Gobierno de Navarra
Nafarroako Gobernua
Departamento de Cultura y Deporte
Kultura eta Kirol Departamentua

Servicio de Archivos y Patrimonio Documental
Artxiboen eta Dokumentu Ondarearen Zerbitzua
Dos de Mayo, s/n
31004 PAMPLONA/IRUÑA
Tel.: 848 42 46 09
servicio.archivos@navarra.es

El Director General de Cultura ha dictado la siguiente Resolución:

"RESOLUCIÓN 20/2021, de 27 de enero, del Director General de Cultura – Institución Príncipe de Viana, por la que se aprueba la Especificación 2, Modelo de Seguridad y acceso, del Modelo de Gestión del Documento Electrónico (MGDE) de la Administración de la Comunidad Foral de Navarra.

El Servicio de Archivos y Patrimonio Documental propone a la Dirección General de Cultura – Institución Príncipe de Viana, la aprobación de la Especificación 2: Modelo de Seguridad y acceso, del Modelo de Gestión del Documento Electrónico (MGDE) de la Administración de la Comunidad Foral de Navarra.

El Modelo de Seguridad y acceso concreta aspectos relativos a la seguridad y acceso a la información y los documentos especificados en el Modelo de Gestión del Documento Electrónico (MGDE) de la Administración de la Comunidad Foral de Navarra, aprobado por la Orden Foral 49/2020, de 21 de diciembre, de la Consejera de Cultura y Deporte. Por su parte, el Modelo aprobado por Orden Foral se vincula a la Política de Gestión de Documentos Electrónicos (PGDE) de la Administración de la Comunidad Foral de Navarra y del Sector Público Institucional Foral, que fue aprobada en sesión del Gobierno de Navarra de fecha 16 de diciembre de 2020. Dicha Política establece la existencia y las características tanto del Modelo de Gestión del Documento Electrónico (MGDE) como de sus especificaciones, de las que concretamente dos, la segunda, relativa al Modelo de Seguridad y acceso, que ahora nos ocupa, y la quinta, relativa al Modelo de Conservación, corresponden al ámbito de la gestión de documentos y archivos, y por lo tanto se incluyen en el ámbito competencial de la Dirección General de Cultura – Institución Príncipe de Viana.

Ambas especificaciones, pese a su vinculación con el referido Modelo de Gestión del Documento Electrónico (MGDE), deben tener carácter autónomo, habida cuenta de la incidencia que tiene en dichos ámbitos la evolución de la tecnología (en especial, el software).

En consecuencia, y en virtud de las atribuciones conferidas por el artículo 23 de la Ley Foral 12/2007, de 4 de abril, de Archivos y Documentos, y por Decreto Foral 273/2019, de 30 de octubre, por el que se establece la estructura orgánica del Departamento de Cultura y Deporte,

ORDENO:

1.º Aprobar la Especificación 2: Modelo de Seguridad y acceso, del Modelo de Gestión del Documento Electrónico (MGDE) de la Administración de la Comunidad Foral de Navarra, cuyo texto se incorpora como Anejo.

2.º Trasladar la presente Resolución al Servicio de Archivos y Patrimonio Documental y a las Secretarías Generales Técnicas de los Departamentos del Gobierno de Navarra, para su conocimiento a los efectos oportunos.

Pamplona, veintisiete de enero de dos mil veintiuno. EL DIRECTOR GENERAL DE CULTURA, Ignacio Apezteguía Morentin."

Lo que notifico a Vd. para su conocimiento y demás efectos.

Pamplona, veintiocho de enero de dos mil veintiuno.

EL DIRECTOR DEL SERVICIO
DE ARCHIVOS Y PATRIMONIO DOCUMENTAL

LLANSO SANJUAN JOAQUIN - DNI 46525578M

Firmado digitalmente por LLANSO SANJUAN JOAQUIN - DNI 46525578M
Fecha: 2021.01.28 13:18:42 +01'00'

Joaquim Llansó Sanjuan

NOTIFICADO A:
SERVICIO DE ARCHIVOS Y PATRIMONIO DOCUMENTAL DEL DEPARTAMENTO DE CULTURA Y DEPORTE.
Secretaría General Técnica, Dpto. Cohesión Territorial.
Secretaría General Técnica, Dpto. Cultura y Deporte.
Secretaría General Técnica, Dpto. Derechos Sociales.
Secretaría General Técnica, Dpto. Desarrollo Económico y Empresarial.
Secretaría General Técnica, Dpto. Desarrollo Rural y Medio Ambiente.
Secretaría General Técnica, Dpto. Economía y Hacienda.
Secretaría General Técnica, Dpto. Educación.
Secretaría General Técnica, Dpto. Ordenación del Territorio, Vivienda, Paisaje y Proyectos Estratégicos.
Secretaría General Técnica, Dpto. Políticas Migratorias y Justicia.
Secretaría General Técnica, Dpto. Presidencia, Igualdad, Función Pública e Interior.
Secretaría General Técnica, Dpto. Relaciones Ciudadanas.
Secretaría General Técnica, Dpto. Salud.
Secretaría General Técnica, Dpto. Universidad, Innovación y Transformación Digital.

Modelo de Gestión del Documento Electrónico (MGDE) de la Administración de la Comunidad Foral de Navarra

Especificación 2: Modelo de Seguridad y acceso

Gobierno de Navarra
Departamento de Cultura y Deporte

Nafarroako Gobernua
Kultura eta Kirol Departamentua

Enero de 2021

Sumario

1. Introducción

Tal y como se establece en la Política de Gestión de Documentos Electrónicos (PGDE) de la Administración de la Comunidad Foral de Navarra, el Modelo de Gestión del Documento electrónico (MGDE) se implementa a través de un conjunto de especificaciones que establecen directrices concretas. Este documento es una especificación que forma parte del Modelo de Gestión del Documento electrónico (MGDE), concretamente la especificación 2, relativa al Modelo de seguridad y acceso.

