo durante el número de días especificados por parámetro y sobre escribe los registros que tengan una antigüedad superior a dicho número de días. |
| **324** | | **No sobrescribir registros**: Se requiere depurar manualmente el archivo que alcance el tamaño máximo definido por parámetro y se impedirá la ejecución de cualquier acción que implique la adición de un registro de seguridad. |
| **325** | | Todas las actividades de administración tales como mantenimiento de usuarios y cambio de parámetros del sistema, deben quedar registradas en un archivo de log que permita hacer seguimiento a dichas actividades, el cual debe poder ser administrado de la misma manera que los demás archivos con registros de seguridad. |
| **326** | | Los reportes generados por la aplicación deben contener un rótulo que permita identificar su nivel de clasificación (Restringido, Interno, Público), de acuerdo con la clasificación asignada mediante parámetro al momento de su creación. |

| | | |
|---|---|---|
| **327** | | Toda la información clasificada como restringida debe ser almacenada, transmitida y transportada, con procesos de encripción o cifrado utilizando algoritmos reconocidos como IP-SEC, DES, 3DES, AES o SSL, usando llaves de, al menos, 128 bits. |
| **328** | | El intercambio de información clasificada como restringida entre los diferentes módulos y capas que componen la aplicación debe garantizar la protección de dicha información haciendo uso de los algoritmos de encripción o cifrado mencionados en el punto anterior y con llaves de al menos 128 bits. |
| **329** | | La aplicación debe poseer un módulo o una opción para la administración de las llaves de encripción utilizadas en los algoritmos y procesos de encripción. En este módulo se debe garantizar la confidencialidad de las llaves que en él se administran y se debe permitir el ingreso de las llaves en, como mínimo, dos partes independientes. |
| **330** | | El sistema debe borrar automáticamente toda la información sensible almacenada temporalmente ante terminaciones exitosas o ante fallas de la aplicación. |
| **331** | | El aplicativo debe permitir controlar por parámetro la emisión de copias adicionales de los informes que genera. |
| **332** | | Deben realizarse validaciones de los valores aceptables para todos los campos de entrada de datos que lo requieran, a través de rangos de fechas permitidos, longitudes de campos, rangos de valores permitidos, rangos de caracteres permitidos y validación de campos numéricos, alfabéticos y alfanuméricos. |
| **333** | | Todas las aplicaciones Web (Web-Oriented) deben permitir el manejo de protocolos seguros con certificados digitales para el intercambio de información confidencial. |
| **334** | | La aplicación debe permitir restringir la conexión por dirección IP específica. |
| **335** | | El aplicativo debe utilizar el protocolo de comunicación TCP-IP para la transmisión de información desde y hacia los diferentes componentes que se encuentren distribuidos a través de la red, de manera que se garanticen adecuados niveles de protección a los datos. |
| **336** | | La aplicación debe permitir cambiar mediante parámetros, los puertos por defecto con los cuales se integran sus diferentes módulos y capas. |
| **337** | | Todas las operaciones o transacciones deben ser monitoreadas y controladas para garantizar su integridad de manera que puedan ser identificadas posibles modificaciones no autorizadas, con o sin intención. |

| | | |
|---|---|---|
| **338** | | La aplicación debe validar la integridad de la información que es transmitida por la red producto de cualquier operación o transacción propia de su funcionalidad. |
| **339** | | La aplicación debe mantener control sobre las sesiones establecidas por las transacciones u operaciones y por los códigos de usuario, de manera que se restrinja y controle la posibilidad de adicionar paquetes o frames por fuera de los estados que controla dicha tabla. Esta tabla de estados y el control que se realice sobre ellos deben estar basados en el estándar del protocolo de comunicaciones utilizado por la aplicación. |
| **340** | | La aplicación debe facilitar la actualización de los sistemas operativos y de todo el software base que lo soporta, mediante los parches, nuevas versiones o paquetes de servicio publicados o facilitados por los fabricantes. |
| **341** | | La aplicación debe generar mensajes que muestren al usuario la fecha y hora de su último ingreso, preferiblemente en la pantalla de Log-In. |
| **342** | | Se debe permitir la autenticación mediante código de usuario y clave. |
| **343** | | La aplicación debe poseer un módulo para administración de la identificación, autenticación y autorización. |
| **344** | | El módulo para administración de la identificación, autenticación y autorización debe ser independiente a la aplicación. |
| **345** | | El módulo de AA (Autenticación, Autorización) debe permitir ejecutar las siguientes operaciones: creación, modificación, deshabilitación, eliminación y desconexión de usuarios, cambio de contraseña, consulta de usuarios del sistema y consulta de usuarios conectados. |
| **346** | | Para la autenticación de las aplicaciones o facilidades catalogadas como críticas para la Entidad, el aplicativo debe permitir la integración con servidores de autenticación TACCACS y RADIUS, poder integrarse con servicios de directorios estándar mediante LDAP y poder integrarse con servicios de autenticación fuerte como SecureID, de manera que se dé la posibilidad de usar mecanismos de identificación y autenticación de doble y triple factor. |
| **347** | | El repositorio de usuarios debe almacenar, al menos, los siguientes datos: código de usuario, hash de la clave, nombre, número de identificación, cargo, área o dependencia, ubicación física, jefe de, reporta a y rol o perfil. Estos campos deberán ser parametrizables de acuerdo con las necesidades del negocio. |
| **348** | | La deshabilitación de los códigos de usuario debe estar restringida a usuarios con privilegios suficientes para hacerlo. |
| **349** | | |

