ANEXO 7.2

SISTEMA DE PROTECCIÓN DE DENUNCIANTES: EJEMPLO DE CANAL INTERNO DE DENUNCIAS APLICABLE A LAS QUE SE PRESENTEN POR MEDIOS ELECTRÓNICOS (BID)

INTRODUCCIÓN

Las empleadas y empleados públicos son, a menudo, los primeros en tener conocimiento de amenazas o perjuicios para el interés público que surgen en ese contexto. Al informar sobre infracciones que tienen lugar dentro de una organización pública que son perjudiciales para el interés público, actúan como denunciantes desempeñando un papel clave a la hora de descubrir y prevenir infracciones y de proteger el bienestar de la sociedad. Sin embargo, las personas denunciantes potenciales suelen renunciar a informar sobre sus preocupaciones o sospechas por temor a represalias.

Por tanto, crece la importancia de prestar una protección equilibrada y efectiva a las personas denunciantes. Para cubrir esta necesidad, el Parlamento y Consejo Europeo aprobaron a finales del año 2019 la Directiva (UE) 2019/1937[25], relativa a la protección de las personas que informen sobre infracciones del Derecho de la Unión. La transposición de esta Directiva se ha realizado a través de la Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción.

El análisis de los canales de denuncia propios ha concluido que es desigual la operatividad de estos canales y su accesibilidad no siempre es universal, por lo que queda cierto margen de desarrollo de los canales internos existentes, con vistas a su adecuación a lo previsto en la Directiva.

Para finalizar con la introducción, es necesario destacar que el siguiente documento se centrará en el canal de denuncias internas y todos los requisitos que se describan se harán partiendo de la Directiva 2019/1937.

REQUISITOS

A continuación, se describen los requisitos, tanto funcionales como no funcionales:

a) Requisitos funcionales. Identificados mediante una descripción y un código alfanumérico formado por RFXXX, donde XXX será un número secuencial.

b) Requisitos no funcionales. Identificados mediante una descripción y un código alfanumérico formado por RNFXXX, donde XXX será un número secuencial.

25 https://www.boe.es/doue/2019/305/L00017-00056.pdf

REQUISITOS FUNCIONALES

Acciones de la persona denunciante (RF001)

La persona denunciante podrá realizar las siguientes acciones:

a) Nueva denuncia. Podrá abrir una o más denuncias.

b) Seguimiento de denuncias abiertas por la misma.

c) Gestión de denuncias abiertas por la misma.

Identificación de denunciantes (RF002)

La persona denunciante podrá realizar las acciones identificadas en el RF001 de forma anónima o identificándose y autenticándose. En el último caso, el sistema identificará y autenticará a la persona denunciante apoyándose en el sistema Autentica.

La forma de abrir una nueva denuncia influirá en cómo deberá gestionarse en el futuro esa denuncia:

a) Si se abre de forma anónima, las sucesivas acciones deberán ser de forma anónima por lo que no se identificará ni autenticará.

b) Si se identifica al abrir la nueva denuncia, las sucesivas acciones exigirán la identificación y autenticación del denunciante.

Nueva denuncia anónima e identificada: información común (RF003)

La persona denunciante podrá crear nuevas denuncias en base al RF002 (anónimas o identificándose) a través de un canal electrónico, descartándose otras opciones indicadas en la Directiva.

La información de entrada que es común de una denuncia anónima e identificada es:

Información	Descripción	¿Obligatorio?
Categorización.	Permite clasificar la denuncia.	No
Título.	Descripción breve de la denuncia.	Sí
Descripción.	Descripción inicial y detallada de la denuncia.	Sí
Nombre y apellidos de la persona denunciada.	Nombre y apellidos de la persona denunciada.	Sí
Documento de identificación de la persona denunciada.	DNI/NIE/Pasaporte de la persona denunciada.	No
Comentarios.	Información que ayude a gestionar la denuncia.	No
Ficheros de apoyo.	Ficheros que permitan investigar los hechos denunciados.	No
Aceptación condiciones y reglas de uso.	Condición de uso del buzón de denuncias.	Sí

Información	Descripción	¿Obligatorio?
Dirección de correo postal de la persona informante (no obligatorio).	Permite, en su caso, el contacto con la persona informante.	No
Dirección de correo electrónico de la persona informante (no obligatorio).	Permite, en su caso, el contacto con la persona informante.	No
Número de teléfono de la persona informante (no obligatorio).	Permite, en su caso, el contacto con la persona informante.	No

Tabla 1. Información de entrada de denuncias anónimas e identificadas

Todos los campos no obligatorios podrán añadirse en cualquier momento mientras la denuncia se encuentre en un estado no final.

Denuncia anónima: eliminación información personal(RF004)

Además de la información indicada en el requisito RF003, en la gestión de denuncias anónimas (creación, modificación, etc.) se debe asegurar que la información que facilita la persona denunciante no contiene datos personales propios.

a) Datos recogidos del formulario de entrada para la creación de la denuncia:

   Es necesario no confundir los datos de la persona denunciante con los datos de la persona denunciada por lo que se crearán campos propios para los datos de esta para que, esos datos, no sean revisados y anonimizados. Todos los datos que se identifiquen como personales fuera del campo de datos de la persona denunciada, se deberán anonimizar.

b) Metadatos de los ficheros anexados:

   Las personas denunciantes podrán incluir ficheros que apoyen su denuncia. Estos ficheros que se anexen deberán ser tratados para eliminar sus metadatos asociados para evitar que aparezca información asociada a aquellas.

Nueva denuncia identificada: información propia (RF005)

Además de la información indicada en el requisito RF003, las denuncias identificadas deberán recoger los siguientes datos de entrada:

Información	Descripción	¿Obligatorio?
Nombre y apellidos.	Nombre y apellidos de la persona denunciante.	Sí
Documento de identificación.	DNI/NIE/Pasaporte de la persona denunciante.	Sí
Comunicación.	Datos necesarios para comunicarse con la persona denunciante.	No

Tabla 2. Información de entrada de denuncias identificadas

Todos los campos no obligatorios podrán añadirse en cualquier momento mientras la denuncia se encuentre en un estado no final.

El nombre, apellidos y el documento de identificación se autorrellenará siendo provista por Autentica.

Información adicional de una denuncia (RF006)

Además de la información recogida en el momento de crear la denuncia por parte de la persona denunciante, tanto anónima como identificada, es necesario registrar más información:

a) Comentarios. Tanto las unidades responsables del tratamiento de la denuncia como las personas denunciantes podrán aportar, siempre que la denuncia se encuentre en un estado no final, comentarios que aporten información relevante para la gestión de la denuncia.

   a.1 Cualquiera de las transiciones entre los estados definidos en el RF008 registrará en los comentarios el estado origen y el estado destino para tener la trazabilidad de los cambios.

b) Fecha y hora. Asociado a cada cambio de estado definido en el requisito RF005 o cada vez que se inserte un comentario, fichero o cualquier otra información, se registrará la fecha y hora de la acción (DD/MM/YYYY HH24: MI: SS).

   Por defecto, al crearse una denuncia se crearán las siguientes fechas:

   b.1 Fecha de creación de la denuncia.

   b.2 Fecha de caducidad. Según la Directiva, son 3 meses a partir del acuse de recibo. Este valor se calculará en base a un campo parametrizable.

   Por otro lado, cuando se cambie al estado «Pendiente de información» para pedir información adicional a la persona denunciante, se calculará automáticamente en función de un campo parametrizable la fecha de caducidad de la acción requerida a la misma.

c) Responsable de la acción. Al igual que en la información de fecha y hora, cada vez tenga lugar un cambio de estado, se inserte un comentario, fichero o cualquier otra información, se registrará quién ha realizado la acción. Los valores serán:

   c.1 «Denunciante». Cada vez que la persona denunciante realice alguna de las acciones comentadas anteriormente.

   c.2 «Unidad X», donde X se corresponderá con la unidad relacionada con la gestión de la denuncia.

Deber de confidencialidad (RF007)

Se debe cumplir el deber de confidencialidad reflejado en la Directiva 2019/1937 que se resumen en:

a) No revelar la identidad de la persona denunciante sin su consentimiento expreso a ninguna persona que no sea un miembro autorizado del personal competente para recibir o seguir denuncias. Lo anterior también se aplicará a cualquier otra información de la que se pueda deducir directa o indirectamente la identidad de aquella.

a.1 Excepción: la identidad de la persona denunciante y cualquier otra información prevista en el apartado 1 solo podrá revelarse cuando constituya una obligación necesaria y proporcionada impuesta por el Derecho de la Unión o nacional en el contexto de una investigación llevada a cabo por las autoridades nacionales o en el marco de un proceso judicial, en particular para salvaguardar el derecho de defensa de la persona afectada.

b) Si se revela, se informará a la persona denunciante antes de revelar su identidad, salvo que dicha información pudiera comprometer la investigación o el procedimiento judicial. Se motivará.

b.1 Si incluye secretos comerciales, se garantizara que las unidades que gestionen la denuncia no usen ni revelen esos secretos comerciales para fines que vayan más allá de lo necesario para un correcto seguimiento.

c) Si se diera alguna o varias de las condiciones anteriores, la denuncia se anulará de manera motivada. La anulación será realizada por una persona asociada a la unidad implicada en el procedimiento de gestión de la denuncia.

Ciclo de vida de una denuncia (RF008)

Una denuncia seguirá el siguiente ciclo de vida:

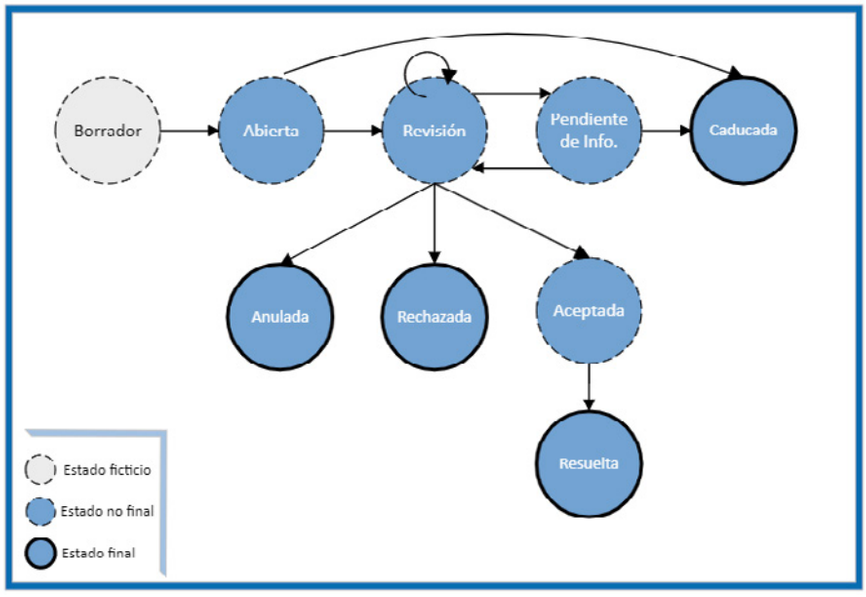

Ilustración 1. Flujo de estados de la denuncia

1. **Borrador**. Una vez la persona denunciante ha rellenado, como mínimo, los datos obligatorios y ha aceptado los términos y condiciones de uso, el sistema comprobará los datos introducidos (RF003, RF004, RF005) y si son correctos, se procederá a registrar la solicitud. Como resultado del registro correcto se generará el identificador definido en el RF008.

