AGTIC
ASESORAMIENTO
Y GESTIÓN EN TIC

Modelo de Gestión del Documento Electrónico

Capítulo 7. Modelo de seguridad

DIPUTACIÓN
DE ALMERÍA

Junio de 2020

ÍNDICE

1. Introducción

La Diputación de Almería dispone de una Política de Seguridad de la Información y de procedimientos relacionados que abarca todos los ámbitos de la seguridad de la información de acuerdo a lo exigido por el Esquema Nacional de Seguridad cuyo alcance es el mismo que el del presente MGDE relativo al procedimiento administrativo.

En consonancia con esta Política de Seguridad de la Información, en este capítulo del Modelo de Gestión del Documento electrónico se desarrolla el modelo de seguridad del documento y expediente electrónico (en adelante, **modelo de seguridad documental**) que tiene por objetivo definir los aspectos específicamente relacionados con la seguridad en el acceso y tratamiento de expedientes y documentos electrónicos. Para el resto de los aspectos relacionados con la seguridad de la información será necesario referirse a la Política de Seguridad mencionada.

En este sentido, si partimos de las principales dimensiones de seguridad establecidas por estándares de referencia como el Esquema Nacional de Seguridad, que comprende el conjunto de criterios y recomendaciones en materia de seguridad, conservación y normalización de la información, de los formatos y de las aplicaciones, o la ISO27001, para el establecimiento de un sistema de gestión de la seguridad de la información, la seguridad de la información aplicada a la gestión documental implica:

- **Autenticidad**: Se garantiza la fuente de la que proviene la información contenida en un documento, es decir, su autoría, quedando el autor vinculado por las declaraciones contenidas en el documento o los metadatos relacionados.
- **Integridad**: Se mantiene de forma continuada y exacta la información contenida en un documento, es decir, que no ha recibido modificaciones no autorizadas.
- **Confidencialidad**: La información de expedientes y documentos electrónicos no se pone a disposición de individuos, entidades o procesos no autorizados o que no necesiten conocerla.
- **Disponibilidad**: Se provee el acceso y utilización de la información y documentos, e incluso los sistemas para su tratamiento, por parte de los individuos, entidades o procesos autorizados cuando lo requieran.
- **Trazabilidad**: las acciones de una entidad sobre un documento pueden ser imputadas exclusivamente a esta entidad y se pueden identificar y reconstruir adecuadamente las acciones que se han hecho sobre el documento, desde su creación y todas sus modificaciones.

Para dar cobertura a estas dimensiones de seguridad, el modelo de seguridad documental de la Diputación de Almería va orientado esencialmente a:

- proteger la información confidencial, en general;

- proteger los datos personales de los documentos, en concreto;
- proteger la propiedad intelectual;
- promover la interoperabilidad de confianza;
- apoyar la divulgación y difusión de forma controlada de la información de la cual es responsable.

Adicionalmente, el modelo de seguridad documental de la Diputación de Almería se rige por:

- Los principios y normas aplicables a la protección de la confidencialidad y privacidad de datos entre los que se encuentra la legislación vigente sobre protección de datos de carácter personal y los estándares de seguridad informática de referencia como el Esquema Nacional de Seguridad o la ISO27001.
- Los informes de la Dirección de Archivo y Biblioteca de la Diputación de Almería el cual es el encargado de la evaluación y la definición de los criterios de acceso a los documentos.
- Las Tablas de Valoración Documental aprobadas por la Comisión Andaluza de Valoración de Documentos.
- Lo establecido por el presente apartado del Modelo de Gestión del Documento Expediente electrónico.

Para dar respuesta a estos requisitos sobre las herramientas de gestión documental de la Diputación de Almería, se establecen cuatro procesos clave cuyo objetivo es asegurar un adecuado control de acceso a la información a lo largo de todo el Ciclo de vida de los expedientes y documentos electrónicos. Estos cuatro procesos clave se enumeran a continuación junto con la pregunta a la que pretenden dar respuesta:

- **Autenticación**: ¿Quién puede acceder al Sistema de gestión de expedientes y documentos electrónicos?
- **Recuperación de la información**: ¿Cómo se asegura la integridad de la información almacenada ante eventuales incidentes de seguridad?
- **Monitorización**: ¿Qué se hace sobre la información y cuándo se hace?
- **Acceso**: ¿Quién puede hacer qué sobre la información almacenada en el sistema de gestión de expedientes y documentos electrónicos?

A continuación, se definen estos cuatro procesos y finalmente se establecen las directrices sobre las cuales se podrá realizar su aplicación práctica en el sistema de gestión de expedientes y documentos electrónicos de la Diputación de Almería.

Antes de ello, resulta importante definir que como **Sistema de gestión de expedientes y documentos electrónicos** se considera cualquier aplicación que participe en la incorporación de documentos en el gestor documental. Para mayor detalle consultar el capítulo 6 de este

Modelo de Gestión del Documento electrónico sobre el modelo tecnológico del documento y expedientes electrónicos.

2. Autenticación y acceso

Para identificar inequívocamente a las personas que acceden al sistema de gestión de expedientes y documentos electrónicos, es necesario disponer de una funcionalidad de autenticación de usuarios. En el caso de la Diputación de Almería, este Sistema está basado en integraciones realizadas con un sistema de autenticación centralizado que permite la gestión del control de acceso de los usuarios a los distintos entornos informáticos de gestión mediante el uso de contraseñas seguras que son renovadas periódicamente por los usuarios, según establece la Política de Seguridad de la Información y procedimientos que la desarrollan.

Asimismo, para garantizar que cada usuario acceda a la información que precise para el desarrollo de sus funciones, las distintas aplicaciones que conforman el sistema de gestión de expedientes y documentos electrónicos disponen de funcionalidades de definición de perfiles de acceso. Estas funcionalidades son descritas con mayor detenimiento en el apartado 5.1 del presente capítulo.

