Universitat Oberta de Catalunya

uoc.edu

Diseño e implementación de la base de datos para una aplicación de control de procesos de seguridad informática

Mirtha Soto Romano
Grado de Ingeniería Informática
Bases de Datos

Jordi Ferrer Duran
Xavier Baró Soler

Junio 2022

Esta obra está sujeta a una licencia de
Reconocimiento-NoComercial-SinObraDerivada
3.0 España de Creative Commons

FICHA DEL TRABAJO FINAL

Título del trabajo:	*Diseño e implementación de la base de datos para una aplicación de control de procesos de seguridad informática*
Nombre del autor:	*Mirtha Soto Romano*
Nombre del consultor/a:	*Jordi Ferrer Duran*
Nombre del PRA:	*Xavier Baró Soler*
Fecha de entrega (mm/aaaa):	*06/2022*
Titulación:	*Grado de Ingeniería Informática*
Área del Trabajo Final:	*Bases de Datos*
Idioma del trabajo:	*Castellano*
Palabras clave	*Seguridad informática, Procesos empresa, Políticas seguridad, Bases de Datos*

Resumen del Trabajo (máximo 250 palabras): *Con la finalidad, contexto de aplicación, metodología, resultados i conclusiones del trabajo.*

En la presente memoria de final de grado se expone todo el proceso llevado a cabo para el diseño e implementación de una base de datos relacional, con el objetivo de gestionar los procesos de seguridad informática de una empresa del sector Automovilístico.

Desde esta aplicación se almacenarán todos los procesos de gestión realizados desde la empresa, así como las vulnerabilidades informáticas encontradas en los mismos, y las acciones de saneamiento o mitigación que se proponen para corregirlas.

De igual manera, desde esta aplicación se deberán poder gestionar todas las políticas de seguridad implantadas por la empresa, además de cualquier incumplimiento a estas políticas llevado a cabo por cualquier de los empleados y departamentos de la empresa.

Finalmente, se requiere la creación de un repositorio estadístico, desde donde se podrán realizar consultas de distintos indicadores clave respecto a la información almacenada en la base de datos

Para la ejecución del proyecto de base de datos, se ha decidido seguir paso a paso el método visto en la asignatura "Diseño de Bases de Datos", el cual consta de 5 fases, en este mismo orden de ejecución: Recogida y análisis de requisitos, Diseño conceptual, Diseño lógico, Diseño físico, Implementación y optimización.

Adjunto a este documento, se entregan una serie de anexos con los scripts necesarios para la creación del proyecto de base de datos, carga de datos y realización de pruebas, junto con una presentación en video de los contenidos más relevantes.

Abstract (in English, 250 words or less):

In this end-of-grade report, is showcased the entire process carried out for the design and implementation of a relational database, with the aim of managing the IT security processes of a company in the Automotive sector.

All the management processes carried out by the company shall be stored in this application, as well as the IT vulnerabilities found in them, with it's corresponding mitigation actions proposed to correct them.

Similarly, from this application it should be possible to manage all the security policies implemented by the company, in addition to any breach of these policies carried out by any of the company's employees and departments.

Finally, it is required the creation of a statistical repository, where different key indicators can be consulted regarding the information stored in the database.

For the execution of this database project, it has been decided to follow through the methodology learned in the subject "Diseño de Bases de Datos", which consisted of 5 phases, in this same order of execution: Collection and analysis of requirements , Conceptual design, Logical design, Physical design, Implementation and optimization.

Attached to this document, a series of annexes are delivered with the necessary scripts for the creation of the database project, data loading and testing, along with a video presentation of the most relevant contents.

Índice

1. Introducción

1.1 Contexto y justificación del Trabajo

Los ataques cibernéticos se han convertido en una de las principales amenazas que aquejan a particulares y empresas por igual en este siglo 20.

Debido en parte a la creciente ola de digitalización provocada por la pandemia del Covid 19, la cantidad de ciberataques se ha elevado de forma acelerada. Se estima que solo en España "se han dado de media unos 40.000 ciberataques cada día durante 2021, lo que supone un incremento del 125 por ciento respecto al año anterior".[11]

Este tipo de ataques no solo supone un problema operativo para las empresas, pero también un coste económico importante, ya que el modus operandi en la mayoría de los casos es el de secuestrar o encriptar los datos para luego solicitar un rescate. Se calcula que uno de los principales *ransomware,* **REvil**, ya ha podido embolsarse más de 10 millones de dólares en rescates[12]. Esto convierte a los ciberataques en una de las actividades delictivas más lucrativas, pero también con menor riesgo de ser rastreadas y detenidas.

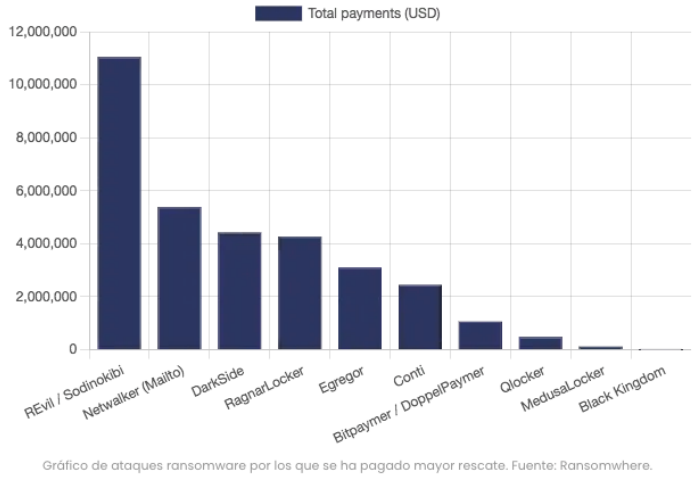


Gráfico de ataques ransomware por los que se ha pagado mayor rescate. Fuente: Ransomwhere.

Fuente Imagen: https://www.criptonoticias.com/seguridad-bitcoin/perdidas-ransomware-2021-superan-60mil-bitcoins/

Es por ello que la ciberseguridad cobra cada vez más importancia en las empresas. Muchas de ellas ya entienden que no tener una buena estrategia de ciberseguridad es como operar sin un seguro ante los riesgos. Los daños pueden ser nefastos si no se toman las medidas preventivas necesarias.

De aquí la razón de ser de este proyecto: Diseñar e implementar el sistema de Base de Datos para una aplicación destinada a controlar los procesos de ciberseguridad para una empresa del sector automovilístico.

En el presente proyecto presentamos todas las fases llevadas a cabo para la implementación de esta base de datos: empezando por la planificación de las tareas necesarias, así como de los recursos requeridos para ejecutar el proyecto. Siguiendo con la extracción y definición de los requisitos, para luego dar inicio al diseño e implementación de la base de datos, la cual se lleva a cabo en distintas fases, siguiendo el proceso de diseño estudiado en la asignatura "Diseño de Base de Datos".
El proceso finaliza con la carga de datos y realización de pruebas, donde se verifica el cumplimiento de las especificaciones y requerimientos esperados del sistema.

1.2 Objetivos del Trabajo

Desde una perspectiva más general, el principal objetivo de este trabajo y de la asignatura como tal, es poner en práctica algunas de las habilidades aprendidas a lo largo del grado de Ingeniería informática, enfocándolas en un caso práctico ya definido en el enunciado.

Entre las habilidades que se ponen en práctica en este proyecto, son:

- **Gestión de proyectos:** Definición del alcance, los recursos y la planificación necesaria para conseguir implementar un proyecto de base de datos.
- **Ingeniería de requisitos:** Análisis y definición de los requisitos y restricciones del sistema a desarrollar. Definición de los requisitos y especificaciones que servirán de guía para el diseño de la solución.
- **Diseño de Base de Datos:** Esencial para poder desarrollar este proyecto en particular, ya que se debe llevar a cabo el proceso al completo: desde el diseño a la implementación de una base de datos.
- **Ingeniería de Software**: De utilidad para la gestión global de un proyecto de desarrollo de software. Unifica la gestión de los requisitos con el diseño y modelado de la información.

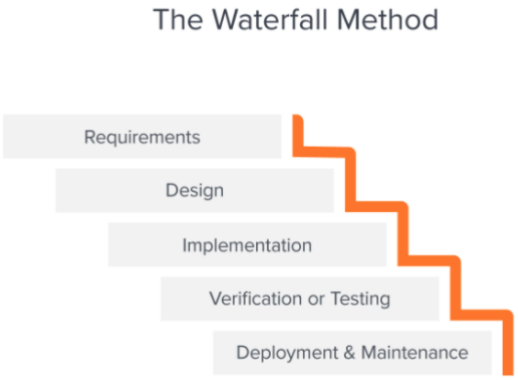
Desde una perspectiva más específica, y enfocándonos en lo que se espera del proyecto según el enunciado, podemos establecer como objetivo fundamental:

- Implementar el sistema de base de datos para una aplicación encargada de gestionar todos los procesos de seguridad informática de una empresa automovilística. Dichos procesos deberán ser almacenados con el fin de proporcionar información sobre la situación actual e histórica correspondiente a la seguridad informática en la empresa, las distintas vulnerabilidades que se van encontrando, así como los mecanismos de mitigación puestos en marcha, y las actividades de formación y simulación realizadas para concienciar al personal de la empresa sobre buenas prácticas en materia de ciberseguridad.

1.3 Enfoque y método seguido

Para este proyecto, dadas las necesidades tan especificas expuestas en el enunciado, y que es la expectativa y principal aspecto a evaluar, se opta por la opción de **diseñar y desarrollar un sistema de base de datos totalmente nuevo**, que dé respuesta a las necesidades del negocio.

Para la gestión del proyecto, se utilizará una metodología *Waterfall* o "En cascada", dado que el alcance del proyecto y los hitos están claramente definidos y no se espera que se añadan o modifiquen los requerimientos.



Fuente imagen: https://www.workfront.com/project-management/methodologies/waterfall

Otra razón importante para elegir esta estrategia es que, como parte de los hitos entregables, se debe proporcionar una planificación detallada de trabajo con las distintas tareas a realizar, cosa que es más sencilla de hacer en una metodología en cascada.

Por último, es imprescindible mantener un control exhaustivo de dicha planificación, ya que tanto las fechas de entrega de las distintas prácticas como la de entrega del trabajo final, son estrictas e inamovibles.

Se ha creado un diagrama de Gantt para visualizar la planificación general de todas las actividades del proyecto. Sin embargo, para simplificar la gestión diaria del trabajo, se tomará prestada una técnica común de la metodología *Kanban* con el uso de un tablero donde se podrán visualizar todas las tareas "Pendientes", "En progreso" y "Finalizadas" (ver sección *1.4.7 Seguimiento de tareas*).

1.4 Planificación del Trabajo

1.4.1 Descripción de los Recursos

Herramientas de Hardware

- Portátil Macbook pro - Uso Personal
- Portátil Windows Dell - Uso Profesional → Se utilizará como *backup* **solo** en caso de emergencia, ya que se trata del ordenador de empresa.
- Monitor externo Samsung de 27" - Uso Personal

Herramientas de Software

- Oracle Database Express Edition, 11g R2: Software SGBD (Sistema Gestor Base de Datos)
- Oracle SQL Developer: IDE para el manejo del SGBD

- Draw.io : Herramienta de modelado UML
- Gantter: Herramienta en línea para la gestión de proyectos
- Trello: Herramienta en línea para la gestión de proyectos
- Microsoft Office: Paquete de herramientas para la productividad de Microsoft.
- *Otras herramientas pendientes de definir*

Recursos Humanos

Se cuenta con un único recurso para la realización de todo el proyecto. Dicho recurso, dado su perfil multidisciplinar, efectuará los distintos roles requeridos para la correcta ejecución del proyecto:

- Gestor de Proyectos
- Analista de Requisitos
- Desarrollador y gestor de Bases de Datos

1.4.2 Planificación personal y gestión del tiempo

El único recurso del que se dispone, debe compaginar la realización de este proyecto con su trabajo a jornada completa (40 horas por semana), así como con la realización de **una segunda asignatura** en la UOC.

Así mismo, se debe reservar tiempo para visitas médicas de rutina y vida personal y familiar.

Por ello, se debe realizar una planificación semanal sumamente precisa para garantizar la consecución de todas las tareas. Es por ello que se realizará la siguiente planificación **semanal**, dedicada exclusivamente para el trabajo en el TFG de la UOC:

Día Semana	Horario Mañana	Horario Tarde/Noche	Total
Lunes	6:30 a 8:30	19:00 a 21:00	4 horas
Martes	-	-	
Miércoles	6:30 a 8:30	19:00 a 21:00	4 horas
Jueves	-	-	
Viernes	-	17:00 a 21:00	4 horas
Sábado	-	-	
Domingo	8:00 a 12:00	-	4 horas
		Horas Semanales	**16 horas**

La planificación anterior se adecua de manera realista a los horarios y necesidades del recurso.

Como plan de contingencia, se cuenta con una serie de días de vacaciones laborales que se podrán destinar para cubrir horas extra, en caso de que existan retrasos y se precise de más tiempo para finalizar las tareas planificadas (ver sección “Análisis de Riesgos).

1.4.3 Planificación de Hitos por entregas y tiempo disponible:

Se ha decidido dividir el proyecto en 5 hitos diferenciados, teniendo en cuenta las distintas prácticas de evaluación continua, definidas en el enunciado y sus fechas límite de entrega:

- 07/03/2022: entrega PEC 1 - plan de trabajo
- 11/04/2022: entrega PEC 2 - estado del trabajo hasta esa fecha, alineado con el plan de trabajo entregado y consensuado con el consultor
- 12/05/2022: entrega PEC 3 - estado del trabajo hasta esa fecha, alineado con el plan de trabajo entregado y consensuado con el consultor
- 10/06/2022: entrega final - memoria + producto + presentación + auto-informe de evaluación
- Del 13/06/2022 al 17/06/2022: debate virtual

Teniendo en cuenta estas entregas, así como la planificación personal indicada en el apartado anterior, obtenemos la siguiente planificación por hitos (alto nivel):

Hito	Fecha inicio	Fecha Fin	Disponible en días/semanas	Disponible en horas
PEC 1: Planificación	17/02/2022	07/03/2022	2 semanas 4 días	40 horas
PEC 2: Diseño	08/03/2022	11/04/2022	4 semanas 6 días	76 horas
PEC 3: Implementación	12/04/2022	12/05/2022	4 semanas 2 días	68 horas
PEC 4: Entrega Final	13/05/2022	10/06/2022	3 semanas 6 días	60 horas
Debate Virtual	13/06/2022	17/06/2022	5 días	12 horas

1.4.4 Descripción de Hitos incluyendo tareas a realizar

Dentro de los distintos hitos, situamos las tareas necesarias para llevar a cabo el proyecto. Tal como pudimos aprender en la asignatura de “Diseño de Bases de Datos”, a lo largo de este tipo de proyectos deben llevarse a cabo las siguientes fases:

- **Recogida y análisis de requisitos:** En esta etapa se obtienen los requisitos esperados, así como las restricciones de datos con las que debe contar el sistema a desarrollar. Esta información debe ser refinada, analizada y convertida en los requisitos formales que debe cumplir sistema.
  Dadas las circunstancias de este proyecto, los requisitos se extraerán exclusivamente del documento “Enunciado TFG BD”.

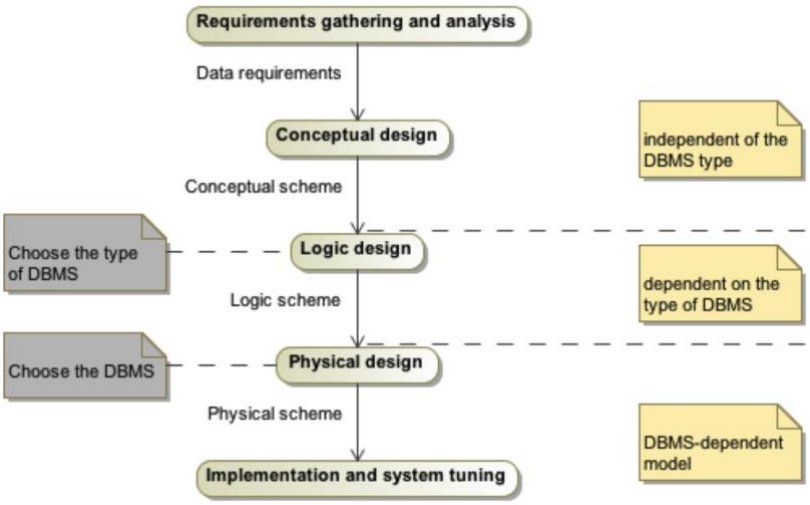
- **Diseño conceptual:** En esta etapa se diseña un esquema conceptual de alto nivel que refleja el sistema a desarrollar. Se crean las distintas entidades, sus atributos y la relación entre ellas. Se trata de sintetizar y proyectar de manera visual todos los datos del sistema, así como los requisitos recopilados en la etapa anterior.

- **Diseño lógico:** En esta etapa se profundiza en el diseño de la solución: se transforma el esquema conceptual en un modelo lógico de datos. Para ello, lo primero que se debe hacer es decidir el tipo de base de datos que se va a utilizar (relacional/no relacional), y a partir de aquí, realizar las tareas necesarias para estructurar la información del modelo conceptual al tipo de base de datos elegido.

  Por ejemplo, en el caso elegir una base de datos de tipo **Relacional**, en esta etapa es cuando se deben formalizar las relaciones entre las entidades, los atributos que serán claves primarias y foráneas, la normalización de los datos utilizando la teoría de conjuntos, entre otros.

  Diseño físico: Esta etapa se trata de adaptar el diseño lógico obtenido en la fase anterior a un diseño físico, utilizando un Sistema Gestor de Base de Datos (SGBD). Para ello, es imprescindible como primer paso haber elegido el SGBD que se utilizara para la implementación del proyecto. Algunos aspectos que deben tenerse en cuenta para esta elección son el rendimiento, el volumen de las transacciones, el almacenamiento, los tiempos de respuesta, entre otros.

- **Implementación y optimización:** Se trata de la última etapa del proceso de DBD. Es aquí donde se realiza la carga de datos y se comienza a optimizar el funcionamiento y rendimiento de la base de datos a través de la implementación de las consultas y procesos, la creación de roles y grupos de usuarios y la realización de pruebas para garantizar que se cumplen las especificaciones y requisitos esperados. En esta etapa también se gestionan aspectos como la seguridad, a través de la asignación de privilegios a los distintos usuarios.



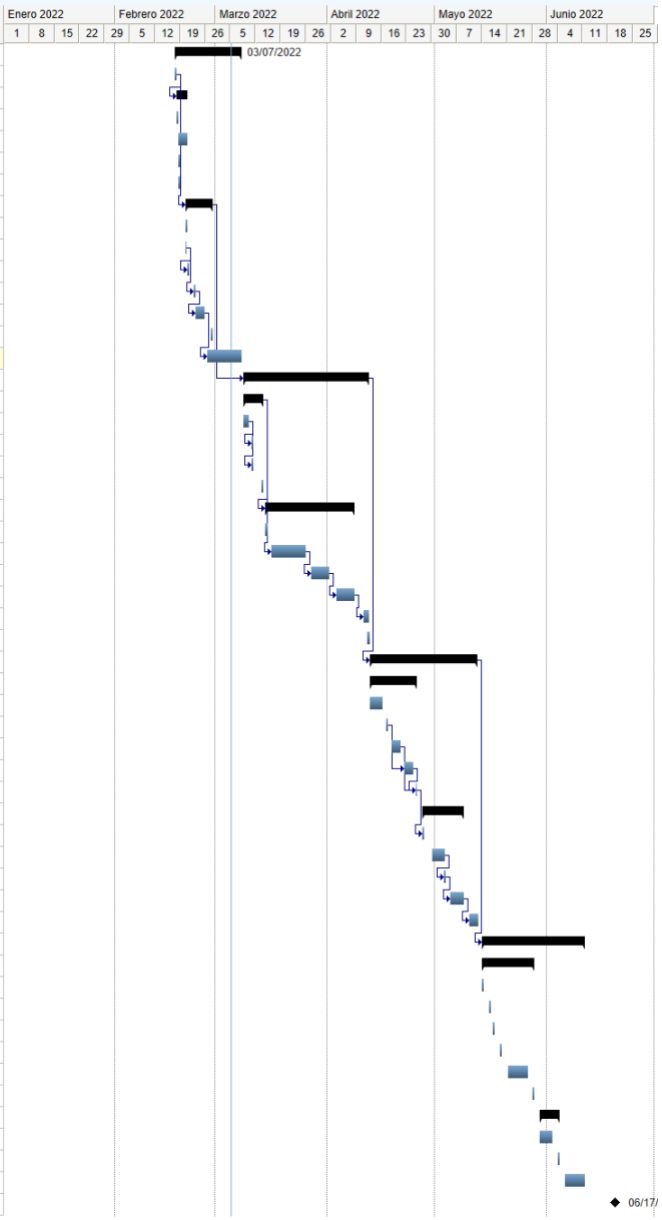
1.4.5 Cronograma Temporal – Diagrama Gantt

A continuación se muestra la planificación al completo, incluyendo todas las tareas requeridas para la ejecución del proyecto, sus fechas de inicio-fin, y la duración estimada en horas (teniendo en cuenta la dedicación semanal del recurso para el TFG):

gantter™

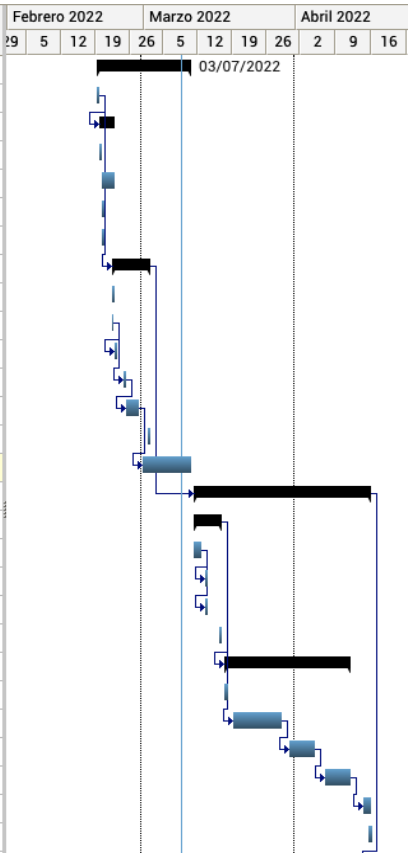
Project Name **Proyecto Base de Datos - TFG**

	Nombre	Duración	Inicio	Fin	Horas
1	**PEC 1 - Planificación**	**18.38días**	**02/17/2022**	**03/07/2022**	**28.5**
2	Lectura Enunciado	0.38día	02/17/2022	02/17/2022	3
3	**Secciones Iniciales Trabajo**	**3días**	**02/17/2022**	**02/20/2022**	**5.5**
4	Definir Contexto Trabajo	0.38día	02/17/2022	02/18/2022	2
5	Definir Objetivos Trabajo	2.38días	02/18/2022	02/20/2022	2
6	Definir Enfoque y método a seguir	0.38día	02/18/2022	02/18/2022	1
7	Descripción recursos necesarios	0.38día	02/18/2022	02/18/2022	0.5
8	**Planificación**	**7.38días**	**02/20/2022**	**02/27/2022**	**12**
9	Planificación Personal Recursos	0.38día	02/20/2022	02/20/2022	0.5
10	Descripción hitos principales y entregables	0.33día	02/20/2022	02/20/2022	2
11	Cronograma de Alto nivel con hitos	0.38día	02/20/2022	02/21/2022	0.5
12	Descomponer hitos en tareas	0.38día	02/22/2022	02/23/2022	3
13	Cronograma Tareas al completo (Gantt)	2.38días	02/23/2022	02/25/2022	4
14	Análisis de riesgos	0.38día	02/27/2022	02/27/2022	2
15	Preparación y subida entregable PEC 1	9.38días	02/26/2022	03/07/2022	8
16	**PEC 2 - Análisis y Diseño de Base de Datos**	**34.63días**	**03/08/2022**	**04/11/2022**	**75**
17	**Requerimientos**	**5.38días**	**03/08/2022**	**03/13/2022**	**9**
18	Análisis Requerimientos del sistema	1.38días	03/08/2022	03/09/2022	2
19	Definición Requerimientos del sistema	0.38día	03/10/2022	03/11/2022	4
20	Definición Restricciones del Sistema	0.38día	03/10/2022	03/11/2022	2
21	Instalación herramientas Software Modelado	0.38día	03/13/2022	03/13/2022	1
22	**Diseño Base de Datos**	**24.67días**	**03/14/2022**	**04/08/2022**	**60**
23	Lectura Módulos Diseño BD	0.63día	03/14/2022	03/14/2022	4
24	Diseño Conceptual BD	9.38días	03/16/2022	03/25/2022	24
25	Diseño Lógico BD	5días	03/27/2022	04/01/2022	16
26	Diseño Físico BD	5días	04/03/2022	04/08/2022	16
27	Preparación y subida entregable PEC 2	1.38días	04/10/2022	04/11/2022	4
28	Lectura Técnicas Data Warehouse	0.63día	04/11/2022	04/11/2022	2
29	**PEC 3 - Implementación Base de Datos**	**29.67días**	**04/12/2022**	**05/12/2022**	**61**
30	**Implementación Base de Datos**	**13días**	**04/12/2022**	**04/25/2022**	**29**
31	Instalación Entorno BD	3.38días	04/12/2022	04/15/2022	8
32	Análisis de Procedimientos	0.38día	04/16/2022	04/17/2022	4
33	Scripts Creación de Tablas	2.38días	04/18/2022	04/20/2022	8
34	Creación de Procedimientos	2.38días	04/21/2022	04/24/2022	8
35	Ejecución de Scripts	0.33día	04/25/2022	04/25/2022	1
36	**Pruebas**	**11.38días**	**04/26/2022**	**05/08/2022**	**28**
37	Carga de Datos	0.38día	04/26/2022	04/27/2022	6
38	Creación Pruebas	3.38días	04/29/2022	05/02/2022	10
39	Ejecución Pruebas	0.38día	05/02/2022	05/03/2022	4
40	Corrección de errores	3.67días	05/04/2022	05/08/2022	8
41	Preparación y subida entregable PEC 3	2.38días	05/09/2022	05/12/2022	4
42	**Entrega Final**	**28.38días**	**05/13/2022**	**06/10/2022**	**60**
43	**Secciones Finales**	**14.38días**	**05/13/2022**	**05/27/2022**	**40**
44	Añadir Conclusiones	0.38día	05/13/2022	05/13/2022	4
45	Añadir Glosario	0.38día	05/15/2022	05/15/2022	4
46	Añadir Bibliografía	0.38día	05/16/2022	05/16/2022	4
47	Añadir Anexos	0.38día	05/18/2022	05/18/2022	4
48	Revisión Documento Memoria	5.38días	05/20/2022	05/25/2022	16
49	Informe Autoevaluación	0.38día	05/27/2022	05/27/2022	8
50	**Presentación Virtual**	**5.38días**	**05/29/2022**	**06/03/2022**	**20**
51	Preparar presentación	3.38días	05/29/2022	06/01/2022	12
52	Grabar Video	0.38día	06/03/2022	06/03/2022	4
53	Preparación ficheros y subida	5.38días	06/05/2022	06/10/2022	4
54	**Debate Virtual**	**4.38días**	**06/13/2022**	**06/17/2022**	