No habrá denuncias registradas como tal en este estado. Es un estado «fantasma» que tiene como propósito explicar qué hacer y, por ello, el denunciante no podrá dejar una denuncia en «borrador» para recuperarla y seguir creándola posteriormente. Deberá empezar de cero.

2. **Abierto.** Estado inicial de la denuncia registrada correctamente. La denuncia pasa de estado «borrador» a «abierto» cuando se registra correctamente en el sistema. Se mantendrá en este estado hasta que sea tratada por primera vez por un o una integrante de la unidad gestora que se defina en el flujo de trabajo de la denuncia o cuando cumpla el plazo total de gestión por parte de las unidades responsables. El plazo definido por la Directiva es de 3 meses, pero, este valor, se parametrizará como atributo para que pueda ser configurado en caso de necesidad.

3. **Revisión.** Estado que indica que la denuncia está siendo tratada por las unidades asignadas para ello. Este estado permite a las diferentes unidades relacionadas escalar la denuncia para que cada una de ellas revise la misma en el ámbito de su responsabilidad o aporte información relevante para el tratamiento de la denuncia. Esta información podrá ser tanto texto en modo de comentarios como ficheros de cualquier tipo.

   Este estado tendrá asociado un atributo que permita indicar a qué unidad de gestión que forma parte del flujo de gestión está asignada la denuncia.

4. **Pendiente de información.** Estado que permite requerir a la persona denunciante aclaraciones con relación a la información ya aportada o pedir información nueva necesaria para la gestión de la denuncia. Al igual que en el estado «borrador», el sistema deberá comprobar los datos introducidos (RF003, RF004, RF005).

5. **Caducada.** Estado final a que se evolucionará de manera automática si desde la fecha de petición de información por parte de las unidades responsables a la persona denunciante supera los meses definidos o si, desde la fecha de creación, se ha superado el plazo máximo de gestión de la denuncia por parte de las unidades responsables. El plazo de caducidad, en ambos casos, será configurable. Se incluirá el motivo de la caducidad.

6. **Anulada.** Estado que permite a las unidades responsables del tratamiento de la denuncia detecta lo definido en el RF007.

7. **Rechazada.** Estado que permite indicar a las unidades responsables del tratamiento si la denuncia no procede. Deberá ser motivada.

8. **Aceptada.** Cuando la persona responsable del tratamiento de la denuncia considera que es necesario tramitar la denuncia.

9. **Resuelta.** Estado que permite indicar si ha habido investigaciones y actuaciones realizadas a raíz de la denuncia y asociar la información.

Estado origen	Estado destino	Disparador de cambio de estado	¿Estado final?	Denunciante aporta info. extra
Borrador	Abierto.	Solicitud enviada por la persona denunciante y verificada por el sistema.	No	Sí
Abierto	Revisión.	La denuncia comienza a ser gestionada o se está gestionando	No	Sí
Revisión	Revisión.	Revisión: cuando una unidad escala la denuncia a otra unidad relacionada con la denuncia y definida dentro del flujo de trabajo.	No	Sí
	Pendiente de información.	Pendiente de información: cuando la unidad que está gestionando la denuncia necesita información adicional de la persona denunciante.		
	Anulada.	Anulada: si las unidades responsables de la gestión detectan que no se cumple el deber de confidencialidad (RF006).		
	Rechazada.	Rechazada: cuando la unidad que está revisando la denuncia considera que el acto expuesto en la denuncia no es denunciable aplicando la Directiva.		
	Aceptada.	Aceptada: la unidad que está revisando la denuncia considera que el acto expuesto en la denuncia es denunciable aplicando la Directiva.		
	Remitida.	Remitida: cuando se remita a la autoridad, entidad u organismo que se considere competente para su tramitación o cuando afecte a los intereses de la Hacienda Pública.		
	Caducada.	Caducada: si pasa el plazo máximo definido para que las unidades responsables gestionen la denuncia.		
	En los casos de rechazada o remitida se comunicará el trámite a la persona informante.			
Pendiente de información	Caducada.	Caducada: cuando la petición de información no es contestada en un tiempo determinado.	No	Sí
	Revisión.	Revisión: cuando la persona denunciante aporta la información requerida.		
Caducada	N/A	N/A	Sí	No
Anulada	N/A	N/A	Sí	No
Rechazada	N/A	N/A	Sí	No
Aceptada	Resuelta.	Resuelta: permite asociar las investigaciones y actuaciones realizadas a raíz de la denuncia y su la información.	No	Sí
Resuelta	N/A	N/A	Sí	No

Tabla 3. Ciclo de vida de una denuncia

Consideraciones generales:

1. Si el estado permite la inserción de comentarios o ficheros adicionales por parte de la persona denunciante, siempre se deberá cumplir el requisito RF004.
2. Cada vez que la denuncia cambie de estado, se registrará en los comentarios y llevará asociada la fecha de realización, así como la unidad que lo ha realizado o, si se ha realizado derivado del incumplimiento de un plazo, aparecerá reflejado.

Confirmación de recepción de denuncia (RF009)

Tanto en el caso de denuncias anónimas como identificadas, es necesario confirmar la recepción correcta de la misma. Esta confirmación se realizará en el momento en el que la persona denunciante envíe la misma y se registre correctamente en el sistema. Generará un número aleatorio no secuencial que servirá como identificador de la denuncia.

Si la denuncia es identificada y, a la hora de generar la denuncia se indica que se quiere activar las comunicaciones, se realizará una notificación por el medio de comunicación elegido (correo electrónico o SMS).

Gestión del sistema (RF010)

Se desarrollará un módulo que permita gestionar y crear nuevos flujos de trabajo asociados a la gestión de las denuncias añadiendo, eliminando o modificando unidades responsables de la gestión de las denuncias.

Perfiles (RF011)

A continuación, se definen los diferentes perfiles:

Perfil	Ámbito	Acciones asociadas	Descripción
Denunciante	Denuncia.	• Crear, consultar y modificar denuncias.	Solo podrá realizar las acciones descritas sobre sus propias denuncias.
Revisor/a	Gestión.	• Consultar denuncias. • Consultar estadísticas.	N/A
Gestor/a	Gestión.	• Mismas acciones que perfil «Revisor/a». • Modificar y consultar denuncias. • Escalar denuncias. • Cambiar estado denuncias. • Consultar unidades y sus usuarios y usuarias.	Este perfil permitirá a las unidades responsables de tramitar la denuncia, gestionar la misma.
Administrador/a	Gestión.	• Mismas acciones que perfil «Gestión» y «Estadístico». • Consultar estadísticas. • Búsqueda avanzada de denuncias. • Crear, consultar y modificar flujos de trabajo asociados a las denuncias. • Definir los ANS para la gestión de las denuncias para cumplir los plazos indicados en la Directiva. • Gestionar unidad y sus usuarios y usuarias.	Habrá dos tipos de administrador/a: Administrador/a global. Sin unidad asignada, puede hacer las acciones comentadas sobre cualquier unidad. Administrador/a de unidad. Solo puede realizar las acciones comentadas de la unidad que tiene asignadas

Tabla 4. Perfiles

Consultar denuncias por parte de denunciante (RF012)

Es necesario diferenciar entre la consulta de denuncias anónimas y la consulta de denuncias donde la persona denunciante se ha identificado:

a) Denuncias anónimas. La consulta de denuncias anónimas se realizará mediante el número secuencial que devolverá el sistema cuando se cree la denuncia (RF009).

   En este caso, y al no estar identificada la persona denunciante, es difícil evitar que, quien no haya abierto la denuncia, pueda consultarla si «averigua» el identificador.

b) Denuncias identificadas. La consulta de denuncias identificadas exigirá la identificación y autenticación de la persona denunciante. Si el identificador proporcionado se corresponde con una denuncia identificada que no fue creada por la persona que realiza la consulta, no devolverá resultados.

Consultar denuncias por parte de unidades gestoras (RF013)

Los perfiles del ámbito de gestión definidos en el RF011 podrán consultar todas las denuncias o hacerlo en función de los campos asociados a la denuncia mediante parámetros que habiliten el filtrado:

a) Identificador de la denuncia.

b) Documento identificativo del denunciante o aquellas que son anónimas.

c) Unidad que está gestionando la denuncia.

d) Unidad que ha participado en la gestión de una denuncia.

e) Estado de la denuncia.

f) Fechas: creación, última creación, etc.

g) Palabras clave en los comentarios.

Se devolverán todas las denuncias que coincidan con los parámetros de entrada para permitir la consulta individual de cada registro devuelto en el resultado.

Modificar denuncias (RF014)

Para poder modificar una denuncia es preciso que antes se realice una consulta de la misma, es decir, RF012 u RF013. La modificación de denuncias deberá cumplir los requisitos RF003, 004, 005, 006, 007 y RNF001.

La modificación de denuncias se podrá realizar en cualquier estado no final, como se comenta en los requisitos RF005 y RF006. Permitirá a las personas denunciantes y a las unidades responsables de tramitar la denuncia gestionar la denuncia y comunicarse entre sí y estas serán las acciones permitidas:

a) Añadir o modificar datos no obligatorios, en el caso de denuncia anónima o identificada:

   a.1 Documento de identificación de la persona denunciada.

   a.2 Comentarios.

   a.3 Ficheros de apoyo.

b) Añadir o modificar información relacionada con los mecanismos comunicación con la persona denunciante identificado.

Eliminar denuncias (RF015)

No se permitirá eliminar denuncias de ningún tipo.

Gestión de estadísticas (RF016)

Se creará un módulo para gestionar K. P. I. asociados a la gestión de las denuncias:

a) Gestión de K. P. I.: añadir, eliminar, modificar y consultar K. P. I.

b) Extracción de información y generación de informes.