La conjunción del sistema de autenticación y de las funcionalidades de segregación de funciones de las aplicaciones del sistema de gestión de expedientes y documentos electrónicos:

- Permiten la validación de todo usuario que intente acceder al sistema y permitirle acceso a recuperar información y documentación en consonancia con los permisos de que disponga.
- Permiten realizar las acciones sobre la información y documentación para las que el usuario tenga capacidad según los permisos asignados.
- No permiten al usuario el acceso y/o edición de documentos en función de los permisos asignados.
- Informan al usuario en caso de que intente acceder a una información dañada ya sea porque se ha corrompido, se haya perdido información, se haya modificado indebidamente o no se pueda validar.

Para asegurar estas premisas, desde el punto de vista de la autenticación al sistema de gestión de expedientes y documentos electrónicos, ésta se llevará a cabo, siempre, de forma nominal con el propio usuario de cada persona con acceso autorizado al sistema. Por lo tanto, los usuarios genéricos quedan terminantemente prohibidos a no ser que cada acción realizada por los mismos pueda ser asociada inequívocamente a una persona o proceso del sistema que las haya ejecutado.

Adicionalmente, esta autenticación se realizará mediante tres vías principales, siendo:

- **Autenticación sobre las aplicaciones de gestión de procedimientos electrónicos.** Los usuarios responsables de la tramitación de procedimientos se autenticarán sobre las herramientas que permiten llevar a cabo las actividades de gestión de los procedimientos de la Diputación de Almería. Estas herramientas accederán a la documentación almacenada en el sistema de gestión de expedientes y documentos electrónicos con base en los permisos otorgados al usuario en la aplicación de gestión de procedimientos correspondiente.
- **Autenticación sobre el sistema de gestión de expedientes y documentos electrónicos.** El personal responsable de la Dirección de Archivo y Biblioteca de la Diputación de Almería, es decir, de las fases de vigencia y de valor histórico de la documentación electrónica, se autenticarán con perfil administrador de gestión documental a la aplicación de gestión de documentos electrónicos. Dicho perfil permitirá acceso de lectura y no de modificación ya que ello se realizará a través de las aplicaciones de gestión de procedimientos electrónicos durante la fase de tramitación.
- **Acceso vía capa de interoperabilidad.** Este modo de acceso aplica en aquellos casos en que mediante acuerdo con la Plataforma de Intermediación de Datos la Diputación ofrece a otras administraciones públicas el acceso a documentación e información emitida por la Diputación y que pueda ser de utilidad en la tramitación de procedimientos de otras Administraciones Públicas con el objetivo de reducir cargas administrativas al ciudadano. En este caso, el control de acceso se fundamentará en identificación basada en el certificado digital de aplicación y garantizará que sólo tengan acceso aquellas administraciones públicas que hayan suscrito el correspondiente convenio y tengan interés legítimo en acceder a la información, guardándose la debida constancia de ello, así como de la información accedida y del momento del acceso.

  Excepcionalmente, entre la Diputación y otras Administraciones Públicas, fuera de la Plataforma de Intermediación de Datos, se implementarán mecanismos alternativos de intercambio de información y de autenticación según se establezca en cada caso.

3. Recuperación de la información

Todo sistema de seguridad debe disponer de un servicio de restauración y recuperación de la información que permita recuperarla en el estado más próximo al momento en el que sucedió un incidente de seguridad con efecto sobre la integridad de la información.

Según esta premisa, todo sistema que participe en la gestión de expedientes y documentos electrónicos debe:

- Permitir guardar todas los expedientes y sus documentos y firmas electrónicas y metadatos asociados.

- Disponer de sistemas automáticos de copias de seguridad y de recuperación.
- Permitir definir la ubicación sobre la que se realizará y recuperará la copia.
- Permitir a un rol administrador la posibilidad de acceder y restaurar las copias de seguridad.
- Facilitar los datos referentes a la situación en qué ha sido recuperada la información y documentación.

En este sentido es necesario asegurar la correcta aplicación de la política de copias de respaldo y recuperación de los sistemas de información definida por la Diputación de Almería y, en el ámbito de la gestión de expedientes y documentos electrónicos, respetar las siguientes directrices:

- Todos los documentos, metadatos y otros contenidos de carácter documental se almacenan sistemáticamente en los repositorios destinados al efecto, sobre los cuales se aplican los procesos de copia de seguridad y recuperación. No existen documentos o datos relevantes para la gestión documental almacenados de manera temporal o provisional en repositorios que no cumplan con la política de recuperación.
- Existe un inventario y clasificación de las copias de seguridad, a fin de posibilitar la identificación de cada una de ellas y su contenido, así como de posibilitar su debida administración y recuperación.
- Se asigna a la información de recuperación las debidas medidas de control de acceso físico y ambiental ubicándose suficientemente alejadas de las instalaciones principales para que un mismo incidente de seguridad no pueda afectar a la información en el entorno de producción y de recuperación.
- Se almacenan los procedimientos de recuperación en una ubicación que cumpla unos requisitos que permitan asegurar su protección, seguridad y, en caso de ser necesario, su debido uso.
- Se verifican y se prueban periódicamente los procedimientos de restauración de información garantizando su eficacia y cumplimiento dentro del tiempo asignado a la recuperación en los procedimientos operativos según su criticidad.
- Se establecen periodos de sustitución de los medios de almacenamiento de las copias de resguardo, una vez concluida la posibilidad de ser reutilizados según las recomendaciones del fabricante.

4. Monitorización

En el sistema de gestión de expedientes y documentos electrónicos es indispensable disponer de mecanismos que permitan monitorizar qué acciones se realizan sobre él con el objetivo de

validar que, tanto el propio sistema como los usuarios que actúan sobre el mismo, pueden realizar sus actividades de forma correcta y en el tiempo adecuado.