| | | |
|---|---|---|
| **350** | | La aplicación debe permitir manejar esquemas de delegación de administración de códigos de usuario. |
| **351** | | Los usuarios que vienen instalados por defecto en la aplicación para propósitos de instalación o configuración inicial de la aplicación deben poder deshabilitarse o eliminarse. |
| **352** | | El sistema debe permitir definir por parámetro y controlar la longitud mínima de las contraseñas. |
| **353** | | El sistema debe permitir definir por parámetro y controlar la longitud máxima de las contraseñas. |
| **354** | | El sistema debe permitir definir por parámetro y controlar el número de contraseñas a recordar (Histórico de contraseñas). |
| **355** | | El sistema debe permitir definir un diccionario de contraseñas no válidas y controlar que las contraseñas no coincidan con las existentes en dicho diccionario. |
| **356** | | La aplicación debe controlar mediante parámetro que las contraseñas contengan o no la identificación del usuario como una parte de éstas. |
| **357** | | La aplicación debe controlar mediante parámetro que la contraseña contenga o no alguna sucesión lógica de números o letras. |
| **358** | | La aplicación debe controlar mediante parámetro que la contraseña pueda o no ser generada de manera aleatoria. |
| **359** | | La aplicación debe controlar mediante parámetro la complejidad de la contraseña. Cuando se habilita la complejidad, la contraseña debe tener una combinación de caracteres numéricos, alfabéticos (Mayúsculas y Minúsculas) y signos o caracteres especiales. |
| **360** | | Las contraseñas nunca pueden ser almacenadas en formato texto. Deben ser almacenadas por medio de un algoritmo de encripción de una sola vía reconocido por la industria como MD5 y SHA. Para estos procesos de cifrado se deben utilizar llaves cuya longitud mínima sea de 128 bits. |
| **361** | | La aplicación debe desconectar los usuarios que hayan permanecido inactivos en el sistema durante un tiempo definido mediante un parámetro que especifique este tiempo. |
| **362** | | La aplicación debe deshabilitar los códigos de usuario que no hayan iniciado sesión en un período de tiempo definido mediante un parámetro que especifique este tiempo. |
| **363** | | El sistema debe permitir definir por parámetro y controlar las siguientes características de las contraseñas: vigencia mínima, vigencia máxima y tiempo de aviso de vencimiento. |

| | | |
|---|---|---|
| **364** | | Se debe impedir realizar operaciones en la aplicación para un código de usuario con contraseña vencida. Cuando un código de usuario tenga vencida la contraseña, debe permitir el ingreso pero deberá presentar como única operación posible el cambio de contraseña. Luego de realizarse el cambio de la contraseña, se permitirá la operación normal del código de usuario. |
| **365** | | El sistema debe exigir a los usuarios cambiar su contraseña de manera automática cuando se presenten las siguientes condiciones: |
| **366** | | a. Acceso por primera vez al aplicativo. |
| **367** | | b. Expiración de la vigencia de la contraseña. |
| **368** | | c. Reactivación o modificación de la contraseña por parte del administrador. |
| **369** | | La aplicación deberá permitir cambiar la contraseña a solicitud del usuario validando la vigencia mínima de la contraseña. |
| **370** | | La aplicación debe poder generar de manera aleatoria las contraseñas de los usuarios ante los eventos de creación de un usuario o de cambio de contraseña por solicitud del administrador. |
| **371** | | El aplicativo debe permitir controlar la no repetición de un número específico de contraseñas, definido por parámetro. |
| **372** | | El sistema debe permitir manejar los siguientes estados para los códigos de usuario: Habilitado, deshabilitado, bloqueado, suspendido. |
| **373** | | El sistema debe permitir administrar y controlar mediante parámetros generales para toda la aplicación y de manera independiente para cada uno de los usuarios el umbral de intentos fallidos de conexión. Cuando se alcance al umbral de intentos fallidos de conexión, el código de usuario deberá pasar a estado deshabilitado. |
| **374** | | El sistema debe permitir administrar y controlar mediante parámetros generales para toda la aplicación y de manera independiente para cada uno de los usuarios el tiempo para reiniciar el contador de intentos fallidos. Este tiempo se validará y se reinicializará el contador de intentos fallidos de conexión, siempre y cuando no se haya alcanzado el umbral de intentos fallidos de conexión. |
| **375** | | El sistema debe permitir administrar y controlar mediante parámetros generales para toda la aplicación y de manera independiente para cada uno de los usuarios el tiempo de bloqueo al alcanzar el umbral de intentos fallidos de conexión. El usuario se mantendrá deshabilitado mientras no se complete este tiempo. |