REQUISITOS NO FUNCIONALES

Eliminación de la información de red personal (RNF001)

En el caso de denuncias anónimas y, con el fin de evitar la identificación de las personas denunciantes, es necesario que no haya rastro de información que permita la deducción de sus datos personales.

Al ser una aplicación Web a la que se accederá a través de un navegador, será necesario eliminar la IP junto con otros posibles datos que se puedan recoger de la conexión del usuario con la red y que permitan saber quién está detrás de la denuncia antes de enviar cualquier petición (nuevas denuncias, consulta o modificación de denuncias, etc.).

La solución implementada deberá tener orientación a la persona usuaria, es decir, deberá realizarse de manera que la persona denunciante no tenga que hacer acciones adicionales.

A continuación, se identifican posibles soluciones al problema que deberán estudiarse para implementar la opción que menos impacte en la persona usuaria y en costes. La presentación de estas opciones no inhabilita para que se presenten nuevas opciones que mejoren las propuestas.

Opción	Descripción	Ventajas	Desventajas
Navegador Web	Existen navegadores Web como DuckDuckGo que ocultan la información de red de la persona usuaria conectada a través de múltiples capas de cifrado.	Sin coste adicional. Afecta al rendimiento de red.	Requiere acción de la persona usuaria para descarga e instalación.
VPN	Servidor intermedio que cifra la conexión a Internet.	Posibles costes monetarios. No interfiere en el rendimiento de red.	Depende del proveedor de VPN ya que se debe elegir un proveedor que no registre la actividad. Requiere acción de la persona usuaria para descarga e instalación.
Proxy	Permite gestionar el tráfico intercambiado enmascarando la IP origen.	Soluciones de servidores proxy ya implementados en la AGE: posible reutilización.	No es totalmente seguro, puede interceptar las peticiones hechas desde el cliente a la red.

Tabla 5. Opciones para eliminar la información de red personal

Impedir acciones masivas (RNF003)

Para evitar acciones masivas (consultas o nuevas denuncias, por ejemplo) se implementará un mecanismo de defensa, como agregar una pregunta de prueba al formulario de consulta o cualquier otro que evite el problema.

Accesibilidad (RNF004)

Se realizará un diseño Web *responsive* para que la interfaz de usuario se adapte al tamaño de la pantalla de cualquier dispositivo, y se seguirá la norma EN301459, definida de cumplimiento en el Real Decreto 1112/2018, de 7 de septiembre, sobre accesibilidad de los sitios web y aplicaciones para dispositivos móviles del sector público, para desarrollar la capa de presentación universal y accesible para llegar a los niveles A y AA de WCAG 2.1 que tienen como objetivo conseguir una interfaz comprensible, operable, robusta y perceptible.

Por otro lado, se hará uso de las guías para la validación de accesibilidad Web y guía para editores finales de contenidos Web [26].

Idiomas (RNF005)

Es necesario que el buzón de denuncias internas anónimas cumpla con el artículo 15 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas por lo que habilitará la gestión de las denuncias en todas las lenguas cooficiales del territorio español.

Soporte de navegadores web (RNF006)

El BID deberá soportar su acceso y uso en todos los navegadores Web de la industria para facilitar su implantación y aceptación por parte de los usuarios.

Seguridad (RNF007)

Se realizará un análisis de las necesidades de seguridad en base al Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad y se implementarán las medidas que se obtengan tras realizar dicho análisis.

Interoperabilidad (RNF008)

Se realizará un análisis de las necesidades de interoperabilidad en base al Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica y se implementarán las medidas que se obtengan tras realizar dicho análisis.

Protección de datos (RNF009)

Se realizará un análisis de las necesidades de protección de datos en base a la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales y se implementarán las medidas que se obtengan tras realizar dicho análisis.

---

26 https://administracionelectronica.gob.es/pae_Home/pae_Biblioteca/pae_PublicacionesPropias/Monografias-administracion-electronica/Guias_Observatorio_Accesibilidad.html

PROPUESTA DE SOLUCIÓN

Alternativas de solución

Las alternativas de solución que se plantean se intentan ajustar a las necesidades de desarrollo y al uso de servicios compartidos cumpliendo así el artículo 10 del Real Decreto 806/2014, de 19 de septiembre, sobre organización e instrumentos operativos de las tecnologías de la información y las comunicaciones en la Administración General del Estado y sus organismos públicos.

Por otro lado, y en base al comentado Real Decreto, la necesidad de un buzón de denuncias anónimas se extiende a todas las unidades de la Administración General del Estado, independientemente del ministerio u organismo. Por tanto, la solución que aquí se propone quedará supeditada al desarrollo de un sistema que cumpla con los requisitos de la Directiva 1937/2019 y que permita ser implantada en toda la AGE maximizando la economía de escala y la eficiencia en el uso de los recursos públicos.

Por tanto, la forma de abordar un sistema que cumpla con los requisitos se puede resumir en tres opciones o alternativas.

a) Desarrollo a medida. En los apartados sucesivos es la opción que se explicará más en detalle ya que es la que más lo precisa.

b) Implementación en ACCEDA 2.0. Actualmente, la SGAD está desarrollando la evolución de ACCEDA. Es necesario comprobar que esta evolución permite cumplir con los requisitos definidos anteriormente. Hay que prestar especial atención a una serie de limitaciones encontradas en la versión actual, y que habrá que revisar en detalle para verificar la posibilidad de reutilización de ACCEDA 2.0. Dentro de las limitaciones encontradas, podemos destacar:

   b.1 La identificación y autenticación es obligatoria.

   b.2 El tamaño de los ficheros adjuntados no puede superar los 15MB.

   b.3 En Acceda, se tramitan procedimientos, y las denuncias no son procedimientos.

   b.4 Implementación de la interfaz de usuario.

   Aun así, la implementación en ACCEDA es altamente recomendable, ya que, además de ser un servicio compartido, recortaría los plazos de implantación y permitiría reutilizar la integración desarrollada con terceros sistemas como Autentica, su BPM para implementar los diferentes flujos de trabajo que den soporte a las denuncias o, incluso, la herramienta de gestión documental que le da soporte.

c) Desarrollo híbrido. Esta alternativa pretende superar las posibles limitaciones de ACCEDA 2.0 generando una interfaz de usuario propia que se integre con su *core* y así, aprovechar al máximo su funcionalidad y cumplir con los requisitos de los buzones de denuncia anónimas.

En esta alternativa de solución se desarrollará una interfaz de usuario o capa de presentación a medida que interactúe con el correo de ACCEDA 2.0 a través de interfaces REST.

Análisis funcional

A continuación, se define el análisis función y técnico de BID basándonos en la primera alternativa antes explicada, al ser la más compleja y extensa.

Inicio

BID presentará la página principal cuando se acceda a ella. En esta primera pantalla, se pretende habilitar la persona usuaria a que seleccione qué acción quiere realizar:

a) Crear una nueva denuncia.

b) Consultar una denuncia.

Ilustración 2. Página principal de BID

Además de las acciones anteriormente descritas, la persona usuaria podrá realizar una serie de acciones que son comunes a toda la aplicación Web:

c) Cabecera: compuesta por el logotipo al que pertenece el buzón de denuncias internas anónimas, el nombre de la aplicación Web, el logotipo de la aplicación Web y un conjunto de enlaces para permitir traducir la aplicación Web a los idiomas oficiales de España.

Para permitir crear denuncias de manera identificada y acceder a las mismas, se habilitará la funcionalidad para acceder.

d) Pie de página: compuesta por un conjunto de enlaces que redirigen a la persona usuaria a:

d.1 Resolución que crea el buzón.

d.2 Información del buzón:

- ¿Qué es y para qué sirve el BID?
- Objetivos del buzón.
- Ámbito de actuación.

- Funcionamiento.
- Seguimiento.
- Comunicaciones anónimas.
- Estatuto de la persona denunciante.

b.3 Enlace a la Directiva 2019/1937.

Cuando se coloca el ratón por cualquiera de las dos opciones, se activará el foco para resaltar la opción que se está seleccionando.

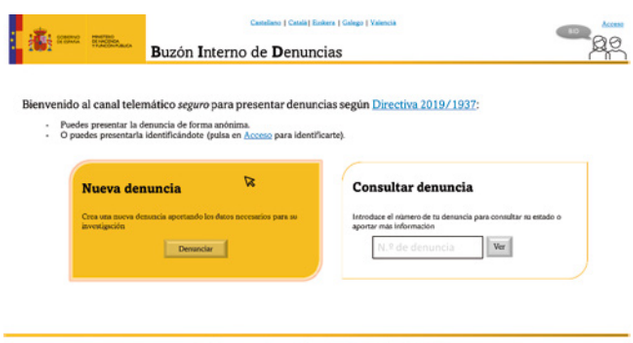

Ilustración 3. Resaltar acción

Creación de una denuncia

La denuncia puede ser creada de forma anónima o identificándose. Cuando se haga clic en el botón «Denunciar» de la página principal, se mostrará un *pop-up* preguntando a la persona denunciante si la denuncia que quiere hacer es anónima o quiere identificarse para iniciarla.

Creación de denuncia anónima

Si la persona denunciante elige realizar la denuncia de manera anónima, le aparecerá la pantalla de «Creación de denuncia anónima: información» (Ilustración 4) permitiéndole ingresar los datos definidos en el RF003, leer las condiciones de uso y término y aceptarlas. Se dividirá en dos pestañas navegables entre sí:

a) Pestaña «Datos de la denuncia». En esta pestaña se habilitará el formulario para introducir los datos relativos a la denuncia que se definen en el RF003.

   – El formulario estará contenido en un marco con un *scroll* que permita navegar por el formulario.

   – Las cajas de texto y combos estarán sombreadas si no están activas (aparecerán en un tono gris). En el momento que la persona usuaria clique en la caja de texto o seleccione el combo, se activará pasando a blanco. En la siguiente ilustración se pretende mostrar el funcionamiento, siendo la caja de texto correspondiente al título la que está activa y, el resto, inactivas.

Ilustración 4. Creación de denuncia anónima: información

b) Pestaña «Condiciones y términos de uso». En esta pestaña se informará a la persona usuaria de las condiciones y términos de uso, haciendo referencia a la Directiva (UE) 2019/1937.