En este sentido es necesario que el sistema sea monitorizado en dos aspectos primordiales:

- **Uso del Sistema:** registro de las actividades sucedidas sobre el sistema por parte de los usuarios y procesos automáticos que garanticen la trazabilidad de las actuaciones sucedidas en el sistema y obtener estadísticas sobre su uso.
- **Operación del Sistema:** actividades encaminadas a asegurar el adecuado mantenimiento y explotación del sistema para garantizar el correcto desempeño de las funcionalidades que le son atribuidas.

Seguidamente se definen estos aspectos con mayor profundidad.

4.1 Uso del sistema

El control y seguimiento del uso del sistema de gestión de expedientes y documentos electrónicos se llevará a cabo a través de un conjunto de indicadores del sistema. Estos indicadores se dividirán en dos ámbitos diferentes:

- **Indicadores unitarios**: Permiten realizar el seguimiento de qué acciones se realizan sobre los expedientes y documentos del sistema. Con estos indicadores será posible determinar quién, cuándo y qué se ha hecho sobre el sistema en un momento concreto y para un expediente o documento concretos.

  Para no afectar al rendimiento del sistema, ya que a mayor nivel de auditoría menor rendimiento del sistema, se plantea un nivel de auditoría medio-alto, donde los indicadores unitarios que se registren sean los siguientes, pudiendo ser más o menos detallados en función de determinados valores del conjunto de metadatos correspondiente a eEMGDE21 – Trazabilidad según se establezca en el Vocabulario de Metadatos de la Diputación:

  - Accesos al sistema
  - Creaciones de objetos, entendiéndose objeto como expediente, documento o firma electrónica.
  - Eliminación de objetos
  - Versionado de documentos.
  - Cambios en el valor del conjunto de metadatos eMGDE8 - Seguridad que participen en el control de acceso a expedientes y documentos electrónicos.
  - Modificaciones sobre los roles de acceso de los usuarios.
  - Modificaciones de usuarios con acceso confidencial a un expediente electrónico.

- Actuaciones realizadas por los usuarios con capacidad de administración del sistema de gestión de expedientes y documentos electrónicos.

- **Indicadores volumétricos**: Permiten dar una visión en conjunto sobre cuál es el uso del sistema de gestión de expedientes y documentos electrónicos. Con estos indicadores se debe disponer de información estadística útil para el análisis del sistema en los ámbitos de:
  - Trazabilidad. Actuaciones realizadas sobre objetos, usuario responsable de la actuación y momento en el que suceden.
  - Uso. Acceso y modificación de expedientes y documentos electrónicos realizada por un usuario.
  - Tiempo. Durante el cual se accede o modifica un expediente o documento electrónico por parte de un usuario.

4.2 Operación del sistema

Como cualquier otro sistema, el sistema de gestión de expedientes y documentos electrónicos requiere de una supervisión continua mediante procesos de monitoreo que registren información sobre su funcionamiento útil para asegurar su correcta ejecución.

Estos procesos de monitoreo son procedimientos internos del sistema, transparentes para el usuario final, que estarán bajo el control del rol de Administrador tecnológico del sistema (ver apartado 5.1.2) y se llevarán a cabo de forma periódica.

Estos procedimientos, que se definen específicamente para cada sistema involucrado en el tratamiento de expedientes y documentos electrónicos sobre el procedimiento de explotación correspondiente, contemplarán como mínimo las siguientes acciones:

- Ejecución de procedimientos de monitorización y revisión para:
  - Detectar a tiempo los errores en los resultados generados por el procesamiento de la información.
  - Identificar incidencias e información útil para su resolución.
  - Determinar si las actividades desarrolladas por las personas y dispositivos tecnológicos para garantizar la seguridad de la información se desarrollan en relación a lo previsto.
  - Detectar y prevenir eventos e incidentes de seguridad mediante el uso de indicadores.
  - Revisar regularmente la efectividad del sistema.
- Revisión, en intervalos planificados, de las evaluaciones de riesgo, los riesgos residuales y sus niveles aceptables, las amenazas internas y externas existentes y la

efectividad de los controles para la mitigación de riesgos tal y como establece la gestión de riesgos establecida por la Política de Seguridad de la Diputación de Almería.

- Realización periódica de auditorías internas y externas de seguridad y actualización de los planes de seguridad en función de las conclusiones y deficiencias detectadas.
- Registro y revisión proactiva de acciones y eventos que puedan haber tenido impacto sobre la efectividad o el rendimiento del sistema.

5. Acceso

El sistema de gestión de expedientes y documentos electrónicos debe asegurar que se pueda restringir y controlar el acceso a los expedientes, a sus documentos y a la información que éstos contienen.

Según esta premisa, el sistema debe:

- Permitir la definición de roles de administrador tecnológico del sistema que pueda configurar los roles de acceso de cada usuario.
- Identificar los usuarios impidiendo el acceso en caso de no estar autorizados ya sea porque su rol de acceso no lo permita o, aun teniendo el rol de acceso adecuado, no dispongan de acceso confidencial a un expediente o documento clasificado con este nivel de seguridad.
- Asignar niveles de seguridad a los expedientes y documentos en función de su clasificación de seguridad según el Cuadro de Clasificación de la Diputación de Almería (configurando el metadato eMGDE8.1.1 – Nivel de Acceso de expediente o documento como de acceso secreto, reservado, confidencial o no clasificado).
- Restringir el acceso a series del cuadro de clasificación documental según el rol del usuario y a ciertas expedientes o documentos según su nivel de seguridad (en caso de estar calificado este metadato de expediente o documento como de acceso secreto, reservado o confidencial).
- Permitir definir advertencias de seguridad para expedientes o documentos que requieran de un tratamiento especial al efecto de su seguridad mediante el valor de los metadatos eEMGDE8.2.1 – Texto de la advertencia y eEMGDE8.2.2 – Categoría de la advertencia.
- Facilitar la identificación de criterios que afecten a la seguridad de expedientes y documentos, concretamente:
    - del contenido de datos sensibles en el expediente o un documento concreto de acuerdo a la normativa de protección de datos según el metadato eEMGDE8.4 – Sensibilidad datos de carácter personal.

