

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

**Jéssica Agudo Serrano**

Grado de Ingeniería Informática  
Bases de Datos

**Jordi Ferrer Durán**

**Xavier Baró Solé**

Junio 2022



Esta obra está sujeta a una licencia de Reconocimiento-  
NoComercial-SinObraDerivada [3.0 España de Creative  
Commons](https://creativecommons.org/licenses/by-nc-nd/3.0/es/)



## FICHA DEL TRABAJO FINAL

<b>Título del trabajo:</b>	<i>Diseño e implementación de la base de datos para una aplicación de control de procesos de seguridad informática</i>
<b>Nombre del autor:</b>	<i>Jéssica Agudo Serrano</i>
<b>Nombre del consultor/a:</b>	<i>Jordi Ferrer Durán</i>
<b>Nombre del PRA:</b>	<i>Xavier Baró Solé</i>
<b>Fecha de entrega (mm/aaaa):</b>	06/2022
<b>Titulación:</b>	<i>Grado de Ingeniería Informática</i>
<b>Área del Trabajo Final:</b>	<i>Bases de Datos</i>
<b>Idioma del trabajo:</b>	<i>Castellano</i>
<b>Palabras clave</b>	<i>Seguridad, Empresa, Vulnerabilidad</i>
<b>Resumen del Trabajo (máximo 250 palabras):</b>	
<p>Este proyecto tiene como objetivo el diseño e implementación de una base de datos para una aplicación de control de procesos de seguridad informática. A pesar de que la aplicación final irá orientada a una empresa del sector automovilístico, el diseño elegido para la BD puede ser aplicable a cualquier otro tipo de empresa ya que su escalabilidad permite adaptarlo a las especificaciones de la empresa en la que se vaya a utilizar.</p> <p>Este trabajo incluye no solo el diseño e implementación de la BD sino también aquellos procedimientos necesarios para mantenerla actualizada en el día a día de la empresa, además, incluye un repositorio estadístico en el que los usuarios podrán valorar de forma rápida cuál es la situación de la empresa en cada momento de forma actualizada.</p> <p>Un proyecto llevado a cabo gracias a un seguimiento del plan de trabajo establecido y a muchas horas invertidas en ello creando un diseño final de la BD que ha estado evolucionando constantemente en todas y cada una de sus etapas.</p>	

**Abstract (in English, 250 words or less):**

The objective of this project is to design and set up a database for a control app of informatic security processes. Despite the final app is aimed for a car company, the design selected for the BD can be used at any other type of company, as its scalability allows adapting it to the characteristics demanded by the company interested in using it.

This project includes not only the design and setting of the BD but also those necessary procedures needed in order to keep it updated daily in the company. Moreover, it also encloses an archive with all the stats, allowing users to value in a fast way the situation of the company at any time in a very updated way.

This project has been carried out thanks to the monitorization of the work program established and all the amount of hours invested in it, having as a final result the creation of the BD which has been evolving constantly in each and every one of its stages.

**A mi pequeña **MÍA**,  
Siempre serás mi mejor Proyecto.**

**“Per tu, tot”**

## Índice

1.	INTRODUCCIÓN .....	1
1.1.	Contexto y justificación del Trabajo .....	1
1.2.	Objetivos del trabajo .....	2
1.3.	Enfoque y método seguido .....	3
1.4.	Planificación del Trabajo.....	3
1.4.1.	Hitos y Tareas .....	3
1.4.2.	Diagrama de Gantt .....	5
1.4.3.	Seguimiento del Proyecto .....	5
1.5.	Breve resumen de productos obtenidos .....	8
1.6.	Plan de contingencia .....	8
1.7.	Breve descripción de los otros capítulos de la memoria .....	9
2.	PROYECTO .....	10
2.1.	Gestión de requisitos .....	10
2.1.1.	Requisitos Funcionales .....	10
2.1.2.	Requisitos No Funcionales → Restricciones .....	14
2.2.	Análisis y Diseño .....	15
2.2.1.	Diseño Conceptual .....	15
2.2.2.	Diseño Lógico.....	18
	TABLAS ENTIDADES FUERTES.....	18
	TABLAS ENTIDADES RELACIÓN .....	21
	TABLAS COMPLEMENTARIAS .....	22
	TABLAS REPOSITORIO ESTADÍSTICO .....	23
	TABLAS ENUMERACIONES .....	24
2.2.3.	Diseño Físico.....	26
	DICCIONARIO DE DATOS .....	26
	TABLAS ENTIDADES FUERTES.....	26
	T_ACCIONMITIGACION .....	26
	T_AUDITORIA.....	27
	T_DEPARTAMENTO .....	27
	T_EMPLEADO .....	27
	T_POLITICASEGURIDAD.....	29
	T_PROCESOGEMPRESA .....	30
	T_SESIONFORMACION.....	30
	T_SIMULACION .....	31
	T_VULNERABILIDAD .....	31
	TABLAS ENTIDADES RELACIÓN .....	32
	T_AUDITORIA_POLITICASEGURIDAD .....	32
	T_DEPARTAMENTO_PROCESOGEMPRESA .....	32
	T_EMPLEADO_SESIÓNFORMACION.....	33
	T_EMPLEADO_SIMULACION .....	33
	T_INCUMPLIMIENTO_DEPTO .....	33
	T_INCUMPLIMIENTO_EMP .....	34
	T_SIMULACION_POLÍTICASEGURIDAD .....	34
	T_VULNERAB_PROCESOGEMPRESA.....	35
	TABLAS COMPLEMENTARIAS .....	35
	T_POBLACION .....	35
	T_PROVINCIA.....	35
	TABLAS REPOSITORIO ESTADÍSTICO .....	36

DATA WAREHOUSE .....	37
T_CI_SUMA .....	37
T_CI_RESULT.....	37
T_C2_SUMA .....	37
T_C2_RESULT.....	38
T_C4.....	38
T_C5.....	38
T_C6_SUMA .....	38
T_C6_RESULT.....	38
T_C7 .....	38
T_C8.....	39
T_C9_SUMA .....	39
T_C9_RESULT.....	39
T_C10.....	39
T_C12.....	39
T_C13.....	39
TABLAS ENUMERACIONES .....	40
T_EstadoAccionMitigacion .....	40
T_AfirmNeg .....	40
T_TipoSesionFormacion .....	41
T_TipoAuditoria .....	41
T_TipoIncumplimiento .....	41
T_TipoProcesoEmpresa .....	42
T_DeteccionVulnerab .....	42
T_MotivoCausaBaja .....	42
T_EstadoVulnerab.....	43
REFERENCIAS .....	43
2.2.4. Análisis de los Procedimientos Almacenados y Disparadores.....	44
PROCEDIMIENTOS ALMACENADOS .....	45
Alta/Baja/Modif de Entidades .....	45
Otros Procedimientos .....	62
DISPARADORES .....	62
2.3. Implementación .....	63
2.3.1. SGBD .....	63
2.3.2. Scripts para la BD .....	63
2.3.3. Repositorio Estadístico.....	64
2.4. Pruebas .....	65
2.4.1. Plan de pruebas .....	65
2.4.2. Elaboración del Juego de Pruebas .....	66
2.4.3. Realización de las Pruebas y Resultado.....	66
2.5. Mejoras .....	66
3. CONCLUSIONES .....	69
4. GLOSARIO .....	71
5. BIBLIOGRAFÍA.....	73
5.1. Libros .....	73
5.2. Webs.....	73
6. ANEXOS .....	75



## Lista de figuras

Ilustración 1. Plan de Trabajo.....	4
Ilustración 2. Diagrama de Gantt.....	5
Ilustración 3. Plan de Contingencia.....	9
Ilustración 4. Requisitos No Funcionales .....	15
Ilustración 5. Modelo Conceptual .....	17
Ilustración 6. Diseño Lógico, Entidades fuertes.....	20
Ilustración 7. Diseño Lógico, Entidades Relación .....	22
Ilustración 8. Diseño Lógico, Tablas Complementarias.....	22
Ilustración 9. Diseño Lógico, Tablas R.E.....	23
Ilustración 10. Diseño Lógico, Tablas Enumeraciones .....	24
Ilustración 11. Modelo Lógico de la BD .....	25

# 1. INTRODUCCIÓN

## 1.1. Contexto y justificación del Trabajo

No es una novedad que durante el siglo XXI la informatización de los procesos y datos empresariales está en un continuo auge. Cada vez son más las empresas, por no decir que ya prácticamente todas, que confían sus datos a un sistema informático.

De esta forma no es de extrañar que las empresas muestren su preocupación por blindar sus datos de ataques informáticos que no solo podrían bloquear su producción, sino que además estarían expuestos a una violación de la LOPD lo cual podría suponer consecuencias graves para la propia empresa.

Según el IBM Cyber Resilient Organization Study 2021<sup>1</sup>, más del 51% de los profesionales de seguridad IT han sufrido un ciberataque en los últimos 12 meses y el 46 % experimentó al menos un ataque de ransomware en los últimos dos años<sup>2</sup> y para este año 2022 seguirá la tendencia en alza de los ataques informáticos basados en el excesivo incremento de los mismos durante el 2021.

La pandemia del COVID-19 y el teletrabajo fueron las causas principales para generar una ola de ataques a gran escala. Debido a esto, las medidas de seguridad informática se han convertido en prioritarias, especialmente para las empresas o entidades que dependen casi al 100% de Internet en sus operaciones.

Red Seguridad<sup>3</sup> e Infobae<sup>4</sup> coinciden en muchos aspectos a tomar en cuenta en las previsiones para el 2022, pero de todas ellas vamos a destacar las siguientes:

- **Filtraciones de datos.** El teletrabajo, las *fake news* y el *phising*, seguirán generando con más frecuencia y a mayor escala estas fugas de información.
- **Ataques a dispositivos móviles.** El uso creciente de aplicaciones móviles y el incremento de celulares a nivel mundial, se convierten en una nueva fuente de suministro de dinero fácil para los hackers con el robo de señal, contraseñas, datos, etc.