La presente especificación tiene por objetivo definir los aspectos concretos relacionados con la seguridad en el acceso y el tratamiento de expedientes y documentos electrónicos.

En este sentido, si partimos de las principales dimensiones de seguridad establecidas por el Esquema Nacional de Seguridad (ENS) y los estándares de referencia, como la norma ISO 27001 (2013), la seguridad de la información aplicada a la gestión documental implica los siguientes puntos:

- **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 los expedientes y documentos electrónicos se pone únicamente a disposición de individuos, entidades o procesos autorizados o que necesitan conocerla.
- **Disponibilidad:** se provee el acceso y la utilización de la información y de los documentos -incluidos los sistemas para su tratamiento- por parte de los individuos, entidades o procesos autorizados cuando se requiera.
- **Trazabilidad:** las acciones de un agente sobre un documento pueden ser imputadas exclusivamente a dicho agente, pudiendo 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 y acceso de la Administración de la Comunidad Foral de Navarra se encuentra especialmente orientado a:

- Proteger los documentos y expedientes electrónicos con información restringida o confidencial, en general.
- Proteger los datos personales de los documentos electrónicos, en concreto.
- Promover una interoperabilidad de confianza.
- Apoyar de forma controlada la puesta a disposición y la difusión de la información de la que es responsable.

El presente Modelo se fundamenta en los principios y normas aplicables a la protección de la confidencialidad y privacidad de los datos, donde destacan la Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales y los convenios y decisiones de la Unión Europea al respecto.

Adicionalmente, para la interpretación y aplicación del Modelo se deben considerar los siguientes aspectos:

- Lo establecido en las Fichas de Identificación de Series Documentales y Calendario de Conservación y Acceso, informadas por la Comisión de Evaluación Documental y aprobadas por la Dirección General de Cultura.
- En defecto del punto anterior:
    - Lo establecido en el resto de las políticas y directrices de la Administración Foral en materia de seguridad de la información.
    - Los dictámenes del ámbito Jurídico de la Administración Foral.
    - Lo establecido en el MGDE y en sus especificaciones, especialmente la especificación 6 referente al Modelo tecnológico.

Para dar respuesta a estos requisitos sobre las herramientas de gestión documental de la Administración Foral, se establecen cuatro procesos clave con el objetivo de asegurar un adecuado control del acceso a la documentación electrónica a lo largo de todo su ciclo de vida. Estos 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 Documental (SGD)?
- **Recuperación de la información:** ¿cómo se asegura la integridad de la documentación electrónica almacenada ante eventuales incidentes de seguridad?
- **Monitorización:** ¿qué se hace sobre la documentación electrónica y la información asociada y cuándo se hace?

- **Acceso:** ¿quién puede hacer qué sobre la documentación electrónica almacenada en el SGD?

A continuación, se definen con más detalle estos cuatro procesos y se establecen las directrices para su aplicación en el SGD de la Administración Foral.

Cabe destacar que en la especificación 6 se identifican las herramientas tecnológicas sobre las que es de aplicación el presente Modelo de seguridad y acceso.

2. Autenticación

Para poder identificar inequívocamente a las personas que acceden al SGD se dispone de una funcionalidad de autenticación de usuarios. Para garantizar que cada usuario puede acceder a la información que precisa para el desarrollo de sus funciones, las diferentes aplicaciones que conforman el SGD permiten la definición de **perfiles de acceso**.

Así pues, la conjunción del sistema de autenticación y de las funcionalidades de segregación de las aplicaciones del SGD permite:

- La validación de todo usuario que intenta acceder al SGD y de la recuperación de la información y documentación en consonancia con los permisos de los que disponga.
- La realización de acciones sobre los documentos y expedientes electrónicos en función de los permisos asignados.
- Informar al usuario en caso de que intente acceder a una documentación no íntegra, ya sea porque se ha corrompido, se ha perdido información, se ha modificado indebidamente o porque no se ha podido validar su autenticidad.

Para asegurar estas premisas, desde el punto de vista de la autenticación en el SGD, el control de acceso debe llevarse a cabo de forma nominal mediante el propio usuario de cada persona con acceso autorizado al sistema. Esto significa que **los usuarios genéricos quedan terminantemente prohibidos**, a menos que cada una de las acciones realizadas por estos puedan asociarse inequívocamente a una persona o proceso del sistema que las haya ejecutado.

Adicionalmente, la autenticación se debe realizar a través de tres vías principales:

- **Autenticación sobre las aplicaciones de gestión de procesos electrónicos.** Los usuarios de las unidades de trabajo responsables de la tramitación de procesos se autentican sobre las herramientas que permiten llevar a cabo las actividades de gestión de los procesos de la Administración de la Comunidad Foral de Navarra. Estas herramientas acceden a la documentación almacenada en el gestor documental en base a los permisos otorgados a cada unidad de trabajo en la aplicación de la gestión de procesos correspondiente.
- **Autenticación sobre el archivo electrónico único.** Los responsables de la documentación electrónica en la etapa archivística se autentican con perfil de súper usuario. Este perfil permite el acceso de lectura de documentos y expedientes, pero no de modificación, excepto para la asignación de nuevos metadatos, la aplicación de la descripción archivística o la realización de los procesos de resellado y migración de formatos.
- **Acceso vía capa de interoperabilidad.** En caso de que otras Administraciones públicas puedan requerir documentación o información emitida por la Administración Foral, tanto en etapa de tramitación como en subetapa semiactiva, y con el objetivo de reducir cargas administrativas a terceras partes, existe la posibilidad de acceso a través de vías de interoperabilidad.