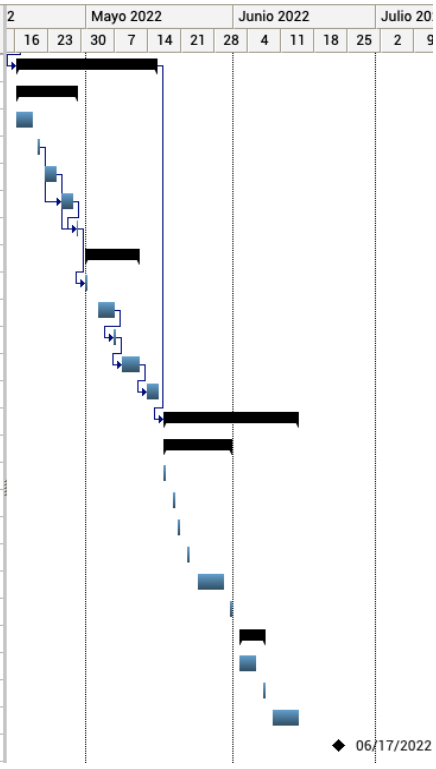
Tareas PEC 1 y PEC 2

	Nombre	Duración	Inicio	Fin	Horas
1	**PEC 1 - Planificación**	18.38días	02/17/2022	03/07/2022	28.5
2	Lectura Enunciado	0.38día	02/17/2022	02/17/2022	3
3	**Secciones Iniciales Trabajo**	3días	02/17/2022	02/20/2022	5.5
4	Definir Contexto Trabajo	0.38día	02/17/2022	02/18/2022	2
5	Definir Objetivos Trabajo	2.38días	02/18/2022	02/20/2022	2
6	Definir Enfoque y método a seguir	0.38día	02/18/2022	02/18/2022	1
7	Descripción recursos necesarios	0.38día	02/18/2022	02/18/2022	0.5
8	**Planificación**	7.38días	02/20/2022	02/27/2022	12
9	Planificación Personal Recursos	0.38día	02/20/2022	02/20/2022	0.5
10	Descripción hitos principales y entregables	0.33día	02/20/2022	02/20/2022	2
11	Cronograma de Alto nivel con hitos	0.38día	02/20/2022	02/21/2022	0.5
12	Descomponer hitos en tareas	0.38día	02/22/2022	02/23/2022	3
13	Cronograma Tareas al completo (Gantt)	2.38días	02/23/2022	02/25/2022	4
14	Análisis de riesgos	0.38día	02/27/2022	02/27/2022	2
15	Preparación y subida entregable PEC 1	9.38días	02/26/2022	03/07/2022	8
16	**PEC 2 - Análisis y Diseño de Base de Datos**	34.63días	03/08/2022	04/11/2022	75
17	**Requerimientos**	5.38días	03/08/2022	03/13/2022	9
18	Análisis Requerimientos del sistema	1.38días	03/08/2022	03/09/2022	2
19	Definición Requerimientos del sistema	0.38día	03/10/2022	03/11/2022	4
20	Definición Restricciones del Sistema	0.38día	03/10/2022	03/11/2022	2
21	Instalación herramientas Software Modelado	0.38día	03/13/2022	03/13/2022	1
22	**Diseño Base de Datos**	24.67días	03/14/2022	04/08/2022	60
23	Lectura Módulos Diseño BD	0.63día	03/14/2022	03/14/2022	4
24	Diseño Conceptual BD	9.38días	03/16/2022	03/25/2022	24
25	Diseño Lógico BD	5días	03/27/2022	04/01/2022	16
26	Diseño Físico BD	5días	04/03/2022	04/08/2022	16
27	Preparación y subida entregable PEC 2	1.38días	04/10/2022	04/11/2022	4
28	Lectura Técnicas Data Warehouse	0.63día	04/11/2022	04/11/2022	2



Tareas PEC 3 y Entrega final

	Nombre	Duración	Inicio	Fin	Horas
29	**PEC 3 - Implementación Base de Datos**	29.67días	04/12/2022	05/12/2022	61
30	**Implementación Base de Datos**	13días	04/12/2022	04/25/2022	29
31	Instalación Entorno BD	3.38días	04/12/2022	04/15/2022	8
32	Análisis de Procedimientos	0.38día	04/16/2022	04/17/2022	4
33	Scripts Creación de Tablas	2.38días	04/18/2022	04/20/2022	8
34	Creación de Procedimientos	2.38días	04/21/2022	04/24/2022	8
35	Ejecución de Scripts	0.33día	04/25/2022	04/25/2022	1
36	**Pruebas**	11.38días	04/26/2022	05/08/2022	28
37	Carga de Datos	0.38día	04/26/2022	04/27/2022	6
38	Creación Pruebas	3.38días	04/29/2022	05/02/2022	10
39	Ejecución Pruebas	0.38día	05/02/2022	05/03/2022	4
40	Corrección de errores	3.67días	05/04/2022	05/08/2022	8
41	Preparación y subida entregable PEC 3	2.38días	05/09/2022	05/12/2022	4
42	**Entrega Final**	28.38días	05/13/2022	06/10/2022	60
43	**Secciones Finales**	14.38días	05/13/2022	05/27/2022	40
44	Añadir Conclusiones	0.38día	05/13/2022	05/13/2022	4
45	Añadir Glosario	0.38día	05/15/2022	05/15/2022	4
46	Añadir Bibliografia	0.38día	05/16/2022	05/16/2022	4
47	Añadir Anexos	0.38día	05/18/2022	05/18/2022	4
48	Revisión Documento Memoria	5.38días	05/20/2022	05/25/2022	16
49	Informe Autoevaluación	0.38día	05/27/2022	05/27/2022	8
50	**Presentación Virtual**	5.38días	05/29/2022	06/03/2022	20
51	Preparar presentación	3.38días	05/29/2022	06/01/2022	12
52	Grabar Video	0.38día	06/03/2022	06/03/2022	4
53	Preparación ficheros y subida	5.38días	06/05/2022	06/10/2022	4
54	**Debate Virtual**	4.38días	06/13/2022	06/17/2022	



1.4.6 Previsión Horas disponibles vs Horas planificadas

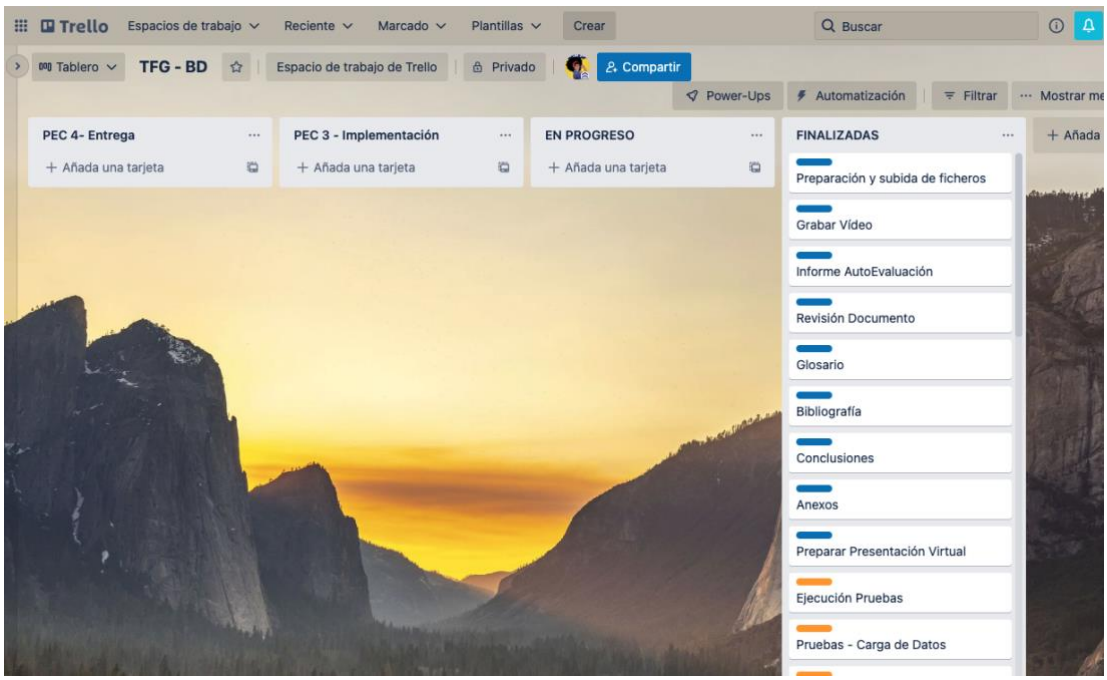
A continuación la comparativa de las horas disponibles del recurso vs las horas planificadas para cada hito.

No	Hito	Fecha inicio	Fecha Fin	Horas Disponibles	Horas Planificadas
1	**PEC 1 - Planificación**	17/02/2022	07/03/2022	40 horas	23 horas
2	**PEC 2 - Diseño**	08/03/2022	11/04/2022	76 horas	75 horas
3	**PEC 3 - Implementación**	12/04/2022	12/05/2022	68 horas	61 horas
4	**PEC 4 – Entrega Final**	13/05/2022	10/06/2022	60 horas	60 horas
5	**Debate**	13/06/2022	17/06/2022	12 horas	-

Se puede observar que para los hitos 2 y 4, la cantidad de horas planificadas es casi igual a las horas disponibles. Esto puede convertirse en un riesgo en caso de que surjan imprevistos o se requiera mas tiempo de ejecución.

1.4.7 Seguimiento de tareas

Tal como se había indicado, para el seguimiento diario de las tareas se hará uso de un tablero *Trello*. A continuación se muestra el estado del mismo, a fecha de la **última entrega:**



Este tablero se ira actualizando de forma casi diaria para reflejar el progreso de las tareas, y se irá compartiendo su evolución con cada entrega de proyecto.

A continuación, se muestra el estado actual de los distintos hitos del plan:

Hito	Fecha inicio	Fecha Fin	Entregada	Estado
PEC 1 – Planificación	17/02/2022	07/03/2022	06/03/2022	Completado
PEC 2 – Diseño	08/03/2022	11/04/2022	10/04/2022	Completado
PEC 3 – Implementación	12/04/2022	12/05/2022	17/05/2022	Completado
PEC 4 – Entrega Final	13/05/2022	10/06/2022	12/06/2022	Completado

1.4.8 Desviaciones en la planificación inicial y otras modificaciones (consensuadas con el tutor)

PEC 2

- Se tuvo que adelantar la tarea "Lectura Técnicas Data Warehouse" dado que se encontró una dependencia con la tarea "Diseño Conceptual". En otras palabras, era necesario comprender los conceptos de DW para poder realizar el diseño conceptual del repositorio estadístico y elegir una estrategia para modelar las distintas entidades y sus atributos. Esta dependencia tuvo un impacto en la tarea "Diseño Conceptual, la cual se finalizó el 28/03/22. Esto provocó un retraso de 3 días en el plan establecido para las siguientes tareas.

- Se tuvo que adelantar la tarea "Instalación Entorno BD" y "Script de Creación de Tablas", ya que las mismas forman parte del "Diseño Físico" de la Base de datos. Este aspecto no se tuvo en cuenta durante la planificación. De todos modos, nos deja más tiempo otras tareas de la PEC 3 como son la "Creación de los procedimientos" y la "Ejecución de las pruebas", las cuales pueden ocupar más tiempo de lo estimado.

- Se encontraron algunos inconvenientes en la instalación del entorno, ya que el SGBD escogido es Oracle XE 11g, el cual no es compatible con Mac. Se elige este SGBD dado que es de licencia libre y ha sido el utilizado durante las asignaturas de BD a lo largo del grado. Para poder trabajar con este SGBD se ha optado por la instalación de una máquina virtual de Windows, para lo que también se tuvieron que resolver algunas dificultades.

PEC 3

En el desempeño de esta última PEC 3, se tomaron algunas decisiones que han tenido un impacto en la planificación inicial:

- Se crearon nuevas tareas no previstas en la planificación:
    - Creación de secuencias para asignar a los identificadores únicos de los procesos
    - Dada la complejidad, y el volumen de trabajo en la creación de Procedimientos, se decidió dividir esta tarea en 3 partes:
        - Creación de Procedimientos ABM

- Creación de Procedimientos DataWarehouse
- Creación de otros Procedimientos
  De las tareas anteriores, solo se consiguió completar la primera. Las siguientes tareas se realizarán en el contexto de la última PEC.

- Se cambió el Data Type para las fechas, de "Date" a "Timestamp" de manera que se pueda almacenar la **fecha y hora** de los distintos registros almacenados en la DB, asi como diferenciar esta información para aquellos registros con una misma fecha de inicio y fin.
- Se decidió incluir un nuevo campo "Eliminado" de tipo booleano/char(1) en algunas tablas, para poder realizar un "borrado lógico" de la información solo en los casos necesarios, para evitar inconsistencias en la información del repositorio estadístico (ej. Borrado físico de usuarios)
- Por motivos imprevistos (viaje de trabajo y otros asuntos personales) algunas de las tareas planificadas para esta entrega se han debido posponer para la siguiente. Dichas tareas son:
  - Creación y Ejecución de Procedimientos para el DW
  - Creación y Ejecución de otros Procedimientos
  - Carga de datos y pruebas de los anteriores procedimientos

  Este cambio no debería comprometer el alcance ni la fecha de la entrega final, teniendo en cuenta que para esta última etapa solo quedaban pendientes la conclusión, bibliografía, anexos y revisión del trabajo. Se consultó al profesor colaborador para este asunto, el cual indicó que era posible realizarlo así.

PEC 4 – Entrega Final

- Debido a errores con los usuarios creados los cuales no podían acceder al espacios virtuales o *tablaspaces* creados para ese fin (de los cuales no se pudo detectar su origen, incluso con la ayuda del profesor); y siguiendo las indicaciones del profesor colaborador de la asignatura, se optó por crear las tablas del repositorio estadístico dentro del mismo espacio virtual de Operaciones: PROCESOS_SEGURIDAD, y no en el espacio virtual de DW tal como se había planificado inicialmente.
- Se decidió una carga inicial de datos de al menos unas 20 registros en las distintas entidades, con el objetivo de realizar las pruebas para verificar el buen funcionamiento del sistema.
- En esta última entrega, se realizaron modificaciones en las tablas del repositorio Estadístico: se suprimió una de ellas, y se agregó otra, para facilitar las consultas mínimas pedidas en los requisitos del sistema. Esto requirió una modificación en el diseño conceptual, lógico y físico, presentado en las entregas anteriores.
- Por motivos de salud debido al estado del único recurso del proyecto (fatiga producida por embarazo avanzado), se solicitó una prórroga de **2 días** adicionales para realizar la entrega final del trabajo y todos sus productos. Dicha prorroga fue autorizada por el profesor colaborador por correo electrónico.

1.4.9 Análisis de riesgos

A continuación, se muestra una tabla con los principales riesgos identificados para este proyecto:

Riesgo	**Tipo Riesgo**	**Impacto**	**Medidas de prevención/mitigación**
Riesgos de salud y familiar - **La alumna cursa un embarazo de 14 semanas a la fecha de la 1era entrega**	Crítico	Retrasos en el plan de trabajo, especialmente si se requiere de reposo u hospitalización	Seguir indicaciones medicas al pie de la letra para mantener un embarazo fuera de riesgos.
			Tomar descansos periódicos durante la ejecución de las tareas para evitar exceso de estrés y fatiga.
			Mantener una alimentación balanceada y no descuidar las horas de sueño
			Tomar días de vacaciones del trabajo habitual para dedicarlos a la realización del proyecto
			Contactar al tutor y al consultor del área en caso extremo
Riesgos de índole laboral: La alumna compagina estudios con su trabajo a jornada completa	Medio	Retrasos en el plan de trabajo debido a urgencias en el trabajo	Se intentarán realizar las entregas previstas al menos 1-2 días antes de plazo, para contar con tiempo suficiente para gestionar ambos asuntos.
Riesgos por falta de conocimiento: poca experiencia en manejo de bases de datos de gran volumen (Data Warehouse)	Medio	Problemas al implementar las funcionalidades necesarias para gestionar grandes volúmenes de información	Lectura de materiales sobre Data Warehouse y Visualización de videos para disponer del conocimiento básico.
			Se solicitará el apoyo del consultor de la asignatura para los puntos en los que se dispone de poca experiencia
Riesgos tecnológicos: problemas con la herramienta de bases de datos, perdida de datos, perdida de conectividad por averías o fallos en el internet	Alto	Perdida de datos y de trabajo realizado. Retrasos en las entregas	Se cuenta con un ordenador personal para trabajar en este proyecto y como plan de contingencia, se podría hacer uso del ordenador del trabajo en caso de emergencia.
			Se realizarán backups tras cada actualización que se guardarán en la nube para no perder el trabajo realizado.
			Se cuenta con acceso a internet por fibra de alta velocidad desde el hogar. En caso de fallo, y como plan de contingencia, se puede trabajar desde otros sitios: como la oficina, bibliotecas y espacios de coworking.
			Se intentará realizar las entregas previstas al menos 1-2 días antes de plazo, para evitar riesgos y nervios de ultimo minuto

1.5 Breve sumario de productos obtenidos

En el presente proyecto se incluyen los siguientes productos:

- Memoria de Trabajo Fin de Grado: Se trata del presente documento, donde se explica de forma detallada todo el proceso de planificación y ejecución del sistema de bases de datos.
- Anexos – Pruebas Repositorio Estadístico: Se incluye un documento anexo con imágenes de las pruebas realizadas para las consultas del repositorio estadístico.
- *Scripts* Sistema de BD: Incluye los *Scripts* de creación de la BD, Creación de Usuarios, Creación de tablas, Creación de Secuencias, Creación de Procedimientos almacenados, Carga inicial de datos y Pruebas.
- Presentación Power Point del proyecto
- Autoinforme del estudiante
- Presentación en Video (subida a la herramienta "Present@" de la UOC)

1.6 Breve descripción de los otros capítulos de la memoria

Capitulo 2: Requerimientos del Sistema
En este capítulo se plasman los resultados del análisis que se ha realizado del enunciado del TFG, del cual se obtienen en su totalidad los requerimientos del proyecto.

Capitulo 3: Diseño de la Base de Datos
En este capítulo se realiza todo el diseño de la Base de Datos. Se lleva a cabo el proceso de diseño pasando por cada una de las etapas ya definidas en la planificación:

- Diseño Conceptual: se realiza el esquema conceptual de alto nivel del sistema a desarrollar, con las entidades, sus atributos y la relación entre ellas.

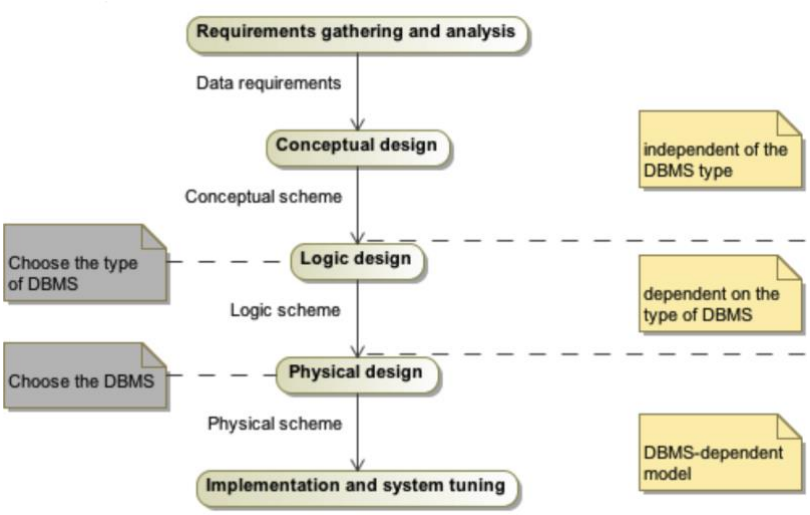
- Diseño lógico: se transforma el esquema conceptual a un modelo lógico de datos.

- Diseño físico: Se trata adaptar el diseño lógico al Sistema Gestor de Base de Datos (SGBD).

Capitulo 4: Implementación y pruebas de la Base de Datos
Se trata de ejecutar finalmente, en el gestor de base de datos, los diseños realizados en el capítulo anterior. En este punto, se crea la base de datos en el espacio virtual, se crean las tablas y los distintos procedimientos almacenados con los que aplicaremos la lógica de negocio definida en los requerimientos.

En esta etapa, también se realiza una carga de datos inicial para poder realizar las pruebas que certifiquen que se cumplen los requerimientos, así como la consulta de datos históricos a través de las tablas del repositorio estadístico

En síntesis, en estos 2 capítulos se han llevado a cabo los 4 primeros pasos del proceso completo de diseño e implementación de una base de datos:



2. Requisitos del sistema

En este apartado damos inicio al proceso de desarrollo de la Base de datos, con la creación de los requisitos formales del sistema. Por requisitos del sistema, entendemos aquellos requerimientos y restricciones con los que debe contar el sistema que se está desarrollando.

Los requerimientos del sistema se pueden clasificar en dos tipos:

1. **Requisitos Funcionales**: Son aquellos que describen la funcionalidad que debe existir en el sistema. A su vez, se pueden dividir en dos tipos:
    - Requisitos de funcionalidad: los que describen el comportamiento que debe tener el sistema.
    - Requisitos de datos: los que describen los datos que deben guardarse de forma persistente en el sistema.

2. **Requisitos No Funcionales**: Son aquellos que describen las características o calidades que se espera que existan en el sistema. También se pueden identificar como *Restricciones del sistema*, ya que si no se verifica su cumplimiento, no se puede dar como valido el requerimiento en cuestión.

Todos los requisitos del sistema de este trabajo se toman de la información incluida en el enunciado del TFG. Con lo que la primera tarea llevada a cabo ha sido el análisis exhaustivo de todo el enunciado, seguido por una serie de conversaciones con el consultor del aula para aclarar las dudas que habían surgido del análisis.

De estas conversaciones con el consultor de la asignatura, se obtienen una serie de datos adicionales al enunciado, los cuales detallamos a continuación:

- Los datos personales de los usuarios del sistema NO deben guardarse en esta base de datos. Se entienden que estos datos podrían estar guardados en otra BD de la empresa, así que con mostrar un identificador para el usuario es suficiente.
- Deben registrarse las acciones punitivas en caso de cualquier tipo de incumplimiento, sea detectado durante una auditoría como en una simulación.
- La lista de vulnerabilidades puede actualizarse durante una auditoria.
- Podemos asumir que las vulnerabilidades serán creadas en la BD por un usuario particular que pertenecerá a un equipo, el cual puede ser interno o externo.
- El "Número de vulnerabilidades críticas detectadas internamente" se puede obtener filtrando por el tipo de usuario creador, según sea interno o externo.
- El "Número total de incumplimientos por política en cada departamento de la empresa" se puede considerar parte del repositorio estadístico.
- El "Número total de acciones de mitigación que en el momento de ejecutar la consulta no están totalmente acabadas", se refiere a todas aquellas acciones cuyo estado sea distinto a "Completada".
- Se deben guardar las acciones punitivas asociadas a cualquier incumplimiento.
- Sobre el estado de las Vulnerabilidades, podemos asumir que: "Identificada", es el estado inicial en el momento de crear una vulnerabilidad, y que : "No mitigada" se refiere a cuando se ha superado la fecha límite de implantación para todas las acciones de mitigación, pero ninguna de ellas se ha iniciado.