---

<sup>1</sup> <https://www.ibm.com/resources/guides/cyber-resilient-organization-study/>

<sup>2</sup> Datos obtenidos de: [https://www.optical.pe/blog/tipos-de-ataques-informaticos-y-previsiones-para-el-2022/#Previsiones\\_para\\_el\\_2022](https://www.optical.pe/blog/tipos-de-ataques-informaticos-y-previsiones-para-el-2022/#Previsiones_para_el_2022)

<sup>3</sup> Red Seguridad: [https://www.redseguridad.com/actualidad/informes-ciberseguridad/que-ciberamenazas-seran-tendencia-en-2022\\_20211103.html](https://www.redseguridad.com/actualidad/informes-ciberseguridad/que-ciberamenazas-seran-tendencia-en-2022_20211103.html)

<sup>4</sup> Infobae: <https://www.infobae.com/america/peru/2021/12/08/cuales-son-las-predicciones-de-ciberseguridad-global-para-el-2022/>

- **Tecnología *deepfake*.** La tendencia de los *fakes* también será innovadora para los *hackers* este 2022. La posibilidad de crear vídeos y audios falsos cada día más reales, permitirá manipular opiniones, datos sensibles y permisos de acceso de formas inimaginables.
- **Ransomware.** Por supuesto, los secuestros de datos e información, así como de sistemas completos serán dejados a un lado por la ciberdelincuencia.

Entonces, ¿Cómo prevenimos los ataques informáticos? Una buena educación tecnológica y saber informarnos correctamente siempre será la mejor arma contra los ciber atacantes. Debemos de tener presente que, por más dinero que una empresa invierta en seguridad informática, “está vendida” si sus propios trabajadores no disponen de esta educación tecnológica sobre amenazas.

## 1.2. Objetivos del trabajo

El objetivo principal de este trabajo es implementar un sistema de Base de Datos para dar respuesta a una necesidad planteada por una gran empresa del sector automovilístico que quiere implantar una nueva aplicación para controlar todos sus procesos de Seguridad Informática.

Dentro de este objetivo principal se engloban otros que, en su conjunto, conformarán las necesidades a cubrir para el correcto funcionamiento de la Base de Datos que solicita el cliente. Estos “subobjetivos” serán los siguientes:

- El sistema debe monitorear en cada momento la situación actual y las acciones llevadas a cabo para mitigar cualquier posible vulnerabilidad abierta.
- El sistema debe registrar los incumplimientos de las políticas de seguridad de obligado cumplimiento establecidas por la empresa a la vez que cumple con las restricciones de confidencialidad oportunas.
- El sistema debe guardar registro tanto de las sesiones de formativas que realice la empresa como de los usuarios que participen en ellas.
- El sistema debe gestionar el control de auditorías a las que se vea sometida la empresa.

Cabe destacar también como objetivo que el sistema a implementar debe poder trabajar con un elevado volumen de datos de la forma más eficiente posible y debe ofrecer los diferentes resultados que se definan en tiempo constante 1.

La Base de Datos a desarrollar deberá de ser escalable y contará con los procedimientos necesarios para su gestión y acceso.

### 1.3. Enfoque y método seguido

Puesto que se trata de un producto diseñado de forma específica para un tipo de empresa en concreto será desarrollado desde 0 siguiendo las especificaciones dadas por el cliente, aun así, cabe destacar que la escalabilidad del producto propicia que este sea aplicable a otro tipo de empresa. Es importante señalar que en este proyecto nos centraremos en los procesos de seguridad por la importancia fundamental que suponen en este trabajo.

Así pues, el proyecto se desarrollará en 5 etapas diferentes:

- **Análisis previo y planificación:** En esta etapa se hará una recopilación de información y se desarrollará el plan de trabajo.
- **Requisitos:** Se definirán las especificaciones que demanda el cliente (enunciado del proyecto)
- **Análisis y diseño:** Etapa en la que se llevará a cabo el análisis y diseño de la futura BD. Cabe destacar que esta etapa se mantendrá “viva” a lo largo de toda la creación del producto.
- **Implementación:** Durante esta etapa se creará tanto la BD como los procedimientos que permitirán la gestión y acceso a la misma.
- **Pruebas:** Creación de los juegos de pruebas para verificar que se cumple con las especificaciones

### 1.4. Planificación del Trabajo

A continuación, se detalla la planificación del proceso de trabajo, aunque hay que señalar que estos tiempos son meramente orientativos. El tiempo fijo disponible, por motivos laborales y familiares, para dedicar a este proyecto es de 12 horas semanales de lunes a viernes, a excepción de las semanas del 18 al 22 de abril y del 16 al 20 de mayo en las que por festivos laborales se dispondrá de más tiempo que será utilizado, al igual que los fines de semana que se incluyen hasta la finalización del proyecto, como recurso de urgencia en caso de imprevistos sobre todo laborales y/o de salud. Se incluye plan de contingencia en el apartado 1.6

#### 1.4.1. Hitos y Tareas

Puesto que la documentación a entregar en cada una de las PEC corresponde al trabajo realizado hasta el momento de su entrega, se va a planificar el trabajo en base al ciclo de vida del producto a desarrollar. El tiempo planificado para la documentación de cada una de las tareas está incluido dentro de las mismas ya que tanto la creación del producto y su propia documentación se entienden como procesos paralelos.

Así pues, las planificaciones iniciales quedarán de la siguiente manera:

DESCRIPCIÓN	DURACIÓN	INICIO	FIN
<b>Análisis Previo y Planificación</b>	<b>10 horas</b>	<b>jue 17/02/22</b>	<b>lun 07/03/22</b>
Recopilar información	2 horas		
Creación y desarrollo de los puntos del plan de trabajo	2 horas	jue 03/03/22	jue 03/03/22
Revisión y Entrega primera versión (V1) al consultor	1 hora		
Creación diagramas Gantt	3 horas		
Realización de correcciones según feedback consultor	1 hora	vie 04/03/22	vie 04/03/22
Entrega en el REC de la PEC 1	1 hora	lun 07/03/22	lun 07/03/22
<b>Requisitos</b>	<b>8 horas</b>	<b>mar 08/03/22</b>	<b>vie 11/03/22</b>
Definición de requisitos	4 horas	mar 08/03/22	mie 09/03/22
Definición de restricciones	4 horas	jue 10/03/22	vie 11/03/22
<b>Análisis y Diseño</b>	<b>41 horas</b>	<b>lun 14/03/22</b>	<b>vie 08/04/22</b>
Instalar herramientas de modelado	3 horas	lun 14/03/22	lun 14/03/22
Diseño Conceptual de la BD	10 horas		
Diseño Lógico de la BD	10 horas	mar 15/03/22	vie 01/04/22
Diseño Físico de la BD	10 horas		
Análisis de los Procedimientos almacenados	8 horas	lun 04/04/22	vie 08/04/22
<b>Implementación</b>	<b>31 horas</b>	<b>lun 11/04/2022</b>	<b>mie 11/05/22</b>
Instalación entorno desarrollo	4 horas	lun 11/04/22	lun 11/04/22
Ejecución Scripts	4 horas	lun 25/04/22	lun 25/04/22
Construcción Procedimientos	9 horas	mar 26/04/22	vie 29/04/22
Revisión y Ajustes en Implementación de la BDD	9 horas	lun 02/05/22	mar 10/05/22
Plan de Pruebas	5 horas	mie 11/05/22	mie 11/05/22
<b>Pruebas</b>	<b>15 horas</b>	<b>jue 12/05/22</b>	<b>vie 27/05/22</b>
Elaboración Juego de Pruebas	5 horas	jue 12/05/2	vie 13/05/22
Realización de Pruebas	5 horas	lun 16/05/2	vie 27/05/22
Ajustes	5 horas		

Ilustración 1. Plan de Trabajo

## 1.4.2. Diagrama de Gantt

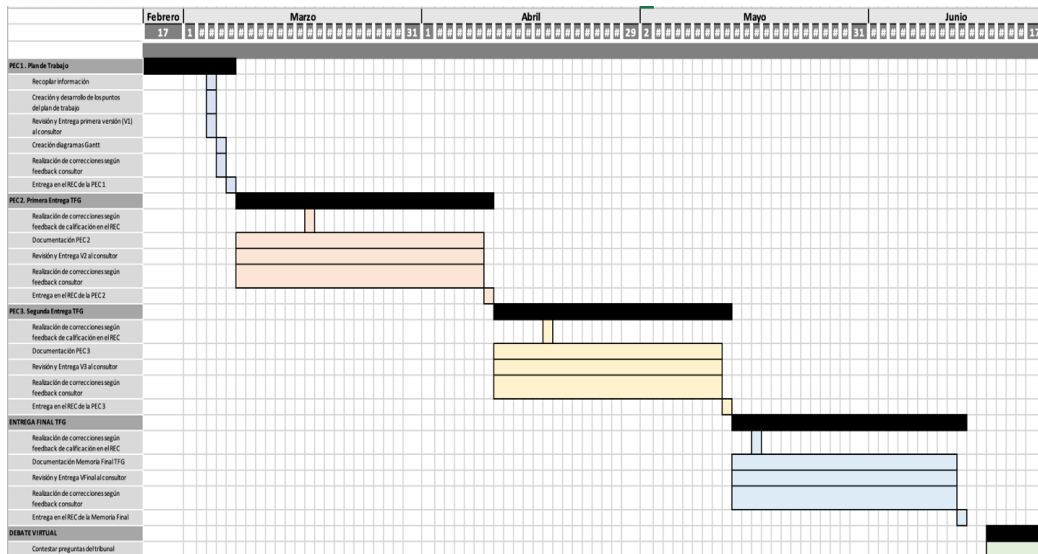


Ilustración 2. Diagrama de Gantt

## 1.4.3. Seguimiento del Proyecto

**PEC 1:** A pesar de haber empezado esta parte del proyecto con fecha bastante avanzada no hubo complicaciones y se pudo entregar dentro de la fecha prevista incluso enviando al consultor una versión más, además de la ya planificada, para revisar últimos cambios.

**PEC 2:** Durante la realización de esta PEC me di cuenta de que en esta parte de la planificación había sido demasiado optimista; esto sumado a la carga laboral inesperada de estas semanas hizo que tuviera que hacer uso del plan de contingencia desarrollado en el apartado 1.6 dentro de esta misma memoria.

El primer punto de dicho plan de contingencia trata el impacto referente a la disminución de horas dedicadas al proyecto. Realmente el problema no ha sido tanto la disminución de horas sino más bien los cambios de comienzo y fin de cada una de las tareas, pero las medidas nos sirven de la misma manera y así han sido convenientemente aplicadas. Al reducir la disponibilidad de horas de proyecto entre semana las primeras semanas he tenido que disponer de las horas de fin de semana para poder llevar a cabo el proyecto. Esto ha provocado que no haya podido profundizar en la búsqueda de datos tal y como tenía pensado así que, puesto que la medida incluía la semana del 18 al 22 de abril, emplearé estos días para profundizar en la búsqueda y revisar los diseños por lo que es posible que en la siguiente entrega estos apartados sufran modificaciones. Puesto que se espera que estos diseños sean modificados se reserva el apartado de “Análisis de los procedimientos almacenados” para la siguiente entrega y así realizar este análisis en base a las modificaciones que se espera realizar.