  En este caso, el control del acceso se basa en la identificación sobre el certificado digital de aplicación, que garantiza que sólo tienen acceso aquellas Administraciones con las que se ha suscrito el correspondiente convenio y las que tienen interés legítimo en acceder a la información, guardando en todo momento la debida constancia de ello, de la información accedida y del momento del acceso.

  Excepcionalmente, existe la posibilidad de implementar mecanismos alternativos de intercambio de información y de autenticación según sea requerido por la Administración Pública receptora de documentación o información emitida por la Administración Foral.

3. Recuperación de la información

Todo sistema de seguridad debe disponer de un servicio de restauración y recuperación de la información que permita restaurarla en el estado más cercano al momento en el que ocurre un incidente de seguridad con efectos sobre su integridad. Según esta premisa, todo sistema que participa en la gestión de documentación electrónica debe:

- Permitir guardar todos los expedientes y sus documentos, firmas electrónicas y metadatos asociados.
- Disponer de sistemas automáticos de copias de seguridad y recuperación.
- Definir la ubicación sobre la que se realizará y recuperará la copia.
- Permitir a un rol de administrador la posibilidad de acceder y restaurar las copias de seguridad.
- Facilitar los datos referentes a la situación en la que ha sido recuperada la información y la documentación.

En este sentido, es necesario asegurar la correcta aplicación de las políticas y normativas relacionadas con las copias de respaldo y recuperación de los sistemas de información, y, en el ámbito de la gestión de expedientes y documentos electrónicos, respetar las siguientes directrices:

- Almacenamiento sistemático de todos los documentos, metadatos y otros contenidos de carácter documental en los repositorios o bases de datos destinadas a tal efecto, sobre los que se aplican los procesos de copia de seguridad y recuperación. No pueden existir documentos o datos relevantes para la gestión documental almacenados de manera temporal o provisional en repositorios que no cumplen con la política de recuperación establecida.
- Existencia de un inventario y una clasificación de las copias de seguridad que posibilite la identificación de cada una de ellas y su contenido, así como su debida administración y recuperación.
- Asignación de las debidas medidas de control de acceso físico y ambiental a la información de recuperación, ubicándose estas suficientemente alejadas de las instalaciones principales para que un mismo accidente de seguridad no afecte a la información en el entorno de producción y recuperación.

- Almacenamiento de los procedimientos de recuperación en una ubicación que cumpla con los requisitos que permitan asegurar su protección, seguridad y, en caso de ser necesario, su uso.
- Verificación y comprobación periódica de los procedimientos de restauración de información para garantizar su eficacia y cumplimiento dentro del tiempo asignado a la recuperación en los procesos operativos.
- Establecimiento de periodos de sustitución de los medios de almacenamiento de las copias de resguardo una vez finalizada la posibilidad de ser reutilizados según las recomendaciones del fabricante.

4. Monitorización

En el SGD 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 puedan realizar sus actividades de forma correcta y en el tiempo adecuado. En este sentido, es necesario que el sistema sea monitorizado en torno a dos aspectos primordiales:

- **Uso del sistema:** registro de las actividades acaecidas sobre el sistema por parte de los usuarios y de procesos automáticos que garantizan la trazabilidad de las actuaciones en el sistema y que permiten obtener estadísticas sobre su uso.
- **Operación del sistema:** actividades destinadas a asegurar el correcto mantenimiento y explotación del sistema para garantizar el cumplimiento de las funcionalidades que le son atribuidas.

A continuación, se definen estos aspectos con más profundidad.

4.1 Uso del sistema

El control y el seguimiento del uso del SGD se lleva a cabo a través de un conjunto de indicadores del sistema. Estos indicadores se dividen en dos ámbitos diferentes:

- **Indicadores unitarios:** permiten realizar el seguimiento de las acciones que se han realizado sobre la documentación del SGD. Con estos indicadores se puede determinar quién, cuándo y qué se ha hecho sobre el sistema en un momento determinado y para un expediente o documento concretos.

Para no afectar al rendimiento del sistema (a mayor nivel de auditoría menor rendimiento del sistema), hay un nivel de auditoría medio-alto donde los indicadores unitarios son los siguientes, pudiendo ser más o menos detallados en función de los valores de los metadatos de los expedientes y documentos según se establece para cada proceso:

- Accesos al sistema.
- Creaciones de objetos, entendiendo objeto como expediente, documento o firma electrónica.
- Eliminación de objetos.
- Versionado de documentos.
- Cambios en el valor de aquellos metadatos que participan en el control de acceso a la documentación electrónica, concretamente el nivel de seguridad del expediente o del documento con los valores: acceso público, acceso restringido o acceso confidencial.
- 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 conjunta sobre el uso del SGD. Con estos indicadores se dispone de información estadística útil para el análisis del sistema en los siguientes ámbitos:
  - **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 realizados por un usuario.
  - **Tiempo.** Momento durante el que se accede o se modifica un expediente o documento electrónico por parte de un usuario.

4.2 Operación del sistema

Como cualquier otro sistema, el SGD requiere de una supervisión mediante procesos de monitorización continua que registran información sobre su funcionamiento, útil para poder asegurar su correcta ejecución. Estos procesos de monitorización son procedimientos internos del sistema -transparentes para el usuario final- que se encuentran bajo el control del administrador tecnológico del sistema y se llevan a cabo de forma periódica.