| | | |
|---|---|---|
| **376** | | El sistema debe permitir administrar y controlar mediante parámetros generales para toda la aplicación y de manera independiente para cada uno de los usuarios el tiempo permitido sin iniciar sesión en la aplicación. Cuando se completa este tiempo, la aplicación deberá deshabilitar el código de usuario. |
| **377** | | El sistema debe permitir administrar y controlar mediante parámetro la fecha desde la cual se inicia la vigencia de un código de usuario (día/mes/año). El sistema debe impedir iniciar sesión con un código de usuario en una fecha anterior a la definida por este parámetro. |
| **378** | | El sistema debe permitir administrar y controlar mediante parámetro la fecha hasta la cual está vigente un código de usuario (día/mes/año). El sistema debe impedir iniciar sesión con un código de usuario en una fecha posterior a la definida por este parámetro. Una vez cumplida esta fecha, se deberá cambiar el estado del código de usuario a deshabilitado. |
| **379** | | El sistema debe permitir administrar y controlar mediante parámetros generales para toda la aplicación y de manera independiente para cada uno de los usuarios el tiempo en días de permanencia luego de haberse deshabilitado un código de usuario. Después de haber transcurrido este tiempo para un código de usuario deshabilitado, el sistema deberá eliminarlo, considerando las restricciones de eliminación definidas para la norma 4.3.6.17. Eliminación de códigos de usuario. |
| **380** | | Se debe almacenar la información histórica de cualquier código de usuario eliminado de manera que se facilite la recuperación en caso de ser requerida. |
| **381** | | La aplicación debe validar que en caso de ser asignado un código de usuario previamente usado, se garantice que el código de usuario anterior ha sido eliminado y que pueda identificarse plenamente el usuario de toda la información histórica de ambos códigos de usuario. |
| **382** | | El aplicativo debe administrar el acceso a las diferentes funciones u operaciones mediante perfiles de administración y uso, los cuales deben poder ser definidos mediante parámetros. |
| **383** | | La aplicación debe permitir, como mínimo, la administración de los siguientes parámetros para definir los perfiles de acceso de los usuarios: |
| **384** | | a. Tabla o archivo del aplicativo. |

| | | |
|---|---|---|
| 385 | | b. Acción a realizar sobre los archivos u objetos (control total, adición, modificación, eliminación, lectura, ejecución, impresión, creación-generación de un nuevo objeto, leer los atributos de un objeto, editar o modificar los atributos de un objeto, exportar/importar objetos o archivos asociados a un objeto, conceder a un código de usuario privilegios sobre un objeto y definir los privilegios sobre un objeto o archivo). |
| 386 | | c. Menú o módulo de la aplicación. |
| 387 | | d. Opción de la aplicación. |
| 388 | | La aplicación debe controlar que no se puedan eliminar roles o perfiles con códigos de usuario asociados y que no se puedan crear códigos de usuarios sin un rol o perfil asociado. |
| 389 | | El acceso a la aplicación se debe controlar de manera que se impida su ingreso a usuarios con clave vencida o caducada, usuarios inexistentes, usuarios con clave errada y usuarios deshabilitados. |
| 390 | GESTION Y TRAMITE DEL EXPEDIENTE ELECTRONICO | La aplicación debe proporcionar opciones, transacciones o facilidades para corregir los posibles errores que se puedan presentar con los datos de la aplicación y estas operaciones de corrección deben tener el mismo comportamiento que las demás opciones de la aplicación, dejando rastros y controlando su uso. |
| 391 | | Se debe permitir definir y controlar mediante parámetros los rangos de días de la semana en que los usuarios pueden establecer sesión en la aplicación, de acuerdo con las necesidades de la Entidad. |
| 392 | | Se debe permitir definir y controlar mediante parámetros los rangos de horas en que los usuarios pueden establecer sesión en la aplicación, de acuerdo con las necesidades de la Entidad. |
| 393 | | El sistema debe permitir agregar documentos electrónicos a expedientes electrónicos contenidos fuera de la plataforma o en esta, y vincularlos a un tipo documental del expediente. |
| 394 | | Los documentos que componen el expediente, heredan los tiempos de conservación establecidos en la TRD. |
| 395 | | El sistema debe permitir establecer niveles de seguridad del expediente, ya sea abierto o confidencial. |
| 396 | | El nivel confidencial de un expediente debe permitir elegir que usuarios tendrán acceso al expediente y debe permitir elegir qué tipo de acceso, ya sea edición o lectura. Lo anterior es aplicable a nivel de expediente y/o tipo documental. |
| 397 | | El sistema debe permitir agregar a un expediente electrónico, documentos provenientes de otros expedientes electrónicos sin que estos impliquen duplicidad del documento. |