**PEC 3:** Como ya se comentó en el seguimiento de la PEC 2, la PEC 3 empezaría con la revisión de los diseños presentados en la última entrega y con esto, el inicio

de la realización del apartado “Análisis de los procedimientos almacenados”, así que dado este cambio se decidió invertir del plan de trabajo el orden de las fases “Construcción de procedimientos” y “Revisión y ajustes en implementación de la BDD”, aunque realmente esta última está en constante cambio ya que siempre aparecen mejoras que se pueden realizar para optimizar el funcionamiento del sistema.

La revisión de la PEC 2 supuso, principalmente, los siguientes cambios:

- Se incluye la restricción RNF-009
- Modificaciones en el diseño lógico:
  - Se incluyen el conjunto de tablas llamado: “ENUMERACIONES”, que no serán de utilidad en la creación y mantenimiento de la BDD, pero si útiles y necesarias de cara a la implementación de la futura aplicación
  - Se incluyen las tablas “POBLACION” y “PROVINCIA”, creadas con el mismo objetivo que las “Enumeraciones” anteriores, facilitarán la introducción de datos de cara a la futura aplicación.
  - Se añaden atributos a las entidades para completar la información disponible en la BDD.
  - Se modifican algunos nombres de atributos y tablas para mejorar su identificación

Este tipo de modificaciones han estado presentes, no únicamente al inicio de la realización de esta entrega, sino a lo largo de toda ella y no se descarta que surjan nuevas modificaciones con la realización de la última entrega.

Los atributos incluidos en las entidades de la BDD se consideran los necesarios y suficientes como para iniciar los servicios requeridos aunque, al tratarse de una BDD escalable, se entiende que estos son ampliables de cara a futuros requerimientos.

Una vez realizadas las primeras modificaciones, y siguiendo con el plan de trabajo, se procedió a la instalación del entorno de desarrollo. Esto llevó también más horas de las planificadas ya que la instalación de Oracle en Mac tiene sus peculiaridades y esto hizo que lo que en principio estaba planificado para 4 horas supusiera, no solo más horas, sino varios días de trabajo.

Durante el tiempo de esta entrega, de alguna manera, la construcción de procedimientos y parte de la fase de pruebas se han entremezclado por lo que esto ha implicado también un consumo de tiempo de la fase de construcción de procedimientos con el que no se contaba, aunque no es de gran gravedad ya que, al fin y al cabo se puede considerar como parte de trabajo ya realizado de la siguiente entrega así que, simplemente, en la siguiente entrega se empleará tiempo de elaboración y realización de pruebas para crear los procedimientos que faltan por elaborar.

Cabe decir también que, debido a su naturaleza, el apartado de Plan de pruebas se reservará para hacerlo conjuntamente con todos los apartados correspondientes a las pruebas del proyecto que tendrán su entrega en la PEC 4.

Estos cambios y la realidad de que en esta entrega no se entregan todos los procedimientos que esta requiere, no supone mayor problema en la próxima entrega ya que, tal y como estaba establecido en el plan de contingencia, la semana del 16 al 20 de mayo tengo mayor disponibilidad debido a vacaciones labores y, por lo tanto, puedo tener mayor dedicación de horas para la realización del proyecto.

**ENTREGA FINAL:** Sin ninguna duda esta ha sido la etapa más complicada en todo el desarrollo del proyecto. Varias confusiones con el enunciado y la complejidad de tener en cuenta todos y cada uno de los detalles a implementar junto con los nervios, el cansancio y la presión de ser “la entrega final” han sido factores que, claramente, han marcado de forma negativa la consecución de esta fase.

En el seguimiento de la PEC anterior concluía diciendo que no haber entregado todo lo necesario no suponía mayor problema ya que durante la fase de esta entrega iba a disponer de mayor disponibilidad de tiempo por tener una semana de vacaciones en el trabajo, pues bien, esa semana llegó y sí, obviamente la empleé en dedicarle todo mi tiempo en avanzar en el trabajo, esto sería una buena noticia de no ser porque al hablar con el tutor la semana siguiente me di cuenta de que todo el trabajo que había estado realizando no me había servido para absolutamente nada ya que no era eso lo que se me pedía en el enunciado del proyecto. Una confusión por mi parte me había hecho perder toda una semana de trabajo... Y por si no era suficiente con esta semana perdida, en una de las noches de trabajo de la semana después de las “vacaciones”, perdí el diseño del modelo lógico y tuve que volver a realizarlo; gracias a que tenía copia de las modificaciones del último día y, en papel, todas las anotaciones de los cambios de esa noche pude salvar unas cuantas horas, aun así, las horas invertidas en volver a realizar lo que ya estaba hecho fueron horas perdidas de cara a poder adelantar tanto como me hubiera gustado.

A todo esto, hay que añadir que en esta entrega no solo se envía la memoria sino ya todo el trabajo al completo por lo que las horas de trabajo respecto a las entregas anteriores se han multiplicado consideradamente.

Tengo que reconocer que, durante esta fase, el seguimiento del plan de trabajo ha sido materialmente inexistente. Las horas de pruebas se entremezclaban con las horas de elaboración de procedimientos, documentación y demás y el trabajo a contrarreloj ha sido el protagonista indiscutible de esta entrega.

He de admitir que las bajadas de ánimo también han asumido un papel importante en esta entrega, sobre todo al hablar con el tutor y darme cuenta de que todo lo que llevaba hecho durante aquella semana de vacaciones no había servido para absolutamente nada. Pero ante esta situación no quedaba otra más que reponerse y seguir. En ese momento mi objetivo estaba en conseguir al menos, 2-3 procedimientos de los que pide el enunciado y al final conseguí sacarlos prácticamente todos, ¿es esto positivo? Pues a pesar de que la respuesta obvia es que sí, esto es algo que, a día de hoy, no acabo de tener muy claro. Sacar once procedimientos es algo que está bien, pero seguramente no he sido tan minuciosa



en los detalles como me gustaría y, además esto ha supuesto restarle horas al resto de elaboración del trabajo, sobre todo a la memoria y al vídeo de presentación, y este equilibrio es algo que ha resultado difícil de mantener.

Dicho todo esto, solo me queda decir que, entre las modificaciones principales realizadas en esta etapa se encuentran:

- Ampliación del apartado 2.3. Con la implementación y documentación de los procedimientos que quedaron pendientes en la última entrega.
- Documentación final
- Por supuesto, la modificación del modelo y diseño lógico tal y como también ha sucedido en las anteriores etapas

### **1.5. Breve resumen de productos obtenidos**

Con la finalización de este proyecto obtendremos, y se hará entrega, de los siguientes productos:

- Memoria del proyecto realizado
- Vídeo explicativo del trabajo realizado
- Producto que incluye los scripts de creación de la BD y los procedimientos de acceso y gestión además de juego de pruebas que verifique que se cumple con los requisitos pedidos.
- Autoinforme de evaluación
- Archivo comprimido con los anexos obtenidos

### **1.6. Plan de contingencia**

Una vez analizados los riesgos potenciales a los que está expuesto el proyecto a lo largo de su ejecución detallamos, a continuación, las medidas que se plantean para paliarlos:

IMPACTO	MEDIDAS
Disminución de horas dedicadas al proyecto	Los fines de semana y las semanas del 18 al 22 de abril y del 16 al 20 de mayo se reservan con mayor disponibilidad para este tipo de contingencias
Pérdida de datos y/o de dispositivo de trabajo	Se guarda diariamente una copia del trabajo realizado hasta el momento y se dispone en el trabajo de equipos a los que tener acceso (limitado a los horarios del entorno laboral)
Pérdida de comunicación con la UOC	Acceso a WIFI desde el entorno de trabajo (limitado a los horarios del entorno laboral)

En casos extremos se plantearía la opción de pedir al tutor una ampliación de plazos de entrega

*Ilustración 3. Plan de Contingencia*

### 1.7. Breve descripción de los otros capítulos de la memoria

A continuación, en el capítulo 2 de la memoria encontraremos todo el proceso de creación de la propia BD, desde la especificación de los requisitos hasta la propia implementación de dicha BD.

## 2. PROYECTO

El desarrollo de bases de datos es un proceso relacionado con la producción de un sistema de bases de datos que cubra las necesidades de una determinada organización<sup>5</sup>. Esta parte del proyecto se dividirá en varias fases según el ciclo de vida de cada momento.

### 2.1. Gestión de requisitos

La obtención de requisitos implica establecer los requisitos técnicos fundamentales que deberá cumplir el sistema a través de un proceso de interacción tanto formal como informal entre los desarrolladores y los *stakeholders* (portavoces) de la organización<sup>6</sup>. En este caso la información de nuestro “cliente” será el enunciado del Trabajo de donde obtendremos la información necesaria para llevarlo a cabo.

#### 2.1.1. Requisitos Funcionales

CÓDIGO	DESCRIPCIÓN
<b>RF-001</b>	Atendiendo al enunciado... <ul style="list-style-type: none"><li>- Pág. 3, párr. 1: <i>"Cada vulnerabilidad detectada debe de estar registrada en la BD"</i></li><li>• El sistema debe guardar un registro de todas las vulnerabilidades, tanto las ya detectadas como las futuras</li></ul>
<b>RF-002</b>	Atendiendo al enunciado... <ul style="list-style-type: none"><li>- Pág. 3, párr. 1: <i>"... y podrá tener alguno de los estados siguientes: identificada, no mitigada, parcialmente mitigada o totalmente mitigada"</i></li><li>• La entidad "Vulnerabilidad" tendrá un campo "Estado" cuyos valores serán : {Identificada, No mitigada, Parcialmente mitigada, Totalmente mitigada}</li></ul>
<b>RF-003</b>	Atendiendo al enunciado... <ul style="list-style-type: none"><li>- Pág 3, párr.1: <i>"También podrán ser críticas o no"</i></li><li>• La entidad "Vulnerabilidad" contendrá un campo "Crítica" cuyos valores serán: {Sí, No}</li></ul>

---

<sup>5</sup> Beynon-Davies, P. (2018). *Sistemas de bases de datos*. Editorial Reverté.

