REQUERIMIENTOS NO FUNCIONALES DETALLADOS

Acceso	1. Permite que el administrador restrinja el acceso a carpetas, documentos y metadatos a determinados usuarios del sistema? 2. 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? 3. Permite vetar el acceso al sistema cuando no se aplique un mecanismo de autenticación aceptado y atribuido al perfil del usuario? 4. Permite vetar el acceso a carpetas y/o documentos? 5. Permite restringir el acceso a funciones como la lectura, modificación y eliminación de documentos y/o metadatos? 6. Permite vetar el acceso después de una fecha concreta? 7. Permite proporcionar las mismas funciones de control tanto para perfiles como para usuarios? 8. Permite definir grupos de usuarios asociados a un conjunto de carpetas y documentos? 9. Permite la creación de grupos de usuarios? 10. Permite que un usuario pertenezca a más de un grupo? 11. Permite que sólo los usuarios administradores creen usuarios, establezcan perfiles de usuario, permisos y asignar usuarios a grupos? 12. 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? 13. Registrar todos los accesos. 14. Permite restringir el acceso a las funciones del sistema según el perfil del usuario? 15. 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?

Pista de auditoría	16. 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? 17. 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? 18. 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? 19. 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? 20. 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? 21. 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? 22. Permite capturar y almacenar en la pista de auditoría datos sobre fecha y hora del cargue del documento? 23. Permite capturar y almacenar en la pista de auditoría datos sobre la reclasificación de los documentos en otro nivel de la estructura de clasificación? 24. 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? 25. Permite capturar y almacenar en la pista de auditoría datos sobre la fecha y la hora de creación, modificación y eliminación de metadatos? 26. 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?

	27. Permite capturar y almacenar en la pista de auditoría datos sobre la eliminación de carpetas o documentos.? 28. Permite exportar la pista de auditoría a medios externos al sistema, sin que esto repercuta en la pista almacenada en el sistema? 29. Permite hacer reportes e informes de las acciones sobre la estructura documental, carpetas y documentos? 30. 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?
Copias de seguridad y recuperación	31. 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)? 32. Permite programar rutinas de copias de seguridad en las que pueda especificar con qué frecuencia se realizará la copia de seguridad? 33. 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? 34. Permite programar rutinas de copias de seguridad en las que pueda seleccionar un medio de almacenamiento al que se destinará la copía de seguridad.? 35. 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? 36. Permite restringir al administrador la actualización de las copias de seguridad, manteniendo la plena integridad de los datos? 37. 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? 38. El sistema permite identificar los documentos vitales[4]?

	39. Permite la restauración de los documentos vitales y los demás en operaciones separadas?
Encripción	40. Permite almacenar junto con los documentos electrónicos la firma o firmas asociadas a tal documento? 41. Permite almacenar junto con los documentos electrónicos el certificado o certificados digitales que validan la firma? 42. 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? 43. Permite presentar una estructura que introduzca fácilmente distintas tecnologías de encripción?
Interoperabilidad	44. Permite encriptar los documentos y hacer imposible su consulta por fuera del sistema? 45. Permite garantizar la captura de documentos encriptados directamente desde la aplicación de software que posea tal capacidad? 46. Permite interactuar en doble vía con otros sistemas de información de la empresa?

Integración con otras aplicaciones	47. Permite procesar transacciones en tiempo real, que sean generadas por otros sistemas externos de aplicaciones? 48. Permite la gestión de procesos para multiples empresas 49. Permite modelar reportes propios según la necesidad del proceso y sin nuevos desarrollos 50. Se debe permitir la gestión de documentos en las diferentes aplicaciones (traslado de documentos entre aplicaciones, cambios de índices, anexo o eliminación de páginas, ..etc.) 51. Debe permitir la visualización y navegación sobre los diferentes aplicaciones y documentos a través de un navegador de internet. 52.