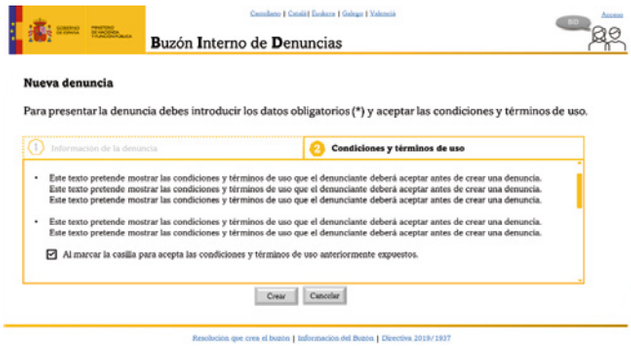

Ilustración 5. Creación de denuncia anónima: condiciones y términos de uso

Cuando la persona usuaria o denunciante pulse en el botón «Crear», BID:

a) Validará los datos de entrada comprobando que se han introducido, como mínimo, los datos obligatorios.

b) Eliminará la información de carácter personal antes de registrar la información cumpliendo así el RF004 y RNF001.

c) Verificará que se ha marcado la casilla de aceptación de condiciones y términos de uso.

Si cualquiera de las validaciones anteriores no se cumple, BID no registrará la nueva denuncia e indicará a la persona denunciante cómo subsanar el problema mediante un *pop-up* informativo.

Si las validaciones anteriores son correctas, BID registrará la nueva denuncia y redirigirá a la persona denunciante a la ventana de «Consulta de una denuncia anónima».

Por otro lado, la documentación que aporte la persona denunciante se almacenará en INSIDE (sistema de gestión documental), permitiendo gestionar e intercambiar la documentación aportada cumpliendo el Esquema Nacional de Interoperabilidad.

Creación de denuncia identificada

Para realizar una denuncia en el que la persona denunciante esté identificada la persona usuaria deberá logarse. El logado se apoyará en el servicio común Autentica (a través de SSO), que permite identificar y autenticar a empleadas y empleados públicos.

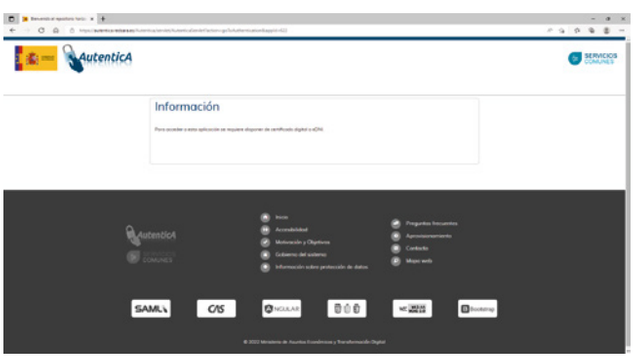

Ilustración 6. Autenticación e identificación de denunciante

Una vez autenticada e identificada correctamente, le aparecerá la pantalla de «Creación de denuncia identificada» permitiéndole ingresar los datos definidos en el RF005, leer las condiciones de uso y término y aceptarlas. El funcionamiento de la ventana será el mismo que cuando se hace una denuncia anónima.

Además, dará información sobre que la persona usuaria está conectada y le permitirá cerrar sesión.

Ilustración 7. Creación de denuncia identificada

Consulta y modificación de una denuncia

Si en la página principal, la persona usuaria introduce el identificador devuelto por BID cuando se creó la denuncia correctamente y pulsa en el botón «Ver» de la sección titulada como «Consultar denuncia», se le mostrará una pantalla con toda la información de la denuncia anónima.

En la búsqueda de las denuncias se deberá cumplir que:

a) El identificador de la denuncia existe.

b) Si el identificador de la denuncia existe y está asociada a una denuncia realizada por una persona denunciante identificada, exigirá el logado de esta para permitirle visualizar la denuncia identificada.

Si las condiciones anteriores se cumplen, se mostrará la información de la denuncia consultada. La siguiente imagen muestra la composición de la ventana que muestra la información de la misma:

a) Enlace para volver a la pantalla principal.

b) Enlace para refrescar la denuncia para comprobar posibles cambios que se hayan producido durante la consulta.

c) Título que permitirá saber el identificador de la denuncia que se está consultando.

d) Cuadro que incluye la información detallada de la denuncia:

- Título de la denuncia.
- Descripción.
- Datos de la persona denunciada.
- Comentarios. Se podrán añadir más comentarios.
- Ficheros de la denuncia. Tanto aportados por la persona denunciante como por las unidades que participan en la tramitación. Se podrán añadir más ficheros.
- Fechas: creación, última actualización y caducidad.
- Estado de la denuncia.
- Unidades destinatarias que tramitarán la denuncia.
- En el caso de ser una denuncia identificada:
  - Nombre y apellidos de la persona denunciante.
  - Documento de identificación de la persona denunciante.
  - Forma de comunicación con la persona denunciante.

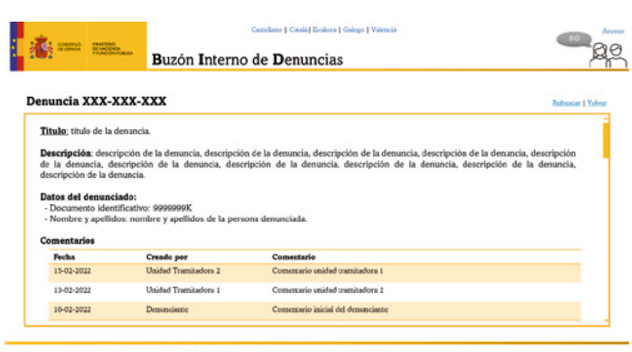

Ilustración 8. Consulta de denuncia

La imagen anterior muestra parte el resultado de la consulta, un resumen. En la siguiente imagen se mostrará cómo se estructurará el contenido del cuadro anteriormente descrito.

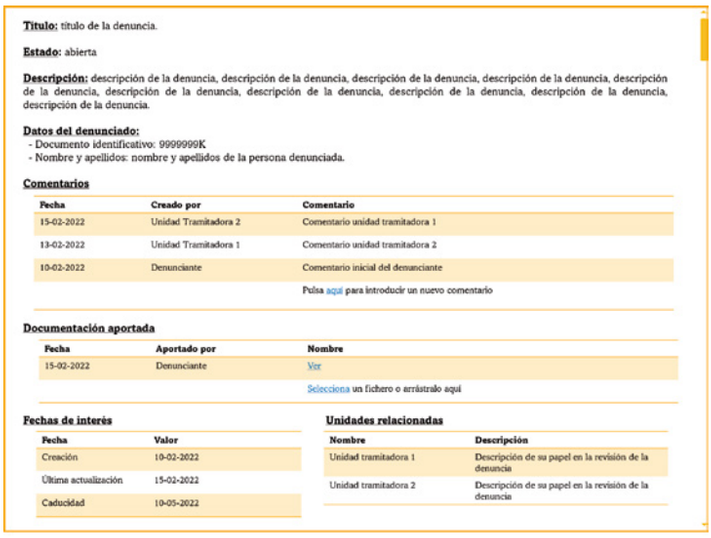

Ilustración 9. Datos de denuncia y su modificación

Con el objetivo de simplificar la aplicación, no se permitirá a las personas denunciantes que han realizado una denuncia de manera identificada consultar sus denuncias más que por el identificador. No se prevé que una misma denunciante realice más de una denuncia.

Por último, si la denuncia se encuentra en estado «Pendiente de información», la persona denunciante podrá aportar la información requerida y volver a enviar la denuncia.

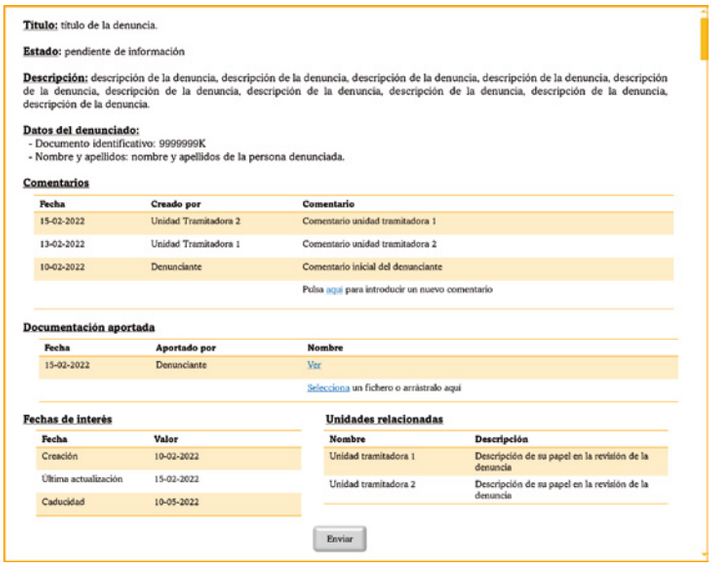

Ilustración 10. Denuncia pendiente de información

Gestión de denuncias

Para poder gestionar las denuncias es necesario que las personas usuarias con el perfil de «gestión» definido en el RF011 se loguen a través de Autentica. Estas serán las únicas que estarán registradas en BID, las personas denunciantes simplemente tendrán asociado a cada uno de sus documentos de identificación las denuncias que hayan creado.

Como se ha comentado la identificación y autenticación se hará por medio de Autentica. Se crearán las tablas necesarias para los perfiles en la base de datos que da soporte a BID. Cuando se despliegue la aplicación, solo existirá una persona usuaria dado de alta con perfil de administrador/a que estará habilitada para crear los flujos de trabajo y los usuarios y usuarias.

En el módulo de gestión se podrá:

1. Gestión de denuncias: consultar y tramitar.
2. Gestión de unidades y sus usuarios y usuarias.
3. Consulta de estadísticas.
4. Gestión de los flujos de trabajo.

Ilustración 11. Gestión de denuncias

Si el usuario o usuaria conectado no tiene permisos para gestionar cualquier de los módulos, estos aparecerán deshabilitados y no se permitirá su elección.

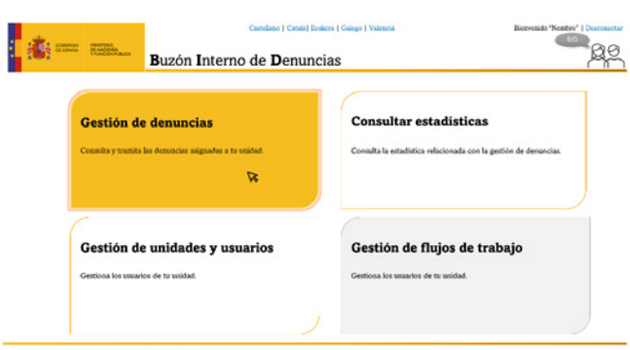

Ilustración 12. Gestión de denuncias. Funcionalidad desactivada por perfil

Gestión de denuncias: consultar

Los usuarios o usuarias con perfil de gestión podrán consultar las denuncias, independientemente de su estado. Por defecto, aparecerán cargadas las asignadas a la unidad a la que pertenezcan en estado «Revisión» y con la siguiente información por defecto:

a) Identificador de la denuncia.

b) Título.

c) Fecha de creación.

d) Fecha de caducidad.

e) Datos de la persona denunciada: nombre, apellidos y documento de identificación.

f) Estado.

g) Unidad asignada.