<sup>6</sup> Beynon-Davies, P. (2018). *Sistemas de bases de datos*. Editorial Reverté.

<b>RF-004</b>	<p>Atendiendo al enunciado...</p> <ul style="list-style-type: none"> <li>- Pág 3, párr.2: <i>"...la empresa iniciará un proceso para analizarlas y definir las acciones de mitigación..."</i></li> </ul> <ul style="list-style-type: none"> <li>• El sistema debe guardar un registro del listado de acciones de mitigación por cada vulnerabilidad</li> </ul>
<b>RF-005</b>	<p>Atendiendo al enunciado...</p> <ul style="list-style-type: none"> <li>- Pág 3, párr.2: <i>"Cada acción de mitigación definida debe tener un responsable y una fecha límite de implantación"</i></li> </ul> <ul style="list-style-type: none"> <li>• La entidad "Acciones" deberá contener los campos "Responsable" y "Fecha límite"</li> </ul>
<b>RF-006</b>	<p>Atendiendo al enunciado...</p> <ul style="list-style-type: none"> <li>- Pág 3, párr.2: <i>"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)"</i></li> </ul> <ul style="list-style-type: none"> <li>• La entidad "Acciones" deberá contener el campo "Estado" que podrá tomar los siguientes valores: {Definida, En proceso, Acabada, En revisión}</li> </ul>
<b>RF-007</b>	<p>Atendiendo al enunciado...</p> <ul style="list-style-type: none"> <li>- Pág 3, párr.3: <i>"Con el objetivo de asegurar su correcta implantación, la empresa definirá unas políticas de seguridad de obligado cumplimiento por parte de todas las personas y departamentos de la empresa"</i></li> </ul> <p>El sistema debe almacenar un registro de las políticas de seguridad definidas por la empresa</p>
<b>RF-008</b>	<p>Atendiendo al enunciado...</p> <ul style="list-style-type: none"> <li>- Pág 3, párr.4: <i>"... y el incumplimiento de alguna de ellas conllevará consecuencias administrativas por parte de RRHH para las personas implicadas"</i></li> </ul> <p>El sistema debe guardar un registro de las consecuencias administrativas ocasionadas por el incumplimiento de las políticas de seguridad.</p>
<b>RF-009</b>	<p>Atendiendo al enunciado...</p> <ul style="list-style-type: none"> <li>- Pág 4, párr.1: <i>"Se deberá registrar también en la BD todos estos incumplimientos..."</i></li> </ul> <p>El sistema debe almacenar un registro del total de incumplimientos cometidos por política en cada departamento</p>

<b>RF-010</b>	<p>Atendiendo al enunciado...</p> <ul style="list-style-type: none"> <li>- Pág 4, párr.2: <i>"La aplicación también deberá llevar un registro exhaustivo de todas las sesiones de formación..."</i></li> </ul> <p>El sistema debe guardar un registro de las sesiones formativas que se realicen en la empresa</p>
<b>RF-011</b>	<p>Atendiendo al enunciado...</p> <ul style="list-style-type: none"> <li>- Pág 4, párr.2: <i>"La aplicación también deberá llevar un registro exhaustivo de todas las sesiones de formación, tanto presenciales como telemáticas..."</i></li> </ul> <ul style="list-style-type: none"> <li>• La entidad "SesionFormacion" dispondrá de un campo: "Tipo" que podrá tomar los valores: {Presencial, Telemática}</li> </ul>
<b>RF-012</b>	<p>Atendiendo al enunciado...</p> <ul style="list-style-type: none"> <li>- Pág 4, párr.2: <i>"Se deberán registrar... y los usuarios que participen en ellas"</i></li> </ul> <ul style="list-style-type: none"> <li>• El sistema debe llevar un registro de los usuarios que participan en cada una de las sesiones formativas</li> </ul>
<b>RF-013</b>	<p>Atendiendo al enunciado...</p> <ul style="list-style-type: none"> <li>- Pág 4, párr.2: <i>"... y la intención es realizar... y simulaciones controladas de ataques para saber qué usuarios no siguen las directrices definidas"</i></li> </ul> <p>El sistema debe registrar las simulaciones de ataques con un registro de aquellos usuarios que no sigan las instrucciones definidas</p>
<b>RF-014</b>	<p>Atendiendo al enunciado...</p> <ul style="list-style-type: none"> <li>- Pág 4, párr.2: <i>"La empresa definirá las acciones punitivas a realizar sobre los usuarios implicados..."</i></li> </ul> <p>El sistema debe guardar un registro de las acciones punitivas a realizar sobre los empleados que no siguen las directrices definidas</p>
<b>RF-015</b>	<p>Atendiendo al enunciado...</p> <ul style="list-style-type: none"> <li>- Pág 4, párr.2: <i>"... pero nos piden que la BD que definiremos tenga en cuenta estos casos y que se añadan a la lista de incumplimientos de cada departamento"</i></li> </ul> <ul style="list-style-type: none"> <li>• A la lista de incumplimientos por departamento que debe registrar el sistema se debe de sumar los casos de usuario que no siguen las directrices definidas en las simulaciones.</li> </ul>

<b>RF-016</b>	<p>Atendiendo al enunciado...</p> <ul style="list-style-type: none"> <li>- Pág 4, párr.3: <i>"... debe permitir gestionar es el control de las diferentes auditorías de seguridad definidas por la empresa."</i></li> </ul> <p>El sistema debe guardar un registro de las auditorías de seguridad definidas por la empresa</p>
<b>RF-017</b>	<p>Atendiendo al enunciado...</p> <ul style="list-style-type: none"> <li>- Pág 4, párr.3: <i>"La auditoría de procesos de seguridad estará ligada a las diferentes políticas definidas y aprobadas por la empresa."</i></li> </ul> <p>Cada una de las auditorías de seguridad almacenadas debe de estar ligada a una política ya aprobada.</p>
<b>RF-018</b>	<p>Atendiendo al enunciado...</p> <ul style="list-style-type: none"> <li>- Pág 4, párr.3: <i>"Dentro de estas auditorías, que serán realizadas por equipos internos o externos según se decida en cada momento, ..."</i></li> </ul> <p>La entidad "Auditoría" debe contener un campo "Tipo" que podrá tomar los valores: {Interno, Externo}</p>
<b>RF-019</b>	<p>Atendiendo al enunciado...</p> <ul style="list-style-type: none"> <li>- Pág 4, párr.3: <i>"El sistema debe permitir guardar todos los muestreos hechos durante la auditoría"</i></li> </ul> <p>El sistema debe guardar un registro de los aspectos analizados en cada auditoría: qué se analiza y qué parámetros se evalúan</p>

## 2.1.2. Requisitos No Funcionales → Restricciones

CÓDIGO	DESCRIPCIÓN
RNF-001	<ul style="list-style-type: none"> <li>• La base de datos será transaccional</li> </ul>
RNF-002	<ul style="list-style-type: none"> <li>• Se utilizará el motor de base de datos ORACLE</li> </ul>
RNF-003	<p>Atendiendo al enunciado...</p> <ul style="list-style-type: none"> <li>- Pág 5, párr.3: <i>"Toda la gestión y acceso a la información se hará mediante procedimientos de BD, siendo esta la única manera de acceder"</i></li> <li>• Como dice en el mismo párrafo: "... no será necesario implementar ninguna interfaz de usuario con un lenguaje de programación de alto nivel"</li> </ul>
RNF-004	<p>Atendiendo al enunciado...</p> <ul style="list-style-type: none"> <li>- Pág 5, párr.4: <i>"... la aplicación ha de funcionar para cualquier volumen de datos"</i></li> </ul>
RNF-005	<p>Atendiendo al enunciado...</p> <ul style="list-style-type: none"> <li>- Pág 6, párr.1: <i>"...debe ofrecer los diferentes resultados que se definan en tiempo constante 1"</i></li> </ul>
RNF-006	<p>Atendiendo al enunciado...</p> <ul style="list-style-type: none"> <li>- Pág 7, párr.2: <i>"La BD deberá de ser escalable para poder ir incorporando progresivamente todas aquellas necesidades que surjan durante su vigencia"</i></li> </ul>
RNF-007	<p>Atendiendo al enunciado...</p> <ul style="list-style-type: none"> <li>- Pág 7, párr.4: <i>"...con tal de facilitar el mantenimiento del sistema... disponer de mecanismos que permitan resolver potenciales problemas de integración con el resto del sistema"</i></li> <li>• Como también especifica el enunciado se creará: "un log de las acciones realizadas con la BD, mecanismos para testear la funcionalidad de la BD, etc."</li> </ul>
RNF-008	<p>Atendiendo al enunciado...</p> <ul style="list-style-type: none"> <li>- Pág 7, párr.5: <i>"Para estandarizar el sistema que se debe desarrollar, se pide explícitamente que los procedimientos almacenados cumplan con las condiciones siguientes"</i> (Se citan a continuación:)</li> <li>• - 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')</li> <li>- Dispondrán de tratamiento de excepciones</li> </ul>

<b>RNF-009</b>	Atendiendo al enunciado... <ul style="list-style-type: none"> <li>- Pág 5, párr.3: <i>"Toda la gestión y acceso a la información se hará mediante procedimientos de BD, siendo ésta la única manera de acceder"</i></li> <li>-</li> </ul>
----------------	---

*Ilustración 4. Requisitos No Funcionales*

## 2.2. Análisis y Diseño

### 2.2.1. Diseño Conceptual

El diseño conceptual parte de las especificaciones de requisitos que se nos solicita en el enunciado del proyecto y su resultado será el esquema conceptual de la base de datos. Es decir, implica construir un modelo del mundo real expresándolo en función de los requisitos establecidos para los datos.<sup>7</sup>

Un esquema conceptual es una descripción de alto nivel de la estructura de la base de datos, independientemente del SGBD que vayamos a utilizar; para manipularla y para especificar los esquemas conceptuales se utilizan los llamados modelos conceptuales mediante los cuales podemos construir una descripción de la realidad fácil de entender.<sup>8</sup>

En este proyecto vamos a utilizar como modelo conceptual el modelo entidad-relación incluyendo las entidades con sus relaciones. Excluiremos de este modelo la parte dedicada al módulo estadístico que será incluida en el modelo lógico por la abstracción que debe de tener este modelo y por centrarnos en el grosor de las relaciones que vamos a trabajar entre las entidades definidas.