2.1. Requisitos Funcionales del Sistema

A continuación, mostramos un listado con todos los requisitos funcionales del sistema que han sido identificados. Para cada requisito se muestra su identificador único, así como la parte del enunciado en donde se hace referencia al mismo:

Identificador	Requisito	Referencia enunciado
RQF - 001	Se debe almacenar un registro con todos los **Procesos de gestión** de la empresa. Para cada proceso, queremos guardar su nombre y un identificador único.	*La primera acción del proyecto de implantación de esta aplicación de control de procesos de seguridad informática será el **análisis de vulnerabilidades**.*
RQF - 002	Se debe almacenar una lista con todas las **vulnerabilidades** asociadas a cada proceso de gestión del sistema. Para cada vulnerabilidad, queremos guardar una descripción, el proceso de gestión que tiene asociado, un identificador único, su fecha de creación, el usuario que la ha creado y si es crítica o no, y su estado. Los estados posibles son: identificada, no mitigada, parcialmente mitigada o totalmente mitigada.	*esta consultora externa analizará todos los servicios informáticos y **creará una lista de vulnerabilidades asociadas a cada uno de los procesos de gestión** de la empresa.....pero la actualización se hará con los recursos internos de la empresa… También podrán ser críticas o no… Cada vulnerabilidad detectada debe de estar registrada en la BD y podrá tener alguno de los estados siguientes: identificada, no mitigada, parcialmente mitigada o totalmente mitigada.*
RQF - 003	Se debe almacenar un registro con las **acciones de mitigación** llevadas a cabo para resolver una vulnerabilidad. Para cada acción de mitigación, se debe almacenar: una descripción, la	*Una vez se han detectado totas las posibles vulnerabilidades, se deben definir e implementar las posibles acciones de mitigación proactiva… Cada acción de mitigación definida debe tener*

	vulnerabilidad a la que está asignada, un identificador único, una fecha límite de implantación, una fecha de inicio, una fecha de fin y un responsable, y su estado. Los estados posibles son: Definida, En proceso, Acabada y en revisión.	*un responsable y una fecha límite de implantación… Las acciones de mitigación podrán tener alguno de los estados siguientes: definida, en proceso, acabada o en revisión*
RQF - 004	Los **estados de las acciones de mitigación** se deben actualizar automáticamente. A continuación, se detallan los estados posibles y cuándo deben actualizarse: - Definida: Estado inicial cuando se crea la acción. - En proceso: Cuando se ha asignado una fecha de inicio. - Acabada: Cuando se ha asignado una fecha de fin. - En revisión: Cuando no se sabe cómo realizarla o no se puede realizar por limitaciones de la empresa. **Este es el único estado que se asignará solo de forma manual.**	*Las acciones de mitigación podrán tener alguno de los estados siguientes: definida, en proceso, acabada o en revisión (para aquellas que no se sabe cómo realizarlas o que no se pueden realizar por limitaciones internas de la empresa).*
RQF - 005	Los **estados de las vulnerabilidades** se deben actualizar automáticamente cuando se actualicen sus acciones de mitigación correspondientes. A continuación, se detallan los estados posibles y cuándo deben actualizarse: - Identificada: Estado inicial al momento de la creación de una vulnerabilidad - Parcialmente mitigada: Cuando alguna de sus acciones de mitigación (pero no todas) se encuentra en estado "Acabada". - Totalmente Mitigada: Cuando todas sus acciones de mitigación se encuentran en estado "Acabada" - No Mitigada: Cuando se ha superado la fecha limite para todas las acciones de mitigación, y todas ellas se encuentran en estado "Definida"	*Se considerará que una vulnerabilidad está parcialmente mitigada cuando hay, como mínimo, una acción de mitigación acabada, y se considerará totalmente mitigada cuando todas las acciones asociadas estén acabadas*
RQF - 007	Se debe mantener un registro con las **políticas de seguridad** de la empresa. De cada política, se debe almacenar su nombre, un identificador único y su fecha de creación.	*La empresa definirá unas políticas de seguridad de obligado cumplimiento*
RQF - 008	Se debe mantener un registro de **Incumplimientos**, o lo que es lo mismo, de las políticas de seguridad de la empresa que han sido incumplidas. Para cada Incumplimiento se debe almacenar: un identificador único, una descripción, la política que incumple, la fecha del incumplimiento y el identificador de la persona que lo ha realizado.	*Se deberá registrar también en la BD todos estos incumplimientos, obviamente, teniendo en cuenta todas las restricciones de confidencialidad que estas acciones requieren.*
RQF - 009	Se debe mantener un registro de U**suarios** del sistema. Para cada usuario, se debe almacenar un identificador único, el departamento de la empresa al que corresponde, y el tipo de usuario, el cual puede ser: interno o externo.	*Se deberán registrar las sesiones formativas y los usuarios que participen en ellas.* [Consensuado con consultor]

RQF - 010	Se debe mantener un registro con los **Departamentos** de la empresa. Para cada departamento, se debe almacenar un identificador único, el nombre y los usuarios que lo forman.	*Para la aplicación de control que se desarrollará solo se deberá registrar el número total de incumplimientos por política en cada departamento de la empresa.*
RQF - 011	Se debe mantener un registro de con las **sesiones de formación** ofrecidas a los usuarios del sistema. Para cada sesión, se debe almacenar: su nombre, un identificador único, la fecha de la sesión, los usuarios que han participado en cada sesión y el formato, el cual puede ser: presencial o telemático,	*La intención es realizar **sesiones de formación**...La aplicación también deberá llevar un registro exhaustivo de todas las sesiones de formación, tanto presenciales como telemáticas, que se realicen en la empresa referentes a temas de seguridad. Se deberán registrar las sesiones formativas y los usuarios que participen en ellas.*
RQF - 012	Se debe mantener un registro de **simulaciones** controladas de ataques informáticos, los cuales se enviarán a grupos de usuarios. Para cada simulación, se debe registrar: un identificador único, la fecha, los usuarios que han recibido la simulación, y si se ha detectado algún incumplimiento de las políticas de seguridad.	*La intención es realizar... s**imulaciones controladas de ataques** para saber qué usuarios no siguen las directrices definidas… nos piden que la BD que definiremos tenga en cuenta estos casos y que se añadan a la lista de incumplimientos de cada departamento.*
RQF - 013	Se deben registrar en la lista de incumplimientos, aquellos que han sido detectados durante las **simulaciones** controladas de ataques informáticos	*La intención es realizar… s**imulaciones controladas de ataques** para saber qué usuarios no siguen las directrices definidas… nos piden que la BD que definiremos tenga en cuenta estos casos y que se añadan a la lista de incumplimientos de cada departamento.*
RQF - 014	Se debe mantener un registro con las **acciones punitivas** asignadas a los usuarios del sistema que realizan incumplimientos. Para cada acción punitiva, se debe almacenar: una descripción, un identificador único, el incumplimiento realizado y el usuario quien ha incumplido	*La empresa definirá las acciones punitivas a realizar sobre los usuarios implicados, pero nos piden que la BD que definiremos tenga en cuenta estos casos y que se añadan a la lista de incumplimientos*
RQF - 015	Se debe mantener un registro con las **Auditorias de seguridad** realizadas en la empresa. Para cada auditoria, se debe almacenar: un identificador único, la fecha de la auditoria, el usuario que la registra, que puede ser: interno o externo, el resultado de la auditoria, el/los procesos de gestión analizados, la(s) políticas de la empresa revisadas y el/los incumplimientos detectados.	*la futura aplicación… debe permitir gestionar es el control de las diferentes **auditorías** de seguridad definidas por la empresa. La auditoría... estará ligada a las diferentes políticas definidas y aprobadas por la empresa...Dentro de estas auditorías, que serán realizadas por equipos internos o externos.. se analizarán los diferentes procesos de gestión con tal de buscar cualquier incumplimiento de las políticas…*
RQF - 016	Se debe mantener un registro con todos los **muestreos** realizados durante una auditoria. Para cada muestreo se debe almacenar un identificador único y una descripción de la muestra.	*El sistema debe permitir guardar todos los muestreos hechos durante la auditoría.*

RQF - 017	Se debe proporcionar un Repositorio estadístico donde se puedan realizar consultas para obtener los siguientes resultados: 1) Departamento que, en un año concreto, tiene un número mayor de incumplimientos de seguridad registrados en la BD. 2) Proceso de gestión interno que, teniendo en cuenta tota la información de que se dispone en la BD, ha tenido un mayor número de vulnerabilidades detectadas. 3) Top5 de usuarios por número de incumplimientos asociados directamente a ellos, o a su departamento, durante el año en curso. 4) Porcentaje de vulnerabilidades que, en el momento de ejecutar la consulta, están totalmente mitigadas. 5) Número total de acciones de mitigación que, en el momento de ejecutar la consulta, no están totalmente acabadas. 6) Política de seguridad que, en el momento de ejecutar la consulta, ha tenido más incumplimientos (teniendo en cuenta todos los departamentos de la empresa) 7) Dado un determinado departamento de la empresa, y teniendo en cuenta el momento de ejecutar la consulta, porcentaje de usuarios del departamento que no han acabado todas las formaciones de seguridad asignadas. 8) Porcentaje de usuarios de la empresa que, en el año en curso, no tienen ningún incumplimiento asignado. 9) Teniendo en cuenta todas las auditorías externas realizadas, año en el cual se han detectado más incumplimientos (teniendo en cuenta sólo los detectados durante la auditoría). 10) Porcentaje de vulnerabilidades críticas que, en el momento de ejecutar la consulta, tienen alguna acción de mitigación abierta (que no esté en estado "acabada"). 11) Teniendo en cuenta el último año (el anterior al año en curso), título de la sesión formativa telemática que ha tenido un porcentaje menor de participantes en total. 12) Número de vulnerabilidades críticas detectadas internamente teniendo en cuenta todos los datos de que se dispone. Se consideran detectadas internamente si se detectaron en posterioridad al análisis realizado al inicio del proyecto por la consultora externa.	*Repositorio estadístico donde se puedan obtener los siguientes resultados:* *· Departamento que, en un año concreto, tiene un número mayor de incumplimientos de seguridad registrados en la BD.* *· Proceso de gestión interno que, teniendo en cuenta tota la información de que se dispone en la BD, ha tenido un mayor nombre de vulnerabilidades detectadas.* *· Top5 de usuarios por número de incumplimientos asociados directamente a ellos, o a su departamento, durante el año en curso.* *· Porcentaje de vulnerabilidades que, en el momento de ejecutar la consulta, están totalmente mitigadas.* *· Número total de acciones de mitigación que, en el momento de ejecutar la consulta, no están totalmente acabadas.* *· Política de seguridad que, en el momento de ejecutar la consulta, ha tenido más incumplimientos (teniendo en cuenta todos los departamentos de la empresa)* *· Dado un determinado departamento de la empresa, y teniendo en cuenta el momento de ejecutar la consulta, porcentaje de usuarios del departamento que no han acabado todas las formaciones de seguridad asignadas.* *· Porcentaje de usuarios de la empresa que, en el año en curso, no tienen ningún incumplimiento asignado.* *· Teniendo en cuenta todas las auditorías externas realizadas, año en el cual se han detectado más incumplimientos (teniendo en cuenta sólo los detectados durante la auditoría).* *· Porcentaje de vulnerabilidades críticas que, en el momento de ejecutar la consulta, tienen alguna acción de mitigación abierta (que no esté en estado "acabada").* *· Teniendo en cuenta el último año (el anterior al año en curso), título de la sesión formativa telemática que ha tenido un porcentaje menor de participantes en total.* *· Número de vulnerabilidades críticas detectadas internamente teniendo en cuenta todos los datos de que se dispone. Se consideran detectadas internamente si se detectaron en posterioridad al análisis realizado al inicio del proyecto por la consultora externa.* *· En el momento de ejecutar la consulta, porcentaje de acciones de mitigación en el sistema que están en los estados "en*

	13) En el momento de ejecutar la consulta, porcentaje de acciones de mitigación en el sistema que están en los estados “en proceso” o “en revisión”. 14) Teniendo en cuenta todas las acciones de mitigación en estado “en proceso”, persona responsable con más acciones asignadas. 15) Número total de **Incumplimientos** por cada departamento de la empresa.	*proceso” o “en revisión”.* *· Teniendo en cuenta todas las acciones de mitigación en estado “en proceso”, persona responsable con más acciones asignadas.* *...Se deberá registrar el número total de incumplimientos por política en cada departamento de la empresa*

2.2 Requisitos No Funcionales del Sistema

A continuación, mostramos un listado con todos los requisitos no funcionales, o restricciones del sistema, que han sido identificados. Para cada requisito se incluye un número de identificación único, así como la parte del enunciado en donde se hace referencia al mismo:

Identificador	Requisito	Referencia enunciado
RQNF - 001	Se dispondrá de procedimientos de Bases de Datos para realizar el Alta, Baja y Modificación (ABM) de cada una de las entidades definidas en los requerimientos funcionales del sistema	*A nivel de procedimientos, se deberá implementar y describir con detalle los procedimientos de ABM (Alta + Baja + Modificación) de todas las entidades (o clases) que se consideren relevantes.*
RQNF - 002	La Base de Datos debe permitir manejar un volumen creciente de datos. Para ello, deben utilizarse técnicas de gestión de grandes volúmenes de datos (Data warehouse)	*la aplicación ha de funcionar para cualquier **volumen de datos,** y por este motivo.. la gestión de los datos almacenados se haga siguiendo las técnicas que se aplican a grandes volúmenes de datos, lo que se denomina gestión de almacenes de datos*
RQNF - 003	Se debe mantener un registro de cada uno de los procesos ejecutados en el sistema: ***Logs***. Estos procesos deben gestionar el manejo de excepciones o errores detectados durante su ejecución. Para cada Log, se debe almacenar al menos: el nombre del procedimiento ejecutado y los parámetros de entrada y de salida. Para los parámetros de salida, se debe disponer como mínimo de un parámetro RSP, de tipo String, que indicará si la ejecución ha finalizado correctamente (valor ‘OK’) o si ha fracasado (valor ‘ERROR+TIPO DE ERROR’).	*se recomienda almacenar todas las llamadas a procedimientos que se hagan en una **tabla de log,** almacenando **el nombre del procedimiento** ejecutado y los **parámetros de entrada y de salida**... se pide explícitamente que los procedimientos almacenados cumplan con las condiciones siguientes:* *· Como mínimo dispondrán de un parámetro de salida llamado RSP, de tipo string, que indicará si la ejecución ha finalizado correctamente (valor ‘OK’) o si ha fracasado (valor ‘ERROR+TIPO DE ERROR’).* *· Dispondrán de tratamiento de excepciones.*

RQNF - 004	Se deben incluir aquellos mecanismos adicionales que se consideren adecuados para facilitar la resolución problemas así como el manejo de errores y excepciones, entre ellos, un log para registrar todas las operaciones realizadas en la Base de Datos.	*se valorará muy positivamente el disponer de mecanismos que permitan resolver potenciales problemas de integración con el resto del sistema: un log de las acciones realizadas con la BD, mecanismos para testear la funcionalidad de la BD, etc. Se valorará el diseño e implementación de estos mecanismos.*
RQNF - 005	La Base de datos debe permitir la realización de consultas estadísticas, como máximo en un tiempo constante (1)	*Sobre estos datos se harán diversas consultas estadísticas que han de poder dar resultados de la forma más eficiente posible en términos de tiempo de respuesta. La única restricción que ha de tener este repositorio estadístico es que debe ofrecer los diferentes resultados que se definan en tiempo constante 1*
RQNF - 006	La Base de datos debe ser Escalable	*La BD deberá de ser escalable para poder ir incorporando progresivamente todas aquellas necesidades que surjan durante su vigencia.*
RQNF - 007	No se deben almacenar datos personales de los usuarios en las Base de datos	*Se deberá registrar también en la BD todos estos incumplimientos, obviamente, teniendo en cuenta todas las restricciones de confidencialidad que estas acciones requieren…solo se deberá registrar el número total de incumplimientos por política en cada departamento de la empresa.*
RQNF - 008	La Base de datos debe ser Transaccional y Relacional	Según Plan de Trabajo
RQNF - 009	Se utilizará el SGBD Oracle Database Express Edition	Según Plan de Trabajo

2.3 Contradicciones en los requisitos

Tras realizar el análisis del enunciado, se encontraron algunas informaciones contradictorias, cosa que suele ser muy normal durante el proceso de recolección y análisis de requisitos.

Por ejemplo, en el enunciado se menciona:

Se deberá registrar también en la BD todos estos incumplimientos, obviamente, teniendo en cuenta todas las restricciones de confidencialidad que estas acciones requieren. ***Para la aplicación de control que se desarrollará solo se deberá registrar el número total de incumplimientos por política en cada departamento de la empresa.***

Sin embargo, también se pide en el repositorio estadístico: *Top5 de usuarios por número de incumplimientos asociados directamente a ellos, o a su departamento, durante el ano en curso.*

Por ello se opta por una solución intermedia, en la que, se lleva un registro con todos los incumplimientos detectados, incluyendo el usuario que realiza el incumplimiento. Sin embargo, para respetar las restricciones de seguridad, se opta por registrar solo el identificador del usuario y su departamento. El identificador del usuario será el mismo que tenga en la base de datos de la empresa, de manera que solo se puede conocer la identidad de los usuarios infractores accediendo a esta otra base de datos.

Esta restricción en el manejo de los datos personales se ha registrado como un requisito no funcional (RQNF – 007)

3 Diseño de la Base de Datos

3.1 Diseño Conceptual

Esta es la etapa inicial de todo el diseño de la base de datos, y en ella se realiza el esquema conceptual de alto nivel del sistema a desarrollar, partiendo de los requisitos que se acaban de recolectar. En este diagrama se incluyen todas las entidades detectadas, sus atributos y la relación entre ellas.

Para el diseño conceptual de bases de datos se ha optado por utilizar una Metodología centralizada *(one shot*), dado que se cuenta con todos los requisitos del sistema recopilados en el mismo documento (enunciado), y con este listado de requisitos se puede construir un único modelo conceptual de toda la base de datos.

Para realizar el modelado de la información, se ha optado por utilizar el lenguaje unificado de modelación UML. A continuación, describimos la notación utilizada para los nombres de entidades, atributos y relaciones:

- Nombre entidad: Se utilizan nombres en singular y grafía Pascal. Ej.: ProcesoGestion.
- Atributos entidad: Se utilizan nombres en singular y grafía Camel. Se evita el uso del nombre de la entidad. Ej.: fechaFin
- Atributos booleanos: Se utiliza nombre precedido de *es*, y grafía Camel. Ej.: esCritico
- Relaciones entre entidades: Se utilizan verbos en la tercera persona del singular y grafía Pascal. Las relaciones con sus verbos se pueden leer de arriba hacia abajo, o de izquierda a derecha.
- Relaciones entre entidades de tipo rol: Se utiliza un rol y grafía Camel. Ej.: responsable

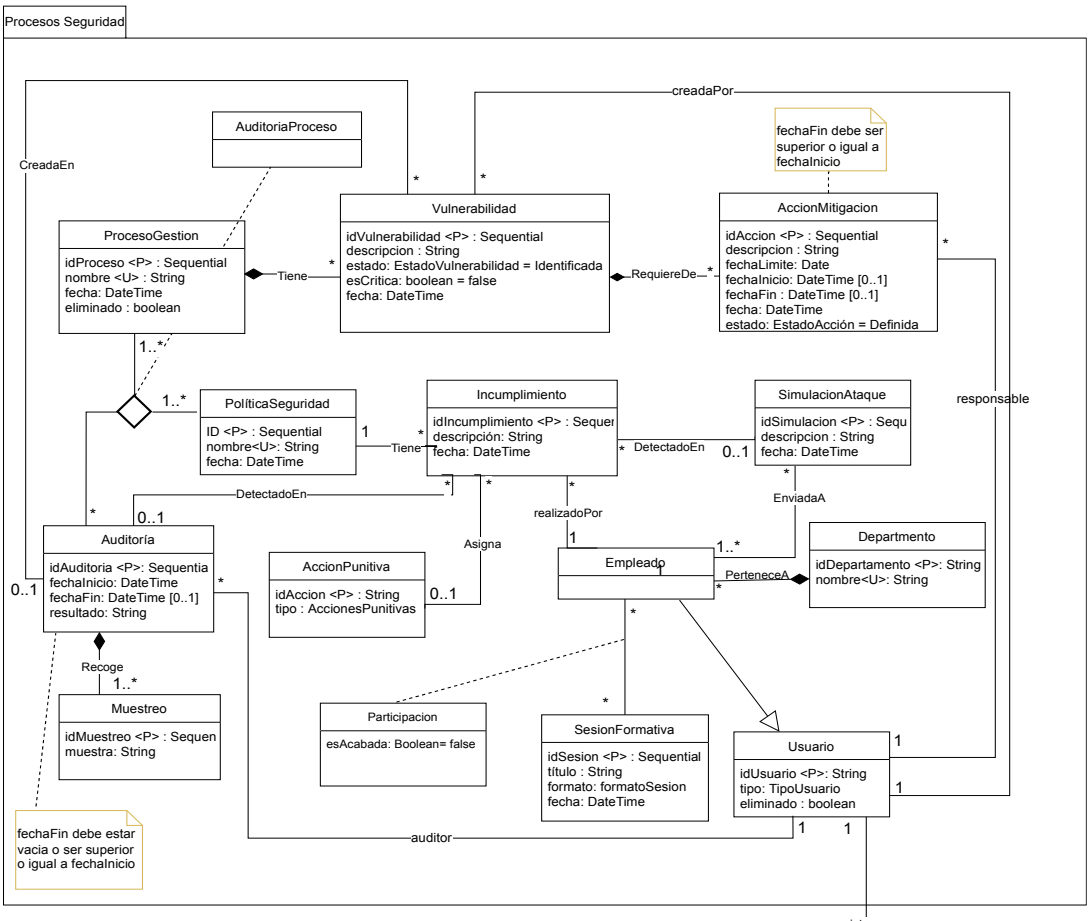
Finalmente, se ha optado por dividir el modelo conceptual mostrando las entidades agrupadas en tres partes:

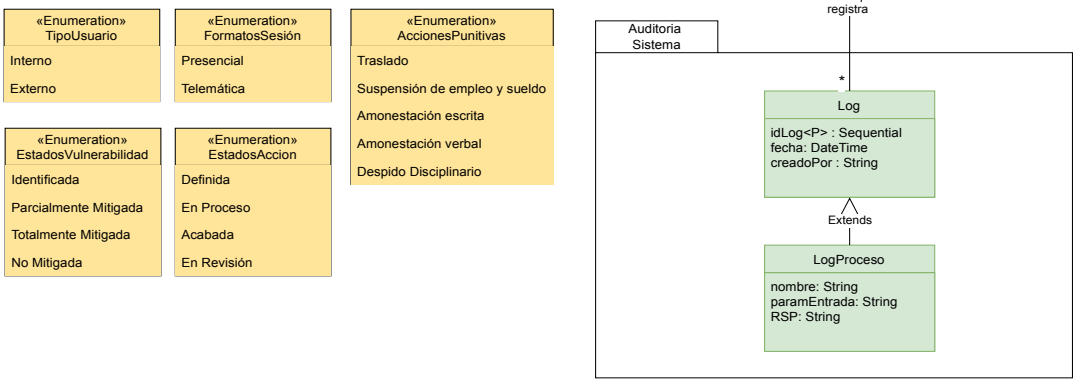
- Procesos de Seguridad: Muestra las entidades principales que interactúan y se relacionan dentro de la aplicación de Procesos de Seguridad.

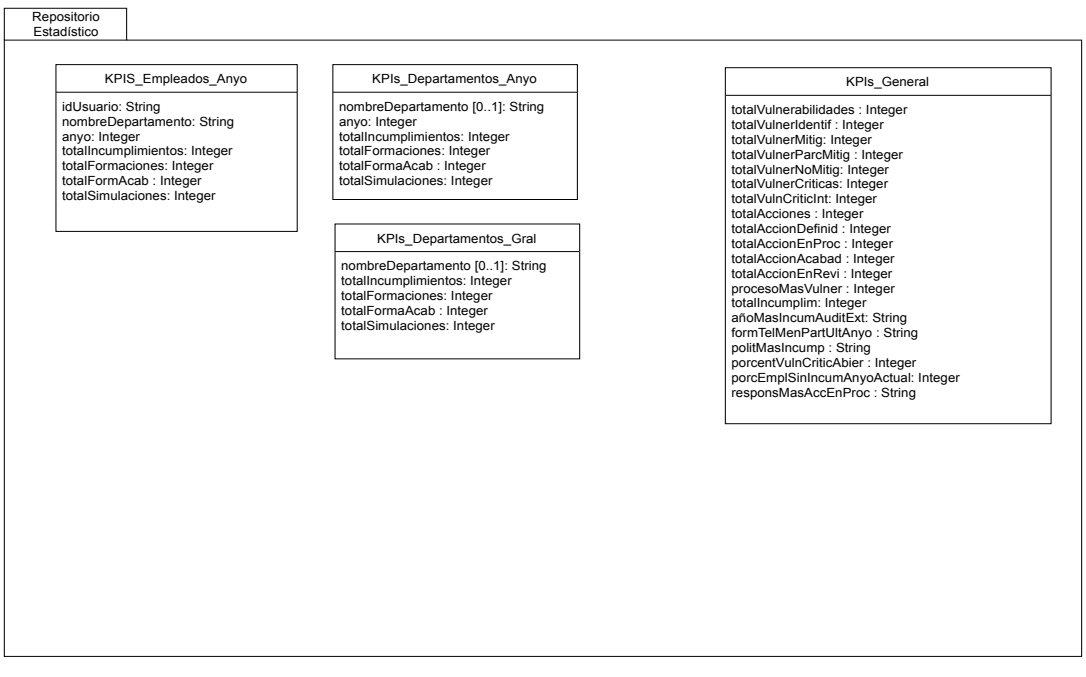
- Auditoria del Sistema: Muestra las entidades en las que se guardan los registros de los eventos o *logs* de todas las operaciones que se realizan, y que sirven para auditar el sistema.

- Repositorio Estadístico: Muestra las entidades creadas para almacenar los datos históricos que se consultaran como parte del repositorio estadístico.

A continuación mostramos el diagrama UML con el Diseño Conceptual de toda la solución:


Procesos Seguridad
AuditoriaProceso
CreadaEn
creadaPor
fechaFin debe ser superior o igual a fechaInicio
ProcesoGestion
idProceso <P> : Sequential
nombre <U> : String
fecha: DateTime
eliminado : boolean
Tiene
Vulnerabilidad
idVulnerabilidad <P> : Sequential
descripcion : String
estado: EstadoVulnerabilidad = Identificada
esCritica: boolean = false
fecha: DateTime
RequiereDe
AccionMitigacion
idAccion <P> : Sequential
descripcion : String
fechaLimite: Date
fechaInicio: DateTime [0..1]
fechaFin : DateTime [0..1]
fecha: DateTime
estado: EstadoAcción = Definida
PolíticaSeguridad
ID <P> : Sequential
nombre<U>: String
fecha: DateTime
Incumplimiento
idIncumplimiento <P> : Sequer
descripción: String
fecha: DateTime
DetectadoEn
SimulacionAtaque
idSimulacion <P> : Sequ
descripcion : String
fecha: DateTime
responsable
EnviadaA
realizadoPor
Asigna
Auditoría
idAuditoria <P>: Sequentia
fechaInicio: DateTime
fechaFin: DateTime [0..1]
resultado: String
AccionPunitiva
idAccion <P> : String
tipo : AccionesPunitivas
Empleado
Departmento
idDepartamento <P>: String
nombre<U>: String
PerteneceA
Recoge
Muestreo
idMuestreo <P> : Sequen
muestra: String
Participacion
esAcabada: Boolean= false
SesionFormativa
idSesion <P> : Sequential
título : String
formato: formatoSesion
fecha: DateTime
Usuario
idUsuario <P>: String
tipo: TipoUsuario
eliminado : boolean
auditor
fechaFin debe estar vacia o ser superior o igual a fechaInicio

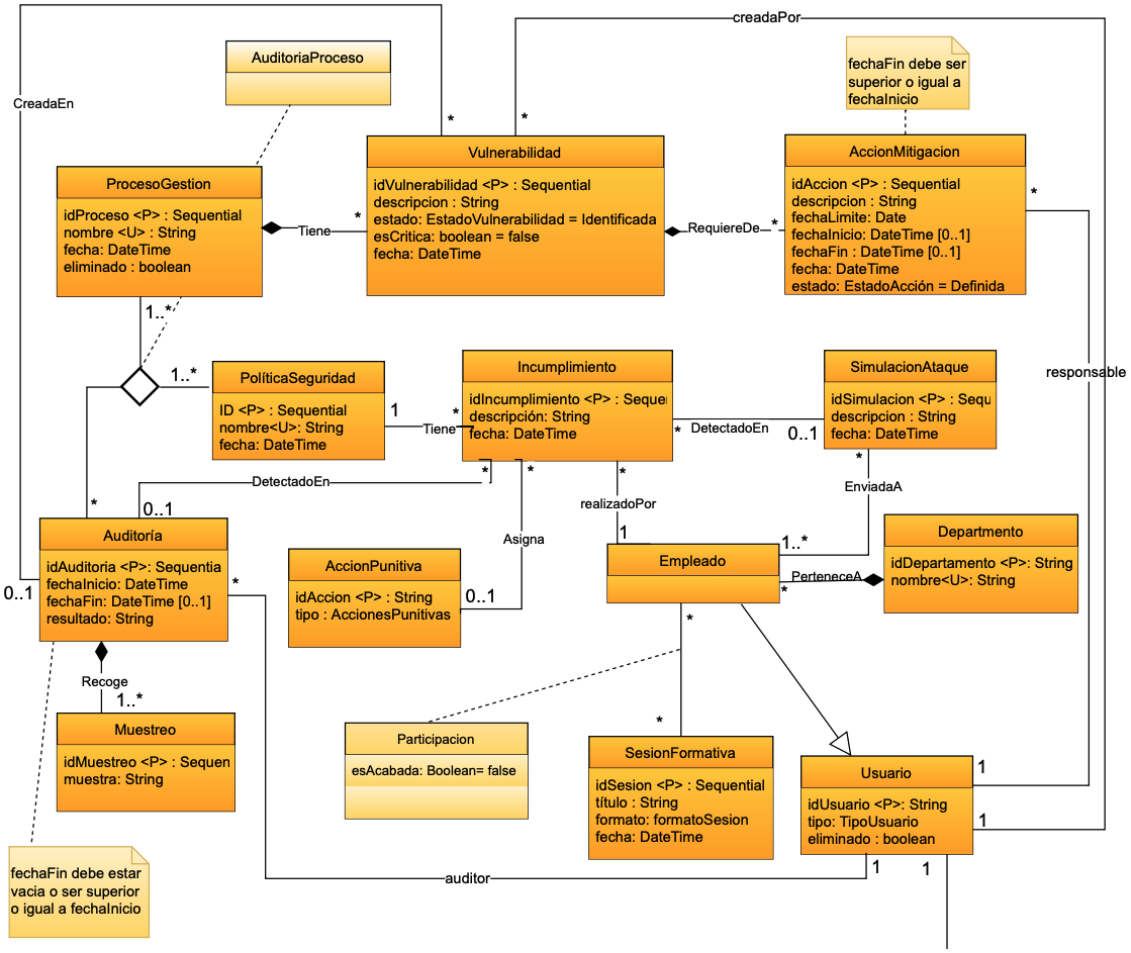

«Enumeration» TipoUsuario
Interno
Externo
«Enumeration» FormatosSesión
Presencial
Telemática
«Enumeration» AccionesPunitivas
Traslado
Suspensión de empleo y sueldo
Amonestación escrita
Amonestación verbal
Despido Disciplinario
«Enumeration» EstadosVulnerabilidad
Identificada
Parcialmente Mitigada
Totalmente Mitigada
No Mitigada
«Enumeration» EstadosAccion
Definida
En Proceso
Acabada
En Revisión
registra
Auditoria Sistema
Log
idLog<P> : Sequential
fecha: DateTime
creadoPor : String
Extends
LogProceso
nombre: String
paramEntrada: String
RSP: String


Repositorio Estadístico
KPIS_Empleados_Anyo
idUsuario: String
nombreDepartamento: String
anyo: Integer
totalIncumplimientos: Integer
totalFormaciones: Integer
totalFormAcab : Integer
totalSimulaciones: Integer
KPIs_Departamentos_Anyo
nombreDepartamento [0..1]: String
anyo: Integer
totalIncumplimientos: Integer
totalFormaciones: Integer
totalFormaAcab : Integer
totalSimulaciones: Integer
KPIs_Departamentos_Gral
nombreDepartamento [0..1]: String
totalIncumplimientos: Integer
totalFormaciones: Integer
totalFormaAcab : Integer
totalSimulaciones: Integer
KPIs_General
totalVulnerabilidades : Integer
totalVulnerIdentif : Integer
totalVulnerMitig: Integer
totalVulnerParcMitig : Integer
totalVulnerNoMitig: Integer
totalVulnerCriticas: Integer
totalVulnCriticInt: Integer
totalAcciones : Integer
totalAccionDefinid : Integer
totalAccionEnProc : Integer
totalAccionAcabad : Integer
totalAccionEnRevi : Integer
procesoMasVulner : Integer
totalIncumplim: Integer
añoMasIncumAuditExt: String
formTelMenPartUltAnyo : String
politMasIncump : String
porcentVulnCriticAbier : Integer
porcEmplSinIncumAnyoActual: Integer
responsMasAccEnProc : String

3.1.2 Descripción Entidades del Sistema

3.1.2.1 Procesos de Seguridad

Tal como se ha comentado, se trata de las entidades clave de la aplicación de Procesos de Seguridad. En estas entidades se recogen la mayor parte de los datos y comportamiento definido en los requisitos del sistema:



A continuación describimos cada una de las entidades contenidas en el diagrama anterior, con sus relaciones y atributos:

1. **ProcesoGestion**

Esta entidad representa el cúmulo de todos los procesos de gestión de la empresa. Dichos procesos de gestión serán objeto de análisis para la detección de posibles vulnerabilidades a nivel informático. Cada uno de estos procesos se debe identificar de forma única e inequívoca.