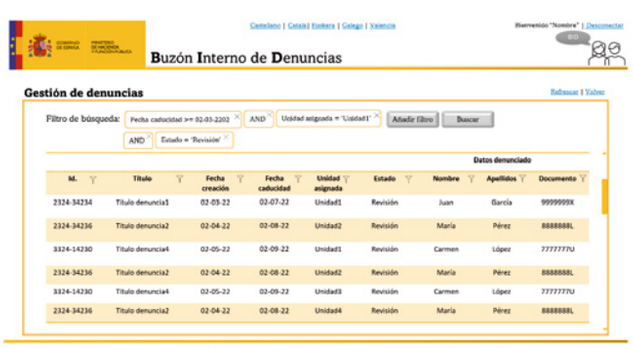

Ilustración 13. Búsqueda de denuncias

Se permitirá la búsqueda y filtrado de denuncias teniendo en cuenta los parámetros que se listan a continuación. Además, se permitirá ordenar en función de cualquiera de ellos.

a) Identificador de la denuncia.

b) Estado.

- Si el estado es «Revisión» o «Aceptada», se habilitará un parámetro que permita filtrar a qué unidad está asignada.

c) Fecha de creación.

d) Fecha de última actualización.

e) Fecha de caducidad.

f) Datos de la persona denunciada: nombre, apellidos y documento de identificación.

g) Datos de la persona denunciante, en caso de ser denuncia identificada.

h) Título.

i) Descripción.

j) Comentarios.

No se permitirá la búsqueda mediante los siguientes parámetros:

a) Documentación aportada.

b) Cualquier metadato asociado a la documentación aportada.

Para poder consultar el detalle de cualquier denuncia devuelta por la búsqueda, la persona usuaria deberá hacer clic en la fila en la que se encuentre el registro que quiera consultar y se mostrará la pantalla asignada a la visualización de denuncias con la siguiente imagen. Como se puede observar, la opción de seleccionar un nuevo estado o seleccionar una unidad para asignarle la incidencia están deshabilitadas.

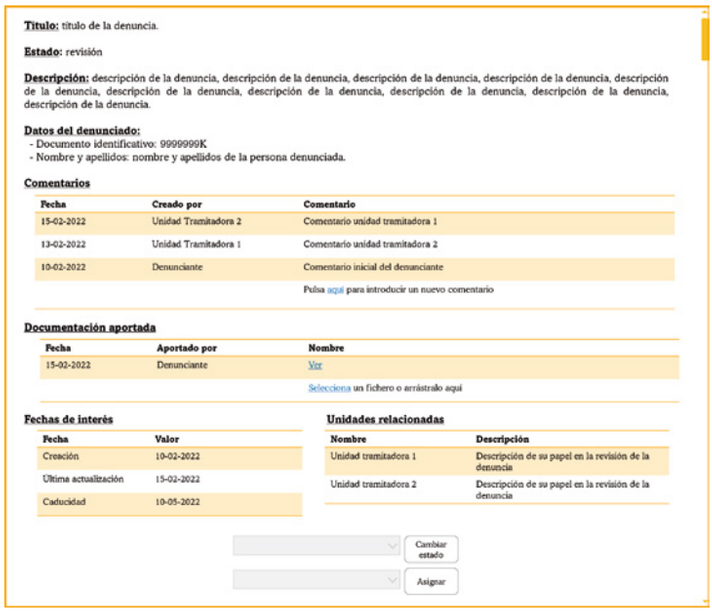

Ilustración 14. Visualización de denuncias no asignada por usuarios gestores/as

Gestión de denuncias: tramitar

Para poder tramitar una denuncia es necesario que se encuentre en estado «Revisión» o «Aceptada» y asignada a la unidad a la que pertenece el usuario. Si no está asignada a la unidad a la que pertenece, la persona usuaria como gestor o gestora podrá añadir ficheros o comentarios, pero no podrá cambiar su estado ni escalar la denuncia a otra unidad tal y como se muestra en la imagen anterior. Si está asignada a su unidad y se encuentra en estado «Revisión» o «Aceptada», se habilitará la opción de cambiar el estado y asignar la denuncia a otra unidad.

La evolución de estados está limitada por el requisito RF008, donde se define el ciclo de vida de la denuncia y las unidades a las que se puede asignar estará definido en el flujo de trabajo que se haya definido para dicha denuncia por parte de los perfiles gestores que puedan establecerlos.

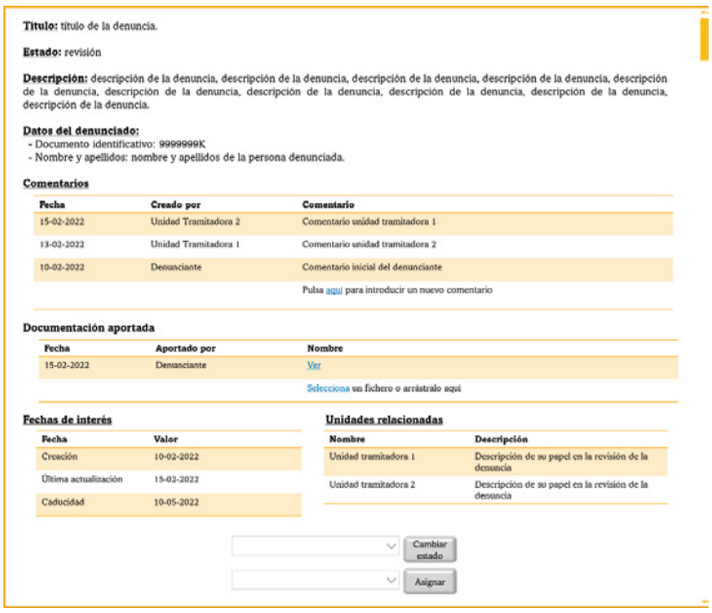

Ilustración 15. Consulta de denuncia asignada

A nivel de comunicaciones, cada vez que:

a) Se abra una nueva incidencia, se enviará una comunicación al correo electrónico asociado de las unidades asignadas a la denuncia abierta en el flujo de trabajo.

b) Se cambie de estado a un estado final o a «pendiente de información». Si la denuncia es identificada, se notificará al denunciante por el medio que haya elegido a la hora de abrir la denuncia.

c) Se cambie de estado final, se enviará una comunicación al correo electrónico asociado de las unidades asignadas a la denuncia en el flujo de trabajo.

d) Se cambie la unidad a la que está asignada la denuncia, se enviará una comunicación al correo electrónico asociado a la unidad a la que se asigna la denuncia.

Gestión de unidades y sus usuarios

Para permitir la tramitación de las denuncias es necesario habilitar una funcionalidad que facilite la gestión de las unidades relacionadas con la denuncia y sus usuarios y usuarias. Por tanto, es necesario habilitar:

a) Alta, baja y consulta de unidades.

b) Alta, baja y consulta de usuarios.

Cuando se acceda a la gestión de unidades y usuarios y usuarias, se mostrará la pantalla de la ilustración que aparece a continuación. En esta pantalla, se cargarán por defecto todas las unidades dadas de alta en BID, se permitirá seleccionar hacer bús-

quedas con filtros personalizados y seleccionar un registro para ver el detalle y gestionar los usuarios y usuarias que tenga asociados.

Ilustración 16. Visualización de unidades

Al hacer doble clic en cualquiera de los registros de la ilustración anterior, se mostrará el detalle de la unidad habilitando la gestión de las unidades y sus usuarios o usuarias.

a) Si el usuario o usuaria conectado hace clic sobre un registro que no pertenece a su unidad, no se cargará la pantalla de modificación.

b) Solo el usuario administrador/a sin unidad asociada podrá gestionar cualquier tipo de unidad y sus usuarios o usuarias asociados.

Además de las acciones anteriormente comentadas, los usuarios o usuarias con perfil de administrador global podrán dar de alta nuevas unidades y modificar los datos de la unidad ya dados de alta. Tendrán un enlace habilitado en cada dato asociado a la unidad que, si clica, se mostrará un *pop-up* que permita modificarlo.

Una vez se ha seleccionado la unidad a consultar, aparecerá el detalle y los usuarios o usuarias que están asociados a esa unidad junto con sus perfiles. Si tiene permisos de administrador de la unidad podrá modificar los datos de la unidad y gestionar los usuarios o usuarias de la misma forma que se realiza la gestión de unidades.

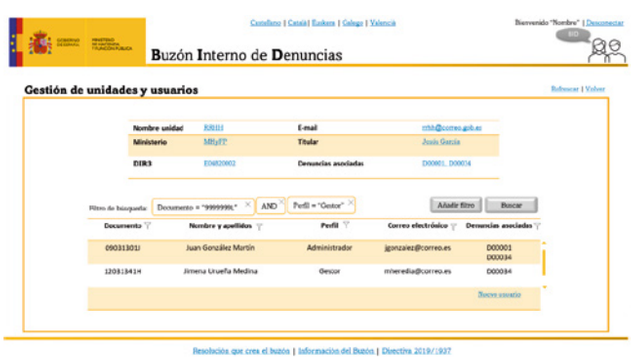

Ilustración 17. Consulta y Modificación de unidad y sus usuarios

El resto de los perfiles no tendrán la funcionalidad habilitada.

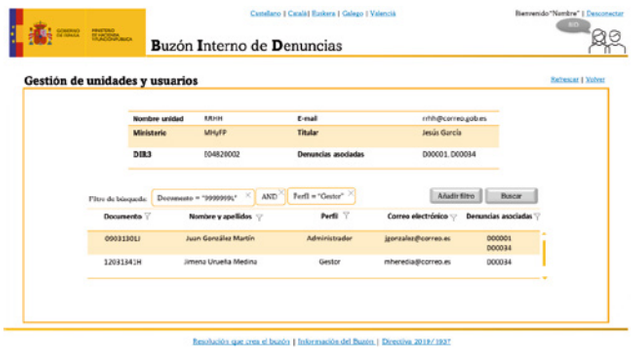

Ilustración 18. Consulta de unidad y sus usuarios

Gestión de flujos de trabajo

En la gestión de flujos de trabajo se podrá consultar, crear, modificar y eliminar flujos de trabajo existentes. Solo podrán acceder a este módulo los usuarios o usuarias con perfil de administrador/a y todos tendrán la misma funcionalidad habilitada.