A continuación, se detallan las decisiones tomadas para la creación del diseño conceptual:

#### VULNERABILIDAD

La empresa realizará un análisis inicial de vulnerabilidades, situaciones de amenaza o sesgos en los que se les puede producir un daño a nivel informático, mediante una consultora externa. Las vulnerabilidades detectadas por dicha consultora serán registradas en la base de datos y serán ampliables a medidas que se vayan detectando de nuevas, por lo tanto, debemos de guardar los registros como entidades fuertes que no dependen de ninguna otra entidad.

---

<sup>7</sup> Beynon-Davies, P. (2018). *Sistemas de bases de datos*. Editorial Reverté.

<sup>8</sup> Mercedes Marqués, Bases de Datos, Universitat Jaume I, 1ª Edición Col·lecció Sapientia, 18, Castellón, 2011



## ACCIONMITIGACION

De la misma forma que las vulnerabilidades, la consultora también realizará un análisis inicial de aquellas acciones a llevar a cabo para mitigar estas vulnerabilidades. Cada una de estas acciones estará directamente relacionada con una vulnerabilidad sobre la que trabajar. Este registro de acciones también se irá completando a medida que surjan nuevas vulnerabilidades o nuevas medidas de mitigación sobre las ya existentes. De esta forma se considerará “ACCIONMITIGACION” como una entidad que estará relacionada con la entidad “VULNERABILIDAD”

## POLITICASEGURIDAD

Para asegurar el cumplimiento de estas medidas de mitigación la empresa creará unas políticas de seguridad de obligado cumplimiento por los empleados. El incumplimiento de estas políticas de seguridad conllevará unas consecuencias determinadas. Estas políticas de seguridad serán registradas como entidad fuerte ya que no dependen de ninguna otra entidad.

## SESIONFORMACION

La empresa realizará sesiones de formación enfocadas a formar a los empleados y en concienciar en la importancia del cumplimiento de las políticas de seguridad. Este registro de sesiones de formación guardará la información relativa a estas y será considerada como entidad fuerte ya que no depende de ninguna otra.

## SIMULACION

Para seguir el adecuado cumplimiento de las políticas de seguridad la empresa organizará simulaciones controladas de ataques para comprobar qué usuarios no siguen con las directrices marcadas. El sistema deberá guardar un registro de estas simulaciones con la información relativa a cada una de ellas. Estas simulaciones tendrán un responsable que será una referencia a un empleado de la empresa registrado en la tabla “Empleado”.

## AUDITORIA

El sistema también deberá guardar un registro de las auditorías de seguridad; estas auditorías serán inspecciones, tanto internas como externas, que controlen el trabajo llevado a cabo. El sistema debe permitir guardar un registro de las auditorías realizadas por lo que se guardará como entidad fuerte ya que no dependerá de ninguna otra.

Además de estas entidades especificadas de forma explícita en el enunciado será necesario crear otras necesarias para el funcionamiento adecuado del sistema, estas entidades serán las que se describen a continuación:

## EMPLEADO

Para conseguir un registro óptimo de las entidades consideradas anteriormente será necesaria la implementación de una entidad que almacene los datos de los empleados de la empresa. Entidad fuerte, puesto que no depende de ninguna otra estará relacionada con la entidad “Departamento” que se detalla a continuación.

## DEPARTAMENTO

Guardaremos también un registro de los departamentos en los que se divide la empresa. A priori no es relevante la información específica a almacenar de cada departamento, pero sí que sabemos por el enunciado que necesitaremos guardar un registro de la cantidad de incumplimientos de las políticas de seguridad que realiza cada departamento.

## PROCESOGEMPRESA

De la misma forma que con los Departamentos, de los procesos de gestión de la empresa tampoco es necesario a priori, guardar un registro detallado de sus datos, pero sabemos que cada una de las vulnerabilidades se asocia con al menos, un proceso, esto nos lleva a la creación de esta entidad.

A continuación, se muestra el resultado de la relación de todas estas entidades en un modelo conceptual que nos servirá de base para el futuro sistema:

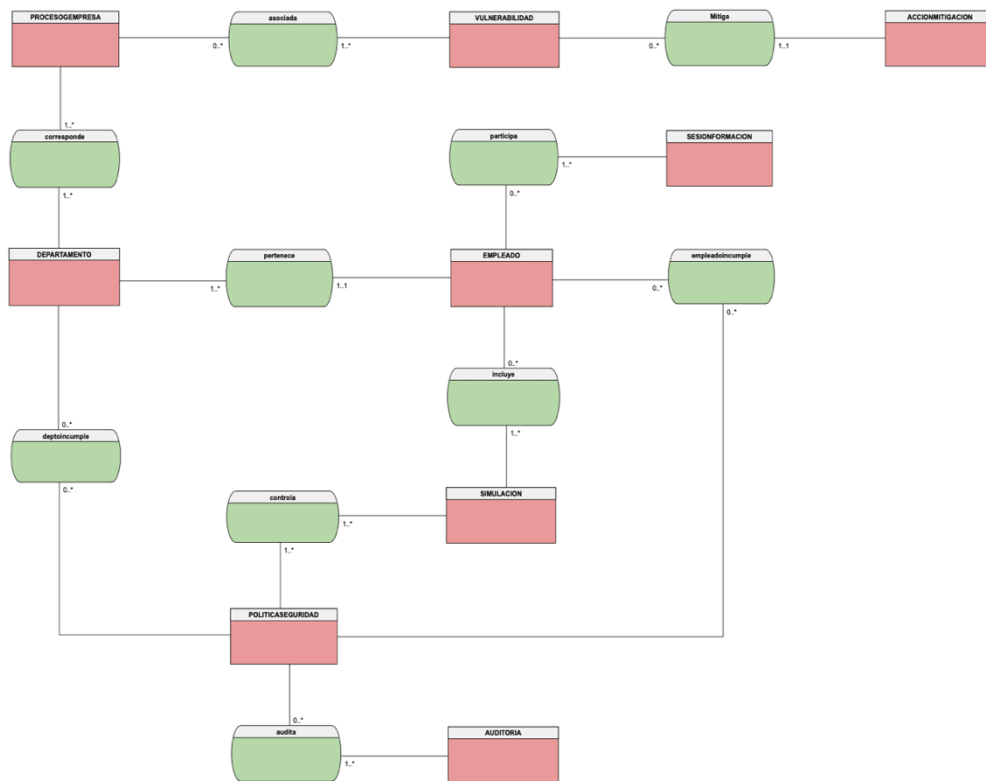


Ilustración 5. Modelo Conceptual

### 2.2.2. Diseño Lógico

Una vez realizado el diseño conceptual y obtenido el esquema correspondiente mediante un diagrama entidad-relación procedemos con la etapa del diseño lógico.

En esta etapa debemos decidir el modelo lógico de base de datos que vamos a utilizar para llevar a cabo la implementación. El modelo lógico implica construir un modelo del mundo real expresado en función de los principios de algún modelo de datos.<sup>9</sup> En este caso utilizaremos el modelo relacional por ser uno de los modelos lógicos más extendidos.

A continuación, detallamos el diseño lógico correspondiente a nuestro proyecto dividido según el tipo de tablas:

#### *TABLAS ENTIDADES FUERTES*

**T\_ACCIONMITIGACION** (IdAccionMit, Responsable, FechaLimiteImplantacion, Estado, Descripcion, IdVulnerab, Observaciones, FechaUltimaModif)

Responsable es clave ajena a T\_EMPLEADO

IdVulnerab es clave ajena a T\_VULNERABILIDAD

Estado ∈ valores gistrados en tabla T\_ESTADOACCIONMITIGACION

Los campos: Responsable, Observaciones y FechaUltimaModif aceptan nulos

**T\_AUDITORIA** (IdAudit, Tipo, Fecha, TipoProcesoEmpresa, Resultado, Observaciones, FechaUltimaModif)

Tipo ∈ valores gistrados en tabla T\_TIPOAUDITORIA

TipoProesoEmpresa ∈ valores gistrados en tabla

T\_TIPOPROCESOEMPRESA

Los campos: Fecha, Resultado, Observaciones y FechaUltimaModif aceptan nulos

TipoProcesoEmpresa toma valor por defecto: 'Seguridad'

---

<sup>9</sup> Beynon-Davies, P. (2018). *Sistemas de bases de datos*. Editorial Reverté.

**T\_DEPARTAMENTO** (IdDepto, Nombre, Responsable, Observaciones, FechaUltimaModif, CantEmpleados)

Nombre es clave alternativa

Responsable es clave ajena a T\_EMPLEADO

CantEmpleados es campo calculado por el sistema, al crear un departamento por defecto tendrá el valor 0

Los campos: Responsable, Observaciones y FechaUltimaModif aceptan nulos

**T\_EMPLEADO** (IdEmp, DNI, Nombre, Apellido1, Apellido2, IdProv, IdPobl, Provincia, Poblacion, FechaInicio, IdDepto, Activo, FechaCausaBaja, MotivoCausaBaja, Observaciones, FechaUltimaModif, FormacionesAsignadas, IncumpAsignados)

DNI es clave alternativa

IdProv es clave ajena a T\_PROVINCIA

IdPobl es clave ajena a T\_POBLACION

IdDepto es clave ajena a T\_DEPARTAMENTO

Activo ∈ valores gistrados en tabla T\_AFIRMNEG

MotivoCausaBaja ∈ valores gistrados en tabla T\_MOTIVOCAUSABAJA

FormacionesAsignadas e IncumplimeintosAsigandos tomarán por defecto el valor 'No'

Los campos: Apellido2, IdProv, IdPobl, Provincia, Poblacion, FechaInicio, IdDepto, FechaCausaBaja, MotivoCausaBaja, Observaciones y FechaUltimaModif aceptan nulos

**T\_POLITICASEGURIDAD** (IdPolSeg, Aprobada, Descripcion, ConsecuenciaAdmin, ConsecuenciaSimul, Activa, FechaActivaDesde, FechaBaja, Observaciones, FechaUltimaModif, IdVulnerab)

IdVulnerab es clave ajena a T\_VULNERABILIDAD

Aprobada y Activa ∈ valores gistrados en tabla T\_AFIRMNEG

Los campos: Aprobada, Descripcion, FechaActivaDesde, FechaBaja, Observaciones y FechaUltimaModif aceptan nulos