- de su clasificación de acuerdo con el Esquema Nacional de Seguridad según el metadato eEMGDE8.5 – Clasificación ENS.
- De su nivel de confidencialidad de acuerdo con el Esquema Nacional de Seguridad según el metadato eEMGDE8.6 – Nivel de confidencialidad de la información.

- Facilitar la identificación de aquellos documentos de acceso público eEMGDE9.1 – Tipo de acceso, fijando las condiciones de reutilización establecidas según el metadato eEMGDE9.4 – Condiciones de reutilización de acuerdo con la normativa aplicable establecida en el metadato eEMGDE9.3 – Causa legal/normativa de limitación.
- Establecer un grupo de usuarios asociado a Series documentales. Si un usuario no tiene asociado el acceso a una Serie documental tampoco podrá acceder a los expedientes relacionados y la documentación que contengan.
- Permitir asignar un usuario a un grupo de usuarios con el mismo rol.
- Permitir que un usuario pertenezca a más de un grupo.
- Vetar el acceso a los expedientes o los documentos electrónicos conforme los niveles de seguridad asignados.
- Si un usuario busca textos contenidos en metadatos o documentos correspondientes a expedientes a las que no tiene acceso no se debe permitir su visualización. Para el usuario este expediente no existe y, por lo tanto, la búsqueda no debe devolver resultados relacionados.
- Permitir que la clasificación de seguridad asignada varíe temporalmente de forma automática en función de determinados parámetros o metadatos del expediente o sus documentos.
- Permitir asignar a expedientes y documentos concretos niveles de seguridad más restrictivos que la serie documental a la que pertenecen.
- Permitir asignar a documentos concretos dentro de un expediente niveles de seguridad más restrictivos que el del expediente al que pertenecen.

Para cumplir con estos requisitos, hay que dar respuesta a dos preguntas primordiales:

- ¿Qué se puede hacer a nivel funcional?
- ¿Cuándo se puede hacer?

La respuesta a estas dos preguntas se estructura en dos modelos que se combinan entre sí, para constituir el modelo de restricción de acceso que se aplicará en todo el sistema durante todo el ciclo de vida de los expedientes y documentos electrónicos. Estos modelos son, respectivamente a cada pregunta: Roles de acceso y Niveles de seguridad, según se describe a continuación.

5.1 Roles de acceso

Para permitir la flexibilidad en la gestión del acceso al sistema y garantizar que cada usuario dispone de acceso a aquella información que requiere para el desempeño de sus funciones, la gestión del acceso se llevará a cabo mediante un modelo de seguridad documental basado en roles.

El "rol" debe entenderse como un perfil de usuario, no como un cargo o un puesto de trabajo. Las personas con el mismo "rol" compartirán responsabilidades y permisos funcionales sobre el sistema de gestión de expedientes y documentos electrónicos.

Cada uno de estos roles tienen asociado un conjunto de acciones a poder llevar a cabo sobre las series documentales y, evidentemente, sobre los expedientes electrónicos y sus respectivos documentos electrónicos.

Existen 2 tipos de roles según su ámbito de aplicación, ya sea a nivel de serie documental o a nivel de todas las series documentales del sistema de gestión de expedientes y documentos electrónicos.

De acuerdo con esta clasificación, los roles del sistema de gestión de expedientes y documentos electrónicos son los que se muestran en la siguiente tabla, identificándose sus permisos funcionales en las fases del ciclo de vida del documento y expedientes electrónicos, y describiéndose detenidamente a continuación de la tabla.

	Fase de tramitación			Fase de vigencia y archivo		Información Pública
Grupo de usuarios	Consulta	Modificación	Eliminación	Consulta	Eliminación	Consulta
Equipo de tramitación	Sí	Sí	Sí	Sí	No	Sí
Consulta restringida	Sí	No	No	Sí	No	Sí
Consulta pública	Sí	No	No	Sí	No	Sí
Aplicación	Sí	Sí	Sí	Sí	No	Sí

	Fase de tramitación			Fase de vigencia y archivo		Información Pública
Administrador de gestión documental	No	No	No	Sí	Sí	Sí
Administrador tecnológico	Sí	Sí	Sí	Sí	Sí	Sí
Terceras partes: colaboradores y usuarios.	Solo si es parte interesada	Solo si es parte interesada	Solo si es parte interesada	Solo si es parte interesada	Solo si es parte interesada	Sí

5.1.1 Roles de serie documental

Los roles de serie documental tienen las siguientes propiedades:

- Los usuarios tienen acceso a series documentales mediante la atribución de roles de acceso.
- Se asignan a todas las series documentales relacionando series documentales con roles de acceso.
- Cada serie documental se puede configurar por separado.
- Cada rol dispone de un conjunto de permisos propio sobre un conjunto de series y fase del ciclo de vida del documento y expediente electrónicos, pudiendo ser de consulta, modificación y eliminación.
- Los permisos de cada rol son los mismos para cada serie que dispongan relacionada.
- A los roles se asignan aquellos usuarios o grupos de usuarios pertinentes para cada serie.

De acuerdo con ello, se definen los siguientes grupos de usuarios:

- **Equipo de tramitación**: Es el equipo responsable de la tramitación de los expedientes de un proceso de la Diputación de Almería. Tiene la potestad de crear expedientes vinculados a series documentales para los que esté autorizado y, mientras permanezcan abiertos, de:
  - Editar los metadatos editables del expediente, entre ellos el siguiente relevante a efectos de seguridad:

- El metadato eMGDE8.1.1 – Nivel de acceso sobre el carácter de secreto, reservado, confidencial o no clasificado de un expediente (ver apartado 5.2 sobre niveles de seguridad). Debe considerarse que:
  - el carácter confidencial de un expediente tendrá como consecuencia que sólo los usuarios que hayan participado en la tramitación del procedimiento que la genera y quienes éstos determinen dispondrán de acceso a la misma, aunque pertenezca a un expediente de una serie documental a la que disponen de acceso de tramitación o de consulta, restringida o pública, más usuarios.
  - el carácter confidencial de un documento tendrá la misma consecuencia sobre el documento en cuestión a pesar de que el expediente al que pertenezca disponga de un nivel de acceso menos restrictivo.