Atributos**:**

Atributo	Tipo	Descripción
idProceso	Secuencial	Identificador único del proceso dentro del sistema de seguridad informática.
nombre	String	Nombre del proceso. Debe ser único.
fecha	DateTime	Fecha de creación del proceso
eliminado	Boolean	Indica si el proceso ha sido eliminado (‘S’ , ‘N’)

Relaciones:

Entidad Relacionada	Cardinalidad	Descripción
ProcesoGestion *Tiene* Vulnerabilidad	1 : 0..*	Un proceso puede tener una, múltiples o ninguna vulnerabilidad.
ProcesoGestion *Tiene* AuditoriaProceso	1..* a 1..* a 0..*	Relación ternaria con entidad asociativa, que indica que en una Auditoria dada se pueden analizar uno o varios procesos de gestión, para los que se revisará el cumplimiento de una o varias políticas de seguridad

2. Vulnerabilidad

En esta entidad se almacenan cada una de las vulnerabilidades identificadas en los distintos procesos de gestión de la empresa. Estas vulnerabilidades se deben identificar de forma única e inequívoca.

Atributos**:**

Atributo	Tipo	Descripción
idVulnerabilidad	Secuencial	Identificador único de la vulnerabilidad dentro del sistema de seguridad informática.
descripción	String	Descripción de la vulnerabilidad encontrada
estado	String	Estados Vulnerabilidad: - identificada - no mitigada - parcialmente mitigada - totalmente mitigada.
esCritica	boolean	Indica si la vulnerabilidad es crítica o no
fecha	DateTime	Indica la fecha y hora en que se da de alta la vulnerabilidad en el sistema

Relaciones**:**

Entidad1<*Relación*>Entidad2	Cardinalidad	Descripción
Proceso *Tiene* Vulnerabilidad	1 : 0..*	Un proceso puede tener una, múltiples o ninguna vulnerabilidad
Vulnerabilidad *Requiere de* AcciónMitigacion	1 : 0..*	Una vulnerabilidad puede requerir de una, múltiples o ninguna acción de mitigación

Vulnerabilidad *Es Creada* Por Usuario	0..* : 1	Un usuario puede crear una, múltiples o ninguna vulnerabilidad
Vulnerabilidad *Creada en* Auditoria	0..* : 0..1	Una vulnerabilidad puede ser creada o no durante una auditoria

3. AcciónMitigación

En esta entidad se almacenan cada una de las Acciones de Mitigación creadas para las distintas vulnerabilidades detectadas. Estas acciones se deben identificar de forma única e inequívoca.

Atributos**:**

Atributo	**Tipo**	**Descripción**
idAccion	Secuencial	Identificador único de la acción de mitigación dentro del sistema de seguridad informática.
descripción	String	Descripción de la acción de mitigación
estado	String	Estados Vulnerabilidad: - definida - en proceso - Acabada - en revisión
fecha	DateTime	Fecha de creación de la acción
fechaInicio	DateTime	Indica la fecha y hora en que se inicia la acción de mitigación
fechaFin	DateTime	Indica la fecha y hora en que se finaliza la acción de mitigación
fechaLimite	DateTime	Indica la fecha y hora límite para finalizar la acción de mitigación

Relaciones:

Entidad1<*Relación*>Entidad2	**Cardinalidad**	**Descripción**
Vulnerabilidad *Requiere de* AcciónMitigacion	1 : 0..*	Una vulnerabilidad puede tener una, múltiples o ninguna acción de mitigación
Usuario *es Responsable de* Acción de Mitigación	1 : 0..*	Un usuario puede ser responsable de una, múltiples o ninguna Acción de Mitigación

4. PolíticaSeguridad

Esta entidad representa las políticas de seguridad que se crean en la empresa. El cumplimiento de estas políticas será evaluado para la detección de incumplimientos. Cada una de estas políticas se debe identificar de forma única e inequívoca.

Atributos:

Atributo	**Tipo**	**Descripción**
idPolitica	Secuencial	Identificador único de la política dentro del sistema de seguridad informática.
nombre	String	Nombre de la política
fecha	DateTime	Fecha y hora en que se crea la política de seguridad

Relaciones:

Entidad1<*Relación*>Entidad2	**Cardinalidad**	**Descripción**
Política *Tiene* Incumplimiento	1 : 0..*	Una política puede tener uno, múltiples o ningún incumplimiento
Política de Seguridad *Tiene* AuditoriaProceso	1..* a 1..* a 0..*	Relación ternaria con entidad asociativa, que indica que en una Auditoria dada se pueden analizar uno o varios procesos de gestión, para los que se revisará el cumplimiento de una o varias políticas de seguridad

5. Auditoria

Esta entidad representa las auditorias, tanto internas como externas, que se realizan a los procesos de gestión y políticas de seguridad de la empresa. Cada una de estas Auditorias se debe identificar de forma única e inequívoca.

Atributos:

Atributo	**Tipo**	**Descripción**
idAuditoria	Secuencial	Identificador único de la auditoria dentro del sistema de seguridad informática.
resultado	String	Resultado obtenido en la auditoria
fechaInicio	DateTime	Fecha y hora en que se inicia la auditoria
fechaFin	DateTime	Fecha y hora en que se finaliza la auditoria

Relaciones:

Entidad1<*Relación*>Entidad2	**Cardinalidad**	**Descripción**
Auditoria *Detecta* Incumplimiento	1 : 0..*	En una Auditoria se puede o no detectar uno, múltiples o ningún incumplimiento
Auditoria *Tiene* AuditoriaProceso	0..* a 1..* a 1..*	Relación ternaria con entidad asociativa, que indica que en una Auditoria dada se pueden analizar uno o varios procesos de gestión, para los que se revisará el cumplimiento de una o varias políticas de seguridad
Auditoria *Es Realizada* Por Usuario	0..* : 1	Una auditoria puede ser realizada por un usuario
Auditoria *Recoge* Muestreo	1 : 0..*	Una auditoria puede recoger uno, múltiples o ningún muestreo
Auditoria *Crea* Vulnerabilidad	0..* : 0..1	En una auditoria puede crearse una, múltiples o ninguna vulnerabilidad

6. AuditoriaProceso

Esta entidad asociativa se crea para representar la relación ternaria entre las auditorias, los procesos de gestión y las políticas de seguridad de la empresa. Se opta por una entidad asociativa debido a la cardinalidad múltiple de las distintas entidades que participan en la relación.

Atributos: *Sin atributos*

Relaciones:

Entidad1<*Relación*>Entidad2	**Cardinalidad**	**Descripción**
AuditoriaProceso *Asocia* Auditoria, Política de seguridad y Proceso de Gestión	0..* a 1..* a 1..*	Relación ternaria con entidad asociativa, que indica que en una Auditoria dada se pueden analizar uno o varios procesos de gestión, para los que se revisará el cumplimiento de una o varias políticas de seguridad

7. Muestreo

Esta entidad representa los muestreos que son recogidos durante las auditorias realizadas en la empresa. Cada uno de estos muestreos se debe identificar de forma única e inequívoca.

Atributos:

Atributo	**Tipo**	**Descripción**
idMuestreo	Secuencial	Identificador único de la auditoria dentro del sistema de seguridad informática.
muestra	String	Contenido de la muestra obtenida en la auditoria

Relaciones:

Entidad1<*Relación*>Entidad2	**Cardinalidad**	**Descripción**
Muestreo *Es Recogido* Auditoria	1..* : 1	Un muestreo dado solo puede ser recogido durante una auditoria

8. Incumplimiento

Esta entidad representa los incumplimientos de la política de seguridad que se detectan en la empresa. Cada instancia de esta entidad representa un hecho/incumplimiento concreto. Cada una de estos incumplimientos se debe identificar de forma única e inequívoca.

Atributos:

Atributo	**Tipo**	**Descripción**
idIncumplimiento	Secuencial	Identificador único del incumplimiento dentro del sistema de seguridad informática.
descripción	String	Descripción del incumplimiento
fecha	DateTime	Fecha y hora en que se ha realizado el incumplimiento

Relaciones:

Entidad1<*Relación*>Entidad2	**Cardinalidad**	**Descripción**
Política *Tiene* Incumplimiento	1 : 0..*	Una política puede tener uno, múltiples o ningún incumplimiento
Incumplimiento *Es Detectado en* SimulacionAtaque	0..* : 0..1	Un incumplimiento dado puede haber sido detectado, o no, durante una simulación de ataque
Incumplimiento *Es Detectado en* Auditoria	0..* : 0..1	Un incumplimiento dado puede haber sido detectado, o no, durante una auditoria
Incumplimiento *Es Realizado por* Empleado	0..* : 1	Un incumplimiento dado es realizado por un empleado de la empresa
Incumplimiento *Se Asigna* AcciónPunitiva	0..* : 0..1	Un incumplimiento dado puede tener asignada o no una Acción Punitiva

9. SimulaciónAtaque

Esta entidad representa las simulaciones de ataques que se envían a un grupo de usuarios de la empresa. Cada una de estas simulaciones se debe identificar de forma única e inequívoca.

Atributos:

Atributo	**Tipo**	**Descripción**
idSimulación	Secuencial	Identificador único de la simulación dentro del sistema de seguridad informática.
descripción	String	Descripción de la simulación
fecha	DateTime	Fecha y hora en que se ha realizado la simulación

Relaciones:

Entidad1<*Relación*>Entidad2	**Cardinalidad**	**Descripcion**
SimulacionAtaque *Se Envía* Empleado	* : 1..*	Una simulación puede enviarse a uno o múltiples empleados
SimulacionAtaque *Detecta* Incumplimiento	0..1 a 0..*	Una simulación puede detectar de uno o múltiples Incumplimientos

10. AccionPunitiva

Esta entidad representa las acciones punitivas que se pueden asignar a los empleados tras haber detectado algún incumplimiento de las políticas de seguridad de la empresa. Cada una de estas acciones se debe identificar de forma única e inequívoca.

Atributos:

Atributo	Tipo	Descripción
idAccion	String	Identificador único de la accion punitiva dentro del sistema de seguridad informática. Dado que se trata de un numero reducido de acciones punitivas posibles, no se require un identificador secuencial, sino que se utilizara un String.
tipo	String	Tipos de acción punitiva: - Traslado - Suspensión de empleo y sueldo - Amonestación escrita - Amonestación verbal - Despido disciplinario

Relaciones:

Entidad1<*Relación*>Entidad2	Cardinalidad	Descripcion
AccionPunitiva *Es Asignada* Incumplimiento	0..1 : 0..*	Una accion punitiva puede ser asignada o no a uno, multiples o ningun incumplimiento

11. Usuario

Esta entidad representa el conjunto de todos los usuarios que pueden utilizar el sistema informatico de la empresa, sean usuarios internos o externos. Cada uno de estos usuarios se debe identificar de forma única e inequívoca. Debido a las restricciones de confidencialidad de la empresa, no debemos registrar información personal de los usuarios.

Atributos:

Atributo	Tipo	Descripcion
idUsuario	String	Identificador único del usuario dentro del sistema de seguridad informática. Este identificador viene dado de la base de datos de la empresa, la cual guarda la información personal del usuario, por lo que no es secuencial.
Tipo	String	Tipo de Usuario: - Interno - Externo
eliminado	Boolean	Indica si el usuario ha sido eliminado (‘S’ , ‘N’)

Relaciones:

Entidad1<*Relación*>Entidad2	Cardinalidad	Descripcion
Usuario *es Responsable* AccionMitigación	1 : 0..*	Un usuario puede ser responsable de una, multiples o ninguna acción de mitigacion
Usuario *Crea* Vulnerabilidad	1 : 0..*	Un usuario puede crear una, multiples o ninguna vulnerabilidad en el sistema
Usuario *es Auditor* Auditoria	1 : 0..*	Un usuario puede ser el Auditor en una, multiples o ninguna auditorias
Usuario *Registra* Log	1 : 0..*	Un usuario puede registrar uno, multiples o ningun log

12. Empleado→Usuario

Esta entidad representa el conjunto de empleados de la empresa, sean internos o externos. Todos los empleados son a su vez usuarios, de manera que la entidad Empleado hereda de la entidad Usuario, y por ende, mantiene los mismos atributos y relaciones.
La principal diferencia entre un empleado y un usuario, es que todos los empleados deben pertenecer a algún departamento, mientras que los usuarios no. Un ejemplo de estos últimos podrían ser los usuarios externos que analizan el sistema de forma inicial para buscar vulnerabilidades, o incluso aquellos que realizan acciones correctivas.

Atributos: *Todas los de la entidad "Usuario".*

Relaciones: Todas las de la entidad "Usuario", además de :

Entidad1<*Relación*>Entidad2	**Cardinalidad**	**Descripción**
Empleado *Pertenece A* Departamento	0..* : 1	Un empleado pertenece solo a un departamento de la empresa
Empleado *Participa En* sesión Formativa	0..* : 0..*	Un empleado puede participar en una, múltiples o ninguna sesión formativa
Empleado *Se le Envia* SimulaciónAtaque	1..* : 0..*	Un empleado puede recibir una, múltiples o ninguna Simulación de Ataque
Empleado *Realiza* Incumplimiento	1 : 0..*	Un empleado puede realizar uno, múltiples o ningún Incumplimiento

13. Departamento

Esta entidad representa todos los departamentos que existen dentro de la empresa. Cada uno de estos departamentos se debe identificar de forma única e inequívoca.

Atributos:

Atributo	**Tipo**	**Descripción**
idDepartamento	String	Identificador único del departamento dentro del sistema de seguridad informática. Este identificador viene dado de la base de datos de la empresa, por lo que no es secuencial.
nombre	String	Nombre del departamento. El nombre del departamento debe ser unico.

Relaciones:

Entidad1<*Relación*>Entidad2	**Cardinalidad**	**Descripción**
Departamento *Pertenecen* Empleado	1 : 0..*	A un departamento pueden pertenecer uno, múltiples o ningún empleado

14. SesionFormativa

Esta entidad representa todas las sesiones formativas en políticas de seguridad realizadas en la empresa. Cada una de estas sesiones se debe identificar de forma única e inequívoca.

Atributos:

Atributo	Tipo	Descripción
idSesion	Secuencial	Identificador único de la sesión de formación dentro del sistema de seguridad informática.
titulo	String	Titulo de la sesión de formación
formato	String	Formato de la sesión: - Telemática - Presencial
fecha	DateTime	Fecha de realización de la sesión de formación

Relaciones:

Entidad1<*Relación*>Entidad2	Cardinalidad	Descripción
SesiónFormativa *Participa* Empleado	0..* : 0..*	En una sesión formativa puede participar uno, múltiples o ningún empleado

15. Participacion

Esta entidad asociativa se crea para representar la relación entre las sesiones formativas y los empleados que se inscriben a la misma. Se opta por una entidad asociativa debido a la cardinalidad múltiple de las distintas entidades que participan en la relación.

Atributos:

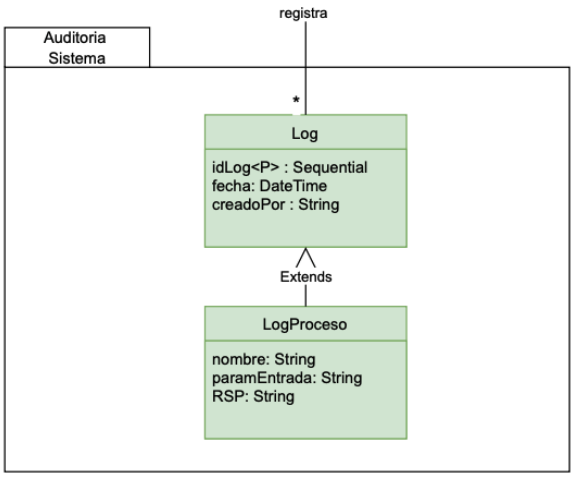
Atributo	**Tipo**	**Descripcion**
esAcabada	Boolean	Indica si el empleado ha acabado la formación

Relaciones:

Entidad1<*Relación*>Entidad2	**Cardinalidad**	**Descripción**
Participacion *Asocia* Empleado y SesiónFormativa	0..* : 0..*	relación con entidad asociativa, que indica que en una Participación se puede asociar a un Empleado con una o varias sesiones formativas, y a una sesión formativa con uno o varios empleados

3.1.2.2 Auditoria del Sistema

Aquí se muestran las entidades creadas para almacenar los registros de los eventos o *logs* de todas las operaciones que se realizan, y que sirven para auditar el sistema.



1. Log

Esta entidad representa todos los *logs* que se guardan en el sistema. Un log es un registro que guarda un acontecimiento o evento sucedido en un sistema informático, y que se utiliza como evidencia del comportamiento que tiene el sistema. El Log es útil para los procesos de auditorias de sistema y para la localización de fallos y errores. Cada Log se debe identificar de forma única e inequívoca.

Atributos:

Atributo	**Tipo**	**Descripción**
idLog	String	Identificador único del log dentro del sistema de seguridad informática
fecha	DateTime	Fecha en que se registra el evento o proceso al que se refiere el log
creadoPor	String	Usuario que ha realizado la acción que ha generado el log

Relaciones:

Entidad1<*Relación*>Entidad2	**Cardinalidad**	**Descripción**
Log *es Registrado Por* Usuario	0..* : 1	Un log solo puede ser creado por un único usuario

2. LogProceso→Log

Esta entidad representa los logs de los procesos creados en el sistema. Como se puede observar en el diagrama conceptual, esta entidad hereda de Log, por lo que recibe los mismos atributos y relaciones.

Atributos: *Todos los de la entidad "Log", además de:*

Atributo	**Tipo**	**Descripción**
nombre	String	Nombre que recibe el proceso que se registra en el sistema
paramEntrada	String	Indica los parámetros de entrada que se reciben para ejecutar el proceso.
RSP	String	Indica el parámetro de salida o respuesta recibida tras la ejecución del proceso. Si la ejecución ha finalizado correctamente se guardará el valor 'OK', pero si ha

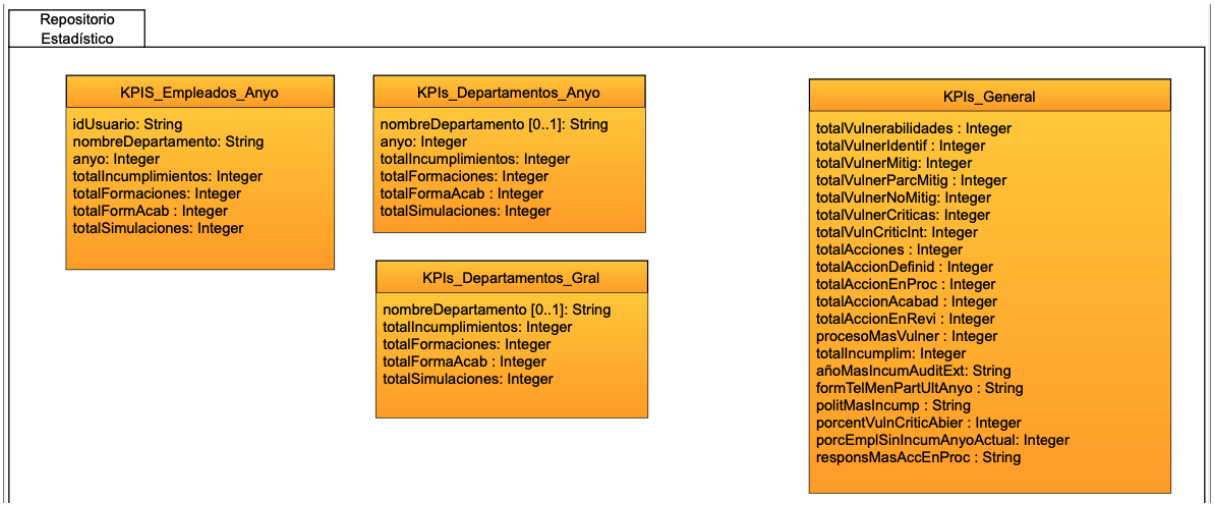
		fracasado se guardará el valor 'ERROR + TIPO DE ERROR'.

Relaciones:

Todas las de la entidad "Log".

3.1.2.3 Repositorio Estadístico

En este grupo se incluyen las entidades necesarias para guardar los datos históricos que se consultaran como parte del repositorio estadístico.



1. **KPIs_Empleados_Anyo**

Esta entidad representa varios indicadores clave de negocio asociados a los empleados del sistema, agrupados por año. Se entiende por "Empleados" aquellos usuarios que están asociados a un departamento de la empresa; se excluyen por tanto aquellos usuarios que no forman parte de ningún departamento de la empresa (ejemplo, Auditores Externos).
En esta entidad se guardará un registro por cada empleado y año, con sus principales indicadores.

Nota: A pesar de que en los requisitos del enunciado no se solicitan tantos indicadores asociados a cada empleado, nos parece útil proporcionar esta información en una misma tabla/histórico, por si en el futuro fuese necesario incorporar otras consultas al repositorio estadístico.

Atributos:

Atributo	**Tipo**	**Descripción**
idEmpleado	String	Identificador único del empleado
nombreDepartamento	String	Departamento al que pertenece el empleado

anyo	Integer	Año al que corresponden los indicadores de este usuario
totalIncumplimientos	Integer	Total de incumplimientos que ha realizado el usuario en el año
totalFormaciones	Integer	Total de formaciones que ha participado el usuario en el año
totalFormAcab	Integer	Total de formaciones que ha acabado el usuario en el año
totalSimulaciones	Integer	Total de simulaciones que ha recibido el usuario en el año

2. KPI_Departamentos_Anyo

Esta entidad representa los indicadores clave de negocio asociados a los departamentos de la empresa, agrupados por año. Existe un registro por cada departamento y año, con sus principales indicadores.

Nota: A pesar de que en los requisitos del enunciado no se solicitan tantos indicadores asociados a cada departamento, nos parece útil proporcionar esta información en una tabla/histórico, por si en el futuro fuese necesario incorporar otras consultas al repositorio estadístico.

Atributos:

Atributo	**Tipo**	**Descripción**
nombreDepartamento	String	Nombre del Departamento
anyo	Integer	Año al cual corresponden los indicadores del departamento
totalIncumplimientos	Integer	Total de incumplimientos que han realizado los empleados del departamento
totalFormaciones	Integer	Total de empleados que tiene alguna formacion asignada
totalFormAcab	Integer	Total de empleados que han acabado todas sus formaciones asignadas
totalSimulaciones	Integer	Total de simulaciones que ha recibido el departamento

3. KPI_Departamentos_Gral

Esta entidad representa los indicadores clave de negocio asociados a los departamentos de la empresa, teniendo en cuenta toda la información que se encuentra en la Base de datos. Existe un registro por cada departamento, con sus principales indicadores.

Nota: A pesar de que en los requisitos del enunciado no se solicitan tantos indicadores asociados a cada departamento, nos parece útil proporcionar esta información en una tabla/histórico, por si en el futuro fuese necesario incorporar otras consultas al repositorio estadístico.

Atributos:

Atributo	**Tipo**	**Descripción**
nombreDepartamento	String	Nombre del Departamento
totalIncumplimientos	Integer	Total de incumplimientos que han realizado los empleados del departamento
totalFormaciones	Integer	Total de empleados que tiene alguna formacion asignada
totalFormAcab	Integer	Total de empleados que han acabado todas sus formaciones asignadas
totalSimulaciones	Integer	Total de simulaciones que ha recibido el departamento

porcentEmplSinIncump	Integer	Porcentaje de empleados sin ningún incumplimiento detectado durante el año
responsMasAccEnProc	String	Identificador del usuario responsable con mas acciones "En Proceso" creadas durante el año

4. KPIs_General

Esta entidad representa una variedad de indicadores clave de negocio, obtenidos de todos los datos históricos del sistema. En esta tabla se guardará solo un único registro, con todos los indicadores.