Cuando se acceda al módulo de gestión de flujos de trabajo, se precargarán los flujos de trabajo existentes y permitirá la búsqueda mediante filtros personalizados para agilizar la gestión. Se podrá:

a) Acceder a un flujo de trabajo para su modificación, haciendo doble clic sobre la fila de la tabla que muestre el flujo de trabajo al que se quiere acceder.

b) Dar de alta un nuevo flujo de trabajo mediante un enlace. Se autogenerará el identificador del flujo de trabajo asociado a la denuncia.

c) Dar de baja un flujo pulsando en el enlace habilitado en la fila que se corresponda con la denuncia a eliminar. Si hay denuncias asociadas a ese flujo pendientes, no se permitirá la baja del flujo.

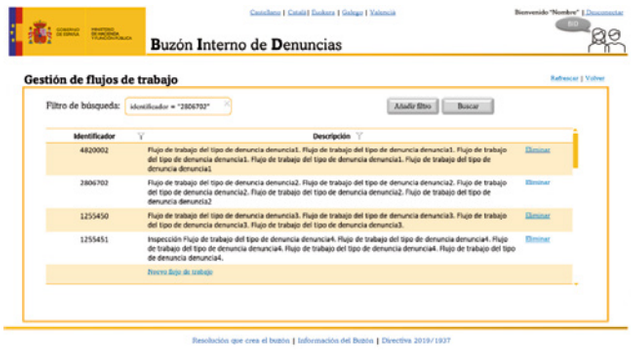

Ilustración 19. Gestión de flujos de trabajo

Cuando el administrador o administradora clica en el enlace habilitado para dar de alta un nuevo flujo de trabajo o lo intente modificar, se le precargarán el flujo definido en el requisito RF008 y una serie de menús con información relativa a:

a) Tiempo máximo de tramitación de la denuncia.

b) Tiempo máximo de permanencia en estados.

c) Tiempo de máximo de asignación a las unidades.

d) Unidades asignadas en estados no finales.

Se activarán solo los menús de las opciones que puedan ser asociadas a cada estado. Para seleccionar cada estado y ver las posibilidades de asignación de información, el usuario o usuaria tendrá que hacer clic sobre cada estado (cambiará el contorno a color rojo) y a la derecha le aparecerá un menú en forma de tabla que le permitirá dar valores a cada parámetro.

Estado	Tiempo máximo de tramitación de la denuncia	Tiempo máximo de permanencia en estado	Tiempo de máximo de asignación a las unidades	Asignación de unidades
Abierta	X	X	–	–
Revisión	–	X	X	X
Pendiente de información	–	X	–	–
Aceptada	–	X	–	X

Tabla 6. Parámetros asignables a estados

Todos los campos de la tabla podrán modificarse haciendo clic sobre la celda. En el caso de la gestión de unidades asignadas, se podrá pulsar en el enlace «Añadir más unidades» y buscar las unidades, entre las existentes en BID y dadas de alta previamente, y asociarlas al estado. También se podrán eliminar pulsando en el correspondiente enlace.

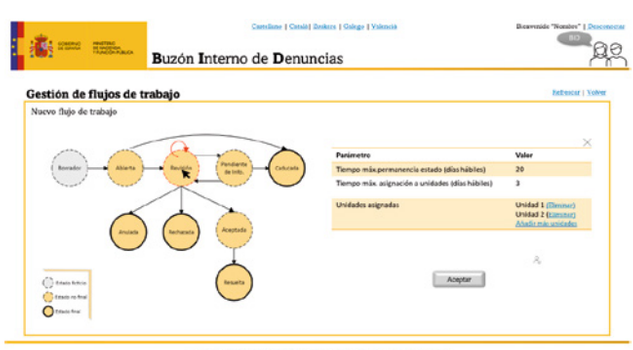

Ilustración 20. Flujo de trabajo: crear y modificar

Consulta de estadísticas

Los usuarios o usuarias con el perfil adecuado podrán consultar estadísticas y realizar extracciones de datos en formato hoja de cálculo para su manejo. Se crearán informes predefinidos y se habilitará la opción de realiza consultas personalizadas.

a) Para consultar un informa predefinido es necesario hacer clic en la tabla superior. Los resultados se presentarán en la tabla inferior.

b) Para generar consultas personalizadas hay que clicar en el botón de añadir filtros para incluir las opciones de búsqueda que se desean.

Ilustración 21. Consulta de estadísticas

Análisis técnico

Alternativas de solución en la arquitectura lógica

Para mostrar las diferentes alternativas de solución descritas en el apartado «Alternativas de Solución», se facilita los diagramas de contexto de las tres alternativas evaluadas que, se recuerda, son:

a) Desarrollo a medida.

b) Implementación en ACCEDA 2.0.

c) Desarrollo híbrido.

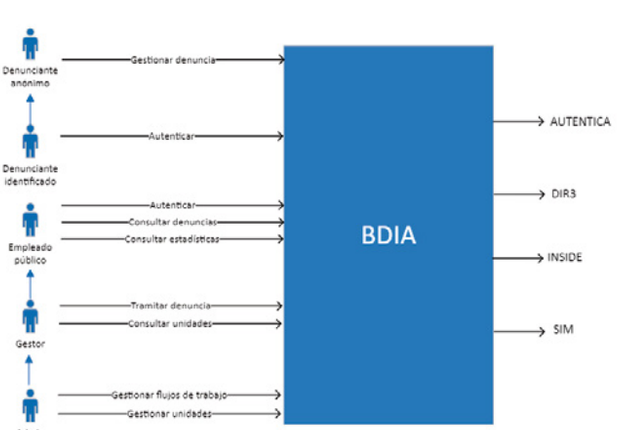

Ilustración 22. Diagrama de contexto para alternativa de desarrollo a medida

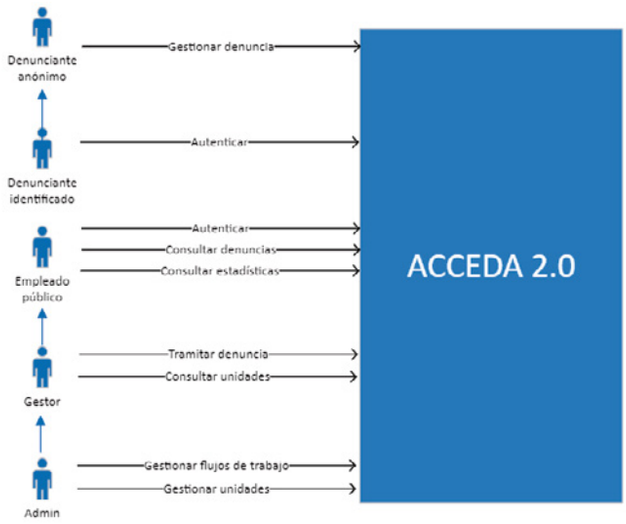

Ilustración 23. Diagrama de contexto para alternativa de implementación en Acceda 2.0

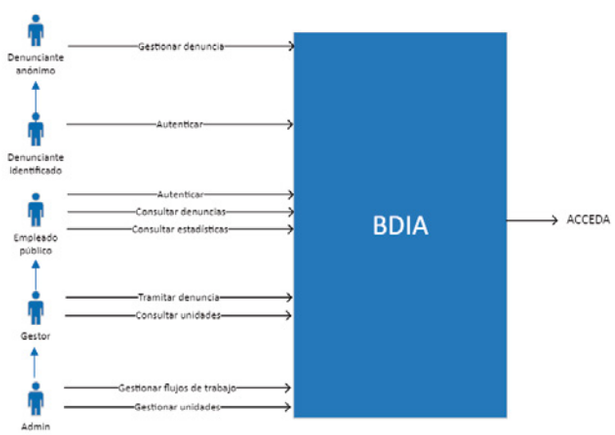

Ilustración 24. Diagrama de contexto para alternativa de desarrollo híbrido

Arquitectura lógica

Se seguirá la arquitectura de n-capas cerrada para diseñar y desarrollar la arquitectura que dará soporte al sistema de información que se ha de desarrollar.

Las capas son agrupaciones horizontales lógicas de componentes de *software* que forman la aplicación o el servicio. Nos ayudan a diferenciar entre los diferentes tipos de tareas a ser realizadas por los componentes, ofreciendo un diseño que maximiza la reutilización y, especialmente, la mantenibilidad. En definitiva, se trata de aplicar el principio de «Separación de Responsabilidades» dentro de una arquitectura. Cada capa lógica de primer nivel puede tener un número concreto de componentes agrupados en subcapas. Dichas subcapas realizan a su vez un tipo específico de tareas. Al identificar tipos genéricos de componentes que existen en la mayoría de las soluciones, podemos construir un patrón o mapa de una aplicación o servicio y usar dicho mapa como modelo de nuestro diseño. La división de una aplicación en capas

separadas que desempeñan diferentes roles y funcionalidades nos ayuda a mejorar el mantenimiento del código; nos permite también diferentes tipos de despliegue y, sobre todo, nos proporciona una claridad en la arquitectura.

La aproximación cerrada en la arquitectura de n-capas nos ayuda en la gestión de dependencias definiendo que los componentes de una capa pueden interactuar solo con componentes de la misma capa o bien con otros componentes de capas inferiores. Se elige ya que facilita el aislamiento de capas y la evolución independiente de cada capa sin afectar al resto de capas. En cada capa, tendremos componentes llamados módulos.

En resumen, el uso de capas nos proporciona los siguientes beneficios:

a) El mantenimiento de mejoras en una solución será mucho más fácil porque las funciones están localizadas. Además, las capas estarán débilmente acopladas entre ellas y con alta cohesión interna, lo cual posibilita variar de una forma sencilla diferentes implementaciones/combinaciones de capas.

b) Otras soluciones deberían poder reutilizar funcionalidad expuesta por las diferentes capas, especialmente si se han diseñado para ello.

c) Los desarrollos distribuidos son mucho más sencillos de implementar si el trabajo se ha distribuido previamente en diferentes capas lógicas.

d) La distribución de capas en diferentes niveles físicos puede mejorar la escalabilidad.