Estos procedimientos se definen específicamente para cada sistema involucrado en el tratamiento de documentación electrónica sobre el procedimiento de explotación correspondiente y contemplan, como mínimo, las siguientes actuaciones:

- 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 por los dispositivos tecnológicos que garantizan la seguridad de la información se desarrollan tal y como se ha previsto.
    - Detectar y prevenir eventos e incidencias de seguridad mediante el uso de indicadores.
    - Revisar regularmente la efectividad del sistema.
- **Revisión en intervalos planificados** de las evaluaciones de riesgos, los riesgos residuales y sus niveles aceptables, de las amenazas internas y externas existentes y de la efectividad de los controles para la mitigación de riesgos.
- Realización periódica de **auditorías internas y externas** de seguridad y actualización de planes de seguridad en función de las conclusiones y deficiencias detectadas.
- **Registro y revisión** proactiva de acciones y eventos que pueden tener impacto sobre la efectividad o el rendimiento del sistema.

4.3 Trazabilidad

Todos los documentos del expediente, desde su creación, se tienen que enviar al gestor documental corporativo, donde tiene lugar el proceso de captura. El

único documento que se considera original y auténtico es el que se encuentra en el gestor documental.

Los documentos que forman parte del expediente y el propio expediente respetan las reglas del MGDE y para garantizar este cumplimiento se hacen comprobaciones automáticas.

Todos los datos de tramitación relevantes para generar una traza de la vida del expediente (quién ha tramitado, cuándo se ha iniciado, cuándo se ha transferido, cuándo se ha publicado, etc.) se recogen automáticamente y se almacenan para conservar su valor como verificador, como información histórica y para centralizar su consulta y explotación.

5. Acceso

El SGD debe asegurar la restricción y el control del acceso a los expedientes, a sus documentos y a la información que estos contienen. Según esta premisa, el sistema debe:

- Permitir la definición del rol de administrador Tecnológico del sistema que pueda configurar los roles de acceso de cada usuario.
- Identificar a los usuarios, impidiendo el acceso en caso de no estar autorizados, bien porque su rol de acceso no lo permite, bien porque, a pesar de disponer del rol adecuado, no dispone de acceso confidencial a un expediente o documento clasificado en este nivel de seguridad.
- Asignar permisos de acceso a los expedientes y documentos de acuerdo con el Cuadro de Clasificación, configurando el metadato relativo al tipo de acceso del expediente o del documento como de acceso público, restringido o confidencial.

  En caso de que el metadato de expediente o documento sea de acceso restringido o confidencial, el sistema debe poder restringir el acceso a series del Cuadro de Clasificación según el rol del usuario y a determinados expedientes o documentos según el tipo de acceso asignado.
- Establecer un grupo de usuarios asociados a series documentales o procedimientos. Si un usuario no tiene asociado el acceso a una serie documental tampoco puede acceder a los expedientes de la serie ni a los documentos que estos contienen.
- Permitir asignar un usuario a un grupo de usuarios con el mismo rol.

- Permitir que un usuario pueda estar en más de un grupo de usuarios.
- Vetar el acceso a los expedientes o documentos electrónicos conforme los niveles de seguridad asignados.
- Si un usuario busca textos contenidos en metadatos o documentos que correspondan a expedientes a los que no tiene acceso, no se debe permitir su visualización. Para el usuario este expediente no existe, por lo que la búsqueda no devolverá ningún resultado relacionado.
- Permitir que la clasificación de seguridad asignada varíe temporalmente de forma automática en función de determinados parámetros y de los metadatos del expediente o de sus documentos.
- Permitir asignar a expedientes y documentos concretos niveles de seguridad más restrictivos que el procedimiento o la serie documental a la que pertenecen.
- Permitir asignar a documentos concretos de un expediente niveles de seguridad más restrictivos que los del expediente al que pertenecen.

Para poder cumplir estos requisitos, se tiene que dar respuesta a dos preguntas primordiales:

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

Las respuestas a estas preguntas se estructuran en dos modelos que se combinan entre ellos, constituyendo un modelo de restricción de acceso que se aplicará en todo el sistema durante todo el ciclo de vida de la documentación electrónica. Concretamente, estos dos modelos son:

- Roles de acceso.
- Niveles de seguridad.

5.1 Roles de acceso

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

El rol debe ser entendido como un perfil de usuario, no como un cargo o puesto de trabajo. Las personas con un mismo rol comparten responsabilidades y permisos funcionales sobre el SGD. Cada uno de los roles tiene un conjunto de acciones asociadas aplicables sobre las series documentales, los expedientes y los documentos electrónicos que contienen.

Existen dos tipos de roles según su ámbito de aplicación: a nivel de serie documental o a nivel de todas las series documentales.

5.1.1 Roles de serie documental

Los **roles de serie documental** tienen las siguientes propiedades:

- Los usuarios tienen acceso a las series documentales a través de la **atribución de roles de acceso**, que son asignados a un usuario o a una unidad de trabajo.
- Se asignan **roles de acceso** a todas las **series documentales**.
- Cada serie documental se puede **configurar por separado**.
- Cada rol dispone de un conjunto de **permisos propios** sobre un conjunto de series y etapas del ciclo de vida de la documentación electrónica, pudiendo ser de **consulta,** de **modificación** o de **eliminación**.
- Los **permisos de cada rol** son los mismos para cada **serie relacionada** que dispongan.
- A los roles se asignan aquellos **usuarios o unidades de trabajo** pertinentes para cada serie.

De acuerdo con esto, se definen diferentes **grupos de usuarios a nivel de serie documental**, que son los siguientes.