| | | |
|---|---|---|
| **398** | | Cuando es cargado un documento al expediente, el sistema debe otorgarle un número único de identificación en la plataforma. |
| **399** | | Debe permitir la incorporación de documentos electrónicos en diferentes formatos, de conformidad con la Guía de Documento Electrónico de Gobierno en Línea. |
| **400** | | El sistema debe permitir crear entradas múltiples para un documento electrónico de archivo en varios expedientes electrónicos, sin duplicación física del documento electrónico. |
| **401** | | El sistema debe permitir diligenciar metadatos de ubicación, que luego van a permitir su ubicación a nivel de unidades documentales, para el caso de los expedientes híbridos. |
| **402** | | Los valores de control y seguridad de información están dados por los tipos documentales. Al quedar asociados a un expediente electrónico, el usuario administrador podrá conservar dicha calificación o modificar la misma. |
| **403** | | El sistema debe permitir cargar documentos adjuntos a los tipos documentales. |
| **404** | | Todas las acciones efectuadas sobre el expediente, deben ser registradas en un historial de eventos que puede ser consultado por usuarios que tengan acceso al expediente electrónico. |
| **405** | | El historial de eventos del expediente electrónico debe permitir ser exportado en un archivo PDF. |
| **406** | | El sistema debe permitir que los documentos de archivo tradicionales y los documentos electrónicos que forman parte de un expediente mixto, utilicen el mismo título y código de referencia numérica, con una indicación añadida que se trata de un expediente mixto. |
| **407** | | Para el caso de expedientes híbridos, debe permitir en el momento de carga del documento digitalizado al expediente electrónico, establecer el tipo de formato, para controlar posteriormente su inclusión en el expediente físico. |
| **408** | | El sistema debe permitir el seguimiento de los expedientes tradicionales, mediante controles de salida y entrada y testigos que reflejen la ubicación del expediente en cada momento. |
| **409** | | El sistema debe permitir cambiar de usuario responsable de un expediente electrónico, bajo un proceso supervisado. |
| **410** | | El sistema debe permitir generar índice electrónico del expediente, de conformidad con lo dispuesto en la Ley 527 de 1999 y Ley 1437 de 2011. |
| **411** | | El índice electrónico debe permitir exportarse a formato XML. |
| **412** | | El sistema debe permitir la incorporación de la firma electrónica para la generación del índice del expediente electrónico. |
| **413** | | El índice electrónico debe permitir cotejar la composición de los documentos electrónicos que lo integra, asegurando su integridad y autenticidad. |
| **414** | | El sistema debe permitir realizar transferencia del expediente electrónico al archivo central del sistema (SGDEA). |
| **415** | | El sistema debe permitir editar el nivel de seguridad al expediente y sus tipos documentales. |

| | | |
|---|---|---|
| **416** | | Para el caso de los documentos cargados al expediente electrónico, de naturaleza física, el sistema debe presentar un reporte de los documentos pendientes por incluir en el expediente físico para el caso de los expedientes híbridos. |
| **417** | | Cuando en la radicación del documento de entrada, el usuario de correspondencia asigne el valor de entrega física al usuario responsable del trámite, el sistema debe permitir al usuario responsable controlar la entrega física del documento, a través de un reporte que permita la recepción de documentos evitando la impresión de planillas o formatos físicos. |
| **418** | | El sistema debe permitir al usuario del sistema compartir un expediente electrónico a uno o varios usuarios de cualquier dependencia, concediendo privilegios para la gestión del expediente. |
| **419** | | El sistema debe permitir al responsable del expediente, revocar permisos de usuarios cuando este lo considere. |
| **420** | | El sistema debe generar un histórico del expediente, donde registra los usuarios a quienes les han compartido un expediente electrónico y cuando han sido revocados. |
| **421** | | El sistema debe registrar como metadatos la fecha y la hora de registro de la carga de un documento al expediente electrónico. |
| **422** | | Dentro de los metadatos del expediente electrónico, debe presentarse metadatos de ubicación del expediente por cada tomo que pueda existir del mismo. |
| **423** | | El sistema debe almacenar el histórico de movimientos del expediente y los usuarios que efectúan el ingreso y modificación de valores de ubicación física. |
| **424** | | El sistema debe permitir autocontener los metadatos en el documento en formato XMP de acuerdo al estándar PDF/A |
| **425** | | El sistema debe permitir múltiples firmas electrónicas o digitales en los documentos electrónicos |
| **426** | | El sistema debe permitir de forma paramétrica la configuración del tipo de firma, de certificación o de aprobación (PDF) |
| **427** | | El sistema debe permitir la generación de documentos PDF /A a partir de documentos ofimáticos. |
| **428** | | El sistema debe disponer de una opción o servicio para la conversión de documentos en otros formatos a PDF/A |
| **429** | | Para los casos en los cuales el formato inicial del archivo no permite su conversión a PDF/A ej.: AVI, MP3, …), es necesario disponer de una opción para ensobrado electrónico que garanticé la integridad de los archivos. |
| **430** | | El sistema debe proveer un mecanismo para asociar al cuadro de clasificación documental desde la plataforma de correo electrónico, los correos que deben declararse en el SGDEA. |
| **431** | | Los correos electrónicos que se declaren desde la plataforma de correo electrónico, deben guardarse en el SGDEA de forma integra (mensaje, metadatos y anexos). |
| **432** | | Permite declarar manualmente un contenido existente como documento de archivo. |