ConsecuenciaAdmin y ConsecuenciaSimul tienen valor por defecto: 'A determinar'

Activa tiene valor por defecto: 'No'

**T\_PROCESOGEMPRESA** (IdProcesoGEmp, Nombre, Tipo, Observaciones, FechaUltimaModif)

Nombre es clave alternativa

Tipo ∈ valores gistrados en tabla T\_TIOPROCESOEMPRESA

Los campos: Observaciones y FechaUltimaModif aceptan nulos

**T\_SESIONFORMACION** (IdSesionForm, Tipo, Titulo, Descripcion, FechaInicioSesionFormacion, FechaFinSesionFormacion, Observaciones, FechaUltimaModif)

Titulo es clave alternativa

Tipo ∈ valores gistrados en tabla T\_TIPOSESIONFORMACION

Los campos: Descripcion, FechaInicioSesionFormacion, FechaFinSesionFormacion, Observaciones y FechaUltimaModif aceptan nulos

**T\_SIMULACION** (IdSimul, Responsable, Descripcion, Fecha, Resultado, Observaciones, FechaUltimaModif)

Responsable es clave ajena a T\_EMPLEADO

Los campos: Responsable, Fecha, Resultado, Observaciones, FechaUltimaModif aceptan nulos

**T\_VULNERABILIDAD** (Idvulnerab, Nombre, Estado, Crítica, Descripcion, FechaDeteccion, DetectadaPor, Observaciones, FechaUltimaModif)

Nombre es clave alternativa

Estado ∈ valores registrados en tabla T\_ESTADOVULNERAB

Crítica ∈ valores registrados en tabla T\_AFIRMNEG

DetectadaPor ∈ valores registrados en tabla T\_DETECCIONVULNERAB

Estado es campo calculado por el sistema

Los campos: Descripcion, FechaDeteccion, Observaciones y FechaUltimaModif aceptan nulos

## TABLAS ENTIDADES RELACIÓN

**T\_AUDITORIA\_POLITICASEGURIDAD** (IdAudit, IdPolSeg, Superada, Observaciones, FechaUltimaModif, Anyo)

IdAudit es clave ajena a T\_AUDITORIA

IdPolSeg es clave ajena a T\_POLITICASEGURIDAD

Superada ∈ valores gistrados en tabla T\_AFIRMNEG

Los campos: Superada, Observaciones y FechaUltimaModif aceptan nulos

**T\_DEPARTAMENTO** **\_PROCESOGEMPRESA** (IdDepto, IdProcesoGEmp, Observaciones, FechaUltimaModif)

IdDepto es clave ajena a T\_DEPARTAMENTO

IdProcesoGEmp es clave ajena a T\_PROCESOGEMPRESA

Los campos: Observaciones y FechaUltimaModif aceptan nulos

**T\_EMPLEADO\_SESIONFORMACION** (IdEmp, IdSesForm, FechaAsignacion, FechaInicioFormacion, FechaFinFormacion, Observaciones, FechaUltimaModif)

IdEmp es clave ajena a T\_EMPLEADO

IdSesForm es clave ajena a T\_SESIONFORMACION

Los campos: FechaInicioFormacion, FechaFinFormacion, Observaciones y FechaUltimaModif aceptan nulos

**T\_EMPLEADO\_SIMULACION** (IdEmp, IdSimul, Observaciones, FechaUltimaModif)

IdEmp es clave ajena a T\_EMPLEADO

IdSimul es clave ajena a T\_SIMULACION

Los campos: Observaciones y FechaUltimaModif aceptan nulos

**T\_INCUMPLIMIENTO\_DEPTO** (IdDepto, IdPolSeg, Anyo, Cantidad)

IdDepto es clave ajena a T\_DEPARTAMENTO

IdPolSeg es clave ajena a T\_POLITICA\_SEGURIDAD

**T\_INCUMPLIMIENTO\_EMP** (IdIncump, IdEmp, IdPolSeg, Tipo, Consecuencia, Anyo, Observaciones, FechaUltimaModif, IdAudit, IdSimul)

IdEmp es clave ajena a T\_EMPLEADO

IdPolSeg es clave ajena a T\_POLITICASEGURIDAD

IdAudit es clave ajena a T\_AUDITORIA

IdSimul es clave ajena a T\_SIMULACION

Tipo ∈ valores gistrados en tabla T\_TIPOINCUMPLIMIENTO

Consecuencia es campo calculado por el sistema según valor del campo Tipo  
(Tipo = Pol. Seguridad → Se copia

T\_POLITICASEGURIDAD.ConsecuenciaAdmin

Tipo = Simulación → Se copia

T\_POLITICASEGURIDAD.ConsecuenciaSimul)

Anyo es campo calculado por el sistema según el año de la auditoría o de la simulación, según corresponda.

Los campos: Observaciones y FechaUltimaModif aceptan nulos

**T\_SIMULACION\_POLITICASEGURIDAD** (IdSimul, IdPolSeg, Observaciones, FechaUltimaModif)

IdSimul es clave ajena a T\_SIMULACION

IdPolSeg es clave ajena a T\_POLITICASEGURIDAD

Los campos: Observaciones y FechaUltimaModif aceptan nulos

**T\_VULNERABILIDAD\_PROCESOGEMPRESA** (IdVulnerab, IdProcesoGEmp, Anyo)

IdVulnerab es clave ajena a T\_VULNERABILIDAD

IdProcesoGEmp es clave ajena a T\_PROCESOGEMPRESA

*Ilustración 7. Diseño Lógico, Entidades Relación*

### *TABLAS COMPLEMENTARIAS*

**T\_POBLACION** (IdPobl, Poblacion, CP, idProv)

CP es una clave alternativa

IdProv es clave ajena a T\_PROVINCIA

**T\_PROVINCIA** (IdProv, Provincia)

Provincia es clave alternativa

*Ilustración 8. Diseño Lógico, Tablas Complementarias*

*TABLAS REPOSITORIO ESTADÍSTICO*

T\_C1\_SUMA (IdDepto, Anyo, Cant)

T\_C1\_RESULT (IdDepto, Anyo, Cant)

T\_C2\_SUMA (IdProces, Nombre, Cant)

T\_C2\_RESULT (IdProces, Nombre, Cant)

T\_C4 (Id, TotalVulnerabs, TotalVulnerabsMit, Porcentaje)

T\_C5 (Id, Cant)

T\_C6\_SUMA (IdPolSeg, Cant)

T\_C6\_RESULT (IdPolSeg, Cant)

T\_C7 (IdDepto, TotalEmp, TotalEmpNoAcabado, Porcentaje)

T\_C8 (Id, TotalEmp, TotalEmpIncumpAsig, PorcentajeNoIncumpAsig, PorcentajeIncumpAsig)

T\_C9\_SUMA (Anyo, Cant)

T\_C9\_RESULT (Anyo, Cant)

T\_C10 (Id, TotalVulnerabsCrit, TotalVulnerabsCritNoAcabada, Porcentaje)

T\_C12 (Id, Cant)

T\_C13 (Id, TotalAM, TotalAMenProcOrRev, Porcentaje)

*Ilustración 9. Diseño Lógico, Tablas R.E.*



## TABLAS ENUMERACIONES

**T\_ESTADOACCIONMITIGACION** (idEAM, EstadoAccionMitigacion)

EstadoAccionMitigacion es clave alternativa

**T\_AFIRMNEG** (idAN, AfirmNeg)

AfirmNeg es clave alternativa

**T\_TIPOSESIONFORMACION** (idTSE, TipoSesionFormacion)

TipoSesionFormacion es clave alternativa

**T\_TIPOINCUMPLIMIENTO** (idTI, TipoIncumplimiento)

TipoIncumplimiento es clave alternativa

**T\_DETECCIONVULNERAB** (idDV, DeteccionVulnerab)

DeteccionVulnerab es clave alternativa

**T\_TIPOAUDITORIA** (idTA, TipoAuditoria)

TipoAuditoria es clave alternativa

**T\_TIPOPROCESOEMPRESA** (idTPE, TipoProcesoEmpresa)

TipoProcesoEmpresa es clave alternativa

**T\_MOTIVOCAUSABAJA** (idMCB, MotivoCausaBaja)

MotivoCausaBaja es clave alternativa

**T\_ESTADOVULNERAB** (idEV, EstadoVulnerab)

EstadoVulnerab es clave alternativa

**T\_ESTADOVULNERAB** (idEV, EstadoVulnerab)

EstadoVulnerab es clave alternativa

*Ilustración 10. Diseño Lógico, Tablas Enumeraciones*

Finalmente, el modelo lógico queda representado en el siguiente esquema relacional UML para visualizar a partir de qué tablas y relaciones nos basamos para la implementación del modelo físico: (Se adjunta como Anexo1 para una mejor visualización)