Nota: A pesar de que en los requisitos del enunciado no se solicitan tantos indicadores generales, nos parece útil proporcionar esta información en una tabla/histórico, por si en el futuro fuese necesario incorporar otras consultas al repositorio estadístico.

Atributos:

Atributo	**Tipo**	**Descripción**
totalVulnerabilidades	Integer	Total de vulnerabilidades detectadas
totalVulnerIdentif	Integer	Total de Vulnerabilidades en estado: Identificada
totalVulnerMitig	Integer	Total de Vulnerabilidades en estado: Mitigada
totalVulnerParcMitig	Integer	Total de Vulnerabilidades en estado: Parcialmente Mitigada
totalVulnerNoMitig	Integer	Total de Vulnerabilidades en estado: No Mitigada
totalVulnerCriticas	Integer	Total de Vulnerabilidades Críticas
totalVulnCriticInt	Integer	Total de Vulnerabilidades Críticas Internas
totalAccionMitig	Integer	Total de acciones de mitigación
totalAccMitDefinid	Integer	Total de acciones de mitigación en estado : Definidas
totalAccMitEnProc	Integer	Total de acciones de mitigación en estado : En Proceso
totalAccMitAcabad	Integer	Total de acciones de mitigación en estado : Acabadas
totalAccMitEnRevi	Integer	Total de acciones de mitigación en estado : En revisión
procesoMasVulner	String	Nombre del proceso que ha tenido más vulnerabilidades
totalIncumplim	Integer	Total de incumplimientos realizados
formacMenosPartic	String	Título de la sesión con menos participación
politMasIncump	String	Nombre de la política que ha tenido mas incumplimientos
porcentVulnCriticAbierta	Integer	Porcentaje de Vulnerabilidades Criticas Abiertas
porcentEmplSinIncump	Integer	Porcentaje de empleados sin ningún incumplimiento asignado
responsMasAccEnProc	String	Identificador del usuario responsable con más acciones "En Proceso"
añoMasIncumAuditExt	Integer	Año en el que se detectaron más incumplimientos en una Auditoría Externa

3.2 Estrategia para Repositorio estadístico – Data Warehouse

Tal como se ha solicitado en los requisitos, se debe mantener un repositorio estadístico que permita un cierto tipo de consultas en base a la información contenida en el modelo de datos. Dichas consultas estadísticas deben realizarse, como máximo en un tiempo constante (1).

Para ello, se utilizarán técnicas de data warehouse o almacenes de datos, con el objetivo de optimizar la realización de estas consultas.

Se ha decidido crear una serie de tablas, en las cuales se guardarán únicamente los datos históricos calculados utilizando los datos de las tablas de operaciones. Estas tablas serán las que se utilicen para realizar las búsquedas del repositorio estadístico.

La estrategia utilizada para modelar las entidades del repositorio estadístico ha sido la de crear, por un lado, varias entidades llamadas "KPIs_Empleados_anyo" y "KPIs_Departamentos_anyo". En cada una de estas entidades se guardan los indicadores correspondientes a los principales usuarios del Proceso de Seguridad de la empresa: Los empleados y los Departamentos, agrupados por año.

Por otro lado, se crean dos tablas más: "KPIs_Departamentos_Gral y "KPIs_General", que tal como su nombre indica, guardan distintos indicadores, teniendo en **toda** la información guardada en el sistema hasta la fecha.

Con este mecanismo se garantiza que se puede escalar el Data Warehouse para hacer estadísticas con un mayor nivel de granularidad (se puede reducir a datos agrupados por mes o por semana), o simplemente añadiendo nuevas tablas por otro tipo de entidad.

Dado que en los requerimientos se prohíbe el uso de funciones agregadas (COUNT(); SUM(), etc.), será necesario crear una serie de procedimientos, los cuales irán calculando y actualizando cada uno de estos indicadores. Para mantener actualizadas dichas tablas, se recomienda la creación de *Jobs* o tareas programadas, las cuales ejecutaran los procedimientos del repositorio estadístico de forma periódica según las necesidades (cada día, cada hora, etc).

Por último, se han incluido muchos más indicadores que los mínimos requeridos en el enunciado, ya que se entiende que los mismos pueden ser relevantes para el repositorio estadístico, y con este enfoque, se facilita la escalabilidad del repositorio para incluir más consultas en el futuro.

3.3 Diseño Lógico

Esta es la segunda fase del diseño de la base de datos. El objetivo de esta etapa es transformar el esquema conceptual del paso anterior a un modelo lógico de datos, para una base de datos relacional.

A continuación se detallan de los conceptos más importantes utilizados para modelar el esquema lógico, su definición y su notación:

- Relación: es el elemento principal y está formada por un grupo de atributos que pueden expresarse dentro de un dominio concreto. Se denota con el nombre de la relación y sus atributos encerrados entre paréntesis.

- Tupla: Consiste en los valores dentro del dominio que corresponden a los distintos atributos de una relación.

- Clave Candidata: Consiste en uno o más atributos de la relación cuyos valores no pueden repetirse en dos o más tuplas diferentes; tampoco pueden contener valores nulos. Se denotan subrayando el atributo(s) con una línea continua.

- Clave Primaria: Es una clave candidata que se elige para identificar una tupla en concreto. Se identifican con la restricción *Primary Key.* Se denotan subrayando el atributo(s) con una línea continua.

- Clave Alternativa: Son aquellas claves candidatas que no han sido elegidas como clave primaria. Se identifican con la restricción *Unique.* Se denotan subrayados con línea discontinua.

- Clave Foránea: Cuando dentro de una relación (R1) se utiliza un atributo que es clave candidata en otra relación (R2) para referenciar los datos de una tupla concreta. Se identifican con la restricción *Foreign Key,* y se denota con la expresión "Atributo *is foreign key to* Relación"

- Valores obligatorios: Se utiliza para aquellos atributos mandatorios, es decir, que no pueden permitir valores nulos. Se identifican con la restricción NOT NULL. Se denotan resaltándolos en **negrita**

3.3.1 Estrategia diseño lógico

Respecto a la estrategia que se ha utilizado para definir las relaciones del esquema lógico, teniendo en cuenta su cardinalidad y tipo de la relación, se puede resumir a continuación:

- Cardinalidad de 1 a 1: clave foránea en alguna de las entidades de la relación
- Cardinalidad de 1 a *: clave foránea en la entidad con cardinalidad *
- Cardinalidad de * a *: se crea una nueva entidad incluyendo las claves foráneas de todas las demas entidades
- Cardinalidad de 1 a 0..1: se crea una nueva entidad incluyendo las claves foráneas de ambas entidades, para evitar la presencia de valores nulos (NULL)
- Cardinalidad de * a 0..1 a: se crea una nueva entidad incluyendo las claves foráneas de ambas entidades, para evitar la presencia de valores nulos (NULL)
- Relaciones de Composición: clave foránea en la entidad dependiente.

Finalmente, se detalla a continuación el esquema lógico del sistema:

3.3.2 Procesos Seguridad:

1. ProcesoGestion (idProceso, nombre, **fecha**, **eliminado**)

2. Vulnerabilidad (idVulnerabilidad,**idProceso descripción**, **estado**, **esCritica**, **fecha**, **creadaPor**)
   {idProceso} is foreign key to ProcesoGestion
   {creadaPor} is foreign key to Usuario

3. AccionMitigacion (idAccion, **idVulnerabilidad**, **descripción**, **fechaLimite**, fechaInicio, fechaFin, **fecha**, **estado**, **responsable**)
   {idVulnerabilidad} is foreign key to Vulnerabilidad
   {responsable} is foreign key to Usuario
   Check(fechaFin >= fechaInicio)

4. PoliticaSeguridad (idPolitica, nombre, **fecha**)

5. Incumplimiento (idIncumplimiento, **idPolitica**, **descripción**, **fecha**, **realizadoPor**)
   {idPolitica} is foreign key to PoliticaSeguridad
   {realizadoPor} is foreign key to Empleado

6. AccionPunitiva (idAccion, **tipo**)

7. IncumplimientoAccion (idIncumplimiento, idAccionPunit)
   {idIncumplimiento} is foreign key to Incumplimiento
   {idAccionPunit} is foreign key to AccionPunitiva

8. Auditoria (idAuditoria, **fechaInicio**, fechaFin, **resultado**, **creadaPor**)
   {creadaPor} is foreign key to Usuario
   Check(fechaFin IS NULL OR fechaFin >= fechaInicio)

9. Muestreo (idMuestra, **idAuditoria**, **muestra**)
   {idAuditoria} is foreign key to Auditoria

10. IncumplimientoAuditoria (idIncumplimiento, idAuditoria)
    {idIncumplimiento} is foreign key to Incumplimiento
    {idAuditoria} is foreign key to Auditoria

11. VulnerabilidadAuditoria (idVulnerabilidad, idAuditoria)
    {idVulnerabilidad} is foreign key to Vulnerabilidad
    {idAuditoria} is foreign key to Auditoria

12. AuditoriaProceso (idAuditoria, idPolitica, idProceso)
    {idAuditoria} is foreign key to Auditoria
    {idPolitica} is foreign key to Politica
    {idProceso} is foreign key to Proceso

13. SimulacionAtaque (idSimulacion, **descripción**, **fecha**)

14. IncumplimientoSimulacion (idIncumplimiento, idSimulacion)

{idSimulacion} is foreign key to Simulacion
{idIncumplimiento} is foreign key to Incumplimiento

15. SimulacionEmpleado(idSimulacion, idEmpleado)
{idSimulacion} is foreign key to Simulacion
{idEmpleado} is foreign key to Empleado

16. Departamento (idDepartamento, nombre)

17. Empleado (idEmpleado, **idDepartamento**)
{idDepartamento} is foreign key to Departamento
{idEmpleado} is foreign key to Usuario

18. Usuario (idUsuario, **tipoUsuario**, **eliminado**)

19. SesionFormativa (idSesion, **titulo**, **formato**, **fecha**)

20. Participacion (idEmpleado, idSesion, **esAcabada**)
{idEmpleado} is foreign key to Empleado
{idSesion} is foreign key to SesionFormativa

Como se ha podido observar, tras realizar el esquema lógico y aplicar la estrategia de crear nuevas relaciones (en algunos casos) según la cardinalidad y el tipo de relación, nuestro esquema ha pasado de tener 16 entidades en el modelo conceptual a tener 20 relaciones en el modelo lógico.

3.3.3 Auditoria Sistema

1. Log (idLog, **fecha**, **creadoPor**)
   {idUsuario} is foreign key to Usuario

2. LogProceso (idLog, **nombre**, **paramEntrada**, paramSalida, **RSP**)
   {idLog} is foreign key to Log

3.3.4 Repositorio Estadístico

1. KPIs_Empleados_Anyo (idEmpleado, nombreDepartamento, anyo, totalIncumplimientos, totalFormaciones, totalFormAcab, totalSimulaciones)

2. KPIs_Departamentos_Anyo (idDepartamento, nombreDepartamento, anyo, totalIncumplimientos, totalFormaciones, totalFormAcab, totalSimulaciones)

3. KPIs_Departamentos_Gral (idDepartamento, nombreDepartamento, totalIncumplimientos, totalFormaciones, totalFormAcab, totalSimulaciones)

4. KPIs_General (totalVulnerabilidades, totalVulnerIdentif, totalVulnerMitig, totalVulnerParcMitig, totalVulnerNoMitig, totalVulnerCriticas, totalVulnCriticInt, totalAcciones, totalAccionDefinid, totalAccionEnProc, totalAccionAcabad, totalAccionEnRevi, procesoMasVulner, totalIncumplim,

```
añoMasIncumAuditExt, formacMenosPartic, politMasIncump,
porcentEmplSinIncump, responsMasAccEnProc)
```

3.4 Diseño Físico

Esta es la tercera y última fase del diseño de la BD. Se trata adaptar el esquema lógico obtenido en la fase anterior al Sistema Gestor de Base de Datos (SGBD).

Tal como se ha comentado en el apartado de "Recursos del Proyecto", se utiliza el SGBD de *Oracle*, versión *Express Edition 11g R2*, así como la IDE de *Oracle SQL Developer* para mayor comodidad en la visualización de datos y manejo de los Scripts.

3.4.1 Creación de la Base de Datos en el SGBD

Tras la instalación del software necesario, se ejecutan los primeros pasos para la creación del proyecto de Base de Datos en el SGBD, los cuales se resumen a continuación:

1. Creación de *tablespaces*: Se trata de los espacios virtuales donde se almacenarán los datos de la base de datos, distribuidos en tablas. Se ha creado un espacio virtual para almacenar los datos de "Procesos de Seguridad" y "Auditoria Sistema" . En este mismo espacio, también se guardan los datos del "Repositorio Estadístico" o Data warehouse. Esto último NO es la práctica habitual, ya que se deberían guardar en un espacio separado, utilizando otro espacio temporal para el tratamiento de datos. Sin embargo se tomó esta decisión bajo recomendación del profesor (En el apartado *1.4.8 Desviaciones en la planificación* de la Entrega final, se explica el motivo de esta decisión).

2. Creación de usuarios y asignación de permisos: Se trata de crear los usuarios que podrán acceder a la BD y otorgarles los permisos necesarios que les permitan realizar las operaciones requeridas para crear la estructura del *tablespace* y los datos (visualización, creación, borrado…).

3. Creación de Tablas: Las tablas son las estructuras donde finalmente se almacenan los datos. Las tablas son el equivalente a las relaciones obtenidas en el modelo lógico, por lo que en esta etapa se debe crear una tabla para cada relación. En este paso, también se incluye la creación de los distintos atributos, sus claves y restricciones correspondientes a cada tabla.

Los pasos anteriores se realizan con una serie de *Scripts* en el lenguaje SQL, los cuales se incluirán adjuntos como parte del producto/entregable final.

3.4.2 Tipos de Datos Utilizados

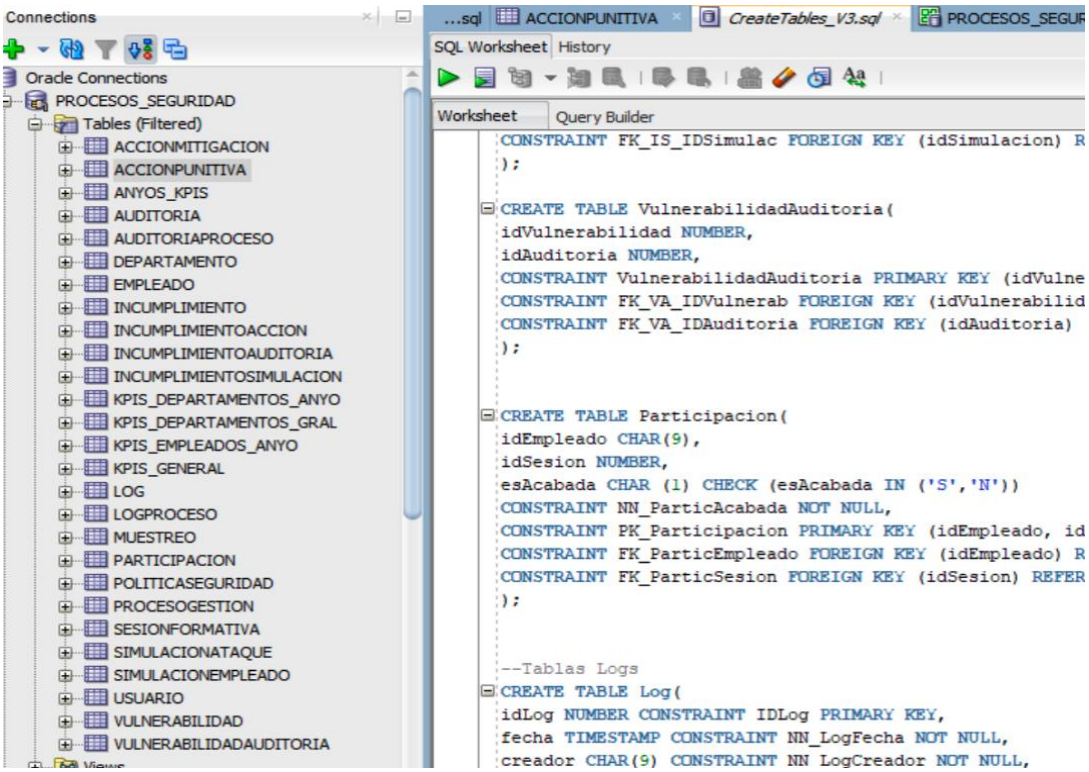
Este SGBD permite múltiples tipos de datos, aunque para la creación de las tablas solo se han requerido los tipos siguientes:

- NUMBER(precisión): Utilizado para almacenar valores numéricos fijos o con punto flotante.

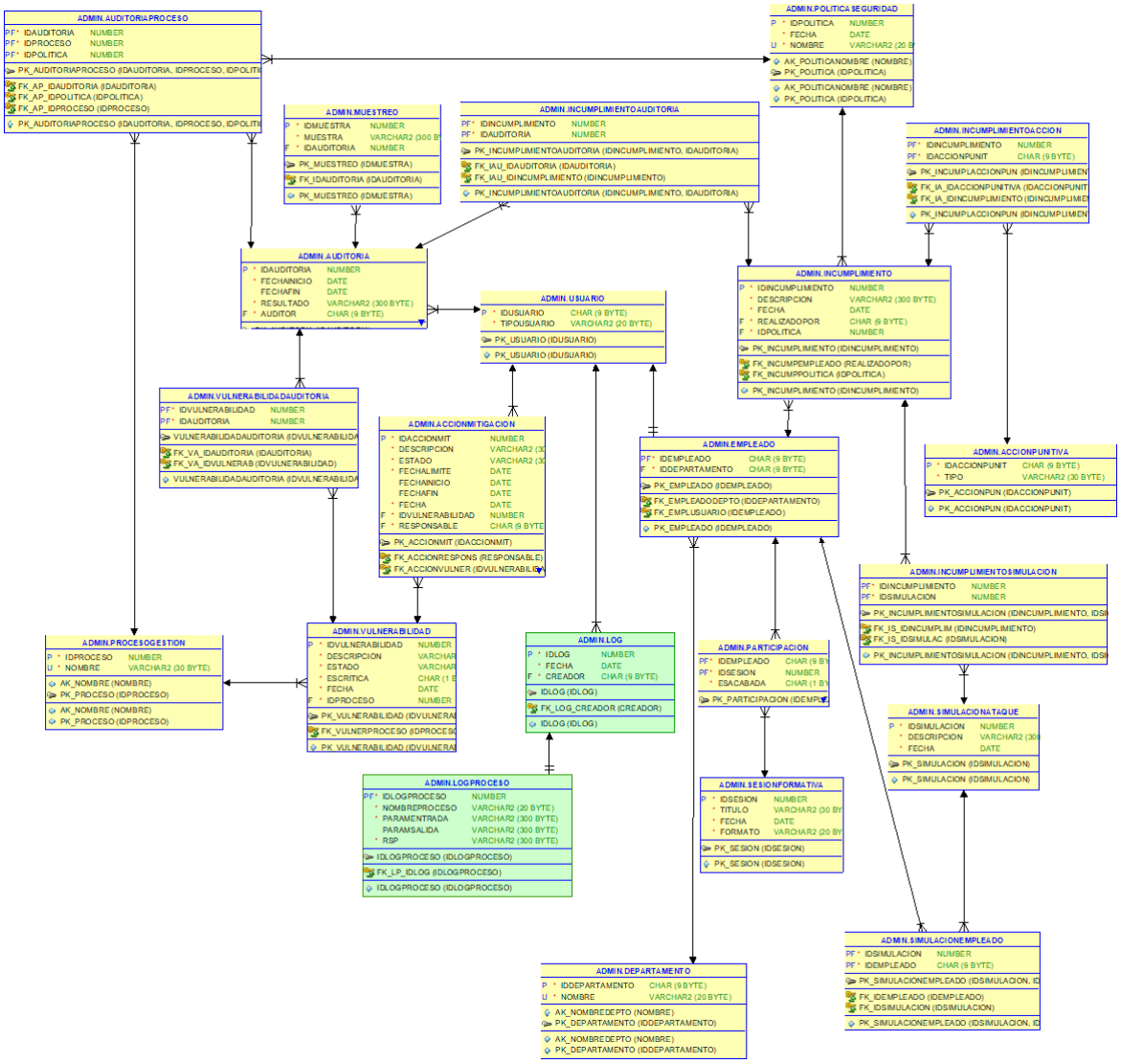
- TIMESTAMP : Utilizado para almacenar una fecha y hora concreta
- CHAR (tamaño) : Utilizado para almacenar caracteres de longitud fija.
- VARCHAR2 (tamaño) : Utilizado para almacenar caracteres de longitud Variable.

3.4.3 Diagrama Entidad Relación

A continuación mostramos una captura del *SQL Developer* con la vista de todas las tablas creadas para el tablespace "Procesos_Seguridad", seguido del Diagrama ER, realizado con el *Data Modeler* de Oracle:



Vista tablas Procesos_Seguridad



Modelo ER de la Base de Datos

3.4.4 Tablas Proceso de Seguridad

1. ProcesoGestion

Esta tabla representa el cúmulo de todos los procesos de gestión de la empresa. Dichos procesos de gestión serán objeto de análisis para la detección de posibles vulnerabilidades a nivel informático. Cada uno de estos procesos se debe identificar de forma única e inequívoca.

	Columna	Tipo Dato	Nullable	Descripción
PK	idProceso	NUMBER	No	Identificador único del proceso dentro del sistema de seguridad informática.
AK	nombre	VARCHAR2(30)	No	Nombre del proceso. Debe ser único.
	fecha	TIMESTAMP	No	Fecha y hora de creación del proceso
	eliminado	CHAR(1)	No	Si el proceso ha sido eliminado (‘S’) o no (‘N’)

2. Vulnerabilidad

En esta tabla se almacenan cada una de las vulnerabilidades identificadas en los distintos procesos de gestión de la empresa. Estas vulnerabilidades se deben identificar de forma única e inequívoca.

	Columna	Tipo Dato	Nullable	Descripción
PK	idVulnerabilidad	NUMBER	No	Identificador único de la vulnerabilidad dentro del sistema de seguridad informática.
	descripción	VARCHAR2(500)	No	Descripción de la vulnerabilidad encontrada
	estado	VARCHAR2(30)	No	Estados Vulnerabilidad: - identificada - no mitigada - parcialmente mitigada - totalmente mitigada.
	esCritica	VARCHAR2(30)	No	Indica si la vulnerabilidad es crítica o no
	fecha	TIMESTAMP	No	Indica la fecha y hora en que se da de alta la vulnerabilidad en el sistema
FK	idProceso	NUMBER	No	Identificador único del proceso donde se detecto la Vulnerabilidad.

3. AccionMitigacion

En esta tabla se almacenan cada una de las Acciones de Mitigación creadas para las distintas vulnerabilidades detectadas. Estas acciones se deben identificar de forma única e inequívoca.

	Columna	Tipo Dato	Nullable	Descripción
PK	idAccion	NUMBER	No	Identificador único de la acción de mitigación dentro del sistema de seguridad informática.
	descripción	VARCHAR2(300)	No	Descripción de la acción de mitigación
	estado	VARCHAR2(30)	No	Estados Vulnerabilidad: - definida - en proceso - Acabada - en revisión
	fecha	TIMESTAMP	No	Fecha y hora de creación de la acción

	fechaInicio	TIMESTAMP	Si	Indica la fecha y hora en que se inicia la acción de mitigación
	fechaFin	TIMESTAMP	Si	Indica la fecha y hora en que se finaliza la acción de mitigación
	FechaLimite	TIMESTAMP	No	Indica la fecha y hora límite para finalizar la acción de mitigación
FK	responsable	CHAR(9)	No	Indica el usuario responsable de ejecutar la acción
FK	idVulnerabilidad	NUMBER	No	Identificador único de la Vulnerabilidad que se subsanará con la acción.

4. PoliticaSeguridad

Esta tabla representa las políticas de seguridad que se crean en la empresa. El cumplimiento de estas políticas será evaluado para la detección de incumplimientos. Cada una de estas políticas se debe identificar de forma única e inequívoca.

	Columna	Tipo Dato	Nullable	Descripcion
PK	idPolitica	NUMBER	No	Identificador único de la política dentro del sistema de seguridad informática.
AK	nombre	VARCHAR2(30)	No	Nombre de la política
	fecha	TIMESTAMP	No	Fecha y hora en que se crea la política de seguridad

5. Auditoria

Esta tabla representa las auditorias, tanto internas como externas, que se realizan a los procesos de gestión y políticas de seguridad de la empresa. Cada una de estas Auditorias se debe identificar de forma única e inequívoca.

	Columna	Tipo Dato	Nullable	Descripción
PK	idAuditoria	NUMBER	No	Identificador único de la auditoria dentro del sistema de seguridad informática.
	resultado	VARCHAR2(300)	No	Resultado obtenido en la auditoria
	fechaInicio	TIMESTAMP	No	Fecha y hora en que se inicia la auditoria
	fechaFin	TIMESTAMP	No	Fecha y hora en que se finaliza la auditoria. Debe ser >= Fecha Inicio
FK	auditor	CHAR(9)	No	Indica el usuario responsable de ejecutar la auditoria

6. AuditoriaProceso

Esta tabla se representa la relación entre las auditorias, los procesos de gestión y las políticas de seguridad de la empresa. Se opta por una tabla asociativa debido a la cardinalidad múltiple de las distintas entidades que participan en la relación.

	Columna	Tipo Dato	Nullable	Descripción
PK FK	idPolitica	NUMBER	No	Identificador único de la política dentro del sistema de seguridad informática.
PK FK	idAuditoria	NUMBER	No	Identificador único de la Auditoria dentro del sistema de seguridad informática
PK FK	idProceso	NUMBER	No	Identificador único del Proceso dentro del sistema de seguridad informática

7. Muestreo

Esta tabla representa los muestreos que son recogidos durante las auditorías realizadas en la empresa. Cada uno de estos muestreos se debe identificar de forma única e inequívoca.

	Columna	Tipo Dato	Nullable	Descripción
PK	idMuestreo	NUMBER	No	Identificador único de la auditoria dentro del sistema de seguridad informática.
	muestra	VARCHAR2(300)	No	Contenido de la muestra obtenida en la auditoria
FK	idAuditoria	NUMBER	No	Identificador único de la Auditoria donde se obtuvo la muestra

8. Incumplimiento

Esta entidad representa los incumplimientos de las políticas de seguridad que se detectan en la empresa. Cada instancia de esta entidad representa un hecho/incumplimiento concreto. Cada una de estos incumplimientos se debe identificar de forma única e inequívoca.

	Columna	Tipo Dato	Nullable	Descripción
PK	idIncumplimiento	NUMBER	No	Identificador único del incumplimiento dentro del sistema de seguridad informática.
	descripcion	VARCHAR2(300)	No	Descripción del incumplimiento
	fecha	TIMESTAMP	No	Fecha y hora en que se ha realizado el incumplimiento
FK	idPolitica	NUMBER	No	Identificador único de la política que se ha incumplido
FK	realizadoPor	CHAR(9)	No	Identificador único del usuario que realizó el incumplimiento

9. VulnerabilidadAuditoria

En esta tabla se almacenan las distintas vulnerabilidades encontradas durante una auditoria. Se registrará una tupla por cada relación Vulnerabilidad-Auditoria.