- Crear, introducir y modificar documentos en el expediente.
- Editar los metadatos editables de los documentos, entre ellos el siguiente relevante a efectos de seguridad:
  - El metadato eEMGDE20A – Versión del documento sobre el estado definitivo de un documento por el cual el documento no podrá ser eliminado aún y encontrándose el expediente en fase de tramitación.
- Realizar firmas electrónicas y editar aquellos metadatos de firma no recopilados automáticamente desde la propia firma como, por ejemplo, la ubicación.
- Eliminar documentos del expediente no considerados como definitivos o con valor borrador en el metadato eEMGDE20A – Versión del documento.
- Cerrar expedientes.

- **Consulta restringida**: Dispondrá de permisos para consultar el expediente y sus respectivos documentos y metadatos, pero no editarlos ni añadir documentos adicionales siempre que estén vinculados a series documentales para los que tiene acceso. En la mayoría de los casos estará formado por las mismas personas que conforman el equipo de tramitación que dispondrán de acceso a expedientes cerrados, en fase de vigencia y archivo, o por personas que para el desempeño de sus funciones requieren de acceso de consulta a los expedientes de una serie documental, tanto en fase de tramitación como de vigencia y archivo. Tiene la potestad de:
  - Consultar documentos de expedientes pertenecientes a series documentales para las que se esté autorizado.
  - Consultar metadatos de expediente.

- Consultar metadatos de documento.
- Consultar metadatos de firma electrónica.

- **Consulta pública:** Rol similar al de consulta restringida, pero reservado a la consulta de expediente y sus respectivos documentos de todo el sistema siempre que sean calificados como de acceso público a través del metadato eEMGDE9.1 – Tipo de acceso en atención a las condiciones de reutilización establecidas según el metadato eEMGDE9.4 – Condiciones de reutilización de acuerdo con la normativa aplicable establecida en el metadato eEMGDE9.3 – Causa legal/normativa de limitación. Tiene la potestad de:
  - Consultar documentos calificados como de acceso público.
  - Consultar metadatos de expediente.
  - Consultar metadatos de documento.
  - Consultar metadatos de firma electrónica con las debidas precauciones de protección de datos personales, no mostrando, por ejemplo el número de DNI.
- **Aplicación:** Rol especial con permisos similares al Equipo de tramitación que permite la interacción automática de herramientas informáticas verticales de gestión de procedimientos con el sistema de gestión documental para aquellas series documentales con las que opere y partiendo de la base de la gestión de permisos de usuario establecida en la aplicación de gestión de procedimientos. Tiene la potestad de:
  - Crear expedientes.
  - Editar los metadatos editables del expediente.
  - Crear, introducir y modificar documentos en los expedientes.
  - Editar los metadatos editables de los documentos y de sus firmas electrónicas.
  - Eliminar documentos del expediente no considerados como definitivos.
  - Cerrar expedientes.
- Terceras partes: colaboradores y usuarios. Este perfil de usuario corresponderá a partes externas a la Diputación de Almería que dispondrán de acceso a la documentación pública en todo caso y al resto de documentación si son parte interesada.

  Mientras el acceso a la información pública se realizará a través de la web pública de la Diputación de Almería sin proceso de autenticación alguno, el acceso al resto de documentación se realizará a través del Portal de Gestión Documental o de las funcionalidades de tramitación electrónica accesibles a través de la Sede electrónica de la Diputación de Almería contando con un proceso de autenticación fehaciente

basado, en función de la proporcionalidad de la información accedida, en certificado digital o usuario y contraseña. En su caso se aplicarán procesos de autorización de acceso a la información que deberán ser otorgados por el Servicio de Organización e Información en coordinación con el departamento responsable de la documentación.

Adicionalmente, en caso de ser parte interesada y en función del procedimiento en el que participen, estas terceras partes podrán modificar o eliminar la documentación lo cual se realizará siempre a partir de las funcionalidades de tramitación electrónica de la Sede electrónica de la Diputación de Almería.

5.1.2 Roles del sistema de gestión de expedientes y documentos electrónicos

Los roles del sistema de gestión de expedientes y documentos electrónicos son el conjunto de roles que tienen aplicación sobre todo el sistema de gestión de expedientes y documentos electrónicos, no asociados a una serie documental concreta, sino a todas. Estos roles son:

- **Administrador de gestión documental:** Es el responsable de la conservación y custodia de los expedientes y sus documentos y de organizar el sistema de gestión de expedientes y documentos electrónicos. Dispone de todos los permisos y todos los roles sobre todas las series documentales, una vez se produce el cierre de los expedientes y durante su tramitación de acceso a nivel de consulta para garantizar la correcta conformación de expedientes con carácter previo a su cierre. Por lo tanto, tiene las mismas potestades que el rol de consulta restringida incluyendo la posibilidad de:
    - Reabrir un expediente para la inclusión de documentación adicional, siempre de forma excepcional y contando con la debida justificación que deberá quedar reflejada en el sistema de gestión de expedientes y documentos electrónicos.
    - Eliminar expedientes dando cumplimiento a la tabla de evaluación documental aplicable a la serie documental a la que pertenece.
    - Realizar transferencias de expedientes a la herramienta de preservación documental.
- **Administrador tecnológico:** El administrador tecnológico del sistema es una figura que debe estar presente para garantizar el correcto funcionamiento del sistema en caso de que se produzca un error o malfuncionamiento. Desde el punto de vista funcional, puede no ser necesario, pero a nivel técnico resulta indispensable.