La arquitectura tiene un diseño clásico, especialmente común en aplicaciones web, que define las siguientes capas:

a) Capa de presentación o *frontend*: encargada de ofrecer las funcionalidades del sistema de información a los usuarios o usuarias de las aplicaciones web se comunica con la capa de lógica de negocio para obtener datos o ejecutar procesos de negocio expuestos. Nuestra arquitectura segmentará la capa de presentación en varias, una por cada módulo de funcionalidad de negocio. Está dividida en diferentes subcapas que conforman una aplicación RIA con la que interactúa directamente el usuario final del sistema.

b) Capa de lógica de negocio: encargada de proveer datos y ejecutar los procesos de negocios invocados por las diferentes aplicaciones web o sistemas externos. Para ello invoca a los sistemas de servicios remotos ubicados en la capa de acceso a datos y servicios. Nuestra arquitectura segmentará esta capa intermedia en varias, una por cada módulo de funcionalidad de negocio y seguirá un diseño guiado por dominio (DDD).

c) Capa de acceso a datos y servicios: la capa de acceso a datos sirve los datos a la capa intermedia y facilita el acceso tanto a las bases de datos de la infraestructura del proyecto como las de la infraestructura externa. Por otro lado, los servicios remotos serán invocados por la capa de intermedia para realizar los procesos o acciones que se requiera de ellos (autenticación, gestión documental, firma de documentos, etc.), y están ubicados en infraestructuras externas a proyecto.

d) Capa transversal: permite implementar el código transversal y mantenerlo abstraído de la lógica específica de la aplicación: el código transversal se refiere a código de aspectos horizontales, cosas como la seguridad, gestión de operaciones, *logging*, etc. La mezcla de este tipo de código con la implementación específica de la aplicación puede dar lugar a diseños que sean en el futuro muy difíciles de extender y mantener.

Principios de diseño

Cuando diseñamos un sistema es importante seguir un conjunto de principios de diseño fundamentales para ayudar a definir una arquitectura que minimice costes de mantenimiento y maximicen la usabilidad y la extensibilidad.

Seguiremos los siguientes principios de diseño:

a) Estructura Headless.

b) Patrón SOLID.

c) Desacoplamiento de componentes.

Estructura Headless

Con la aparición del paradigma de desarrollo de SPA en entornos de cliente (navegadores Web) las tendencias en el desarrollo de aplicaciones se han dirigido en gran medida a favor de este paradigma. Se debe principalmente a los beneficios que presenta el desarrollo de SPAs: mejoras en la experiencia de usuario, interfaces más ricas en funcionalidad, tiempos de carga entre páginas reducidos, etc.

Este paradigma conlleva la implementación de a la arquitectura Headless. La arquitectura Headless es un subconjunto de la arquitectura desacoplada y se diferencia en que no se define un sistema de *frontend* o entorno de presentación proporcionándose una interfaz de comunicación API REST preparada para ser consumida por cualquier cliente o cualquier otro sistema dejando libertad a la hora de presentar o de hacer uso del resultado de la comunicación. La naturaleza del proyecto exige este desacoplamiento entre sistemas *frontend* y *backend*, y así ofrecer a los usuarios de todas las ventajas de este tipo arquitecturas. A nivel general, nos aportará los siguientes beneficios:

a) Independencia y desacoplamiento entre sistemas.

b) Mejora del rendimiento de los sistemas, resiliencia a fallos y escalabilidad bajo demanda.

c) Reutilización de lógica de negocio.

d) Facilidad de integración entre sistemas.

e) Mejora en la experiencia de usuario.

f) Entrega rápida de contenido.

g) Integraciones de terceros sencillas y seguras.

h) Se integra con nuevas tecnologías fácilmente.

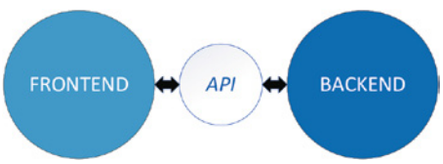

Ilustración 25. Estructura Headless

Por tanto, en la parte del *frontend*, se crearán módulos de negocio diferenciados que actuarán como aplicaciones independientes, que permitirá desacoplar los procesos de desarrollo, despliegue, escalado y mantenimiento de los aplicativos. Por cada nueva funcionalidad global independiente se creará un módulo que actuará como aplicación independiente.

La parte *backend* será diseñada bajo una estrategia de APIficación y también estará compuesta por módulos. Estos módulos expondrán una API que dará acceso a los datos y funcionalidad correspondiente a la entidad y procesos de negocio a los que representa. Estas APIs estarán expuestas mediante una capa de servicios RESTFul (cumpliendo la RFC 3986), idónea para que los componentes *frontend* puedan integrarse con ella.

Patrón SOLID

El patrón SOLID está definido por la siguiente serie de principios:

a) Principio de Única Responsabilidad: una clase debe tener una única responsabilidad o característica. Es decir, una clase debe de tener una única razón para justificar realizar cambios sobre su código fuente. Una consecuencia de este principio es que, de forma general, las clases deberían tener pocas dependencias con otras clases/tipos.

b) Principio Abierto-Cerrado: una clase debe estar abierta para la extensión y cerrada para la modificación. Es decir, el comportamiento de una clase debe poder ser extendido sin necesidad de realizar modificaciones sobre el código de esta.

c) Principio de Sustitución de Liskov: los subtipos deben poder ser sustituibles por sus tipos base (interfaz o clase base). Este hecho se deriva de que el comportamiento de un programa que trabaja con abstracciones (interfaces o clases base) no debe cambiar porque se sustituya una implementación concreta por otra. Los programas deben hacer referencia a las abstracciones, y no a las implementaciones.

d) Principio de Segregación de Interfaces: los implementadores de Interfaces de clases no deben estar obligados a implementar métodos que no se usan. Es decir, los interfaces de clases deben ser específicos dependiendo de quién los consume y, por lo tanto, tienen que estar granularizados/segregados en diferentes interfaces, no debiendo crear nunca grandes interfaces. Las clases deben exponer interfaces separados para diferentes clientes/consumidores que difieren en los requerimientos de interfaces.

e) Principio de Inversión de Dependencias: Las abstracciones no deben depender de los detalles si no que los detalles deben depender de las abstracciones. Las dependencias directas entre clases deben ser reemplazadas por abstracciones (interfaces) para permitir diseños *top-down* sin requerir primero el diseño de los niveles inferiores. Este principio será explicado en el apartado dedicado al desacoplamiento de componentes, ya que es en lo que se basa.

Desacoplamiento entre componentes

Es fundamental destacar que no solo se deben delimitar los componentes de una aplicación entre diferentes capas. Por ello, la arquitectura tiene en cuenta la manera en cómo interaccionan unos componentes con otros, es decir, cómo se consumen y en especial cómo se instancian unas clases desde otras. En general, este desacoplamiento se da entre todos los componentes pertenecientes a las diferentes capas, ya que es inherente la comunicación entre estas en una arquitectura de n-capas donde cada capa invoca a la capa inferior.

En definitiva, la arquitectura está diseñada para que las capas se relacionen de manera desacoplada a nivel de código, evitando la instanciación de clases directamente en sus clases. Este desacoplamiento también se implementa entre componentes que pertenecen a una misma capa, ya que este desacoplamiento no es sólo deseable en las interacciones de las diferentes capas sino entre los propios componentes de las capas. Favorece que las piezas implementadas pueden ser sustituidas o ampliadas con un impacto mucho menor en la arquitectura en cuanto a cambios se refiere.

La técnica aplicada para lograr este desacoplamiento es el PID especificado por el patrón SOLID anteriormente mencionado. El propósito es disponer de capas de alto nivel que sean independientes de la implementación y detalles concretos de las capas de más bajo nivel, y por lo tanto también independientes de las tecnologías subyacentes. Como hemos mencionado anteriormente, el PID establece que las capas de alto nivel no deben depender de las capas de bajo nivel, sino que las capas de alto nivel deben depender de abstracciones (interfaces) y las de nivel inferior deben cumplir con los contratos definidos por dichas interfaces (implementación).

El objetivo del PID es desacoplar los componentes de alto nivel de los componentes de bajo nivel, de forma que sea posible llegar a reutilizar los mismos componentes de alto nivel con diferentes implementaciones de componentes de bajo nivel. Por ejemplo, poder reutilizar el mismo componente de capa de negocio con diferentes componentes de capas de infraestructura que implementen diferentes tecnologías (por ejemplo, sustituir un componente de base de datos MySQL por uno de Postgres), siempre que los sustitutos cumplan con los mismos interfaces de los que depende el componente de la capa de negocio (Principio de Sustitución de Liskov y de Segregación de Interfaces).

Utilizaremos interfaces definiendo un contrato sobre el comportamiento requerido a los componentes de bajo nivel por los componentes de alto nivel. Exigiendo a los componentes de bajo nivel que implementen los interfaces a cumplir en capas de alto nivel, se invierte la tradicional relación de dependencia y se obtiene la Inversión de Dependencias. Para conseguir esta inversión de dependencias, la arquitectura implementa un sistema de inyección de dependencias en las factorías de componentes, de tal manera que a la hora de instanciar los componentes se especificarán cuáles son los

componentes de los que dependen, procediendo la factoría a instanciarlos e inyectarlos en el componente.

Implementación de capas *software*

En este apartado se detallará cada una de las capas de la arquitectura mencionadas anteriormente, se hará una descripción general y en detalle de la tecnología que se utilizará para implementar las capas *software*.

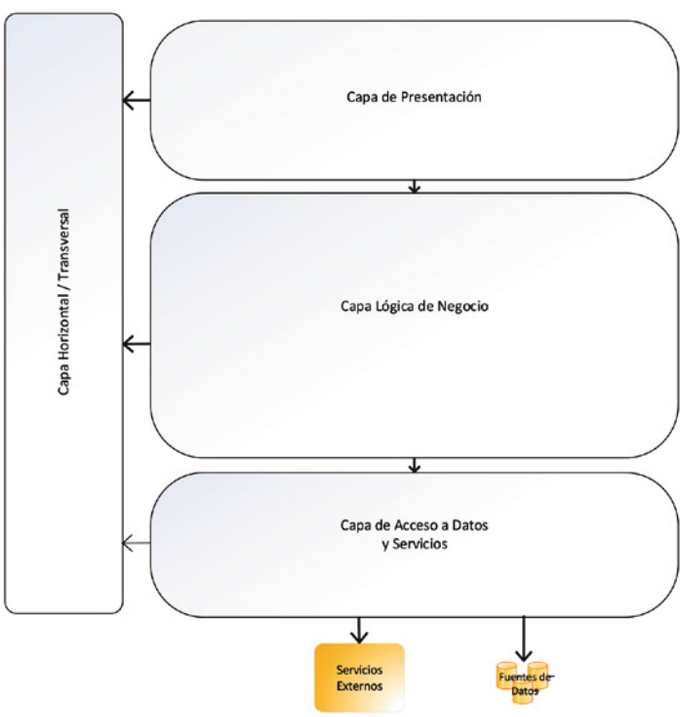

Ilustración 26. Arquitectura n-capas orientada al dominio

Capa de presentación

Esta capa es la responsable de generar la interfaz de usuario o usuaria cuyo objetivo primordial es mostrarle información y reaccionar a sus acciones. Los componentes de las capas de presentación implementan por lo tanto la funcionalidad requerida para que interactúen con la aplicación y lleven a cabo los flujos de trabajo que le provee el sistema de información.