	Columna	Tipo Dato	Nullable	Descripción
PK FK	idVulnerabilidad	NUMBER	No	Identificador único de la vulnerabilidad dentro del sistema de seguridad informática.
PK FK	idAuditoria	NUMBER	No	Identificador único de la Auditoria dentro del sistema de seguridad informática

10. IncumplimientoAuditoria

En esta tabla se almacenan los distintos incumplimientos encontrados durante una auditoria. Se registrará una tupla por cada relación Incumplimiento-Auditoria.

	Columna	Tipo Dato	Nullable	Descripción
PK FK	idIncumplimiento	NUMBER	No	Identificador único del incumplimiento dentro del sistema de seguridad informática.
PK FK	idAuditoria	NUMBER	No	Identificador único de la Auditoria dentro del sistema de seguridad informática

11. SimulaciónAtaque

Esta tabla representa las simulaciones de ataques que se envían a un grupo de usuarios de la empresa. Cada una de estas simulaciones se debe identificar de forma única e inequívoca.

	Columna	Tipo Dato	Nullable	Descripción
PK	idSimulacion	NUMBER	No	Identificador único de la simulación dentro del sistema de seguridad informática.
	descripcion	VARCHAR2(300)	No	Descripción de la simulación
	fecha	TIMESTAMP	No	Fecha y hora en que se ha realizado la simulación

12. IncumplimientoSimulacion

En esta tabla se almacenan los distintos incumplimientos encontrados durante una simulación de ataque. Se registrará una tupla por cada relación Incumplimiento-Simulación.

	Columna	Tipo Dato	Nullable	Descripción
PK FK	idIncumplimiento	NUMBER	No	Identificador único del incumplimiento dentro del sistema de seguridad informática.
PK FK	idSimulacion	NUMBER	No	Identificador único de la simulación dentro del sistema de seguridad informática.

13. SimulaciónEmpleado

En esta tabla se almacenan las distintas simulaciones de ataques y los empleados a los que han sido enviadas dentro la empresa. Se registrará una tupla por cada relación Simulación-Empleado.

	Columna	Tipo Dato	Nullable	Descripción
PK FK	idSimulacion	NUMBER	No	Identificador único de la simulación dentro del sistema de seguridad informática.
PK FK	idEmpleado	CHAR(9)	No	Identificador único del empleado dentro del sistema de seguridad informática. Este identificador viene dado de la base de datos de la empresa, la cual guarda la información personal del usuario, por lo que no es secuencial.

14. AccionPunitiva

Esta tabla representa las acciones punitivas que se pueden asignar a los empleados tras haber detectado algún incumplimiento de las políticas de seguridad de la empresa. Cada una de estas acciones se debe identificar de forma única e inequívoca.

	Columna	Tipo Dato	Nullable	Descripción
PK	idAccionPunit	CHAR(9)	No	Identificador único de la acción punitiva dentro del sistema de seguridad informática. Dado que solo existe un numero limitado de Acciones

				punitivas posibles, el identificador no es un incremental, sino un String.
	tipo	VARCHAR2(30)	No	Tipos de acción punitiva: - Traslado - Suspensión de empleo y sueldo - Amonestación escrita - Amonestación verbal - Despido disciplinario

15. IncumplimientoAccion

En esta tabla se almacenan las acciones punitivas asignadas por motivo de un incumplimiento. Se registrará una tupla por cada relación Incumplmiento-Accion.

	Columna	Tipo Dato	Nullable	Descripcion
PK FK	idIncumplimiento	NUMBER	No	Identificador único del incumplimiento dentro del sistema de seguridad informática.
PK FK	idAccionPunit	CHAR(9)	No	Identificador único de la acción punitiva dentro del sistema de seguridad informática.

16. Usuario

Esta tabla representa el conjunto de todos los usuarios que pueden utilizar el sistema informático de la empresa, sean usuarios internos o externos. Cada uno de estos usuarios se debe identificar de forma única e inequívoca. Debido a las restricciones de confidencialidad de la empresa, no debemos registrar información personal de los usuarios.

	Columna	Tipo Dato	Nullable	Descripción
PK	idUsuario	CHAR(9)	No	Identificador único del usuario dentro del sistema de seguridad informática. Este identificador viene dado de la base de datos de la empresa, la cual guarda la información personal del usuario, por lo que no es secuencial.
	tipo	VARCHAR2(20)	No	Tipo de Usuario: - Interno - Externo
	eliminado	CHAR(1)	No	Eliminado: S = Si / N = No

17. Empleado

Esta tabla representa el conjunto de empleados de la empresa, sean internos o externos. Todos los empleados son a su vez usuarios, de manera que la entidad Empleado hereda de la entidad Usuario, y por ende, mantiene los mismos atributos y relaciones.
La principal diferencia entre un empleado y un usuario, es que todos los empleados deben pertenecer a algún departamento, mientras que los usuarios no. Un ejemplo de estos últimos podrían ser los usuarios externos que analizan el sistema de forma inicial para buscar vulnerabilidades, o incluso aquellos que realizan acciones correctivas.

	Columna	Tipo Dato	Nullable	Descripción
PK FK	idEmpleado	CHAR(9)	No	Identificador único del usuario dentro del sistema de seguridad informática. Este identificador viene dado

				de la base de datos de la empresa, la cual guarda la información personal del usuario, por lo que no es secuencial.
FK	idDepartamento	CHAR(9)	No	Identificador único del departamento dentro del sistema de seguridad informática. Este identificador viene dado de la base de datos de la empresa, por lo que no es secuencial.

18. Departamento

Esta tabla representa todos los departamentos que existen dentro de la empresa. Cada uno de estos departamentos se debe identificar de forma única e inequívoca.

	Columna	Tipo Dato	Nullable	Descripción
PK	idDepartamento	CHAR(9)	No	Identificador único del departamento dentro del sistema de seguridad informática.
AK	nombre	VARCHAR2(20)	No	Identificador único del departamento dentro del sistema de seguridad informática. Este identificador viene dado de la base de datos de la empresa, por lo que no es secuencial.

19. SesiónFormativa

Esta tabla representa todas las sesiones formativas en políticas de seguridad realizadas en la empresa. Cada una de estas sesiones se debe identificar de forma única e inequívoco.

	Columna	Tipo Dato	Nullable	Descripción
PK	idSesion	NUMBER	No	Identificador único de la sesión de formacion dentro del sistema de seguridad informática.
	titulo	VARCHAR2(30)	No	Titulo de la sesión de formacion
	formato	VARCHAR2(20)	No	Formato de la sesión: - Telemática - Presencial
	fecha	TIMESTAMP	No	Fecha de realización de la sesión de formacion

20. Participacion

Esta tabla asociativa se crea para representar la relación entre las sesiones formativas y los empleados que se incriben a la misma. Se opta por una entidad asociativa debido a la cardinalidad múltiple de las distintas entidades que participan en la relación.

	Columna	Tipo Dato	Nullable	Descripción
PK FK	idSesion	NUMBER	No	Identificador único de la sesión a la que participo el empleado
PK FK	idEmpleado	CHAR(9)	No	Identificador único del usuario que participo en la sesión.
	esAcabada	CHAR(1)	No	Acabada: S = Si / N = No

3.4.5. Tablas Auditoria del Sistema

1. Log

Esta tabla representa todos los logs que se guardan en el sistema. Un log es un registro que guarda un acontecimiento o evento sucedido en un sistema informático, y que se utiliza como evidencia del comportamiento que tiene el sistema. El Log es útil para los procesos de auditorias de sistema y para la localización de fallos y errores. Cada Log se debe identificar de forma única e inequívoco.

	Columna	**Tipo Dato**	**Nullable**	**Descripcion**
PK	idLog	NUMBER	No	Identificador único del log dentro del sistema de seguridad informática
	fecha	DATE	No	Fecha en que se registra el evento o proceso al que se refiere el log
FK	creadoPor	CHAR(9)	No	Usuario que ha realizado la acción que ha generado el log

2. LogProceso

Esta tabla representa los logs de los procesos creados en el sistema. Como se puede observar en el diagrama conceptual, esta entidad hereda de Log, por lo que para cada Log de proceso se registrará una entrada en tanto en la tabla *Log* y como en *LogProceso*. Representamos la relación incluyendo el identificador del *Log* correspomndiente como clave foránea.

	Columna	**Tipo Dato**	**Nullable**	**Descripción**
PK, FK	idLog	NUMBER	No	Identificador único del log dentro del sistema de seguridad informática
	nombre	VARCHAR2(20)	No	Nombre que recibe el proceso que se registra en el sistema
	paramEntrada	VARCHAR2(300)	No	Indica los parámetros de entrada que se reciben para ejecutar el proceso.
	paramSalida	VARCHAR2(300)	Si	Indica los parámetros de Salida que se retornan tras la ejecución del proceso. Este atributo es opcional.
	RSP	VARCHAR2(300)	No	Indica la respuesta recibida tras la ejecución del proceso. Si la ejecución ha finalizado correctamente se guardará el valor 'OK', pero si ha fracasado se guardará el valor 'ERROR + TIPO DE ERROR'.

3.4.6. Tablas Repositorio Estadistico

1. KPIs_Empleados_Anyo

Esta tabla almacena los indicadores clave de negocio asociados a los empleados del sistema, agrupada por año. Existe una tupla por cada empleado/año, con sus principales indicadores.

Nota: A pesar de que en los requisitos del enunciado no se solicitan tantos indicadores asociados a cada usuario, nos parece útil proporcionar esta información en una

tabla/histórico, por si en el futuro fuese necesario incorporar otras consultas al repositorio estadístico.

	Columna	Tipo Dato	Nullable	Descripción
PK	idEmpleado	CHAR(9)	No	Identificador único del empleado
	nombreDepartamento	VARCHAR2(20)	No	Departamento al que pertenece el empleado
	anyo	NUMBER(4)	No	Año al que corresponden los indicadores de este usuario
	totalIncumplimientos	NUMBER(9)	No	Total de incumplimientos que ha realizado el usuario en el año
	totalFormaciones	NUMBER(9)	No	Total de formaciones que ha participado el usuario en el año
	totalFormAcab	NUMBER(9)	No	Total de formaciones que ha acabado el usuario en el año
	totalSimulaciones	NUMBER(9)	No	Total de simulaciones que ha recibido el usuario en el año

2. KPI_Departamentos_Anyo

Esta tabla almacena los indicadores clave de negocio asociados a los departamentos de la empresa, agrupados por año. Existe un registro por cada departamento/año, con sus principales indicadores.

Nota: A pesar de que en los requisitos del enunciado no se solicitan tantos indicadores asociados a cada departamento, nos parece útil proporcionar esta información en una tabla/histórico, por si en el futuro fuese necesario incorporar otras consultas al repositorio estadístico.

	Columna	Tipo Dato	Nullable	Descripción
	nombreDepartamento	VARCHAR2(20)	No	Departamento al que pertenece el empleado
	anyo	NUMBER(4)	No	Año al que corresponden los indicadores de este departamento
	totalIncumplimientos	NUMBER	No	Total de incumplimientos que han realizado los empleados del departamento
	totalFormaciones	NUMBER(9)	No	Total de empleados que tiene alguna formacion asignada
	totalFormAcab	NUMBER(9)	No	Total de empleados que han acabado todas sus formaciones asignadas
	totalFormNoAcab	NUMBER(9)	No	Total de empleados que No han acabado todas sus formaciones asignadas
	totalSimulaciones	NUMBER(9)	No	Total de simulaciones que ha recibido el departamento
	rankingIncumpl	NUMBER	No	Posición del departamento en un ranking por numero de incumplimientos

3. KPI_Departamentos_Gral

Esta tabla almacena los indicadores clave de negocio asociados a los departamentos de la empresa. Existe un registro por cada departamento, con sus principales indicadores.

Nota: A pesar de que en los requisitos del enunciado no se solicitan tantos indicadores asociados a cada departamento, nos parece útil proporcionar esta información en una tabla/histórico, por si en el futuro fuese necesario incorporar otras consultas al repositorio estadístico.

	Columna	Tipo Dato	Nullable	Descripción
	nombreDepartamento	VARCHAR2(20)	No	Departamento al que pertenece el empleado
	totalIncumplimientos	NUMBER	No	Total de incumplimientos que han realizado los empleados del departamento
	totalFormaciones	NUMBER(9)	No	Total de empleados que tiene alguna formacion asignada
	totalFormAcab	NUMBER(9)	No	Total de empleados que han acabado todas sus formaciones asignadas
	totalFormNoAcab	NUMBER(9)	No	Total de empleados que No han acabado todas sus formaciones asignadas
	totalSimulaciones	NUMBER(9)	No	Total de simulaciones que ha recibido el departamento
	rankingIncumpl	NUMBER	No	Posición del departamento en un ranking por numero de incumplimientos

4. KPIs_General

Esta tabla almacena una variedad de indicadores clave de negocio, obtenidos de todos los datos históricos del sistema. Existe solo un registro en esta tabla, con todos los indicadores.

Nota: A pesar de que en los requisitos del enunciado no se solicitan tantos indicadores generales, nos parece útil proporcionar esta información en una tabla/histórico, por si en el futuro fuese necesario incorporar otras consultas al repositorio estadístico.

	Columna	Tipo Dato	Nullable	Descripción
	totalVulnerabilidades	NUMBER	No	Total de vulnerabilidades detectadas durante el año
	totalVulnerIdentif	NUMBER	No	Total de Vulnerabilidades en estado: Identificada detectadas durante el año
	totalVulnerMitig	NUMBER	No	Total de Vulnerabilidades en estado: Mitigada detectadas durante el año
	totalVulnerParcMitig	NUMBER	No	Total de Vulnerabilidades en estado: Parcialmente Mitigada detectadas durante el año
	totalVulnerNoMitig	NUMBER	No	Total de Vulnerabilidades en estado: No Mitigada detectadas durante el año
	totalVulnerCriticas	NUMBER	No	Total de Vulnerabilidades Criticas detectadas durante el año
	totalVulnCriticInt	NUMBER	No	Total de Vulnerabilidades Críticas Internas detectadas durante el año
	totalAccionMitig	NUMBER	No	Total de acciones de mitigación detectadas durante el año
	totalAccMitDefinid	NUMBER	No	Total de acciones de mitigación en estado : Definidas detectadas durante el año
	totalAccMitEnProc	NUMBER	No	Total de acciones de mitigación en estado : En Proceso detectadas durante el año
	totalAccMitAcabad	NUMBER	No	Total de acciones de mitigación en estado : Acabadas detectadas durante el año

	totalAccMitEnRevi	NUMBER	No	Total de acciones de mitigación en estado : En revisión detectadas durante el año
	procesoMasVulner	VARCHAR2(30)	No	Nombre del proceso que ha tenido más vulnerabilidades durante el año
	totalIncumplim	NUMBER	No	Total de incumplimientos detectados durante el año
	formacMenosPartic	VARCHAR2(30)	No	Título de la sesión con menos participación del año
	politMasIncump	VARCHAR2(20)	No	Nombre de la política que ha tenido más incumplimientos durante el año
	porcentVulnCriticAbierta	NUMBER(3,2)	No	Porcentaje de Vulnerabilidades Criticas Abiertas detectadas durante el año
	porcentEmplSinIncump	NUMBER(3,2)	No	Porcentaje de empleados sin ningún incumplimiento detectado durante el año
	responsMasAccEnProc	CHAR(9)	No	Identificador del usuario responsable con más acciones “En Proceso” creadas durante el año
	añoMasIncumAuditExt	NUMBER(4)	No	Año en el que se detectaron más incumplimientos en una Auditoría Externa

4 Implementación de la Base de Datos

Durante esta etapa, se empieza a trabajar con la base de datos ya creada en la fase anterior (Diseño físico), creando los procedimientos almacenados, insertando los datos en la base de datos, y finalmente realizando las pruebas.

4.1 Scripts de Creación

4.1.1 Creación de *TableSpace* y Usuarios

Se utilizan *TableSpaces* o Espacios Virtuales para el almacenamiento de las tablas que componen la base de datos. Se decide crear los siguientes espacios virtuales:

- PROCESOS_SEGURIDAD: Para almacenar las tablas permanentes de la base de datos y el repositorio estadístico.
- PROCESOS_SEGURIDAD_TEMP: Que se puede utilizar para el tratamiento de los datos y en la implementación de la DW.

```
SELECT * FROM dba_TABLESPACES;
```

Query Result

SQL | All Rows Fetched: 10 in 0.019 seconds

	TABLESPACE_NAME	BLOCK_SIZE	INITIAL_EXTENT	NEXT_EXTENT	MIN_EXTENTS	MAX_EXTENTS	
7	PROCESOS_SEGURIDAD	8192	65536	(null)	1	2147483645	2
8	PROCESOS_SEGURIDAD_TEMP	8192	1048576	1048576	1	(null)	2

No	Nombre *Script*	Descripción
1	Creacion_TableSpaces_Usuario.sql	incluye los *scripts* para la creación de los *Tablespaces* y lo usuarios
2	Creacion_Tablas.sql	incluye los *scripts* para la creación de las tablas del *Tablespace* PROCESOS_SEGURIDAD
3	Creacion_Secuencias.sql	incluye los *scripts* para la creación de las secuencias numéricas para los identificadores de las tablas
4	Creacion_Procedimientos_ABM.sql	incluye los *scripts* para la creación de los procedimientos almacenados de alta, baja y modificación de las entidades.
5	Creacion_Procedimientos_DW.sql	incluye los *scripts* para la creación de los procedimientos almacenados encargados de calcular los datos para las tablas del repositorio estadístico.
6	Creacion_Procedimientos_Estados.sql	incluye los *scripts* para la creación de los procedimientos almacenados para añadir las fechas de inicio y fin de las acciones de mitigación, las cuales a su vez actualizan el estado de las acciones y vulnerabilidades
7	Carga_Datos_Inicial.sql	incluye los *scripts* para la carga de los datos necesarios para realizar las pruebas
8	Prueba_Procedimientos_Estados	incluye los *scripts* para la realización de un set de prueba para los procedimientos almacenados de cambio de estado
9	Consultas_Repositorio_Estadistico	incluye las consultas mínimas del repositorio estadístico, según los requerimientos.
10	Pruebas_Repositorio_Estadistico	incluye otras consultas, donde se comprueban las consultas del repositorio estadístico..
11	Borrado_Datos_Tablas.sql	Incluye una serie de sentencias de bases de datos para el borrado del contenido de las tablas, en caso necesario.

Antes de proceder a crear los usuarios, se crea un role llamado “ADMINISTRATOR”, el cual tiene permisos para Crear, Alterar y Eliminar otros usuarios, procesos, tablas, secuencias, entre otros.

A continuación, se crean los usuarios para acceder a las bases de datos:

Usuario	Role	Base de Datos	Descripción
ADMIN	ADMINISTRATOR	PROCESOS_SEGURIDAD	Usuario Encargado de crear y actualizar las tablas, procedimientos, entre otros…
ADMIN	ADMINISTRATOR	PROCESOS_SEGURIDAD_TEMP	
USER_TEST	-	PROCESOS_SEGURIDAD	Usuario solo de lectura, para hacer las consultas del
USER_TEST	-	PROCESOS_SEGURIDAD_TEMP	

			repositorio estadístico

4.2 Procedimientos almacenados

Los procedimientos almacenados o "*Stored Procedures*" son un conjunto de instrucciones o comandos que se ejecutan en el motor de base de datos con el objetivo de ejecutar una acción o conjunto de acciones utilizando los datos guardados en el servidor base de datos.

Para este proyecto, se precisa de la creación de distintos tipos de procedimiento, los cuales clasificamos en tres tipos:

- Procedimientos ABM: Son los procedimientos de Alta, Baja y Modificación de los datos almacenados en las tablas del *tablespace* PROCESOS_SEGURIDAD
- Procedimientos DW: Son los procedimientos para el tratamiento y carga de los datos del repositorio estadístico.
- Procedimientos cambios de Estados: Son los procedimientos para añadir fecha de inicio y fin a las acciones de mitigación. Estas actualizaciones, a su vez, provocarán un cambio en el estado de las acciones de mitigación, y de las vulnerabilidades asociadas a las mismas.

4.2.1. Procedimientos ABM

Estos son los procedimientos que se deben utilizar para realizar el alta, baja y modificación de los registro en las diferentes tablas de la Base de Datos.

Hay que tener en cuenta solo se han creado **procedimientos de baja y modificación** para aquellas tablas en las cuales se precisó necesario según la lógica de negocio extraída de los requerimientos.

Por ejemplo, no se crean **procedimientos de modificación y baja** para aquellas tablas creadas para indicar la relación entre varias entidades, y donde la clave primaría es una combinación de todas las claves primarias de las distintas entidades relacionadas.

Respecto a los **procedimientos de baja**, en algunos casos la baja se realiza a través de "borrado lógico", donde no se eliminan los datos del registro, sino que simplemente se cambia su estado a "Eliminado".

Finalmente, se ha llevado a cabo la gestión de excepciones, tal como se pide en los requerimientos, para los siguientes casos:

- Inserción de valores nulos en campos mandatorios
- Inserción de valores duplicados en campos únicos
- Revisión de las claves foráneas en las tablas asociadas, según corresponda
- Cualquier otro tipo de error

A continuación, se muestra el listado de los procedimientos ABM creados para cada una de las tablas:

1. ProcesoGestion

Nombre	altaProcesoGestion
Descripción	Da de alta un nuevo proceso de Gestión en el sistema de seguridad
Parámetros Entrada	nombre, fecha
Parámetros Salida	Proceso realizado correctamente = OK Error detectado en Proceso = ERROR+TIPO DE ERROR
Operativa Proceso	- El proceso verifica que los datos mandatorios pasados no sean nulos - El proceso verifica que el nombre dado no exista en la base de datos - El proceso verifica cualquier otro tipo de excepción - Si no se detecta error, se realiza el alta y se guarda un log con RSP OK. Si se detecta un error, NO se realiza el alta y se guarda un log con RSP ERROR

Nombre	bajaProcesoGestion
Descripción	Da de baja un proceso de Gestión existente en el sistema de seguridad. Se realiza un borrado lógico, es decir, que se cambia el estado de la columna “Eliminado” a “Sí”. De manera que no se pierdan datos del sistema.
Parámetros Entrada	idProceso
Parámetros Salida	Proceso realizado correctamente = OK Error detectado en Proceso = ERROR+TIPO DE ERROR
Operativa Proceso	- El proceso verifica que el proceso exista en la base de datos - El proceso verifica que los datos mandatorios pasados no sean nulos - El proceso verifica cualquier otro tipo de excepción - Si no se detecta error, se realiza la baja y se guarda un log con RSP OK. Si se detecta un error, NO se realiza la baja y se guarda un log con RSP ERROR

Nombre	modProcesoGestion
Descripción	Modifica un proceso de Gestión existente en el sistema de seguridad
Parámetros Entrada	idProceso, nombre, fecha
Parámetros Salida	Proceso realizado correctamente = OK Error detectado en Proceso = ERROR+TIPO DE ERROR
Operativa Proceso	- El proceso verifica que el proceso exista en la base de datos y no esté dado de baja - El proceso verifica que los datos mandatorios pasados no sean nulos

	- El proceso verifica que el nombre no existe ya en la tabla Proceso Gestión - El proceso verifica cualquier otro tipo de excepción - Si no se detecta error, se realiza la modificación y se guarda un log con RSP OK. Si se detecta un error, NO se realiza la modificación y se guarda un log con RSP ERROR

2. Usuario

Nombre	altaUsuario
Descripción	Da de alta un nuevo usuario en el sistema de seguridad
Parámetros Entrada	Id usuario, tipo usuario
Parámetros Salida	Proceso realizado correctamente = OK Error detectado en Proceso = ERROR+TIPO DE ERROR
Operativa Proceso	- El proceso verifica que los datos mandatorios pasados no sean nulos - El proceso verifica que el usuario dado no exista ya en la base de datos - El proceso verifica cualquier otro tipo de excepción - Si no se detecta error, se realiza el alta y se guarda un log con RSP OK. Si se detecta un error, NO se realiza el alta y se guarda un log con RSP ERROR

Nombre	bajaUsuario
Descripción	Da de baja un proceso de Gestión existente en el sistema de seguridad. Se realiza un **borrado lógico**, es decir, que se cambia el estado de la columna "Eliminado" a "Sí". De manera que no se pierdan datos del sistema.
Parámetros Entrada	Id usuario, tipo usuario
Parámetros Salida	Proceso realizado correctamente = OK Error detectado en Proceso = ERROR+TIPO DE ERROR
Operativa Proceso	- El proceso verifica que los datos mandatorios pasados no sean nulos - El proceso verifica que el usuario dado exista ya en la base de datos y no esté ya dado de baja - El proceso verifica cualquier otro tipo de excepción - Si no se detecta error, se realiza el alta y se guarda un log con RSP OK. Si se detecta un error, NO se realiza el alta y se guarda un log con RSP ERROR

Nombre	modUsuario
Descripción	Modifica un usuario existente en el sistema de seguridad
Parámetros Entrada	idUsuario, Tipo
Parámetros Salida	Proceso realizado correctamente = OK Error detectado en Proceso = ERROR+TIPO DE ERROR
Operativa Proceso	- El proceso verifica que el usuario exista en la base de datos y no esté eliminado

	- El proceso verifica que los datos mandatorios pasados no sean nulos - El proceso verifica cualquier otro tipo de excepción - Si no se detecta error, se realiza la modificación y se guarda un log con RSP OK. Si se detecta un error, NO se realiza la modificación y se guarda un log con RSP ERROR

3. Empleado

Nombre	altaEmpleado
Descripción	Da de alta un nuevo Empleado en el sistema de seguridad
Parámetros Entrada	idEmpleado, idDepartamento
Parámetros Salida	Proceso realizado correctamente = OK Error detectado en Proceso = ERROR+TIPO DE ERROR
Operativa Proceso	- El proceso verifica que los datos mandatorios pasados no sean nulos - El proceso verifica que el id dado del empleado exista en la tabla usuarios y que no esté eliminado - El proceso verifica que el id del departamento dado exista en la base de datos - El proceso verifica cualquier otro tipo de excepción - Si no se detecta error, se realiza el alta y se guarda un log con RSP OK. Si se detecta un error, NO se realiza el alta y se guarda un log con RSP ERROR

Nombre	modVulnerabilidad
Descripción	Modifica una empleado existente en el sistema de seguridad
Parámetros Entrada	idEmpleado, idDepartamento
Parámetros Salida	Proceso realizado correctamente = OK Error detectado en Proceso = ERROR+TIPO DE ERROR
Operativa Proceso	- El proceso verifica que los datos mandatorios pasados no sean nulos - El proceso verifica que el id dado del empleado exista en la tabla Empleados - El proceso verifica que el id del departamento dado exista en la base de datos - El proceso verifica cualquier otro tipo de excepción - Si no se detecta error, se realiza el alta y se guarda un log con RSP OK. Si se detecta un error, NO se realiza el alta y se guarda un log con RSP ERROR