- **Equipo de tramitación:** es el equipo responsable de la tramitación de los expedientes de un proceso. Tiene la potestad de crear expedientes y, mientras estén abiertos, de:
    - Modificar los metadatos editables del expediente, entre ellos:
        - El metadato de nivel de acceso sobre el carácter público, restringido o confidencial de un expediente (apartado 5.2

sobre niveles de seguridad). Debe considerarse que el carácter confidencial de un expediente debe tener como consecuencia que sólo el usuario creador de aquel expediente y aquellos a quienes el mismo usuario creador dé permiso dispondrán de acceso al mismo, aunque pertenezca a un expediente de una serie documental de la que dispongan de acceso más usuarios.

- Crear, introducir y modificar documentos en el expediente.
- Modificar los metadatos editables de los documentos, entre ellos los siguientes relevantes a efectos de seguridad:
  - La determinación del estado definitivo de un documento, por el que el documento no puede ser eliminado encontrándose el expediente en etapa de tramitación.
  - El carácter confidencial de un documento (apartado 5.2 sobre niveles de seguridad), por el que sólo el usuario creador del documento y aquellos a quienes el mismo usuario creador dé permiso pueden disponer de acceso al mismo, aunque pertenezca al expediente de una serie documental de la que disponen de acceso más usuarios.

    Es importante considerar que el carácter confidencial de un documento no tiene efecto sobre el conjunto del expediente al que pertenece, pudiéndose aplicar individualmente por documento o de forma global a todos los documentos pertenecientes al expediente.
- Realizar firmas electrónicas y modificar aquellos metadatos de firma no recopilados automáticamente desde la propia firma, como por ejemplo la ubicación.
- Eliminar documentos del expediente no considerados como definitivos.
- Cerrar expedientes.
- Gestionar los permisos de acceso en la etapa de tramitación.

- **Aplicación:** rol especial con permisos similares a los de las unidades de trabajo. Permite la interacción automática de las herramientas informáticas verticales de gestión de procesos con el SGD por aquellas series documentales con las que operen, partiendo de la base de la gestión de permisos de usuario establecida en la aplicación de gestión de procesos. Tiene la potestad de:

- Crear expedientes.
- Modificar los metadatos editables del expediente.
- Crear, introducir y modificar documentos en los expedientes.
- Modificar los metadatos editables de los documentos y de sus firmas electrónicas.
- Eliminar documentos del expediente no considerados como definitivos.
- Cerrar expedientes.

- **Cargos políticos:** rol que dispone de permisos para consultar el expediente y sus respectivos documentos y metadatos, pero no para modificarlos ni para añadir documentos adicionales. En la mayor parte de los casos, estará formado por personas que, para el buen desarrollo de sus funciones, requieren consultar temporalmente los expedientes de una serie documental en su etapa de tramitación. En caso de querer acceder a documentos o expedientes en subetapa semiactiva deben realizar la correspondiente solicitud al responsable de Gestión Documental y Archivo.

  Este rol tiene la potestad de:

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

- **Terceras partes (ciudadanía):** este perfil se corresponde con las partes externas a la Administración de la Comunidad Foral de Navarra, que disponen de acceso a la documentación sólo si son parte interesada, aplicándose las medidas de despersonalización de datos que sean de aplicación.

  - El acceso a la documentación electrónica en etapa de tramitación se debe realizar a través de la Carpeta ciudadana con previa autenticación. El acceso al resto de la documentación se realizará mediante las herramientas de consulta incluidas en las herramientas de gestión de los repositorios. En cualquiera de los casos, es necesaria la previa autenticación, exceptuando los casos donde la información se considere pública.

- Para cualquier acceso por parte de la ciudadanía a documentación en etapa archivística se debe realizar la correspondiente solicitud al responsable de Gestión Documental y Archivo. Para determinar el acceso, se aplicarán las Fichas de Identificación de Series Documentales y el Calendario de Conservación y Acceso, de acuerdo con la legislación aplicable en cada caso.
- Adicionalmente, en caso de ser parte interesada y si el procedimiento se encuentra en etapa de tramitación y es requerido, estas terceras partes pueden añadir documentación, siempre a partir de las funcionalidades de la tramitación electrónica de la Sede electrónica y con un proceso previo de validación mediante actuación administrativa automatizada u operada por personal al servicio de la Administración Foral.

5.1.2 Roles del sistema: súper usuarios

Los roles del SGD son el conjunto de roles que tienen aplicación sobre todo el sistema y que se encuentran asociados a todas las series documentales existentes. También se denominan **súper usuarios**. Son los siguientes:

- **Administrador de Gestión Documental y Archivo:** es el responsable de la conservación y la custodia de los expedientes y de sus documentos, así como de organizar el SGD. Dispone de todos los permisos y de todos los roles sobre todas las series documentales una vez cerrado el expediente. El administrador de Gestión Documental y Archivo tiene la potestad de:
  - Eliminar expedientes dando cumplimiento a las Fichas de Evaluación y el Calendario de Conservación y Acceso aplicables.
  - Aceptar transferencias de expedientes.
- **Administrador Tecnológico:** es la figura que garantiza el correcto funcionamiento del sistema en caso de que se produzca un error o cualquier mal funcionamiento. 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 de la documentación electrónica y se encarga de otorgar y mantener operativos en la herramienta los roles de acceso a los usuarios siguiendo las instrucciones de los responsables funcionales.

Las actuaciones de los súper usuarios se tienen que monitorizar para asegurar que son las mínimas necesarias y que responden siempre a peticiones realizadas por los usuarios responsables de las series documentales o por el administrador de Gestión Documental y Archivo.