  Este perfil posee todos los permisos y todos los roles en cualquier momento del ciclo de vida del documento y expedientes electrónicos (tramitación, vigencia y archivo) y se encarga de otorgar y mantener los roles de acceso a los usuarios siguiendo las instrucciones de los responsables funcionales.

Las actuaciones de los usuarios con este perfil sobre los expedientes y documentos electrónicos deberán ser monitorizadas para asegurar que sean las mínimas necesarias y respondan siempre a peticiones realizadas por los usuarios responsables de las series documentales o el Administrador de gestión documental.

5.2 Niveles de seguridad

Los niveles de seguridad del sistema de gestión de expedientes y documentos electrónicos se definen en dos niveles: nivel de Serie documental o Expediente y nivel de Documento. Los expedientes heredarán el nivel de seguridad establecido para la serie documental a la que pertenecen y, en su caso, podrá asignarse un nivel más restrictivo tanto a un expediente como de los documentos que contiene.

Así pues, en la Serie documental o Expediente, se definen tres niveles de seguridad que se propagan a los documentos que lo conforman:

- **Libre acceso:** La información contenida es de libre acceso para todos los usuarios del Sistema. Excepcionalmente, un expediente de una Serie de libre acceso podrá ser configurado como de acceso restringido o confidencial dejando constancia de los motivos que lo justifican.
- **Restringido:** La información contenida sólo es accesible para un grupo de usuarios reducido, correspondiente al equipo de tramitación o de consulta restringida, además de los usuarios de la serie documental correspondientes a Aplicación, el Administrador tecnológico y el Administrador de gestión documental. Excepcionalmente, un expediente de una Serie de acceso restringido podrá ser configurado como de acceso confidencial dejando constancia de los motivos que lo justifican.
- **Confidencial:** La información contenida en un expediente concreto sólo es accesible por las personas que hayan participado directamente en su tramitación, y quienes éstos determinen, aunque el expediente pertenezca a una serie a la que disponen de acceso, restringido o público, más usuarios. Estos usuarios podrán pertenecer al grupo de usuarios del Equipo de tramitación o de Consulta restringida.

  Asimismo, podrán acceder el Responsable tecnológico y el Administrador de gestión documental para la ejecución de las funciones que les son atribuidas debiendo quedar estos accesos debidamente registrados en el sistema para garantizar su posterior monitorización.

  Finalmente, el usuario Aplicación con acceso a la Serie documental podrá acceder en el caso de realizar procedimientos automatizados y para conferir el acceso al expediente a aquellos usuarios de aplicaciones de gestión de expedientes que mediante la gestión de permisos de la misma dispongan de acceso confidencial al expediente.

De la misma forma, con respecto a los documentos, también tendrán tres niveles de seguridad, independientemente del nivel de Serie documental o Expediente asignado, siendo en cualquier caso de igual o mayor restricción que el de Serie documental o Expediente. Estos tres niveles aplicados a los documentos implican:

- **Documentos públicos.** Los documentos públicos son aquellos que en su estado definitivo son visibles por personas ajenas a la Diputación de Almería en general, así como por todos los usuarios del sistema de cualquier rol. Durante su elaboración (estado borrador) su tratamiento será de documento reservado o confidencial, según se determine en cada caso.
- **Documentos reservados:** Documentación generada por la Diputación de Almería o aportada por un tercero de uso interno en la Serie documental o Expediente. No es visible ni por los interesados ni por personas ajenas a la Diputación de Almería sino sólo por los usuarios internos con acceso a la documentación contenida en la Serie documental en cuestión, pudiendo pertenecer al grupo de usuarios de Equipo de tramitación o de Consulta restringida. Asimismo, podrán acceder además los usuarios de la serie documental correspondientes a Aplicación, el Administrador tecnológico y el Administrador de gestión documental.
- **Documentos confidenciales:** Documentación generada por la Diputación de Almería o aportada por un tercero de uso interno en la Serie documental o Expediente. No es visible ni por los interesados ni por terceros con los que se relaciona la Diputación de Almería sino sólo por los usuarios internos que hayan participado en la tramitación del expediente al que pertenece o quienes éstos determinen, aunque el documento pertenezca a un expediente de una serie a la que disponen de acceso, restringido o público, más usuarios. Los usuarios con acceso podrán pertenecer al grupo de usuarios del Equipo de tramitación o de Consulta restringida.

  Asimismo, podrán acceder el Responsable tecnológico y el Administrador de gestión documental para la ejecución de las funciones que les son atribuidas debiendo quedar estos accesos debidamente registrados en el sistema para garantizar su posterior monitorización.

  Finalmente, el usuario Aplicación con acceso a la Serie documental podrá acceder en el caso de realizar procedimientos automatizados y para conferir el acceso al documento a aquellos usuarios de aplicaciones de gestión de expediente que mediante la gestión de permisos de la misma dispongan de acceso confidencial al documento.

De acuerdo con esta clasificación de niveles de seguridad y el conjunto de roles definidos, se pueden definir los niveles de seguridad del Sistema y sus respectivas políticas de seguridad para cada serie documental.