4. Departamento

Nombre	altaDeparmento
Descripción	Da de alta un nuevo Departamento en el sistema de seguridad
Parámetros Entrada	idDepartamento, nombre
Parámetros Salida	Proceso realizado correctamente = OK Error detectado en Proceso = ERROR+TIPO DE ERROR
Operativa Proceso	- El proceso verifica que los datos mandatorios pasados no sean nulos - El proceso verifica que el id dado no exista en la tabla Departamento - El proceso verifica que el nombre dado no exista en la tabla Departamento - El proceso verifica cualquier otro tipo de excepción

	- Si no se detecta error, se realiza el alta y se guarda un log con RSP OK. Si se detecta un error, NO se realiza el alta y se guarda un log con RSP ERROR

Nombre	modVulnerabilidad
Descripción	Modifica un departamento existente en el sistema de seguridad
Parámetros Entrada	idDepartamento, nombre
Parámetros Salida	Proceso realizado correctamente = OK Error detectado en Proceso = ERROR+TIPO DE ERROR
Operativa Proceso	- El proceso verifica que los datos mandatorios pasados no sean nulos - El proceso verifica que el id dado sí exista en la tabla Departamento - El proceso verifica que el nombre dado no exista para otro Departamento - El proceso verifica cualquier otro tipo de excepción - Si no se detecta error, se realiza el alta y se guarda un log con RSP OK. Si se detecta un error, NO se realiza el alta y se guarda un log con RSP ERROR

5. Vulnerabilidad

Nombre	altaVulnerabilidad
Descripción	Da de alta una nueva Vulnerabilidad en el sistema de seguridad
Parámetros Entrada	idVulnerabilidad,idProceso descripción, estado, esCritica, fecha
Parámetros Salida	Proceso realizado correctamente = OK Error detectado en Proceso = ERROR+TIPO DE ERROR
Operativa Proceso	- El proceso verifica que los datos mandatorios pasados no sean nulos - El proceso verifica que el id dado no exista en la base de datos - El proceso verifica que el id del proceso de gestion dado exista en la base de datos - El proceso verifica cualquier otro tipo de excepción - Si no se detecta error, se realiza el alta y se guarda un log con RSP OK. Si se detecta un error, NO se realiza el alta y se guarda un log con RSP ERROR

Nombre	modVulnerabilidad
Descripción	Modifica una vulnerabilidad existente en el sistema de seguridad
Parámetros Entrada	idVulnerabilidad,idProceso descripción, estado, esCritica, fecha
Parámetros Salida	Proceso realizado correctamente = OK Error detectado en Proceso = ERROR+TIPO DE ERROR
Operativa Proceso	- El proceso verifica que el proceso exista en la base de datos - El proceso verifica que el id del proceso de gestion dado exista en la base de datos - El proceso verifica que los datos mandatorios pasados no sean nulos - El proceso verifica cualquier otro tipo de excepción - Si no se detecta error, se realiza la modificación y se guarda un log con RSP OK. Si se detecta un error, NO se realiza la modificación y se guarda un log con RSP ERROR

6. Accion Mitigacion

Nombre	altaAccionMit

Descripción	Da de alta una nueva acción de mitigacion en el sistema de seguridad
Parámetros Entrada	idAccion, idVulnerabilidad, descripción, fechaLimite, fecha, estado, responsable
Parámetros Salida	Proceso realizado correctamente = OK Error detectado en Proceso = ERROR+TIPO DE ERROR
Operativa Proceso	- El proceso verifica que los datos mandatorios pasados no sean nulos - El proceso verifica que el id dado no exista en la base de datos - El proceso verifica que el id de la vulnerabilidad asociada exista en la base de datos - El proceso verifica que el id del usuario responsable de la vulnerabilidad exista en la base de datos y no se encuentre eliminado - El proceso verifica cualquier otro tipo de excepción - Si no se detecta error, se realiza el alta y se guarda un log con RSP OK. Si se detecta un error, NO se realiza el alta y se guarda un log con RSP ERROR

Nombre	ModAccionMit
Descripción	Modifica una acción de mitigacion existente en el sistema de seguridad
Parámetros Entrada	idVulnerabilidad, idProceso descripción, estado, esCritica, fecha, creadaPor
Parámetros Salida	Proceso realizado correctamente = OK Error detectado en Proceso = ERROR+TIPO DE ERROR
Operativa Proceso	- El proceso verifica que los datos mandatorios pasados no sean nulos - El proceso verifica que el id dado no exista en la base de datos - El proceso verifica que el id de la vulnerabilidad asociada exista en la base de datos - El proceso verifica cualquier otro tipo de excepción - Si no se detecta error, se realiza la modificación y se guarda un log con RSP OK. Si se detecta un error, NO se realiza la modificación y se guarda un log con RSP ERROR

7. PoliticaSeguridad

Nombre	altaPolitica
Descripción	Da de alta una nueva Politica de seguridad en el sistema de seguridad
Parámetros Entrada	idPolitica, nombre, fecha
Parámetros Salida	Proceso realizado correctamente = OK Error detectado en Proceso = ERROR+TIPO DE ERROR
Operativa Proceso	- El proceso verifica que los datos mandatorios pasados no sean nulos - El proceso verifica que el id dado no exista en la base de datos - El proceso verifica que el nombre sea unico - El proceso verifica cualquier otro tipo de excepción - Si no se detecta error, se realiza el alta y se guarda un log con RSP OK. Si se detecta un error, NO se realiza el alta y se guarda un log con RSP ERROR

Nombre	ModPolitica
Descripción	Modifica una política de seguridad existente en el sistema de seguridad
Parámetros Entrada	idPolitica, nombre, fecha
Parámetros Salida	Proceso realizado correctamente = OK Error detectado en Proceso = ERROR+TIPO DE ERROR

Operativa Proceso	- El proceso verifica que los datos mandatorios pasados no sean nulos - El proceso verifica que el id dado no exista en la base de datos - El proceso verifica que el nombre sea unico El proceso verifica cualquier otro tipo de excepción - Si no se detecta error, se realiza la modificación y se guarda un log con RSP OK. Si se detecta un error, NO se realiza la modificación y se guarda un log con RSP ERROR

8. Auditoria

Nombre	altaAuditoria
Descripción	Da de alta una nueva Politica de seguridad en el sistema de seguridad
Parámetros Entrada	idAuditoria, fechaInicio, fechaFin, resultado, creadaPor
Parámetros Salida	Proceso realizado correctamente = OK Error detectado en Proceso = ERROR+TIPO DE ERROR
Operativa Proceso	- El proceso verifica que los datos mandatorios pasados no sean nulos - El proceso verifica que el id dado no exista en la base de datos - El proceso verifica que el creador de la auditoria existe en la tabla usuarios y no está eliminado - El proceso verifica cualquier otro tipo de excepción - Si no se detecta error, se realiza el alta y se guarda un log con RSP OK. Si se detecta un error, NO se realiza el alta y se guarda un log con RSP ERROR

Nombre	modAuditoria
Descripción	Modifica una auditoria existente en el sistema de seguridad
Parámetros Entrada	idAuditoria, fechaInicio, fechaFin, resultado, creadaPor
Parámetros Salida	Proceso realizado correctamente = OK Error detectado en Proceso = ERROR+TIPO DE ERROR
Operativa Proceso	- El proceso verifica que los datos mandatorios pasados no sean nulos - El proceso verifica que el id dado no exista en la base de datos - El proceso verifica que el creador de la auditoria existe en la tabla usuarios y no está eliminado - Si no se detecta error, se realiza la modificación y se guarda un log con RSP OK. Si se detecta un error, NO se realiza la modificación y se guarda un log con RSP ERROR

9. AuditoriaProceso

Nombre	altaAuditoria
Descripción	Da de alta una nueva Politica de seguridad en el sistema de seguridad
Parámetros Entrada	idAuditoria, fechaInicio, fechaFin, resultado, creadaPor
Parámetros Salida	Proceso realizado correctamente = OK Error detectado en Proceso = ERROR+TIPO DE ERROR
Operativa Proceso	- El proceso verifica que los datos mandatorios pasados no sean nulos - El proceso verifica que el id dado no exista en la base de datos - El proceso verifica que el creador de la auditoria existe en la tabla usuarios - El proceso verifica cualquier otro tipo de excepción - Si no se detecta error, se realiza el alta y se guarda un log con RSP OK. Si se detecta un error, NO se realiza el alta y se guarda un log con RSP ERROR

10. VulnerabilidadAuditoria

Nombre	altaVulnerAudit
Descripción	Da de alta una nueva vulnerabilidad asociada a una auditoria en el sistema de seguridad
Parámetros Entrada	idAuditoria, IdVulnerabilidad
Parámetros Salida	Proceso realizado correctamente = OK Error detectado en Proceso = ERROR+TIPO DE ERROR
Operativa Proceso	- El proceso verifica que los datos mandatorios pasados no sean nulos - El proceso verifica que el id de la auditoria exista en la tabla Auditoria - El proceso verifica que el id de la Vulnerabilidad exista en la tabla Vulnerabilidad - El proceso verifica cualquier otro tipo de excepción - Si no se detecta error, se realiza el alta y se guarda un log con RSP OK. Si se detecta un error, NO se realiza el alta y se guarda un log con RSP ERROR

11. IncumplimientoAuditoria

Nombre	altaIncumpAudit
Descripción	Da de alta un nuevo incumplimiento asociada a una auditoria en el sistema de seguridad
Parámetros Entrada	idAuditoria, IdIncumplimiento
Parámetros Salida	Proceso realizado correctamente = OK Error detectado en Proceso = ERROR+TIPO DE ERROR
Operativa Proceso	- El proceso verifica que los datos mandatorios pasados no sean nulos - El proceso verifica que el id de la auditoria exista en la tabla Auditoria - El proceso verifica que el id del incumplimiento exista en la tabla Incumplimiento - El proceso verifica cualquier otro tipo de excepción - Si no se detecta error, se realiza el alta y se guarda un log con RSP OK. Si se detecta un error, NO se realiza el alta y se guarda un log con RSP ERROR

12. Muestreo

Nombre	altaMuestreo
Descripción	Da de alta un nuevo muestreo en el sistema de seguridad
Parámetros Entrada	idMuestra, idAuditoria, muestra
Parámetros Salida	Proceso realizado correctamente = OK Error detectado en Proceso = ERROR+TIPO DE ERROR
Operativa Proceso	- El proceso verifica que los datos mandatorios pasados no sean nulos - El proceso verifica que el id dado no exista en la base de datos - El proceso verifica que la auditoria existe en la tabla Auditoria - El proceso verifica cualquier otro tipo de excepción - Si no se detecta error, se realiza el alta y se guarda un log con RSP OK. Si se detecta un error, NO se realiza el alta y se guarda un log con RSP ERROR

Nombre	modMuestreo

Descripción	Modifica un muestreo existente en el sistema de seguridad
Parámetros Entrada	idMuestra, idAuditoria, muestra
Parámetros Salida	Proceso realizado correctamente = OK Error detectado en Proceso = ERROR+TIPO DE ERROR
Operativa Proceso	- El proceso verifica que los datos mandatorios pasados no sean nulos - El proceso verifica que el id dado no exista en la base de datos - El proceso verifica que la auditoria existe en la tabla Auditoria - El proceso verifica cualquier otro tipo de excepción - Si no se detecta error, se realiza el alta y se guarda un log con RSP OK. Si se detecta un error, NO se realiza el alta y se guarda un log con RSP ERROR

13. Incumplimiento

Nombre	altaIncumplimiento
Descripción	Da de alta un nuevo incumplimiento en el sistema de seguridad
Parámetros Entrada	idIncumplimiento, idPolitica, descripción, fecha, realizadoPor
Parámetros Salida	Proceso realizado correctamente = OK Error detectado en Proceso = ERROR+TIPO DE ERROR
Operativa Proceso	- El proceso verifica que los datos mandatorios pasados no sean nulos - El proceso verifica que el id dado no exista en la base de datos - El proceso verifica que la politica existe en la tabla PoliticaSeguridad - El proceso verifica que el usuario existe en la tabla Usuarios - El proceso verifica cualquier otro tipo de excepción - Si no se detecta error, se realiza el alta y se guarda un log con RSP OK. Si se detecta un error, NO se realiza el alta y se guarda un log con RSP ERROR

Nombre	modIncumplimiento
Descripción	Modifica un incumplimiento existente en el sistema de seguridad
Parámetros Entrada	idIncumplimiento, idPolitica, descripción, fecha, realizadoPor
Parámetros Salida	Proceso realizado correctamente = OK Error detectado en Proceso = ERROR+TIPO DE ERROR
Operativa Proceso	- El proceso verifica que los datos mandatorios pasados no sean nulos - El proceso verifica que el id dado no exista en la base de datos - El proceso verifica que la politica existe en la tabla PoliticaSeguridad - El proceso verifica que el usuario existe en la tabla Usuarios - El proceso verifica cualquier otro tipo de excepción - Si no se detecta error, se realiza el alta y se guarda un log con RSP OK. Si se detecta un error, NO se realiza el alta y se guarda un log con RSP ERROR

14. SimulaciónAtaque

Nombre	altaSimulacionAtaque
Descripción	Da de alta una nueva simulación de ataque en el sistema de seguridad
Parámetros Entrada	idSimulacion, descripción, fecha
Parámetros Salida	Proceso realizado correctamente = OK Error detectado en Proceso = ERROR+TIPO DE ERROR

Operativa Proceso	- El proceso verifica que los datos mandatorios pasados no sean nulos - El proceso verifica que el id dado no exista en la base de datos - El proceso verifica cualquier otro tipo de excepción - Si no se detecta error, se realiza el alta y se guarda un log con RSP OK. Si se detecta un error, NO se realiza el alta y se guarda un log con RSP ERROR

Nombre	modSimulacionAtaque
Descripción	Modifica un incumplimiento existente en el sistema de seguridad
Parámetros Entrada	idSimulacion, descripción, fecha
Parámetros Salida	Proceso realizado correctamente = OK Error detectado en Proceso = ERROR+TIPO DE ERROR
Operativa Proceso	- El proceso verifica que los datos mandatorios pasados no sean nulos - El proceso verifica que el id dado no exista en la base de datos - El proceso verifica cualquier otro tipo de excepción - Si no se detecta error, se realiza el alta y se guarda un log con RSP OK. Si se detecta un error, NO se realiza el alta y se guarda un log con RSP ERROR

15. SimulaciónEmpleado

Nombre	altaSimulEmpl
Descripción	Da de alta una nueva simulacion asociada a un empleado del sistema de seguridad
Parámetros Entrada	idEmpleado, idSimulacion
Parámetros Salida	Proceso realizado correctamente = OK Error detectado en Proceso = ERROR+TIPO DE ERROR
Operativa Proceso	- El proceso verifica que los datos mandatorios pasados no sean nulos - El proceso verifica que el id de la simulación exista en la tabla simulación - El proceso verifica que el id del empleado exista en la tabla Empleados, y que el empleado (usuario) no esté dado de baja. - El proceso verifica cualquier otro tipo de excepción - Si no se detecta error, se realiza el alta y se guarda un log con RSP OK. Si se detecta un error, NO se realiza el alta y se guarda un log con RSP ERROR

16. IncumplimientoSimulacion

Nombre	altaIncumpSimul
Descripción	Da de alta un nuevo incumplimiento asociada a una simulación en el sistema de seguridad
Parámetros Entrada	idSimulacion, IdIncumplimiento
Parámetros Salida	Proceso realizado correctamente = OK Error detectado en Proceso = ERROR+TIPO DE ERROR
Operativa Proceso	- El proceso verifica que los datos mandatorios pasados no sean nulos - El proceso verifica que el id de la simulación exista en la tabla simulación - El proceso verifica que el id del incumplimiento exista en la tabla Incumplimiento - El proceso verifica cualquier otro tipo de excepción

	- Si no se detecta error, se realiza el alta y se guarda un log con RSP OK. Si se detecta un error, NO se realiza el alta y se guarda un log con RSP ERROR

17. AccionPunitiva

Nombre	altaAccionPunit
Descripción	Da de alta un nuevo tipo de acción punitiva en el sistema de seguridad
Parámetros Entrada	idAccion, tipo
Parámetros Salida	Proceso realizado correctamente = OK Error detectado en Proceso = ERROR+TIPO DE ERROR
Operativa Proceso	- El proceso verifica que los datos mandatorios pasados no sean nulos - El proceso verifica que el id dado no exista ya en la base de datos - El proceso verifica cualquier otro tipo de excepción - Si no se detecta error, se realiza el alta y se guarda un log con RSP OK. Si se detecta un error, NO se realiza el alta y se guarda un log con RSP ERROR

18. IncumplimientoAccion

Nombre	altaIncumpAccion
Descripción	Da de alta una nueva acción punitiva asociada incumplimiento asociada a una simulacion en el sistema de seguridad
Parámetros Entrada	idSimulacion, IdIncumplimiento
Parámetros Salida	Proceso realizado correctamente = OK Error detectado en Proceso = ERROR+TIPO DE ERROR
Operativa Proceso	- El proceso verifica que los datos mandatorios pasados no sean nulos - El proceso verifica que el id de la acción exista en la tabla acción punitiva - El proceso verifica que el id del incumplimiento exista en la tabla Incumplimiento - El proceso verifica cualquier otro tipo de excepción - Si no se detecta error, se realiza el alta y se guarda un log con RSP OK. Si se detecta un error, NO se realiza el alta y se guarda un log con RSP ERROR

19. IncumplimientoSimulacion

Nombre	altaIncumpSimul
Descripción	Da de alta un nuevo incumplimiento asociada a una simulación en el sistema de seguridad
Parámetros Entrada	idSimulacion, IdIncumplimiento
Parámetros Salida	Proceso realizado correctamente = OK Error detectado en Proceso = ERROR+TIPO DE ERROR
Operativa Proceso	- El proceso verifica que los datos mandatorios pasados no sean nulos - El proceso verifica que el id de la simulación exista en la tabla simulación - El proceso verifica que el id del incumplimiento exista en la tabla Incumplimiento - El proceso verifica cualquier otro tipo de excepción - Si no se detecta error, se realiza el alta y se guarda un log con RSP OK. Si se detecta un error, NO se realiza el alta y se guarda un log con RSP ERROR

20. SesiónFormativa

Nombre	altaSesion
Descripción	Da de alta una nueva sesión formativa en el sistema de seguridad
Parámetros Entrada	idSesion, titulo, formato, fecha
Parámetros Salida	Proceso realizado correctamente = OK Error detectado en Proceso = ERROR+TIPO DE ERROR
Operativa Proceso	- El proceso verifica que los datos mandatorios pasados no sean nulos - El proceso verifica que el id dado no exista en la base de datos - El proceso verifica cualquier otro tipo de excepción - Si no se detecta error, se realiza el alta y se guarda un log con RSP OK. Si se detecta un error, NO se realiza el alta y se guarda un log con RSP ERROR

Nombre	modSesion
Descripción	Modifica una sesion existente en el sistema de seguridad
Parámetros Entrada	idSesion, titulo, formato, fecha
Parámetros Salida	Proceso realizado correctamente = OK Error detectado en Proceso = ERROR+TIPO DE ERROR
Operativa Proceso	- El proceso verifica que los datos mandatorios pasados no sean nulos - El proceso verifica que el id dado sí exista en la base de datos - El proceso verifica cualquier otro tipo de excepción - Si no se detecta error, se realiza el alta y se guarda un log con RSP OK. Si se detecta un error, NO se realiza el alta y se guarda un log con RSP ERROR

21. Participacion

Nombre	altaParticipacion
Descripción	Da de alta una nueva simulación de ataque en el sistema de seguridad
Parámetros Entrada	idEmpleado, idSesion, esAcabada
Parámetros Salida	Proceso realizado correctamente = OK Error detectado en Proceso = ERROR+TIPO DE ERROR
Operativa Proceso	- El proceso verifica que los datos mandatorios pasados no sean nulos - El proceso verifica que el empleado exista en la base de datos - El proceso verifica que la sesión exista en la base de datos - El proceso verifica que la combinación del empleado-sesión no exista ya en la base de datos - El proceso verifica cualquier otro tipo de excepción - Si no se detecta error, se realiza el alta y se guarda un log con RSP OK. Si se detecta un error, NO se realiza el alta y se guarda un log con RSP ERROR

Nombre	modParticipacion
Descripción	Modifica un incumplimiento existente en el sistema de seguridad
Parámetros Entrada	idEmpleado, idSesion, esAcabada
Parámetros Salida	Proceso realizado correctamente = OK Error detectado en Proceso = ERROR+TIPO DE ERROR
Operativa Proceso	- El proceso verifica que los datos mandatorios pasados no sean nulos - El proceso verifica que el empleado exista en la base de datos - El proceso verifica que la sesión exista en la base de datos - El proceso verifica que la combinación del empleado-sesión no exista ya en la base de datos

	- El proceso verifica cualquier otro tipo de excepción - Si no se detecta error, se realiza el alta y se guarda un log con RSP OK. Si se detecta un error, NO se realiza el alta y se guarda un log con RSP ERROR

4.2.2. Pruebas Procedimientos ABM

Durante la creación de cada uno de los procedimientos ABM del apartado anterior, se realizaron múltiples pruebas para comprobar la inserción correcta de los datos, en caso de ingresar los datos correctos; y en caso contrario, el correspondiente mensaje de error.

Pruebas realizadas:

No	Proceso Probado	Descripción	Resultado
1	AltaProcesoGestion	Crear proceso con Id y nombre no existente	OK: Proceso creado
2	AltaProcesoGestion	Crear proceso con Id o nombre repetido	OK: Proceso No creado – nombre ya existe
3	AltaProcesoGestion	Crear proceso con valores nulos	OK: Proceso No creado - detectados valores nulos
4	BajaProcesoGestion	Dar de Baja proceso existente	OK: Baja realizada – Eliminado = "Si"
5	BajaProcesoGestion	Dar de Baja con valores nulos	OK: Baja No realizada – detectados valores nulos
6	BajaProcesoGestion	Dar de Baja proceso no existente	OK: Proceso No creado – Nombre ya existe
7	ModProcesoGestion	Modificar proceso con Id existente	OK: Proceso Modificado
8	ModProcesoGestion	Modificar proceso con Id No existente	OK: Proceso No Modificado – Proceso no existe
9	ModProcesoGestion	Modificar proceso con nombre repetido	OK: Proceso No Modificado – Nombre ya existe
10	ModProcesoGestion	Modificar proceso con valores nulos	OK: Proceso No Modificado - detectados valores nulos
11	AltaUsuario	Crear Usuario con Id y nombre no existente	OK: Usuario creado
12	AltaUsuario	Crear Usuario con valores nulos	OK: Usuario No creado - detectados valores nulos
13	BajaUsuario	Dar de Baja Usuario existente	OK: Baja realizada – Eliminado = "Si"
14	BajaUsuario	Dar de Baja Usuario con valores nulos	OK: Baja No realizada – detectados valores nulos
15	Baja Usuario	Dar de Baja Usuario no existente	OK: Usuario No creado – ID ya existe
16	Mod Usuario	Modificar Usuario con Id existente	OK: Usuario Modificado
17	Mod Usuario	Modificar Usuario con Id No existente	OK: Usuario No Modificado – Usuario no existe
18	Mod Usuario	Modificar Usuario con valores nulos	OK: Usuario No Modificado - detectados valores nulos
19	AltaPolitica	Crear política con Id y nombre no existente	OK: Política creada

20	AltaPolitica	Crear política con Id o nombre repetido	OK: Política No creada – nombre ya existe
21	AltaPolitica	Crear Política con valores nulos	OK: Política No creada - detectados valores nulos
22	ModPolitica	Modificar Política con Id existente	OK: Política Modificada
23	ModPolitica	Modificar Política con Id No existente	OK: Política No Modificada – Politica no existe
24	ModPolitica	Modificar Política con nombre repetido	OK: Política No Modificada – Nombre ya existe
25	ModPolitica	Modificar Política con valores nulos	OK: Política No Modificada - detectados valores nulos
26	AltaVulnerabilidad	Crear Vulnerabilidad con datos mandatorios	OK: Vulnerabilidad creada
27	AltaVulnerabilidad	Crear Vulnerabilidad con valores nulos	OK: Vulnerabilidad No creada - detectados valores nulos
28	ModVulnerabilidad	Modificar Vulnerabilidad con Id existente	OK: Vulnerabilidad Modificada
29	ModVulnerabilidad	Modificar Vulnerabilidad con Id No existente	OK: Vulnerabilidad No Modificada – Vulnerabilidad no existe
20	ModVulnerabilidad	Modificar Vulnerabilidad con valores nulos	OK: Vulnerabilidad No Modificada - detectados valores nulos
31	AltaAccionMit	Crear Acción Mitigación con datos mandatorios	OK: Acción Mitigación creada
32	AltaAccionMit	Crear Acción Mitigación con valores mandatorios nulos	OK: Acción Mitigación No creada - detectados valores nulos
33	ModAccionMit	Modificar Acción Mitigación con Id existente	OK: Acción Mitigación Modificada
34	ModAccionMit	Modificar Acción Mitigación con Id No existente	OK: Acción Mitigación No Modificada – Vulnerabilidad no existe
35	ModAccionMit	Modificar Acción Mitigación con valores nulos	OK: Acción Mitigación No Modificada - detectados valores nulos
36	AltaIncumplimiento	Crear Incumplimiento con datos mandatorios	OK: Incumplimiento creado
37	AltaIncumplimiento	Crear Incumplimiento con valores mandatorios nulos	OK: Incumplimiento No creado - detectados valores nulos
38	ModIncumplimiento	Modificar Incumplimiento con Id existente	OK: Incumplimiento Modificado
39	ModIncumplimiento	Modificar Incumplimiento con Id No existente	OK: Incumplimiento No Modificado – Incumplimiento no existe
40	ModIncumplimiento	Modificar Incumplimiento con valores nulos	OK: Incumplimiento No Modificado - detectados valores nulos
41	AltaSimulacionAtaque	Crear Simulación con datos mandatorios	OK: Simulación creada
42	AltaSimulacionAtaque	Crear Simulación con valores nulos	OK: Simulación No creada - detectados valores nulos
43	ModSimulacionAtaque	Modificar Simulación con Id existente	OK: Simulación Modificada
44	ModSimulacionAtaque	Modificar Simulación con Id No existente	OK: Simulación No Modificada – Simulación no existe
45	ModSimulacionAtaque	Modificar Simulación con valores nulos	OK: Simulación No Modificada - detectados valores nulos