5.2 Niveles de seguridad y permisos de acceso

Los niveles de seguridad (bajo, sustancial o medio y alto) se corresponden con los tipos de acceso (libre, restringido y confidencial), en conformidad con el Esquema Nacional de Interoperabilidad (ENI) y el Esquema Nacional de Seguridad (ENS). Los tipos de acceso se definen en permisos de consulta, modificación y eliminación de documentos para dos rangos: uno común para **Serie documental / Expediente** y otro para **Documento**.

Los expedientes heredan el nivel de seguridad asignado a la serie documental a la que pertenecen, si bien se puede asignar un rango más restrictivo, respecto a la serie, tanto a nivel de expediente como de documento. El nivel de seguridad se establece en función tanto de la serie documental como de la tipología documental, a través de los correspondientes metadatos recogidos en el Esquema de Metadatos de Navarra, conforme al Esquema de Metadatos de Gestión de Documentos Electrónicos (e-EMGDE) del ENI.

5.2.1 Acceso a Serie documental / Expediente

Así pues, en cuanto al **nivel de Serie documental / Expediente**, se definen los tres tipos de acceso que, a su vez, heredan los documentos que conforman el expediente:

- **Libre acceso:** la información contenida es consultable para todos los grupos de usuarios del sistema, si bien no todos tendrán permisos de modificación y/o eliminación, en atención a sus roles. Excepcionalmente, el acceso para consulta a un expediente de una serie definida como de libre acceso puede ser configurado como restringido o confidencial, dejando constancia de los motivos que lo justifican.

  El libre acceso corresponde, como norma general, a expedientes cerrados cuya vigencia haya finalizado, por lo que se inscriben en la subetapa inactiva o histórica. Pueden existir expedientes de libre acceso en las etapas previas, en función del carácter de la información que contienen, si así ha sido determinado en las Fichas de Identificación de Series Documentales y Calendario de Conservación y Acceso.

Las series o expedientes de libre acceso se identifican a través del metadato correspondiente, por lo que el usuario tiene la potestad de:

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

	Libre acceso en subetapa histórica (excepcionalmente en etapas previas)		
Grupo de usuarios	**Consulta**	**Modificación**	**Eliminación**
Equipo de tramitación	Sí	No	No
Aplicación	Sí	No	No
Cargos políticos	Sí	No	No
Terceras partes (ciudadanía)	Sí	No	No
Administrador de Gestión Documental y Archivo	Sí	Sí (atributos de descripción)	No
Administrador Tecnológico	Sí	No	No

El administrador de Gestión Documental y Archivo podrá modificar únicamente los atributos de descripción archivística, nunca los metadatos incorporados en la fase de tramitación.

- **Acceso restringido:** por el carácter de la información contenida en el expediente aquella sólo es accesible para determinados grupos de usuarios: el equipo de tramitación, el administrador Tecnológico, el administrador de Gestión Documental y Archivo y personas ajenas al procedimiento que, para el buen desarrollo de sus funciones, requieran de acceso de consulta a los expedientes de una serie documental restringida en su etapa de vigencia.

  Excepcionalmente, el expediente de una serie de acceso restringido puede ser declarado como de acceso confidencial, dejando constancia de los motivos que lo justifican.

Los usuarios que tienen acceso tienen la potestad de:

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

El acceso restringido se limita a la etapa de tramitación y a la subetapa de vigencia del ciclo de vida. Una vez que alcanza la subetapa histórica, la documentación pasa a ser de libre acceso.

	Acceso restringido en etapa de tramitación		
Grupo de usuarios	**Consulta**	**Modificación**	**Eliminación**
Equipo de tramitación	Sí	Sí	Sí
Aplicación	Sí	Sí	Sí
Cargos políticos	Sí (temporal)	No	No
Terceras partes (ciudadanía)	Sólo interesados	No	No
Administrador de Gestión Documental y Archivo	Sí (metadatos)	No	No
Administrador Tecnológico	Sí	Sí	Sí

	Acceso restringido en subetapa de vigencia		
Grupo de usuarios	**Consulta**	**Modificación**	**Eliminación**
Equipo de tramitación	Sí	No	No
Aplicación	Sí	No	No
Cargos políticos	No	No	No
Terceras partes (ciudadanía)	Sólo interesados	No	No

Administrador de Gestión Documental y Archivo	Sí	Sí (atributos de descripción)	Sí
Administrador Tecnológico	Sí	No	No

El administrador de Gestión Documental y Archivo podrá modificar únicamente los atributos de descripción archivística, nunca los metadatos incorporados en la fase de tramitación.

- **Serie documental o Expediente confidencial:** la información contenida en un expediente confidencial sólo es accesible para las personas que han participado directamente en su tramitación, aunque el expediente pertenezca a una serie a la que tengan acceso - restringido o público - más usuarios. Asimismo, pueden acceder el administrador Tecnológico y el administrador de Gestión Documental y Archivo, que sólo dispondrán de acceso de consulta a los metadatos durante la etapa de tramitación y, una vez cerrado el expediente, podrán acceder a toda la información contenida, con el fin de ejecutar las funciones que le son atribuidas. Debe quedar constancia de estos accesos para garantizar su posterior monitorización.

  La información contenida en un expediente confidencial se almacena de manera cifrada y sólo se descifra durante el acceso por parte del personal autorizado.

  La declaración de confidencialidad sobre una serie o expediente, y su levantamiento, la lleva a cabo una autoridad conforme a una norma jurídica vinculante. En el momento en que se levante la declaración de confidencialidad el expediente con valor permanente entra, en cuanto a su régimen de acceso, en subetapa histórica.