Documentos no electrónicos	Permite configurar la productividad esperada diaria por cada proceso?
	Permitir visualizar en una línea de tiempo y saber el avance de los procesos programados?
	Permite generar alertas cuando un proceso esta incumpliendo las metas programadas?
	Permite definir carpetas y subcarpetas en el sistema de clasificación?
	Permite que la presencia de registros de documentos físicos, se refleje y se gestione del mismo modo que los documentos electrónicos?
	Permite que en el sistema de clasificación las carpetas y subcarpetas contengan tanto documentos electrónicos, como físicos mediante el registro de su información?
	Permite la administración integrada de carpetas fisicas y electrónicas de documentos? Esto es carpetas o expedientes híbridos.
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?
	Permite registrar información básica de identificación de los documentos físicos, como sus fechas y ubicación física?
	Permite que los registros de los documentos físicos hagan parte integral de los resultados de búsquedas?
	Permite controlar los documentos fisicos que se han incluido a traves del ECM en expedientes electronicos
	El sistema debe permitir parametrizar el tiempo de vencimiento de los préstamos documentales.

	El sistema debe ofrecer una funcionalidad que permita solicitar el préstamo de expedientes.
	El sistema debe permitir aceptar o rechazar el préstamo.
Flujos de trabajo	El sistema debe controlar la devolución del préstamo.
	El sistema debe registrar en el histórico del expediente el registro de la operación en torno al proceso de préstamo documental.
	Permite controlar las ubicaciones fisicas de los expedientes, con metadatos tales como estante, cara, entrepaño etc
	Permite limitar el número de pasos que componen una tarea o flujo de trabajo?
	El flujo de trabajo permite el uso de correo electrónico como medio de notificación de las acciones que se realizan en el flujo?
	Permite que los flujos de trabajo inicien o no con un documento?
	Permite que en los flujos de trabajo se agreguen más documentos de ser necesario?
	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?
	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?
	La función de flujos de trabajo permite consignar en la pista de auditoría todas las acciones propias del desarrollo del flujo?
	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?
	La función de flujos de trabajo permite reconocer como "participantes" tanto a los individuos como a los grupos de trabajo?
	La funcion de flujos de trabajo permite hacer ruteo de contenido y de tareas
	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
	Permite hacer ruteo basado en un motor de reglas de negocio
	Permite definir los flujos de trabajo basado en plantillas
	Permite la administracion de los flujos creados en una consola unificada
	Permite hacer encadenamiento e integracion de flujos
	Permite el ruteo y asignacion de tareas ad hoc
	Permite la creacion grafica de flujos
	Permite incluir scripts para logica avanzada
	Permite ruteo paralelo
	Permite asignar precedencia y prioridad a las tareas del flujo
	Permite cambiar la precedencia y prioridad a las tareas del flujo en ejecución

	Realiza manejo de excepciones y errores
	Permite detener un flujo
	Permite definir limites de tiempo, escalamiento y reasignacion basado en timers
	Notificacion automatica de los estados de las tareas configurable
	Ejecucion del flujo programada y/o iniciada por eventos
	Permite manejar grupos de flujos
	Maneja una cola de trabajo de los usuarios y una lista de tareas
	Monitoreo de flujos
	Reportes de flujos
	Soporte a firmas electronicas dentro del flujo
Firmas Electrónicas y Estampado Cronológico	La función de flujos de trabajo permite asociar fechas límite a pasos o procesos individuales de cada flujo?
	La función de flujos de trabajo permite informar de los elementos atrasados conforme a los límites?
	Permite incluir instrumentos de informes exhaustivos que permitan a los gestores controlar el volúmen, los resultados y las excepciones del proceso?
	Permite que se incluyan metodos que garanticen la integridad de la información, como las firmas electrónicas?
	Permite que se incluyan metodos que garanticen la integridad de la información, como el estampado cronológico?
	Permite presentar una estructura que facilite la introducción de distintas tecnologías de firma electrónica?
	Permite verificar la validez de una firma electrónica?
	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?
	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?
	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?
	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?
Encripción	Permite almacenar junto con los documentos electrónicos la firma o firmas asociadas a tal documento?
	Permite almacenar junto con los documentos electrónicos el certificado o certificados digitales que validan la firma?