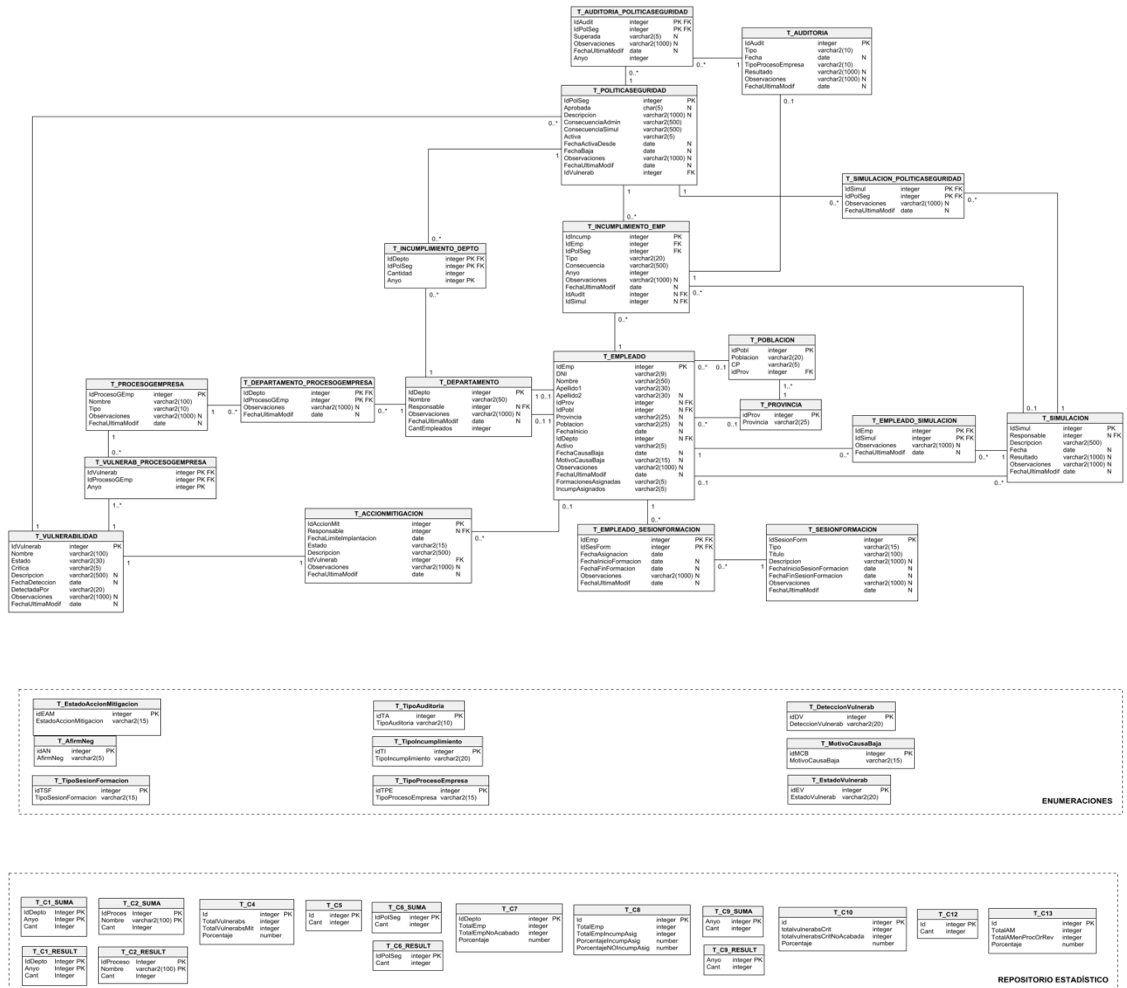


Ilustración 11. Modelo Lógico de la BD

### 2.2.3. Diseño Físico

Mientras que en el diseño lógico especificamos qué se guarda, en el diseño físico especificamos cómo se guarda. Implica la construcción de un modelo del mundo real expresado mediante estructuras de datos y mecanismos de acceso disponibles en un SGBD elegido.<sup>10</sup>

El diseño físico es el proceso de producir la descripción de la implementación de la base de datos en memoria secundaria, a partir del esquema lógico obtenido en la etapa anterior. Puesto que el modelo lógico utiliza el modelo relacional, la implementación del diseño físico la realizaremos en SQL.<sup>11</sup>

Como hemos dicho anteriormente el proceso de esta fase debemos de haber decidido cuál será el SGBD que vamos a utilizar ya que el sistema físico estará adaptado a este; En nuestro caso el SGBD a utilizar será Oracle.

#### *DICCIONARIO DE DATOS*

La finalidad del diccionario de datos es documentar los metadatos más ligados a su almacenamiento en la base de datos. Estos metadatos ayudarán a los usuarios a entender los datos desde el punto de vista técnico para poder explotarlos adecuadamente.<sup>12</sup>

A continuación, se detalla el diccionario de datos del resultado del modelo físico de nuestra base de datos, comenzaremos por la relación de entidades fuertes listadas en orden alfabético:

#### *TABLAS ENTIDADES FUERTES*

##### *T\_ACCIONMITIGACION*

**Descripción:** Tabla que contiene el listado de acciones que se deben de llevar a cabo para hacer frente a las vulnerabilidades.

COLUMNA	TIPO	PROP.	DESCRIPCIÓN
IdAccionMit	integer	PK	Atributo que identifica cada una de las acciones de mitigación que lleva a cabo la empresa. Su valor se asignará mediante proceso con enteros correlativos
Responsable	integer	null	Empleado que está al cargo como responsable de la acción de mitigación
FechaLimiteImplantacion	date		Fecha Límite en la que debe de estar implantada la acción de mitigación

<sup>10</sup> Beynon-Davies, P. (2018). *Sistemas de bases de datos*. Editorial Reverté.

<sup>11</sup> Mercedes Marqués, Bases de Datos, Universitat Jaume I, 1ª Edición Col·lecció Sapientia, 18, Castellón, 2011

<sup>12</sup> (3 mayo 2022) <https://datos.gob.es/es/blog/que-es-un-diccionario-de-datos-y-por-que-es-importante>

Estado	varchar2(15)		Atributo discriminativo. Puede tomar aquellos valores incluidos en "EstadoAccionMitigacion"
Descripcion	varchar2(500)		Descripción de cada una de las acciones de mitigación
IdVulnerab	integer		Vulnerabilidad a la que hace referencia dicha acción de mitigación
Observaciones	varchar2(1000)	null	Campo para anotaciones
FechaUltimaModif	date	null	Fecha de la última modificación del registro

### T\_AUDITORIA

**Descripción:** Tabla que contiene el listado de auditorías que se realizan en la empresa. Se realizará una auditoría por cada tipo de proceso a auditar.

COLUMNA	TIPO	PROP.	DESCRIPCIÓN
IdAudit	integer	PK	Atributo que identifica cada una de las auditorías que se realizan en la empresa. Su valor se asignará mediante proceso con enteros correlativos
Tipo	varchar2(10)		Atributo discriminativo que indica el tipo de auditoría. Puede tomar aquellos valores incluidos en "TipoAuditoría"
Fecha	date	null	Fecha de realización de la auditoría
TipoProcesoEmpresa	varchar2(10)		Atributo que indica qué tipo de procesos se van a auditar. Puede tomar aquellos valores incluidos en "TipoProcesoEmpresa"
Resultado	varchar2(1000)	null	
Observaciones	varchar2(1000)	null	Campo para anotaciones
FechaUltimaModif	date	null	Fecha de la última modificación del registro

### T\_DEPARTAMENTO

**Descripción:** Tabla que contiene cada uno de los departamentos que conforman la empresa

COLUMNA	TIPO	PROP.	DESCRIPCIÓN
IdDepto	integer	PK	Identificador del departamento. Se asigna por defecto mediante enteros correlativos
Nombre	varchar2(50)		Nombre del Departamento
Responsable	integer	null	Empleado que es jefe del departamento
Observaciones	varchar2(1000)	null	Campo para anotaciones
FechaUltimaModif	date	null	Fecha de la última modificación del registro
CantEmpleados	integer		

Clave Alternativa: T\_DEPARTAMENTO\_ak Columna: Nombre

### T\_EMPLEADO

**Descripción:** Tabla que contiene los datos de los trabajadores de la empresa.

Podría parecer que, en los datos referentes a población y provincia hay redundancia de datos, en realidad esta desnormalización es apta para evitar los

join entre tablas. El sistema de introducción de datos consistirá en que el usuario seleccionará una provincia de entre las opciones pre-insertadas en el sistema. Una vez hecha la selección podrá escoger entre los pueblos relacionados a esta provincia. Con esto, en la tabla quedarán guardados tanto el id de la población como el de la provincia. Pero, además, en la propia tabla de Empleado estamos guardando el nombre tanto de la provincia como de la población, ¿redundancia de datos? Sí, ¿nos interesa? Como hemos dicho anteriormente, también. Aquí nos surgen, además, dos temas a tratar:

Uno es que tanto de la provincia como de, sobre todo, la población puede ser que queramos almacenar más información (el CP, por ejemplo); teniendo estos campos en tablas resulta más organizado al ser datos que corresponden a la propia entidad.

El otro es que cada vez que busquemos la información del cliente no tendremos que hacer join para obtener los nombres de población y provincia, ya los tendremos directamente. Aunque... esto nos presenta un “problema”: no es común, pero, se ha dado el caso de que una población, por ejemplo, pueda cambiar de nombre. Si fuera el caso lo que nos pasaría es que en la tabla Empleado estaríamos guardando un nombre que ya no es el que corresponde a la Id de dicha población, por lo que nos interesaría crear un disparador que, cuando se modifique la información de las tablas T\_PROVINCIA, T\_POBLACION, actualizase los campos “Poblacion” y “Provincia” de la tabla empleado (Sugerido como mejora de siguiente fase en apartado 2.5

COLUMNA	TIPO	PROP.	DESCRIPCIÓN
IdEmp	integer	PK	Identificador del empleado
DNI	varchar2(9)		DNI del empleado. Lo identifica como tal, , será clave alternativa
Nombre	varchar2(50)		Nombre del empleado
Apellido1	varchar2(30)		Primer apellido del empleado
Apellido2	varchar2(30)	null	Segundo apellido del empleado. puede ser nulo ya que según la nacionalidad puede ser que tenga solo un apellido
IdProv	integer	null	
IdPobl	integer	null	
Provincia	varchar2(25)	null	Provincia del empleado
Poblacion	varchar2(25)	null	Población en la que reside el empleado
FechaInicio	date	null	Fecha en la que el empleado comenzó a trabajar en la empresa
IdDepto	integer	null	Departamento al que pertenece el empleado
Activo	varchar2(5)		Atributo que nos indica si el trabajador está en activo en ese momento. Puede estar inactivo por excedencia, baja prolongada...) En ningún caso se refiere a los trabajadores que ya han causado baja en la empresa. Puede tomar aquellos valores incluidos en "AfirmNeg"
FechaCausaBaja	date	null	Atributo que indica la fecha en la que el trabajador causó baja en la empresa por cualquiera de los motivos definidos en MOTIVOCAUSABAJA

MotivoCausaBaja	varchar2(15)	null	Atributo que hace referencia al motivo por el que el empleado ha causado baja en la empresa. Puede tomar aquellos valores incluidos en "MotivoCausaBaja"
Observaciones	varchar2(1000)	null	Campo para anotaciones
FechaUltimaModif	date	null	Fecha de la última modificación del registro
FormacionesAsignadas	varchar2(5)		
IncumpAsignados	varchar2(5)		

Clave Alternativa: T\_EMPLEADO\_ak Columna: DNI

## T\_POLITICASEGURIDAD

**Descripción:** Tabla que contiene el listado de las políticas de seguridad que establece la empresa.

La diferencia entre una política de seguridad y la acción de mitigación de una vulnerabilidad radica en que la acción de mitigación sirve para, efectivamente mitigar la vulnerabilidad, es decir, reducirla; y la política de seguridad lo que quiere conseguir es establecer unas “leyes” que establezcan qué no se debe hacer y cómo actuar en consecuencia a ello.