46	AltaAuditoria	Crear Auditoria con datos mandatorios	OK: Auditoria creada
47	AltaAuditoria	Crear Auditoria con valores nulos	OK: Auditoria No creada - detectados valores nulos
48	ModAuditoria	Modificar Auditoria con Id existente	OK: Auditoria Modificada
49	ModAuditoria	Modificar Auditoria con Id No existente	OK: Auditoria No Modificada – Auditoria no existe
50	ModAuditoria	Modificar Auditoria con valores nulos	OK: Auditoria No Modificada - detectados valores nulos
51	AltaAuditProces	Crear Auditoria de Proceso con datos mandatorios	OK: Auditoria de Proceso creada
52	AltaAuditProces	Crear Auditoria de Proceso con valores nulos	OK: Auditoria de Proceso No creada - detectados valores nulos
53	ModAuditProces	Modificar Auditoria de Proceso con Id existente	OK: Auditoria de Proceso Modificada
54	ModAuditProces	Modificar Auditoria de Proceso con Id No existente	OK: Auditoria de Proceso No Modificada – Auditoria no existe
55	ModAuditProces	Modificar Auditoria de Proceso con valores nulos	OK: Auditoria de Proceso No Modificada - detectados valores nulos
56	AltaAccionPunit	Crear Acción Punitiva con Id existente	OK: Auditoria creada
57	AltaAccionPunit	Crear Acción Punitiva con valores nulos	OK: Auditoria No creada - detectados valores nulos
58	AltaIncumpAccion	Crear Acción Punitiva para un incumplimiento con Id existente	OK: Acción Punitiva para un incumplimiento creada
59	AltaIncumpAccion	Crear Acción Punitiva para un incumplimiento con valores nulos	OK: Acción Punitiva para un incumplimiento No creada - detectados valores nulos
60	AltaIncumpSimul	Crear de un incumplimiento detectado en simulación con Id existente	OK: Incumplimiento detectado en simulación creado
61	AltaIncumpSimul	Crear un incumplimiento detectado en simulación con valores nulos	OK: Incumplimiento detectado en simulación No creado - detectados valores nulos
62	AltaIncumpAudit	Crear de un incumplimiento detectado en auditoria con Id existente	OK: Incumplimiento detectado en auditoria creado
63	AltaIncumpAudit	Crear un incumplimiento detectado en auditoria con valores nulos	OK: Incumplimiento detectado en auditoria No creado - detectados valores nulos
64	AltaEmpleado	Crear Empleado con Id existente y usuario no eliminado	OK: Empleado creado
65	AltaEmpleado	Crear Empleado con valores mandatorios nulos	OK: Empleado No creado - detectados valores nulos
66	AltaEmpleado	Crear Empleado con Id No existente o usuario no eliminado	OK: Empleado No creado – usuario no existe
67	ModEmpleado	Modificar Empleado con Id existente	OK: Empleado Modificado
68	ModEmpleado	Modificar Empleado con Id No existente o usuario no eliminado	OK: Empleado No Modificado – usuario no existe
69	ModEmpleado	Modificar Empleado con valores nulos	OK: Empleado No Modificado - detectados valores nulos

70	AltaDepartamento	Crear Departamento con Id No existente	OK: Departamento creado
71	AltaDepartamento	Crear Departamento con nombre repetido	OK: Departamento No creado – nombre ya existe
72	AltaDepartamento	Crear Departamento con valores mandatorios nulos	OK: Departamento No creado - detectados valores nulos
73	ModDepartamento	Modificar Departamento con Id existente	OK: Departamento modificado
74	ModDepartamento	Modificar Departamento con nombre repetido	OK: Departamento No modificado – nombre ya existe
75	ModDepartamento	Modificar Departamento con valores mandatorios nulos	OK: Departamento No modificado - detectados valores nulos
76	AltaMuestreo	Crear Muestreo con Id No existente y ID auditoria existente	OK: Muestreo creado
77	AltaMuestreo	Crear Muestreo con Id auditoria No existente	OK: Muestreo No creado – la auditoria no existe
78	AltaMuestreo	Crear Muestreo con valores mandatorios nulos	OK: Muestreo No creado - detectados valores nulos
79	ModMuestreo	Modificar Muestreo con Id Existente	OK: Muestreo modificado
80	ModMuestreo	Crear Muestreo con Id auditoria No existente	OK: Muestreo No creado – la auditoria no existe
81	ModMuestreo	Modificar Muestreo con valores mandatorios nulos	OK: Muestreo No modificado - detectados valores nulos
82	AltaSesion	Crear Sesión Formativa con Id No existente	OK: Sesión Formativa creado
83	AltaSesion	Crear Sesión Formativa con valores mandatorios nulos	OK: Sesión Formativa No creada- detectados valores nulos
84	ModSesion	Modificar Sesión Formativa con Id existente	OK: Sesión Formativa modificado
85	ModSesion	Modificar Sesión Formativa con valores mandatorios nulos	OK: Sesión Formativa No modificado - detectados valores nulos
86	AltaParticipacion	Crear Participación con ID sesión y usuario existente	OK: Participación creada
87	AltaParticipacion	Crear Participación con ID sesión y usuario no existente	OK: Participación No creada – la sesión y usuario no existen
88	AltaParticipacion	Crear Participación con valores mandatorios nulos	OK: Participación No creada - detectados valores nulos
89	ModParticipacion	Modificar Participación con ID sesión y usuario existente	OK: Participación Modificada
90	ModParticipacion	Modificar Participación con ID sesión y usuario no existente	OK: Participación No Modificada – la sesión y usuario no existen
91	ModParticipacion	Modificar Participación con valores mandatorios nulos Participación	OK: Participación No modificada - detectados valores nulos
92	AltaSimulEmpl	Crear Simulación con ID simulación y usuario existente	OK: Simulación del empleado creada
93	AltaSimulEmpl	Crear Simulación con ID simulación y usuario no existente	OK: Simulación del empleado No creada – la sesión y usuario no existen
94	AltaSimulEmpl	Crear Simulación con valores mandatorios nulos	OK: Simulación del empleado No creada - detectados valores nulos

4.2.3. Procedimientos Cambio de Estados

Tal como se indica en el apartado de "Requerimientos", tanto las acciones de mitigación y sus vulnerabilidades pueden cambiar de un estado a otro, dependiendo de la situación en que se encuentren.

A continuación, se detallan los estados posibles para cada una, y cuándo deben actualizarse:

Acciones de mitigación :

- Definida: Estado inicial al momento de la creación de una acción.
- En proceso: Cuando se ha asignado una fecha de inicio.
- Acabada: Cuando se ha asignado una fecha de fin.
- En revisión: Cuando no se sabe cómo realizarla o no se puede realizar por limitaciones de la empresa. Este es el único estado que NO se asignará de forma automática.

Vulnerabilidades:

- Identificada: Estado inicial al momento de la creación de una vulnerabilidad
- Parcialmente mitigada: En el momento en el que alguna de sus acciones de mitigación (pero no todas) se encuentra en estado "Acabada".
- Totalmente Mitigada: En el momento en el que todas sus acciones de mitigación se encuentran en estado "Acabada"

Nombre	accMitigEnRevi
Descripción	Cambia el estado de la acción a "En Revisión"
Parámetros Entrada	Id Accion Mitigación
Parámetros Salida	Proceso realizado correctamente = OK Error detectado en Proceso = ERROR+TIPO DE ERROR
Operativa Proceso	- El proceso verifica que los datos mandatorios pasados no sean nulos - El proceso verifica que el identificado de la acción exista en la base de datos - El proceso verifica cualquier otro tipo de excepción - Si no se detecta error, se realiza el alta y se guarda un log con RSP OK. Si se detecta un error, NO se realiza el alta y se guarda un log con RSP ERROR

Nombre	altaFechIniAccMit
Descripción	Se añade una fecha de inicio a la acción de mitigación. Se cambia el estado de la acción a "En Proceso"
Parámetros Entrada	Id Accion Mitigación, fecha Inicio
Parámetros Salida	Proceso realizado correctamente = OK Error detectado en Proceso = ERROR+TIPO DE ERROR
Operativa Proceso	- El proceso verifica que los datos mandatorios pasados no sean nulos - El proceso verifica que el identificado de la acción exista en la base de datos - El proceso verifica cualquier otro tipo de excepción

	- Si no se detecta error, se realiza el alta y se guarda un log con RSP OK. Si se detecta un error, NO se realiza el alta y se guarda un log con RSP ERROR

Nombre	altaFechFinAccMit
Descripción	Se añade una fecha de fin a la acción de mitigación. Se cambia el estado de la acción a "Acabada". Se cambia el estado de la vulnerabilidad asociada a la acción : - Si existiese alguna otra acción no acabada, cambia al estado "Parcialmente Mitigada" - De lo contrario, cambia al estado "Totalmente Mitigada" -
Parámetros Entrada	Id Accion Mitigación , fechaFin
Parámetros Salida	Proceso realizado correctamente = OK Error detectado en Proceso = ERROR+TIPO DE ERROR
Operativa Proceso	- El proceso verifica que los datos mandatorios pasados no sean nulos - El proceso verifica que el identificado rde la acción exista en la base de datos - El proceso verifica cualquier otro tipo de excepción - Si no se detecta error, se realiza el alta y se guarda un log con RSP OK. Si se detecta un error, NO se realiza el alta y se guarda un log con RSP ERROR

4.2.4. Pruebas Procedimientos Cambio de Estados

Durante la creación de cada uno de los procedimientos del apartado anterior, se realizaron algunas pruebas para comprobar la actualización correcta de los datos:

Pruebas realizadas:

No	Proceso Probado	Descripción	Resultado
1	accMitigEnRevi	Cambiar el estado de una acción existente a "En Revision"	OK: Actualización Realizada
2	altaFechIniAccMit	Añadir la fecha de inicio a una acción de mitigación existente	OK: Actualización Realizada – Se añade una fecha de inicio a la acción de mitigación. Se cambia el estado de la acción a "En Proceso"
3	altaFechFinAccMit	Añadir la fecha de fin a una acción de mitigación existente. Existen otras acciones "no acabadas" asociadas a la misma vulnerabilidad.	OK: Actualización Realizada – Se añade una fecha de fin a la acción de mitigación. Se cambia el estado de la acción a "Acabada". Se cambia el estado de la vulnerabilidad asociada a "Parcialmente_Mitigada".
4	altaFechFinAccMit	Añadir la fecha de fin a una acción de mitigación existente. NO existen otras acciones "no acabadas" asociadas a la misma vulnerabilidad.	OK: Actualización Realizada – Se añade una fecha de fin a la acción de mitigación. Se cambia el estado de la acción a "Acabada". Se cambia el estado de la vulnerabilidad asociada a "Totalmente_Mitigada".

4.2.5. Procedimientos Repositorio Estadístico

Se han creado los siguientes procedimientos almacenados para el cálculo de los valores almacenados en las tablas del Repositorio Estadístico:

KPIs_Empleados_Anyo

Nombre	**CalcKpiEmplAnyo**
Descripción	Proceso que calcula los distintos KPIs relacionados con los empleados de la empresa, agrupados por año, y almacenados en la tabla de eventos KPIs_Empleados_Anyo. El proceso elimina los datos históricos existentes hasta la fecha y los vuelve a insertar teniendo en cuenta los datos actuales.
Parámetros Entrada	Ninguno
Parámetros Salida	Ninguno. Dado que no existen parámetros de entrada, Error detectado en Proceso = ERROR+TIPO DE ERROR

KPIs_Departamentos_Anyo

Nombre	**CalcKpiDeptoAnyo**
Descripción	Proceso que calcula los distintos KPIs relacionados con los departamentos de la empresa, agrupados por año, y almacenados en la tabla de eventos KPIs_Departamen tos_Anyo. El proceso elimina los datos históricos existentes hasta la fecha y los vuelve a insertar teniendo en cuenta los datos actuales.
Parámetros Entrada	Ninguno
Parámetros Salida	Ninguno. Dado que no existen parámetros de entrada, Error detectado en Proceso = ERROR+TIPO DE ERROR

KPIs_Departamentos_Gral

Nombre	**CalcKpiDeptoGral**
Descripción	Proceso que calcula los distintos KPIs relacionados con los departamentos de la empresa, agrupados por año, y almacenados en la tabla de eventos KPIs_Departamen tos_Gral. El proceso elimina los datos históricos existentes hasta la fecha y los vuelve a insertar teniendo en cuenta los datos actuales.
Parámetros Entrada	Ninguno
Parámetros Salida	Ninguno. Dado que no existen parámetros de entrada, Error detectado en Proceso = ERROR+TIPO DE ERROR

KPIs_General

Nombre	**CalcKpiGeneral**
Descripción	Proceso que calcula los distintos KPIs relacionados con los departamentos de la empresa, agrupados por año, y almacenados en la tabla de eventos KPIs_General. El proceso elimina los datos históricos existentes hasta la fecha y los vuelve a insertar teniendo en cuenta los datos actuales.
Parámetros Entrada	Ninguno
Parámetros Salida	Ninguno. Dado que no existen parámetros de entrada, Error detectado en Proceso = ERROR+TIPO DE ERROR

4.2.6 Pruebas Consultas Repositorio Estadístico:

Se debe proporcionar un Repositorio estadístico donde se puedan realizar consultas para obtener los siguientes resultados:

No	Consulta	Resultado
1	Departamento que, en un año concreto, tiene un número mayor de incumplimientos de seguridad registrados en la BD.	OK
2	Proceso de gestión interno que, teniendo en cuenta tota la información de que se dispone en la BD, ha tenido un mayor número de vulnerabilidades detectadas.	OK
3	Top5 de usuarios por número de incumplimientos asociados directamente a ellos, o a su departamento, durante el año en curso.	OK
4	Porcentaje de vulnerabilidades que, en el momento de ejecutar la consulta, están totalmente mitigadas.	OK
5	Número total de acciones de mitigación que, en el momento de ejecutar la consulta, no están totalmente acabadas.	OK
6	Política de seguridad que, en el momento de ejecutar la consulta, ha tenido más incumplimientos (teniendo en cuenta todos los departamentos de la empresa)	OK
7	Dado un determinado departamento de la empresa, y teniendo en cuenta el momento de ejecutar la consulta, porcentaje de usuarios del departamento que no han acabado todas las formaciones de seguridad asignadas	OK
8	Porcentaje de usuarios de la empresa que, en el año en curso, no tienen ningún incumplimiento asignado	OK
9	Teniendo en cuenta todas las auditorías externas realizadas, año en el cual se han detectado más incumplimientos (teniendo en cuenta sólo los detectados durante la auditoría).	OK
10	Porcentaje de vulnerabilidades críticas que, en el momento de ejecutar la consulta, tienen alguna acción de mitigación abierta (que no esté en estado “acabada”).	OK
11	Teniendo en cuenta el último año (el anterior al año en curso), título de la sesión formativa telemática que ha tenido un porcentaje menor de participantes en total.	OK
12	Número de vulnerabilidades críticas detectadas internamente teniendo en cuenta todos los datos de que se dispone. Se consideran detectadas internamente si se detectaron en posterioridad al análisis realizado al inicio del proyecto por la consultora externa.	OK
13	En el momento de ejecutar la consulta, porcentaje de acciones de mitigación en el sistema que están en los estados “en proceso” o “en revisión”.	OK
14	Teniendo en cuenta todas las acciones de mitigación en estado “en proceso”, persona responsable con más acciones asignadas.	OK
15	Número total de **Incumplimientos** por cada departamento de la empresa.	OK

Adjunto a esta memoria, se proporciona un documento anexo con todas las pruebas realizadas a las consultas del Repositorio estadístico, utilizando el set de datos iniciales proporcionados en los scripts.

4.2.7 Scripts Aportados

En el anexo se incluyen los siguientes scripts para la creación de los tablespaces, tablas, procedimientos y carga de datos entre otros:

No	**Nombre *Script***	**Descripción**
1	Creacion_TableSpaces_Usuario.sql	incluye los *scripts* para la creación de los *Tablespaces* y lo usuarios
2	Creacion_Tablas.sql	incluye los *scripts* para la creación de las tablas del *Tablespace* PROCESOS_SEGURIDAD
3	Creacion_Secuencias.sql	incluye los *scripts* para la creación de las secuencias numéricas para los identificadores de las tablas
4	Creacion_Procedimientos_ABM.sql	incluye los *scripts* para la creación de los procedimientos almacenados de alta, baja y modificación de las tablas del *Tablespace* PROCESOS_SEGURIDAD, así como pruebas para cada uno
5	Creacion_Procedimientos_DW.sql	incluye los *scripts* para la creación de los procedimientos almacenados encargados de calcular los datos para las tablas del repositorio estadístico.
6	Creacion_Procedimientos_Estados.sql	incluye los *scripts* para cear los procedimientos almacenados para añadir fechas de inicio y fin a las acciones de mitigación, las cuales a su vez actualizan el estado de las acciones y vulnerabilidades,
7	Carga_Datos_Inicial.sql	incluye los *scripts* para la carga de los datos necesarios para realizar las pruebas
8	Prueba_Procedimientos_Estados	incluye los *scripts* para la realización de un set de prueba para los procedimientos almacenados de cambio de estado de las acciones de mitigación y sus vulnerabilidades.
9	Consultas_Repositorio_Estadistico	incluye las consultas mínimas del repositorio estadístico, según los requerimientos.
10	Pruebas_Repositorio_Estadistico	incluye otras consultas, donde se comprueban las consultas del repositorio estadístico..
	Borrado_Datos_Tablas.sql	Incluye sentencias de bases de datos para el borrado del contenido de las tablas, en caso necesario.

5. Conclusiones

A grandes rasgos, se puede valorar el proceso de trabajo agrupando las actividades en dos grandes fases: La de planificación de las tareas y la ejecución del proyecto en sí.

La etapa de planificación ha sido bastante sencilla, ya que fue relativamente simple decidir cuáles eran las tareas necesarias para la consecución de los objetivos, y alinearlas en el tiempo.

Adicionalmente, se pudo anticipar en el análisis de riesgos algunas circunstancias que podrían dificultar la consecución de los objetivos, y que al final acabaron sucediendo:

- De Índole personal: principalmente, el de que la alumna cursa un estado avanzado de **embarazo**, con los síntomas propios del mismo
- De Índole profesional: un trabajo de alta responsabilidad (*Product Manager*), y a jornada completa, que ya se preveía iba a impactar en las horas de trabajo.

En esta etapa, quizás la mayor autocrítica que se extrae es la **previsión excesivamente optimista de las horas que se dedicarían al proyecto**.

Respecto a la etapa de Ejecución, y durante la primera fase, la de "Recolección y Definición de Requisitos", el reto encontrado fue el de aclarar todas las dudas que iban surgiendo, ya que solo se contaba con un documento (el enunciado) con toda la información correspondiente a la funcionalidad, aspectos no funcionales, y objetivos esperados. Se requirió de una **comunicación exhaustiva con el profesor** para aclarar ciertas ambigüedades y suposiciones que iban apareciendo.

La fase siguiente, la del Diseño: Conceptual, Lógico y Físico, fue la más sencilla de implementar en cuanto a complejidad, pues se conocían perfectamente las técnicas y herramientas a aplicar en cada caso. Se decidió seguir las fases de diseño de bases de datos vistas en la asignatura del grado, lo cual facilitó enormemente la ejecución de las tareas, las cuales estaban bastante asentadas.

Finalmente, en la fase de implementación fue donde se encontró el mayor grado de complejidad. Para esta parte se planificaron 4 semanas de trabajo, que justo coincidieron con algunos temas profesionales (viaje de trabajo), y con algunos problemas de salud ocasionados por el estado de embarazo de la alumna.
Además de que se subestimó bastante una tarea concreta: la **creación de los procedimientos**, tanto los de ABM como los del repositorio estadístico.

A pesar de que se contaba con cierta experiencia en la creación de procedimientos, este conocimiento no fue del todo suficiente para enfrentarse a la actividad con rapidez, por lo que se requirió de mucho más estudio y "prueba y error" para conseguir crear los procedimientos.

Por este motivo, la etapa de Implementación se acabó extendiendo durante los 2 últimos hitos: La entrega de la PEC 3 (donde se aportaron los Procedimientos ABM y sus pruebas) y la Entrega final, donde se aportaron los procedimientos del repositorio estadístico y sus pruebas.

Este hecho provocó un efecto bola de nieve, retrasando a su vez el resto de tareas previstas para la parte final de Entrega de proyecto.

Finalmente, se puede concluir que a la última entrega, los objetivos principales del trabajo han sido cubiertos, se han podido entregar todos los productos esperados con una calidad aceptable. Sin embargo, la planificación prevista se ha desviado bastante de lo previsto debido a todas los motivos expuestos anteriormente. Ha sido sin duda una lección aprendida, aplicable a este y otros proyectos.

Como líneas de evolución futuras para el Proyecto de Seguridad realizado, vemos necesaria la creación de una interfaz visual o aplicación que sirva para el registro de los datos en el sistema. No es sostenible utilizar procedimientos ejecutados directamente en la base de datos para ingresar la información. Entendemos que no estaba en el alcance de este proyecto, pero es evidente que esta sería la evolución lógica de este producto para poder realizar un buen uso del mismo.

6. Glosario

Definición de los términos y acrónimos más relevantes utilizados dentro de la Memoria.

- Almacen de datos (Data Warehouse) : colección de datos orientada a un determinado dominio, que ayuda a la toma de decisiones en la empresa en la que se utiliza.

- Atributo: Define o identifica una característica o propiedad de una entidad

- Base de Datos (BD): conjunto de datos estructurados que pertenecen a un mismo contexto y que se utiliza para administrar de forma electrónica grandes cantidades de información.

- Cascada (Waterfall): Metodología de gestión de proyectos de desarrollo de software, en la que se ordenan las etapas del proceso de forma secuencial.

- Clave Alternativa: Son aquellas claves candidatas que no han sido elegidas como clave primaria.

- Clave Candidata: Consiste en uno o más atributos de la relación cuyos valores no pueden repetirse en dos o más tuplas diferentes; tampoco pueden contener valores nulos.

- Clave Foránea: Atributo que se utiliza para referenciar los datos de una tupla concreta en relación a los de otra tupla de una tabla distinta.

- Clave Primaria: Es una clave candidata que se elige para identificar una tupla en concreto.

- Entidad: elemento principal del diseño conceptual utilizado para representar objetos del dominio

- ER (Entity Relation) / Modelo ER. Modelo entidad-interrelación de datos de alto nivel que permite modelizar los requisitos, las especificaciones y las restricciones de un sistema.

- Espacio Virtual (TableSpace): Se trata de los espacios donde se almacenarán los datos de la base de datos.

- Gantt (Diagrama de Gantt): herramienta gráfica utilizada en gestión de proyectos para indicar el tiempo de dedicación previsto para las diferentes tareas a lo largo de un tiempo determinado.

- Kanban: método de gestión de proyectos, basado en el uso de tableros y tarjetas para la visualización de las tareas y actividades.

- Procedimientos Almacenados (Stored procedure) es un programa almacenado en una base de datos, tilizado para ejecutar una serie de acciones con los datos del sistema.

- RansomWare: tipo de programa dañino que restringe el acceso a determinadas partes o archivos del sistema operativo infectado y pide un rescate a cambio de eliminar esta restricción

- Registro: Equivalente a Tupla

- Relación : en diseño lógico, es equivalente a la entidad y está formada por un grupo de atributos que pueden expresarse dentro de un dominio concreto. Se denota con el nombre de la relación y sus atributos encerrados entre paréntesis.

- Secuencia: Sentencia SQL empleada para generar valores enteros secuenciales únicos y asignárselos a campos numéricos.

- Sistema Gestor de Base de Datos (SGBD) . Tipo de software específico que sirve de interfaz entre la base de datos, el usuario y las aplicaciones que la utilizan.

- SQL (Structured Query Language)**:** lenguaje diseñado para administrar y recuperar la información almacenada en un sistema de base de datos relacional.

- Tabla : En diseño físico, estructuras donde se almacenan los datos. Las tablas son el equivalente a las relaciones obtenidas en el modelo lógico

- Tupla: Consiste en los valores dentro del dominio que corresponden a los distintos atributos de una relación

- UML (Unified Modeling Language): es un lenguaje gráfico de propósito general para modelizar sistemas de software.

7. Bibliografía

1- Casas Roma, Jordi. Introducción al diseño de bases de datos [Recurso de aprendizaje]. Barcelona: Universitat Oberta de Catalunya (UOC);

2- Casas Roma, Jordi; Cuartero Olivera, Josep. Diseño Conceptual de Bases de Datos [Recurso de aprendizaje]. Barcelona: Universitat Oberta de Catalunya (UOC); 2020.

3- Burgués Illa, Xavier; Cuartero Olivera, Josep. Diseño Lógico de Bases de Datos [Recurso de aprendizaje]. Barcelona: Universitat Oberta de Catalunya (UOC); 2020.

4- Cabré i Segarra, Blai; Casas Roma, Jordi; Costal Costa, Dolors; Juanola Juanola, Pere; Plana Vallvé, Ivo; Rius Gavidia, Àngels; Segret i Sala, Ramon. Diseño Físico de Bases de Datos [Recurso de aprendizaje]. Barcelona: Universitat Oberta de Catalunya (UOC); 2020.

5- Oracle® Database Administrator's Guide 11*g* Release 2 (11.2) [Internet]; [consultado entre 1 de abril y el 11 de Junio de 2022]. Disponible en: https://docs.oracle.com/cd/B14117_01/appdev.101/b10795/adfns_pc.htm

6- Using Procedures and Packages [Internet];
[consultado entre 1 de abril y el 11 de Junio de 2022]. Disponible en: https://docs.oracle.com/cd/E18283_01/server.112/e17120/toc.htm

7- Handling PL/SQL Errors [Internet];
[consultado entre 1 de abril y el 11 de Junio de 2022]. Disponible en: https://docs.oracle.com/cd/B14117_01/appdev.101/b10807/07_errs.htm

8- Lane, Paul. Database DataWarehousing Guide - [Oracle Database Data Warehousing Guide, 11*g* Release 2 (11.2) [Internet]. 2001-2013 [consultado entre Marzo ye Junio de 2022]. Disponible en: https://docs.oracle.com/cd/E11882_01/server.112/e25554/title.htm

9- Oracle Tutorial PL/SQL Stored procedure [Internet];
[consultado entre 20 de abril y el 05 de Junio de 2022]. Disponible en: https://www.oracletutorial.com/plsql-tutorial/plsql-procedure/

10- Data Warehousing Guide - Core Concepts [Internet]; Agosto 2020.
[consultado entre 20 de abril y el 05 de Junio de 2022]. Disponible en: https://qimia.io/en/blog/Data-Warehousing-Guide-Core-Concept

11- Pixel. El año de los grandes ciberataques en España**.** Diario El Mundo [internet]. 2021 Diciembre [consultado 20 Feb 2022]; Disponible en: https://www.elmundo.es/tecnologia/2021/12/01/61a63b4ae4d4d8db5a8b4577.html

12- Redacción. Pérdidas por Ransomware en 2021 ya superan los 60mil bitcoins**.** Criptonoticias.com [internet]. 2021 Julio [consultado 21 Feb 2022]; Disponible en: https://www.criptonoticias.com/seguridad-bitcoin/perdidas-ransomware-2021-superan-60mil-bitcoins/

13- Redacción. Waterfall Methodology**.** Workfront.com [internet]. [consultado 24 Feb 2022]; Disponible en: https://www.workfront.com/project-management/methodologies/waterfall

14- Creating, Running and managing Jobs, Oracle® Database Administrator's Guide 11*g* [Internet]; [consultado 10 de Junio de 2022]. Disponible en: https://docs.oracle.com/cd/E18283_01/server.112/e17120/scheduse002.htm

8. Anexos

Ver Documento Adjunto: Anexo 1: Pruebas Repositorio Estadístico.