	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?
Inter-operabilidad	Permite encriptar los documentos y hacer imposible su consulta por fuera del sistema?
	Permite garantizar la captura de documentos encriptados directamente desde la aplicación de software que posea tal capacidad?
otros	Permite presentar una estructura que introduzca fácilmente distintas tecnologías de encripción?
	Permite interactuar en doble vía con otros sistemas de información de la empresa?
Integracion con otras aplicacines	Permite procesar transacciones en tiempo real, que sean generadas por otros sistemas externos de aplicaciones?
	Permite la gestión de procesos para multiples empresas
	Permite modelar reportes propios según la necesidad del proceso y sin nuevos desarrollos
	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.)
	Debe permitir la visualización y navegación sobre los diferentes aplicaciones y documentos a través de un navegador de internet.
Facilidad de uso	Recuperacion de información de los índices de documentos, numero de paginas, retornar documento.
	Se debe permitir realización de OCR sobre los documentos con marcaciones identificadas.
	Debe permitir la marcación y categorización de las marcaciones sobre los documentos.
	Tiene asistencia en línea al usuario 7/24?
	Permite contar con mensajes de error claros, de forma que el usuario pueda identificar la falla y darle solución?
	Permite proporcionar al usuario final y al administrador en todo momento, funciones de uso fácil e intuitivo?
	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?
	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?
	Siempre que se lleve a cabo la función anterior, permite que el sistema envíe, en lugar de copias, referencias a tales elementos de correo?

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: - Contenidos de los menús, - Disposición de las pantallas, - Uso de teclas de funciones y atajos de teclado, - Colores y tamaño de las fuentes que se muestran en pantalla?
	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?
	Incluye alguna función de ayuda sobre el uso del sistema de clasificación?
	Debe ofrecer tiempos de respuesta adecuados para la realización de las funciones habituales en ciertas condiciones normalizadas, como: - Con el 10% de la totalidad de la población prevista de usuarios conectada y activa, - Con el 100% del volúmen total previsto de documentos gestionados por el sistema, - Con usuarios realizando una combinación de tipos de transacción a distintas velocidades. En estas condiciones, el rendimiento se deberá mantener estable durante un mínimo de diez intentos de transacción.
	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
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.
	Debe permitir la expansión controlada del sistema hasta al menos 5000 usuarios sin perjudicar la continuidad y eficacia del servicio
	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.
	El sistema deberá estar disponible las 24 horas del día, 7 días de la semana, 365 días del año.
	El período de inactividad previsto del sistema, no debe superar las 40 horas al año
Flexibilidad	El tiempo de inactividad no prevista del sistema, no debe superar las 10 horas al trimestre.
Despliegue	La disponibilidad debe ser flexible para ofertas de servicio en nube
	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.

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.
	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.
	Los plugins y desarrollos personalizados, deben permitir su fácil instalación y despliegue.
	Debe ser 100% web y su administración y parametrización debe realizarse desde el navegador. Se deben proveer interfaces de escritorio opcionales.
	Integracion con almacenamiento secundario (para documentos con acceso infrecuente) en nube y onPremises
	Soporte a multiples repositorios
	Soporte completo al estandar CMIS 1.1
	Funcionalidades publicadas como servicios que soporten al menos Web Services (SOAP) y REST
	Cache de contenidos para acceso frecuente
	Almacenamiento y administracion nativas de tipos BLOB
	Soporte para NAS
	Soporte para SANs
	Soporte para DAS

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. La solución debe proveer al menos dos intefaces para la Gestión del ECM y sus componentes: * Interface de comandos * Interface gráfica de usuario 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.
	Se deben incluir avisos de derechos de propiedad intelectual en todo el código fuente y en la presentación de la aplicación.