	Acceso confidencial en etapa de tramitación		
Grupo de usuarios	**Consulta**	**Modificación**	**Eliminación**
Equipo de tramitación	Sí	Sí	Sí
Aplicación	No	No	No
Cargos políticos	No	No	No

Terceras partes (ciudadanía)	Sólo interesados	No	No
Administrador de Gestión Documental y Archivo	Sí (metadatos)	No	No
Administrador Tecnológico	Sí	Sí	Sí

	Acceso confidencial en subetapa de vigencia		
Grupo de usuarios	**Consulta**	**Modificación**	**Eliminación**
Equipo de tramitación	No	No	No
Aplicación	No	No	No
Cargos políticos	No	No	No
Terceras partes (ciudadanía)	Sólo interesados	No	No
Administrador de Gestión Documental y Archivo	Sí	Sí (atributos de descripción)	Sí
Administrador Tecnológico	Sí	No	No

El administrador de Gestión Documental y Archivo podrá modificar únicamente los atributos de descripción archivística, nunca los metadatos incorporados en la fase de tramitación.

5.2.2 Acceso a Documentos

Del mismo modo, al **nivel de documento** existen los mismos tres tipos de acceso, señalado con independencia respecto al que haya sido asignado a nivel de Serie documental o Expediente que le corresponda. Así, un documento puede ser de acceso libre en la fase de tramitación, cuando así lo marque el procedimiento administrativo (convocatorias, acuerdos de órganos colegiados, resoluciones de publicación de resultados de pruebas en procedimientos de selección de personal, etc.).

Estos tres niveles aplicados a los documentos son los siguientes:

- **Documentos de acceso público.** Son aquellos documentos que en su estado definitivo son visibles a cualquier persona ajena a la

Administración de la Comunidad Foral de Navarra, así como para todos los usuarios del sistema con cualquier rol. Durante su elaboración (estado borrador), y por lo tanto antes de su captura en el sistema, su tratamiento se corresponde al de un documento reservado, o confidencial si así está declarada la información.

- **Documentos de acceso limitado o restringido.** Son aquellos documentos producidos por la Administración de la Comunidad Foral de Navarra o aportados por un interesado o tercero que se integran en un expediente en la fase de tramitación de un procedimiento. El acceso, por lo general, está limitado a los usuarios del Equipo de tramitación, si bien pueden acceder también usuarios de otros grupos si están autorizados, el administrador Tecnológico y el administrador de Gestión Documental y Archivo.

- **Documentos confidenciales.** Son aquellos documentos generados por la Administración de la Comunidad Foral de Navarra o aportados por un tercero, de uso sólo por los usuarios internos que hayan participado en la tramitación del expediente al que pertenece, aunque el documento pertenezca a un expediente de una serie de acceso libre o restringido al que accedan otros grupos de usuarios. Además de los usuarios del Equipo de tramitación, pueden acceder asimismo el administrador Tecnológico y, una vez cerrado el expediente, el administrador de Gestión Documental y Archivo, con el fin de ejecutar las funciones que les son atribuidas y que deben quedar debidamente registradas en el SGD para garantizar su posterior monitorización.

  Por su parte, el grupo de usuarios pertenecientes al rol Aplicación con acceso a la serie documental puede acceder en caso de realizar procedimientos automatizados y para poder conferir acceso al expediente a aquellos usuarios de las aplicaciones de gestión de expedientes mediante la gestión de permisos para disponer de acceso confidencial al expediente.

  Finalmente, los documentos considerados confidenciales son almacenados de forma cifrada y sólo se deben descifrar durante el acceso por parte del personal autorizado.

De acuerdo con esta clasificación de tipos de acceso y el conjunto de roles definidos, se definen los diferentes niveles de seguridad del sistema existentes y sus respectivas políticas de seguridad para cada serie documental.

6. Aplicación del modelo de seguridad y acceso

Las directrices sobre las que llevar a cabo la aplicación práctica de los contenidos expuestos anteriormente que definen el Modelo de seguridad y acceso, son las siguientes:

a. La **responsabilidad** de la gestión documental durante la **etapa de tramitación** corresponde a la unidad de trabajo que tramita los expedientes. Las diferentes unidades departamentales tienen asignadas series documentales en función de los tipos de expedientes que tramitan. Por lo tanto, el acceso a los documentos electrónicos durante la etapa de tramitación se determina en base al Cuadro de Clasificación de la Administración de la Comunidad Foral de Navarra a nivel de serie documental.

   Cada serie documental debe tener asociados los siguientes elementos:

   - **Responsable de la unidad de trabajo.** Un responsable funcional con el que es necesario confirmar cualquier aspecto relacionado con los criterios de gestión y acceso aplicables a la serie documental. El responsable de la unidad de trabajo gestiona y asigna los permisos de acceso en la etapa de tramitación en base a las series documentales.
   - **Usuarios de la unidad de trabajo.** Los usuarios del departamento funcional y otros departamentos que participan en la tramitación de los expedientes asociados a la serie documental.
   - **Cargos políticos.** Los usuarios que requieren acceso temporal de consulta a los expedientes asociados a la serie documental.

b. Una vez **cerrados los expedientes**, estos pasan a estar bajo la responsabilidad del ámbito de Gestión Documental y Archivo en su etapa archivística:

   - El responsable de Gestión Documental y Archivo resuelve, en aplicación de la normativa vigente, de las Fichas de Series Documentales aplicables y de la coordinación con el propietario del proceso que genera el expediente, las peticiones de acceso a la documentación semiactiva o de vigencia por parte de usuarios diferentes a los del Equipo de tramitación, Aplicación y Cargos políticos, ya que los accesos por parte de los usuarios productores no requieren de autorización al haber participado en la etapa de tramitación.