| | | | |
|---|---|---|---|
| 433 | | | Permite declarar automaticamente un contenido existente como documento de archivo. |
| 434 | | | Permite declarar que un contenido sea un documento de archivo, desde el punto de creación. |
| 435 | | | Permite administrar todas las fases de archivo desde su creación hasta su disposición final. |
| 436 | | | Permite suspender los tiempos de retención para un conjunto de series y/o expedientes. |
| 437 | | | Permite definir eventos de cierre de los expedientes a partir de los cuales empiecen a aplicar los tiempos de retención, tanto manualmente como automaticamente. |
| 438 | | | Permite hacer referencias cruzadas de expedientes y/o documentos de archivos. |
| 439 | | | Los usuarios deben ser capaces de acceder a todos los expedientes de los que están autorizados a través de una interfaz de usuario común, área de trabajo o portal . El contenido de un registro, todos los metadatos asociados y cualquier enlace o agregaciones deben estar disponibles a través de la espacio de trabajo. |
| 440 | | | Permite a usuarios autorizados cerrar y reabrir manualmente expedientes cerrados y agregar documentos, con su respectiva traza de auditoría y metadatos. |
| 441 | Prestamos Documentales | ARCHIVOS DE GESTION | Permite hacer transferencias entre las diferentes fases de archivo manual y automaticamente. |
| 442 | | | Permite generar reportes de los expedientes que han cumplido su tiempo de retención, a los cuales se les puede aplicar disposición final. |
| 443 | | | Permite migrar los documentos de archivo a otros sistemas de información/conservación, garantizado toda su fidelidad e integridad de los metadatos asociados. |
| 444 | | | El sistema debe ofrecer una funcionalidad que permita solicitar el préstamo electrónico y físico de expedientes y documentos que este contenga. |
| 445 | | | Los préstamos solicitados deben permitir ser aceptados o rechazados por el usuario responsable del expediente. |
| 446 | | ARCHIVOS CENTRALES | El sistema debe permitir parametrizar el tiempo de vencimiento de los préstamos documentales. |
| 447 | | | El sistema debe presentar a los usuarios que utilizan esta funcionalidad, un reporte con los expedientes en préstamos, solicitados, devueltos y rechazados. |
| 448 | | | El sistema debe registrar en el histórico del expediente, el registro de la operación en torno al proceso de préstamo documental. |
| 449 | | | La solicitud de préstamos documentales al archivo central debe ser un rol que se agrupa a un perfil de usuario. |

| | | |
|---|---|---|
| **450** | Transferencias Documentales y Disposición Final | El sistema debe permitir a los usuarios del sistema, efectuar búsquedas de expedientes o documentos transferidos al archivo central y solicitar en versión física y electrónica según corresponda. |
| **451** | | El sistema debe permitir al Archivo Central que recibe la solicitud de préstamo, aceptar o rechazar un préstamo físico, de radicado o expediente. |
| **452** | | El sistema debe generar un reporte de las solicitudes enviadas y recibidas, préstamos aceptados y devoluciones entre usuarios. |
| **453** | | El sistema debe monitorear el tiempo de conservación de los expedientes electrónicos, tomando como base la fecha del último documento que contiene el expediente, conforme la disposición final de la TRD. |
| **454** | | El sistema debe notificar al usuario para que inicie la elaboración del inventario documental y transferencia, de acuerdo al calendario de transferencia. |
| **455** | | El sistema debe permitir al usuario solicitar ampliación de plazo de transferencia. Debe registrarse una observación que se debe registrar en el histórico del expediente. |
| **456** | | El sistema debe facilitar la generación del inventario documental y su aprobación por archivo central. |
| **457** | | El sistema debe permitir realizar modificaciones del inventario cuando se encuentre errores. |
| **458** | | El sistema debe permitir generar el inventario para aprobación. |
| **459** | | El sistema debe permitir gestionar los inventarios documentales elaborados y recibidos. |
| **460** | | El sistema debe permitir exportar el inventario documental a Excel. |
| **461** | | El sistema debe generar un acta de transferencia, asignando un número de acta, fecha y expedientes transferidos. |
| **462** | | El nuevo estado del expediente transferido debe ser “Archivo Central”. |
| **463** | | El sistema debe presentar al archivo central, metadatos que faciliten la ubicación física para el caso de los expedientes híbridos. |
| **464** | | En la transferencia del expediente electrónico, el sistema no puede degradar el contenido ni la estructura de sus documentos electrónicos; conservando todos los vínculos entre el documento y sus metadatos. |
| **465** | | El sistema debe presentar un informe en el que se detalle cualquier fallo que se haya producido durante la transferencia, la exportación o el borrado. El informe deberá indicar cuáles de los registros que estaba previsto transferir han generado errores durante la operación. |
| **466** | | El sistema debe monitorear el tiempo de conservación de los expedientes electrónicos e híbridos, tomando como base la fecha del último documento que contiene el expediente conforme la disposición final de la TRD para su eliminación. |