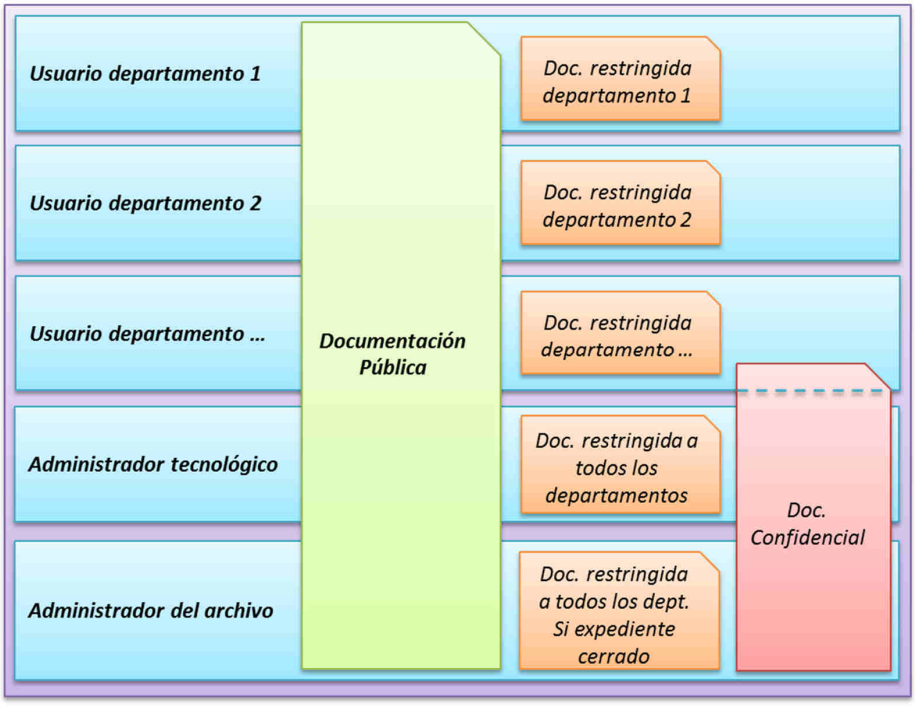
5.3 Representación gráfica

A continuación, se incluye una representación gráfica de la gestión de acceso al sistema de gestión de expedientes y documentos electrónicos. Siguiendo lo que se acaba de exponer, el presente gráfico tiene por objetivo ilustrar que para conferir acceso a un expediente electrónico habrá que responder a dos preguntas básicas:

- Si el usuario dispone de acceso funcional a la documentación, ya sea porqué pertenezca a los grupos de usuarios con acceso restringido a la serie documental a la que pertenece el expediente: equipo de tramitación, grupo de usuarios de consulta restringida, Aplicación. Ello se gestionará a partir de roles de acceso.
- Si el usuario, aun disponiendo del acceso funcional anterior, dispone del nivel de acceso suficiente para un expediente o un documento clasificados como confidencial, es decir, que haya participado en su tramitación o, en su defecto, un usuario que haya participado en la tramitación le haya conferido acceso. Ello se gestionará a partir de los metadatos de expediente o documento.

En cualquier caso, todo usuario dispondrá de acceso a la documentación calificada como de acceso público y los siguientes usuarios podrán acceder a toda la documentación en cualquier momento:

- Administrador tecnológico
- Administrador de gestión documental



6. Aplicación del modelo de seguridad documental

Una vez expuesto el modelo de seguridad documental, es conveniente definir las directrices sobre las cuales se podrá realizar su aplicación práctica en el sistema de gestión de expedientes y documentos electrónicos de la Diputación de Almería. Estas directrices se incluyen a continuación:

1. La **responsabilidad** de la gestión documental durante la fase de tramitación corresponderá al departamento responsable de cada serie documental según determine su responsable funcional. Una vez cerrados los expedientes, en su fase de vigencia y archivo, será responsabilidad de la Dirección de Archivo y Biblioteca, quien:
    a. Resolverá, coordinándose con el propietario del procedimiento que generó el expediente, sobre las peticiones de acceso por parte de usuarios distintos a los del Equipo de tramitación, Consulta restringida y Aplicación ya que los accesos por parte de estos usuarios no deberán ser autorizados al haber participado durante la fase de tramitación. Tampoco será necesario autorizar los accesos de los roles Consulta pública y Administrador tecnológico, aunque los de este último deberán quedar registrados para su posterior monitorización.
    b. De forma excepcional, tendrá la posibilidad de autorizar la reapertura de un expediente para que el personal asignado al equipo de tramitación o, si el expediente es confidencial, aquellos usuarios con acceso confidencial, por haber participado durante la tramitación del expediente, puedan añadir nueva documentación.
2. El acceso a los documentos electrónicos, durante la fase de tramitación, se determinará según la estructura del **cuadro de clasificación de la documentación** de la Diputación de Almería en el nivel de Serie documental. Cada Serie documental tendrá asociado:
    a. Un responsable funcional con el que será necesario confirmar cualquier aspecto relacionado con los criterios de gestión y acceso aplicables a la Serie.
    b. Los usuarios del departamento funcional y de otros departamentos que participen en la tramitación de los expedientes asociados a la Serie y que se plasmarán en el sistema con el rol de Equipo de tramitación.
    c. Los usuarios de otros departamentos que requieran tener acceso de consulta de los expedientes asociados a la Serie y que se plasmarán en el sistema con el rol de Consulta restringida.
3. El catálogo de procedimientos de la Diputación de Almería describirá todos los trámites y fases de cada procedimiento y en los sistemas de tramitación de procedimientos se mantendrán actualizados los perfiles de usuario y el área funcional al que pertenecen

y que podrán participar accediendo o modificando los documentos de los expedientes asociados al procedimiento.

Asimismo, el catálogo recogerá los documentos y actos de comunicación asociados a los mismos, de forma que se puedan identificar los documentos mínimos que conformaran cada expediente en su fase de tramitación, así como en su fase de vigencia y archivo, una vez cerrado y foliado el expediente.

A su vez, cada expediente y documento electrónicos tendrá asignados un conjunto de metadatos descriptivos de su contenido y de otros aspectos de este según el **Vocabulario de metadatos** de la Diputación de Almería. Para estos metadatos, el catálogo de procedimientos especificará para cada documento electrónico el valor a asignar a aquellos metadatos cuyo valor sea uniforme para todas los expedientes y documentos de un procedimiento o la forma y momento de obtenerlo durante su tramitación. En lo que respecta a los metadatos de gestión del control de acceso, necesariamente se tendrá en cuenta:

- La determinación general del tipo de acceso otorgado: secreto, reservado, confidencial o no clasificado. Ello podrá ser modificado por el equipo de tramitación en el nivel del expediente o de documento electrónico.
- Las razones aplicables para la limitación de acceso por parte del Equipo de tramitación definidas de forma específica para cada expediente. Ello es de aplicación en el caso excepcional que:
  - Un expediente de una serie de acceso público se determine por el Equipo de tramitación de la Serie como de acceso restringido
  - o una serie de acceso público o restringido se determine como confidencial.