- El responsable de Gestión Documental y Archivo crea y gestiona los grupos de usuarios. En su caso, serán los responsables de unidad quienes identifiquen y gestionen las personas incluidas en los grupos de usuarios.
- No es necesario autorizar los accesos del administrador Tecnológico, aunque deben quedar registrados para su posterior monitorización.

c. Cada expediente y documento electrónico tiene asignados un conjunto de **metadatos descriptivos** sobre su contenido y otros aspectos, según el Esquema de Metadatos de Navarra. Los metadatos de gestión sobre el control de acceso deben tener en cuenta necesariamente los siguientes aspectos:

- La determinación general del tipo de acceso otorgado: público o reservado, o, residualmente, confidencial. El Equipo de tramitación puede modificar la tipología tanto a nivel de expediente como de documento y siempre a un nivel más restringido de lo que ya disponga.
- Las razones aplicables para la limitación de acceso por parte de las unidades de trabajo específicamente para cada expediente. Se aplica en los casos excepcionales en que:
  - un expediente de una serie de acceso público se determine como de acceso restringido.
  - un expediente de una serie de acceso público o restringido se determine como confidencial.
- La presencia de datos de carácter personal y el nivel de las medidas de seguridad aplicables, siendo de aplicación lo dispuesto en el reglamento de protección de datos. En los casos donde el valor de los metadatos de un expediente o documento electrónico no se les haya atribuido expresamente, el valor asignado por defecto debe impedir los accesos indebidos a su información. En este sentido, los departamentos de la Administración Foral deben evitar que la aplicación de este principio deje sin efecto los derechos de consulta y acceso a la información administrativa por parte de las partes interesadas.

d. El **acceso a los documentos nominativos**. Aquellos expedidos o asociados a una persona concreta y los documentos que contengan datos relativos a la intimidad de las personas y los expedientes no finalizados

queda reservado a las personas que participan en su elaboración y a aquellas que acrediten las condiciones de interesado previstas por la ley en cada caso. Para garantizar que el derecho de consulta a través de medios telemáticos sea ejercido por terceras partes legalmente habilitadas, los departamentos de la Administración Foral deben exigir su identificación mediante cualquier procedimiento de identificación segura, bien electrónica o, en su defecto, presencial.

e. Respecto al **acceso al SGD por parte del personal interno**, se establecen los siguientes criterios de aplicación:

   - Para que un usuario pueda acceder a los sistemas de tratamiento de documentación electrónica debe superar un proceso de identificación (por ejemplo, a través de un identificador de usuario), de 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 y expedientes tienen acceso los usuarios y con qué potestades).
   - Los usuarios, salvo situaciones excepcionales donde se deben identificar y aprobar, disponen de un identificador de usuario unívoco.
   - Las credenciales de acceso de cada usuario son personales e intransferibles y el proceso de asignación y comunicación debe garantizar la confidencialidad y prevenir el acceso no autorizado a través de suplantaciones de identidad.
   - Los usuarios son responsables de preservar la confidencialidad de las contraseñas y de 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 el certificado digital.
   - Los usuarios tienen acceso al SGD hasta el momento que lo precisen para el desarrollo de sus funciones. Se prevén procedimientos específicos para controlar la vigencia de los usuarios temporales, como el listado actualizado de usuarios con acceso autorizado a los sistemas.
   - Cada usuario tiene acceso a los expedientes y documentos de las series documentales que precise sobre la base de las necesidades derivadas de sus funciones y responsabilidades. Se aplican dos niveles de acceso: Equipo de tramitación y Cargos políticos.

- La concesión del acceso a los sistemas de tratamiento de documentación electrónica de la Administración Foral lleva asociado un proceso previo formal de solicitud, evaluación y aprobación. Para la aprobación se establecen responsables funcionales para cada serie documental, ya que son los encargados de decidir el acceso.
- Siempre que se produzca un cambio en las funciones o responsabilidades de un usuario se deben evaluar las consecuencias sobre los derechos de acceso a los sistemas de tratamiento de documentación electrónica de la Administración Foral.
- Para la definición de los perfiles de acceso a la documentación electrónica, la Administración Foral dispone de las utilidades de segregación de funciones de los sistemas de tratamiento de documentación electrónica, donde para cada proceso y para cada una de sus fases de tramitación -y, en consecuencia, para cada uno de los estados de un documento- se determinan los grupos de usuarios que tienen acceso y en qué grado: consulta, modificación y eliminación.
- Adicionalmente, en cada fase del proceso se definen qué documentos son accesibles, modificables o eliminables, quedando prohibida en cualquier caso la eliminación de documentos considerados definitivos. Se establecen tablas de segregación de funciones que identifican todas las transacciones posibles en un sistema de tratamiento de documentación electrónica y que pueden ser ejecutadas por cada tipo de usuario o rol.
- Periódicamente, se realiza un proceso de revisión para verificar que sólo los usuarios autorizados tienen acceso a los diferentes sistemas de información y a las aplicaciones que permiten gestionarlos y que su perfil no excede las autorizaciones mínimas necesarias para el desarrollo de sus funciones ni se suceden conflictos de segregación de funciones.
- Se establecen mecanismos de registro y monitorización de acceso y/o uso de los sistemas que garantizan que los documentos están protegidos de forma efectiva de usos indebidos no autorizados, de alteraciones y de destrucciones, tal y como ha quedado reflejado en el apartado 4.