| | | |
|---|---|---|
| **467** | | Conviene que el sistema permita la destrucción total de expedientes concretos que según la TRD así lo indiquen, de forma que queden eliminados por completo y no se puedan restaurar con instrumentos especializados de recuperación de datos. |
| **468** | | El sistema debe ser capaz de conservar los metadatos de los expedientes electrónicos eliminados, para consultas posteriores. |
| **469** | | El sistema debe generar el acta de eliminación de los expedientes eliminados. |
| **470** | | Una vez se realice la transferencia del expediente electrónico al SGDEA, debe asegurar conservación, autenticidad, integridad y recuperación a medio y largo plazo conforme lo estipulado en la TRD |
| **471** | Colaboración | El sistema debe evitar en todo momento que se elimine un expediente o cualquier parte de su contenido, salvo en caso de: destrucción conforme a la norma de conservación o eliminación llevada a cabo por un administrador como parte de un procedimiento auditado |
| **472** | | El sistema debe ser capaz de rastrear de forma automática los períodos de conservación asignados al expediente conforme la TRD, tomando como fecha final del documento incorporado más reciente. |
| **473** | | El expediente electrónico debe permitir realizar empaquetado del mismo en un archivo .ZIP, el cual debe contener el índice electrónico y metadatos del expediente electrónico en formato XML, además copia de los documentos contenidos en el expediente. |
| **474** | | El sistema debe permitir enviar documentos a usuarios y estos puedan abrir y editar cuyos cambios deben ser registrados directamente sobre el documento. En todo caso debe gestionarse una sola versión del documento. |
| **475** | | El sistema debe permitir sobre plantillas de Word la creación, asignación, modificación, preparación, aprobación secuencial. Todas estas funciones desde la misma plataforma. |
| **476** | Gestión de correspondencia | Los plantillas deben contar con un buscador para su fácil recuperación. |
| **477** | | La plantilla utilizada por el usuario debe alojarse nativamente en la plataforma, el cual debe permitir la edición del documento las veces que el usuario lo requiera. |
| **478** | | El sistema debe facilitar los análisis de antecedentes, proyección de respuesta y tramite que haya lugar hasta culminación del asunto. |
| **479** | | El sistema debe cumplir en su totalidad con el Acuerdo 060 de 2001. |

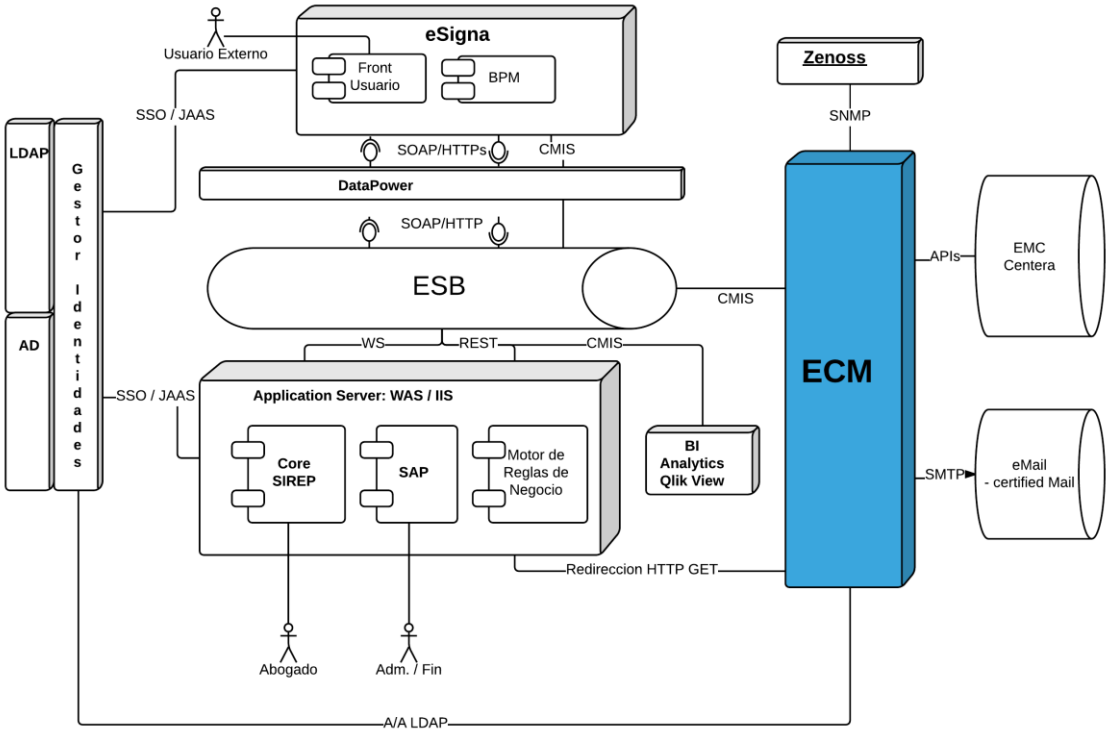
| | | |
|---|---|---|
| **480** | | El sistema debe permitir con los radicados de entrada la función de asignación simple y múltiple. Ejemplo cuando un radicado debe ser tramitado por varios usuarios simultáneamente. |
| **481** | | El sistema debe presentar un reporte de los radicados físicos pendientes por entregar físicamente al usuario asignado. |
| **482** | | Cuando en la radicación del documento de entrada el usuario de correspondencia asigno el valor de entrega física al usuario responsable del trámite, el sistema debe en todo momento el control de la entrega física del documento a través de un reporte que permita la recepción de documentos evitando la impresión de planillas físicas. |
| **483** | | El sistema debe permitir en la radicación de documentos que ingresan por correspondencia, la impresión de rótulos de identificación para incorporar al documento físico el cual incluya códigos de barras, fecha, hora y usuario radicador. |
| **484** | | La radicación de documentos internos cuyo destino sea interno o externo se debe realizar desde el área que los produce. |
| **485** | | Para los radicados de entrada marcados como físicos, el sistema debe permitir la carga del archivo digitalizado. Una vez digitalizado es enviado al usuario asignado. |
| **486** | | El sistema debe contar con un módulo integrado y expuesto desde el portal Web de la entidad, que permita el registro de ciudadanos para la generación de PQRS. |
| **487** | | El sistema debe permitir la validación de la existencia del correo electrónico provisto por el ciudadano. |
| **488** | | Validado el ciudadano, este puede formular PQRS desde la Web. |
| **489** | | El sistema debe permitir la formulación de PQRS Anónimas. |
| **490** | | El ciudadano debe contar con un módulo que permita consultar las respuestas emitidas por la entidad. |
| **491** | | El sistema debe permitir reasignar un radicado de entrada o PQRS a otro usuario del sistema, conforme un árbol de jerarquía. |
| **492** | | El sistema debe permitir incluir los radicados de entrada, salida, internos y PQRS generados desde el mismo sistema. |
| **493** | | El sistema debe contar con un buscador de expedientes que facilite la inclusión de radicados. |
| **494** | | El sistema debe permitir con los radicados de entrada y PQRS, la delegación del mismo a varios usuarios, de tal forma que cada usuario aporte los documentos y comentarios necesarios para emitir una sola respuesta. |
| **495** | | El sistema debe proveer en la mayor cantidad posible, la generación de reportes para las distribuciones físicas de documentos, facilitando su control mediante formularios del sistema y evitando la impresión de planillas de entrega. |
| **496** | | El sistema debe permitir el cálculo de la fecha de vencimiento de los radicados, cuando este se ha establecido. |
| **497** | | El sistema debe permitir generar radicados de salida desde la dependencia productora. |