	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).
	La aplicación debe disponer de un módulo para manejo de eventos y alertas de seguridad.
	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:
	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,
	Error: Cualquier evento que represente un intento de violación a las políticas o controles de seguridad definidos para la aplicación.
	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.
	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.
	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.
	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.

	Se deben generar registros de control o hashes que permitan validar la integridad de los registros de seguridad generados.
	Se debe permitir definir y controlar por parámetro las siguientes acciones a realizar con los archivos que contienen los registros de seguridad:
	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.
	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.
	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.
	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.
	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.
	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.
	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.

	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.
	El sistema debe borrar automáticamente toda la información sensible almacenada temporalmente ante terminaciones exitosas o ante fallas de la aplicación.
	El aplicativo debe permitir controlar por parámetro la emisión de copias adicionales de los informes que genera.
	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.
	Todas las aplicaciones Web (Web-Oriented) deben permitir el manejo de protocolos seguros con certificados digitales para el intercambio de información confidencial.
	La aplicación debe permitir restringir la conexión por dirección IP específica.
	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.
	La aplicación debe permitir cambiar mediante parámetros, los puertos por defecto con los cuales se integran sus diferentes módulos y capas.
	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.
	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.

	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.
	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.
	La aplicación debe generar mensajes que muestren al usuario la fecha y hora de su último ingreso, preferiblemente en la pantalla de Log-In.
	Se debe permitir la autenticación mediante código de usuario y clave.
	La aplicación debe poseer un módulo para administración de la identificación, autenticación y autorización.
	El módulo para administración de la identificación, autenticación y autorización debe ser independiente a la aplicación.
	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.
	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.
	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.

	La deshabilitación de los códigos de usuario debe estar restringida a usuarios con privilegios suficientes para hacerlo.
	La aplicación debe permitir manejar esquemas de delegación de administración de códigos de usuario.
	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.
	El sistema debe permitir definir por parámetro y controlar la longitud mínima de las contraseñas.
	El sistema debe permitir definir por parámetro y controlar la longitud máxima de las contraseñas.
	El sistema debe permitir definir por parámetro y controlar el número de contraseñas a recordar (Histórico de contraseñas).
	El sistema debe permitir definir un diccionario de contraseñas no válidas y controlar que las contraseñas no coincidan con las existentes en dicho diccionario.
	La aplicación debe controlar mediante parámetro que las contraseñas contengan o no la identificación del usuario como una parte de éstas.
	La aplicación debe controlar mediante parámetro que la contraseña contenga o no alguna sucesión lógica de números o letras.
	La aplicación debe controlar mediante parámetro que la contraseña pueda o no ser generada de manera aleatoria.
	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.
	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.
	La aplicación debe desconectar los usuarios que hayan permanecido inactivos en el sistema durante un tiempo definido mediante un parámetro que especifique este tiempo.

	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.
	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.
	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.
	El sistema debe exigir a los usuarios cambiar su contraseña de manera automática cuando se presenten las siguientes condiciones:
	a. Acceso por primera vez al aplicativo.
	b. Expiración de la vigencia de la contraseña.
	c. Reactivación o modificación de la contraseña por parte del administrador.
	La aplicación deberá permitir cambiar la contraseña a solicitud del usuario validando la vigencia mínima de la contraseña.
	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.
	El aplicativo debe permitir controlar la no repetición de un número específico de contraseñas, definido por parámetro.
	El sistema debe permitir manejar los siguientes estados para los códigos de usuario: Habilitado, deshabilitado, bloqueado, suspendido.
	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.

	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.
	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.
	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.
	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.
	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.
	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.
	Se debe almacenar la información histórica de cualquier código de usuario eliminado de manera que se facilite la recuperación en caso de ser requerida.

	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.
	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.
	La aplicación debe permitir, como mínimo, la administración de los siguientes parámetros para definir los perfiles de acceso de los usuarios:
	a. Tabla o archivo del aplicativo.
	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).
	c. Menú o módulo de la aplicación.
	d. Opción de la aplicación.
	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.
	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.