  No obstante, en cualquier caso, un expediente o documento no será de acceso público hasta que esté en estado cerrado o definitivo.
- La limitación a las reproducciones del documento.
- En su caso, la presencia en el contenido de datos de carácter personal y el nivel de las medidas de seguridad aplicables a los mismos siendo de aplicación lo dispuesto en la legislación vigente en materia de protección de datos de carácter personal.

En los casos en que el valor de los metadatos de un expediente o documento electrónicos no quede fijado en el catálogo de procedimientos y tampoco se le hayan atribuido de forma expresa, el valor asignado por defecto deberá ser tal que impida los accesos indebidos a su información. Sin embargo, el personal de la Diputación de Almería actuará con la debida diligencia para evitar que la aplicación de este principio

deje sin efecto, en su caso, los derechos de consulta y de acceso a la información administrativa por las partes interesadas, tanto internas como externas.

4. El acceso a los documentos nominativos, es decir, aquellos expedidos o asociados a una persona concreta, a los documentos que contengan datos relativos a la intimidad de las personas, y a los expedientes no finalizados queda reservado a las personas que participen en su elaboración, así como las que acrediten las condiciones previstas por la ley en cada caso. Para garantizar que el derecho de consulta a través de medios telemáticos sea ejercido por terceras partes que se encuentran legalmente habilitadas o habilitadas para hacerlo, la Diputación de Almería exigirá su **identificación** por medio de cualquier procedimiento de identificación segura, electrónico o, en su defecto, presencial.
5. En lo que respecta al **acceso al sistema de gestión de expedientes y documentos electrónicos de la Diputación de Almería por parte de su personal** se establecen los siguientes criterios de aplicación:
    - Para que un usuario pueda acceder a los sistemas de tratamiento de documentos electrónicos de la Diputación de Almería deberá superar un proceso de identificación (por ejemplo, a través de un identificador de usuario), autenticación (por ejemplo, a través de una contraseña) y autorización (por ejemplo, a través de roles de acceso y niveles de seguridad que determinen a qué series documentales y expedientes tendrán acceso los usuarios y con qué potestades).
    - Los usuarios, salvo situaciones excepcionales que se deberán identificar y aprobar, dispondrán de un identificador de usuario unívoco.
    - Las credenciales de acceso de cada usuario son personales e intransferibles, y su proceso de asignación y comunicación garantizará la confidencialidad y prevendrá el acceso no autorizado a través de la suplantación de identidad.
    - Los usuarios serán responsables de preservar la confidencialidad de las contraseñas y asegurar el uso correcto de los sistemas de información a los que tienen acceso, así como de cualquier otro mecanismo de control de acceso a los sistemas de información como podría ser el certificado digital.
    - Los usuarios tendrán acceso al sistema de gestión de expedientes y documentos electrónicos de la Diputación de Almería hasta el momento que lo precisen para el desarrollo de sus funciones. Se preverán procedimientos específicos para controlar la vigencia de los usuarios temporales como, por ejemplo, personal externo. Se mantendrá, por tanto, un listado actualizado de usuarios con acceso autorizado a los sistemas.
    - Cada usuario tendrá acceso a los expedientes y documentos de la Series documentales que precise sobre la base de las necesidades derivadas de sus

funciones y responsabilidades, de acuerdo con el análisis que se haya hecho de los procedimientos de la Diputación de Almería según figure en su catálogo de procedimientos. Se aplicarán los niveles de acceso: Equipo de tramitación o Consulta restringida.

- La concesión del acceso a los sistemas de tratamiento de documentos electrónicos de la Diputación de Almería lleva asociado un proceso previo formal de solicitud, evaluación y aprobación. Para la aprobación es necesario que se establezcan responsables funcionales de cada Serie documental que decidirán sobre el acceso a los expedientes y documentos pertenecientes a cada Serie documental.
- Siempre que se produzca un cambio en las funciones o responsabilidades de un usuario, se evaluarán sus consecuencias en lo que respecta a derechos de acceso a los sistemas de tratamiento de documentos electrónicos de la Diputación de Almería.
- Para la definición de los perfiles de acceso a la documentación en formato electrónico, partiendo de lo que establezca el Catálogo de Procedimientos, la Diputación de Almería utilizará las utilidades de segregación de funciones de los sistemas de tratamiento de documentos electrónicos donde, para cada procedimiento y para cada una de sus fases de tramitación y en consecuencia cada uno de los estados del documento, se determinará qué grupos de usuarios tienen acceso y en qué grado: consulta, modificación y eliminación. Adicionalmente en cada fase del procedimiento se definirá qué documentos serán accesibles, modificables o eliminables quedando prohibida en cualquier caso la eliminación de documentos considerados definitivos. Se establecerán para ello tablas de segregación de funciones que identifiquen todas las transacciones posibles en un sistema de tratamiento de documentos electrónicos y cuáles podrán ser ejecutadas por cada tipo de usuario o rol.
- Periódicamente se realizará un proceso de revisión para verificar que sólo los usuarios autorizados tienen acceso a los diferentes sistemas de información y aplicaciones que permiten gestionarlos y que su perfil no exceda las autorizaciones mínimas necesarias para el desarrollo de sus funciones ni se sucedan conflictos de segregación de funciones.
- Se establecerán mecanismos de registro y monitorización de acceso y/o uso de los sistemas que garanticen que los documentos son protegidos de forma efectiva de usos no autorizados, alteración o destrucción, tal y como ha quedado definido en el apartado 4.