| | | | |
|---|---|---|---|
| **498** | | | El sistema debe permitir la carga de plantillas de Word para la generación de radicados de salida. |
| **499** | | | Después de radicado el documento de salida, el sistema debe convertirlo automáticamente a un formato PDF/A. |
| **500** | | | El sistema debe permitir generar radicados de salidas digitales y físicas. Para el primero debe enviarlo al ciudadano o empresa destinataria. |
| **501** | | | Cuando se trate de radicados de salida digitales producto de una respuesta a una PQRS, el sistema debe publicarla en el sitio Web de la entidad, de tal manera que permita la consulta al ciudadano de la misma. |
| **502** | | | Para los radicados de salida físicos, el sistema debe asignar un numero temporal hasta tanto no sea entregado a ventanilla. |
| **503** | | | Cuando se recibe en ventanilla un radicado de salida físico, el sistema debe permitir asignar un número definitivo, generación del adhesivo y digitalizar el radicado de salida. |
| **504** | | | El sistema debe permitir la asignación de rutas de correspondencia y mensajería con terceros para radicados de salida en soporte físico. |
| **505** | | | El sistema debe permitir la generación de planillas de envío, donde se relacione los radicados de salida a distribuir físicamente. |
| **506** | | | El sistema debe permitir establecer cuando ha sido entregada exitosamente un radicado de salida, en caso tal permitir su reprogramación. |
| **507** | | | El sistema debe enviar en puntos críticos notificaciones al correo del usuario que tramita un documento. |
| **508** | | | El sistema debe permitir la personalización de los rótulos de los adhesivos de correspondencia. |

**ESCENARIOS INTEGRACIÓN ECM**

Para todas las solicitudes de integración a continuación (excepto las de redirección), el proveedor debe desarrollar un mecanismo alineado con el estándar CMIS en la medida de lo posible, y sustentar la propuesta de un servicio personalizado en la inexistencia de la funcionalidad en el estándar. Se solicita cumplir con el estándar CMIS 1.1 incluyendo todas las funcionalidades excepto las opcionales del estándar http://docs.oasis-open.org/cmis/CMIS/v1.1/cs01/CMIS-v1.1-cs01.html

El siguiente gráfico muestra las integraciones básicas que debe proveer la plataforma. Se debe tener en cuenta que el visor se utilizará principalmente mediante redirección http, pero para flujos documentales puede requerirse la interacción directa con el ECM.