La funcionalidad principal de la capa de presentación es gestionar la interfaz de usuario o usuaria, y comunicar con la capa intermedia de lógica de negocio, siguiendo el modelo jerárquico de la arquitectura de n-capas, y así garantizar el bajo acoplamiento y cohesión entre la capa de presentación y la de lógica de negocio.

A su vez, la capa de presentación está subdividida en capas de segundo nivel, organizadas según la naturaleza de la responsabilidad que ejerce dentro de la capa de presentación. Cada subcapa a su vez estará formada por componentes que tienen una única responsabilidad dentro la subcapa a la que pertenecen.

Capa de lógica de negocio orientada al dominio

a) Capa de servicios. La arquitectura sirve de base para que la aplicación actúe como proveedor de servicios para otras aplicaciones remotas y facilitará servicios a la capa de presentación, por lo que publicaremos la lógica de negocio (capas de negocio internas) mediante una capa de servicios. Esta capa de servicios proporciona un medio de acceso remoto basado en canales de comunicación y mensajes de datos. Es importante destacar que esta capa debe ser lo más ligera posible y que no debe incluir nunca lógica de negocio.

b) Capa de aplicación. La capa de aplicación realiza tareas de coordinación de aspectos de la aplicación, pero que no tienen que ver con la lógica de negocio. Estas tareas de coordinación del trabajo permiten dar soporte a la lógica de negocio como, por ejemplo, la coordinación de transacciones o ejecución de unidades de trabajo; es una capa que puede asemejarse a la «fachada del negocio» ya que hace de fachada del modelo de dominio.

   Además de ejercer de fachada realiza las siguientes funciones:

   – Coordinación de la mayoría de las llamadas a objetos de la capa de persistencia y acceso a datos.

   – Acciones que consolidan o agrupan operaciones del dominio dependiendo de las acciones mostradas en la interfaz de usuario, relacionando dichas acciones con las operaciones de persistencia y acceso a datos.

   – Mantenimiento de estados relativos a la aplicación.

   – Coordinación de acciones entre el dominio y aspectos de infraestructura.

   Es importante mencionar las partes en las que se divide la capa de lógica:

   – Adaptadores DTO. Son agrupaciones de datos de diferentes entidades para ser enviadas de una forma más eficiente, minimizando las llamadas remotas, por la capa superior de servicios web. Envía objetos llamadas DTOs y el código en la capa de aplicación son DTO-Adapters.

   La diferencia entre un objeto de transferencia de datos y un objeto de negocio o un objeto de acceso a datos es que un DTO no tiene más funcionalidad que almacenar y entregar sus propios datos. No tienen identidad ninguna, solo nos interesan sus atributos, ya que complementan la descripción del dominio, pero no se identifican por sí mismos.

   – Servicios de aplicación. Los servicios de aplicación coordinan el trabajo de otros servicios de capas inferiores como pueden ser servicios de la capa de dominio o repositorios de la capa de acceso a datos para conseguir el comportamiento deseado para el negocio. Son servicios cuyo tiempo de vida es equivalente al tiempo que tarda en procesarse el comportamiento de negocio deseado.

– Workflows. Permite definir procesos de negocio que necesitan ejecutar una serie de pasos en función de unas reglas concretas dependiendo de eventos que se puedan producir en el sistema y, normalmente, con un tiempo de ejecución largo.

c) Capa de dominio. La capa de dominio será la responsable de representar conceptos de negocio, información sobre la situación de los procesos de negocio e implementación de las reglas del dominio. También debe contener los estados que reflejan la situación de los procesos de negocio, y siguiendo los patrones de arquitecturas n-capas con orientación al dominio, tiene que ignorar completamente los detalles de persistencia de datos, ya que las tareas de persistencia deben ser realizadas por las capas de infraestructura y coordinadas por la capa de aplicación.

Se definen los siguientes elementos dentro de la capa de dominio:

– Entidades del dominio: las entidades son clases que representan las entidades de negocio. Son entidades desconectadas (datos y lógica) utilizadas para guardar y transferir datos de entidades entre las diferentes capas. Una característica fundamental en DDD es que también contienen la lógica del dominio relativo a cada entidad.

– Las entidades de datos que la aplicación utiliza internamente son en cambio objetos en memoria con datos y cierta lógica relacionada. Además, estas clases entidad serán también objetos POCO, es decir, clases independientes de tecnologías concretas de acceso a datos, con código que está completamente bajo el control del desarrollador; consiguiendo que las clases del dominio «no sepan nada» de las interioridades de los repositorios ni de las tecnologías de acceso a datos. Cuando se trabaja en las capas del dominio, se debe ignorar cómo están implementados los repositorios. Las clases entidad se sitúan dentro del dominio, puesto que son entes del dominio e independientes de cualquier tecnología de infraestructura (persistencia de datos, ORMs, etc.). En cualquier caso, las entidades serán objetos flotantes a lo largo de toda o casi toda la arquitectura.

– Especificaciones del dominio: forma abierta y extensible de definir criterios de consulta. Son definidas desde la Capa de Dominio, pero aplicadas en los repositorios de la capa de Infraestructura de acceso a datos.

– Servicios del dominio: en las capas del dominio, los servicios son clases agrupadoras de comportamientos y/o métodos con ejecución de lógica de este, coordinando e iniciando operaciones contra las entidades del dominio. La base de los servicios en DDD son todos aquellos comportamientos que debemos tener en nuestra aplicación y que no pertenezcan a ninguna entidad, es decir, son operaciones, funciones, métodos, no «cosas». No tienen estado, y modifican una o varias entidades de dominio, pero que no son propias de la entidad.

– Contratos de repositorios: a pesar de que la implementación del repositorio no está en la capa de dominio ya que los repositorios están ligados a una tecnología de persistencia de datos, la interfaz del repositorio sí forma parte de la capa de dominio. Lógicamente, para poder cumplir este punto,

las «Entidades del Dominio» y los «Value-Objects» serán POCO, es decir, serán totalmente independientes a la tecnología de acceso a datos. En definitiva, con este diseño se busca que las clases del dominio «no sepan nada directamente» de los repositorios.

d) Capa de infraestructura de persistencia de datos y servicios remotos. Esta capa proporciona la capacidad de persistir datos, así como acceder a ellos. Pueden ser datos propios del sistema o acceso a datos expuestos por sistemas. Así pues, esta capa de persistencia de datos expone el acceso a datos a las capas superiores, normalmente las capas del dominio. Esta exposición se realizará de una forma desacoplada.

Uso de servicios compartidos

A continuación, se describen los servicios compartidos de los que hará uso BID. Es necesario recordar que se está desarrollando la alternativa de solución en la que se implementa un sistema a medida. Las otras dos opciones ya comentadas (reutilización de Acceda 2.0 y la opción híbrida) harían uso de servicios compartidos también, pero de manera menos intensa ya que son soluciones que tienen integrados ya el uso de servicios compartidos por definición.

a) DIR3. Cada vez que se quiera dar de alta, consultar o modificar una unidad que intervenga en una denuncia se consultará el directorio común de unidades orgánicas y oficinas. No se almacenará nunca esta información en la base de datos que de soporte a la aplicación ya que DIR3 es el maestro. Si se almacenara sería necesario realizar un mantenimiento.

   Con el objetivo de mejorar el rendimiento, la consulta a DIR3 se realizará una vez al día, y una vez hecha, se almacenará en la aplicación. La integración se realizará mediante el protocolo SOAP mediante el servicio Web SD01UN_DescargaUnidades expuesto por DIR3.

b) AUTENTICA. La integración se realizará vía SSO y permitirá identificarse y autenticarse a:

   – Empleadas y empleados públicos que quieran realizar una denuncia interna identificándose.

   – Miembros de las unidades que gestionan las denuncias para poder tramitarlas.

c) INSIDE. Como herramienta de gestión documental se utilizará INSIDE, delegando en este servicio compartido la gestión de la documentación que aporte la persona denunciante. INSIDE es un sistema para la gestión de documentos electrónicos que cumple los requisitos para que ambos puedan almacenarse y/o obtenerse según el ENI, esquema que establece las normas básicas para el intercambio y almacenamiento de documentos electrónicos.

d) SIM. Se utilizará la plataforma de mensajería SIM para el envío de comunicaciones a las unidades que participan en la gestión de la denuncia y a las personas denunciantes que notifiquen su dirección de correo para seguir la evolución de su denuncia.

Diagrama entidad-relación

En este apartado se muestra el diagrama de entidad-relación que es la representación y definición de todos los datos que se introducen, almacenan, transforman y producen dentro de un sistema de información, sin tener en cuenta las necesidades de la tecnología existente, ni otras restricciones.

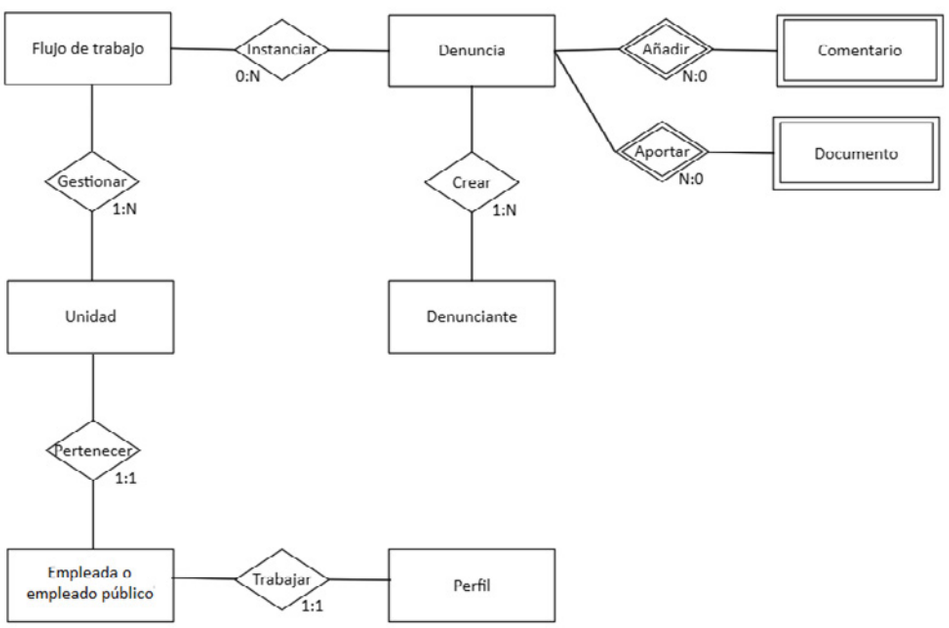

Ilustración 27. Diagrama de E/R