En la siguiente tabla se describen las integraciones mencionadas.

| Integración | Sistema / Usuario Objetivo | Protocolo / Mecanismo | Atributos de Calidad | Observaciones |
|---|---|---|---|---|
| **Visualizar Documentos** | Usuario Final | Interfaz WEB de visualización/ Redirección HTTP | Usabilidad, tolerancia a fallos | Deseable interfaz móvil (app) |
| **Crear/Consultar/ Actualizar y Borrar Documentos** | SIREP / SAP / SIMASC | Estándar CMIS 1.1 WS/REST | En promedio 1 TPS con un máximo de 5 TPS en Carga de Digitalización. Carga útil promedio de 600K y Máxima de 40MB para Servicios Públicos y Gestión interna. Hasta 5GB para documentos probatorios en CAC. | Se debe proponer el método concreto dentro del estándar a ser utilizado para cada integración |
| **Digitalización de Documentos** | Usuario Final / Digitalizador | Interfaz WEB / Aplicación – Redirección HTTP | Calidad, Velocidad, Estabilidad | Deseable interfaz móvil (app) |
| **Adición de Página / Imagen de Rotulo** | SIREP | WS/REST | 1 TPS / Rotulo 100K | Rotulo en formato TIFF, esta funcionalidad debe soportarse y se debe redefinir en proceso de implementación |
| **Versionamiento** | SIREP | CMIS 1.1 WS /REST | 0,1 TPS | El esquema debe ser flexible frente a posibles cambios en el versionamiento |
| **Autenticación y Autorización** | Active Directory | LDAP / Soporte ACLs | 1500 usuarios internos | |
| **Monitoreo** | Zenoss 4.2.4 | SNMP v1, v2c, v3 | | Deseable interfaz / tablero de monitoreo |
| **Almacenamiento** | Centera | APIs EMC Centera | 14TB | El almacenamiento inicial es centera pero debe poder cambiarse por cualquier otro almacenamiento estándar. |
| **eSigna** | Usuarios Externos | CMIS / SOAP/HTTP | | Según indicaciones del proveedor inDenova |
| **Firmas Digitales y Estampado de Tiempo** | TSA, PKI | RFC 3161, FIPS | | Requeridos para la gestión de índices electrónicos al momento del evento de cierre de un expediente. |
| **Correo Electronico** | Buzón de Correo | SMTP | | Notificaciones, puede incluir correo electrónico certificado, inicialmente mediante la modificación de la dirección destino incluyendo el gateway |

A continuación se detallan algunas de las integraciones descritas.

**Visor de Documentos**
Se requiere que el ECM provea un visor para los documentos que están almacenados, este visor debe tener las siguientes herramientas:

- Vista por pagina
- Zoom
- Búsqueda de textos
- Marcaciones y Anotaciones
    - El visor entregado por el ECM debe tener la capacidad de realizar marcaciones de tipo resaltado sobre el documento, esta marcaciones deben ser parametrizables, adicionalmente debe tener la opción de almacenar anotaciones que se hagan en el documento. Se debe manejar perfiles de seguridad para el acceso al documento, no todos los usuarios podrán realizar marcaciones y anotaciones.
    - El visor del ECM debe mostrar las marcaciones y anotaciones que se hayan realizado previamente en el documento.
- OCR
    - Es necesario que el ECM tenga utilidades para poder realizar operaciones de OCR (Optical Character Recognition) sobre los documentos que estén almacenados.

Se incluye como integración, puesto que este visor debe tener una interfaz web, y el ECM debe permitir realizar una redirección a esta interfaz con la metadata como parámetro GET.

**Verifica Existencia de Documento**
Se requiere que el ECM exponga un servicio que permita verificar si un documento existe o no a partir de una metadata de entrada.

**Crear Documento**
Es necesario que se exponga un servicio que reciba un documento y una metadata asociada para que sea almacenada en el ECM.

**Eliminar Documento**
El ECM debe proveer un servicio para que se elimine un documento a partir de una metadata de entrada que se le envíe y según la configuración de perfiles de usuario.

**Consultar Documento**
Es necesario que el ECM provea un servicio que retorne un documento a partir de una metadata de entrada.

**Digitaliza Documentos**
El ECM debe proveer una utilidad mediante la cual se puedan digitalizar los documentos entregados en las sedes de la CCB para que sean almacenados en el formato estándar que se defina, estos documentos debe tener asociada una metadata la cual se utilizara para realizar búsquedas. Se incluye como integración puesto que la interfaz de digitalización debe ser web y el ECM debe permitir realizar una redirección a esta interfaz con metadata inicial como parámetro GET.

**Adición de Pagina (Imagen de Rotulo)**
Se requiere que el ECM exponga un servicio que permita adicionar una página al inicio o al final de un documento ya existente, dependiendo de un indicador que especifique la ubicación. La página se

entrega en formato TIF y debe convertirse al formato estandarizado de almacenamiento de documentos del ECM.

**Versionamiento de Documentos**

Se requiere que el ECM exponga un servicio mediante el cual se puedan versionar documentos a partir de una metadata de entrada. El versionamiento que se manejara será descendente. Ejemplo: Siempre la versión más reciente será la 0, luego seguirá la 1 y así sucesivamente. La definición de las tablas de retención documental puede modificar o sugerir un esquema diferente de versionamiento.

**Traslado de Documentos a Centera**

Se debe implementar en el ECM un mecanismo mediante el cual se "congele" la versión del documento, es decir, que no se permitan más cambios y se conserve la última versión como definitiva. Este comportamiento debe ser iniciado por el sistema origen mediante un servicio expuesto por el ECM. Actualmente se tiene implementado el almacenamiento definitivo con CENTERA.