COLUMNA	TIPO	PROP.	DESCRIPCIÓN
IdPolSeg	integer	PK	Atributo que identifica cada una de las políticas de seguridad que se definen en la empresa. Su valor se asignará mediante proceso con enteros correlativos
Aprobada	char(5)	null	Atributo que indica si la política de seguridad ha sido o no aprobada. Puede tomar aquellos valores incluidos en "AfirmNeg", por defecto será: "No".
Descripcion	varchar2(1000)	null	Atributo que indica la DESCRIPCIÓN de la política de seguridad
ConsecuenciaAdmin	varchar2(500)		Consecuencia derivada del incumplimiento de esta política de seguridad en caso de ser por un hecho real
ConsecuenciaSimul	varchar2(500)		Consecuencia derivada del incumplimiento de esta política de seguridad en caso de ser por una simulación
Activa	varchar2(5)		
FechaActivaDesde	date	null	
FechaBaja	date	null	
Observaciones	varchar2(1000)	null	Campo para anotaciones
FechaUltimaModif	date	null	Fecha de la última modificación del registro
IdVulnerab	integer		

## T\_PROCESOGEMPRESA

**Descripción:** Tabla que contiene todos los procesos de gestión de la empresa

COLUMNA	TIPO	PROP.	DESCRIPCIÓN
IdProcesoGEmp	integer	PK	
Nombre	varchar2(100)		Nombre del proceso de gestión de la empresa
Tipo	varchar2(10)		Atributo que hace referencia al tipo de proceso de gestión. Puede tomar aquellos valores incluidos en "TipoProcesoEmpresa"
Observaciones	varchar2(1000)	null	Campo para anotaciones
FechaUltimaModif	date	null	Fecha de la última modificación del registro

Clave Alternativa: T\_PROCESOGEMPRESA\_ak Columna: Nombre

## T\_SESIONFORMACION

**Descripción:** Tabla que contiene el listado de las sesiones formativas que realiza la empresa.

COLUMNA	TIPO	PROP.	DESCRIPCIÓN
IdSesionForm	integer	PK	Atributo que identifica a cada una de las sesiones de formación. Su valor se asignará mediante proceso con enteros correlativos
Tipo	varchar2(15)		Atributo discriminativo. Indicará el tipo de la sesión de formación; Puede tomar aquellos valores incluidos en "TipoSesionFormacion"
Titulo	varchar2(100)		Título asignado a la sesión de formación
Descripcion	varchar2(1000)	null	DESCRIPCIÓN de los contenidos de la sesión de formación
FechaInicioSesionFormacion	date	null	Fecha en la que se inicia la sesión de formación (Ojo, no confundir con el campo de la tabla T_EMPLEADO_SESIONFORMACION)
FechaFinSesionFormacion	date	null	Fecha en la que finaliza la sesión de formación (Ojo, no confundir con el campo de la tabla T_EMPLEADO_SESIONFORMACION)
Observaciones	varchar2(1000)	null	Campo para anotaciones
FechaUltimaModif	date	null	Fecha de la última modificación del registro

Clave Alternativa: T\_SESIONFORMACION\_ak Columna: Titulo

## T\_SIMULACION

**Descripción:** Tabla que contiene el listado de simulaciones de ataques controlados que realiza la empresa

COLUMNA	TIPO	PROPS.	DESCRIPCIÓN
IdSimul	integer	PK	Identificador de la simulación. Su valor se asignará mediante proceso con enteros correlativos
Responsable	integer	null	Atributo que indica el empleado responsable de la simulación
Descripcion	varchar2(500)		Atributo que describe la simulación
Fecha	date	null	Fecha de realización de la simulación
Resultado	varchar2(1000)	null	
Observaciones	varchar2(1000)	null	Campo para anotaciones
FechaUltimaModif	date	null	Fecha de la última modificación del registro

NOTA: Además de la evidente diferencia entre las auditorías y las simulaciones cabe decir que el sistema está diseñado de forma que las auditorías se focalizan especialmente en las políticas de los empleados mientras que las simulaciones lo hacen en las acciones de los empleados.

## T\_VULNERABILIDAD

**Descripción:** Tabla que contiene el listado de las vulnerabilidades que se detectan

COLUMNA	TIPO	PROPS.	DESCRIPCIÓN
IdVulnerab	integer	PK	
Nombre	varchar2(100)		Nombre que identifica a la vulnerabilidad
Estado	varchar2(30)		Campo calculado mediante proceso. Actualmente solo podrá tomar los valores: {Identificada, No mitigada, Parc. mitigada, Tot. mitigada}
Critica	varchar2(5)		Atributo discriminativo. Puede tomar aquellos valores incluidos en "AfirmNeg"
Descripcion	varchar2(500)	null	DESCRIPCIÓN sobre la vulnerabilidad en cuestión
FechaDeteccion	date	null	Fecha en la que se detecta la vulnerabilidad
DetectadaPor	varchar2(20)		Atributo que hace referencia a quién detectó la vulnerabilidad. Permite cualquier valor incluido en la enumeración DETECCIONVULNERABILIDAD
Observaciones	varchar2(1000)	null	Campo para anotaciones
FechaUltimaModif	date	null	Fecha de la última modificación del registro

Clave Alternativa: T\_VULNERABILIDAD\_ak. Columna: Nombre



## TABLAS ENTIDADES RELACIÓN

A continuación, el listado de entidades que nacen como producto de las relaciones entre las entidades fuerte. De la misma manera que las anteriores, listadas en orden alfabético:

### T\_AUDITORIA\_POLITICASEGURIDAD

**Descripción:** Relación entre las auditorías que se realizan y los muestreos realizados sobre las políticas de seguridad que se auditan en estas. Estos registros se realizan a posteriori de la auditoría ya que, antes de su realización no se sabe qué políticas se van a Auditar.

Solo se pueden auditar las políticas de seguridad que están aprobadas por la empresa

COLUMNA	TIPO	PROPS.	DESCRIPCIÓN
IdAudit	integer	PK	Identificador de la auditoría
IdPolSeg	integer	PK	Identificador de la política de seguridad
Superada	varchar2(5)	null	Puede tomar aquellos valores incluidos en "AfirmNeg"
Observaciones	varchar2(1000)	null	Campo para anotaciones
FechaUltimaModif	date	null	Fecha de la última modificación del registro
Año	integer		

### T\_DEPARTAMENTO\_PROCESOGEMPRESA

**Descripción:** Tabla que relaciona los departamentos y los procesos de gestión que corresponden a estos

COLUMNA	TIPO	PROPS.	DESCRIPCIÓN
IdDepto	integer	PK	Identificador del departamento
IdProcesoGEmp	integer	PK	Identificador del proceso de gestión
Observaciones	varchar2(1000)	null	Campo para anotaciones
FechaUltimaModif	date	null	Fecha de la última modificación del registro

## T\_EMPLEADO\_SESIONFORMACION

**Descripción:** Relación entre los empleados y las sesiones de formación que se le asignan.

Será la futura aplicación la encargada de controlar que, al realizar la asignación de sesiones de formación al usuario solo estén disponibles para asignar aquellas sesiones que ya tienen confirmadas tanto fecha de inicio como fecha de fin.

COLUMNA	TIPO	PROPS.	DESCRIPCIÓN
IdEmp	integer	PK	Identificador del empleado
IdSesForm	integer	PK	Identificador de la sesión de formación
FechaAsignacion	date		Fecha en la que se le asigna la formación al empleado
FechaInicioFormacion	date	null	Fecha en la que el empleado inicia la formación (Ojo, no confundir con el campo de la tabla T_SESIONFORMACION)
FechaFinFormacion	date	null	Fecha en la que el empleado finaliza la formación (Ojo, no confundir con el campo de la tabla T_SESIONFORMACION)
Observaciones	varchar2(1000)	null	Campo para anotaciones
FechaUltimaModif	date	null	Fecha de la última modificación del registro

## T\_EMPLEADO\_SIMULACION

**Descripción:** Relación que une los empleados con las simulaciones a las que es sometido

COLUMNA	TIPO	PROPS.	DESCRIPCIÓN
IdEmp	integer	PK	Identificador de empleado
IdSimul	integer	PK	Identificador de la simulación
Observaciones	varchar2(1000)	null	Campo para anotaciones
FechaUltimaModif	date	null	Fecha de la última modificación del registro

## T\_INCUMPLIMIENTO\_DEPTO

**Descripción:** Relación entre los departamentos y las políticas de seguridad que son incumplidas por sus trabajadores.

COLUMNA	TIPO	PROPS.	DESCRIPCIÓN
IdDepto	integer	PK	Identificador del departamento
IdPolSeg	integer	PK	Identificador de la política de seguridad
Cantidad	integer		Cantidad de veces que los empleados del departamento han incumplido la política de seguridad
Anyo	integer	PK	

## T\_INCUMPLIMIENTO\_EMP

**Descripción:** Tabla que contiene los incumplimientos de las políticas de seguridad realizados por los empleados

COLUMNA	TIPO	PROPS	DESCRIPCIÓN
IdIncump	integer	PK	Atributo que identifica cada uno de los incumplimientos de las políticas de seguridad. Su valor se asignará mediante proceso con enteros correlativos
IdEmp	integer		Identificador del empleado que incumple
IdPolSeg	integer		Identificador de la política de seguridad incumplida
Tipo	varchar2(20)		Atributo discriminatorio. Hace referencia a si el empleado ha incumplido la política de seguridad en un hecho real o en una simulación. Puede tomar aquellos valores incluidos en "TipoSesionFormacion"
Consecuencia	varchar2(500)		Campo calculado por proceso. Tomará el mismo valor que contenga el campo POLITICASEGURIDAD.ConsecuenciaAdmin o POLITICASEGURIDAD.ConsecuenciaSimul, según corresponda por su tipo, en el momento de crearse la relación
Anyo	integer		Año en que se detecta, lo toma el sistema del campo fecha de la Auditoría o de la simulación según corresponda
Observaciones	varchar2(1000)	null	Campo para anotaciones
FechaUltimaModif	date	null	Fecha de la última modificación del registro
IdAudit	integer	null	
IdSimul	integer	null	

Clave Alternativa: T\_INCUMPLIMIENTO\_EMP\_ak

Columna: IdEmp, IdPolSeg, Anyo

## T\_SIMULACION\_POLITICASEGURIDAD

**Descripción:** Relación entre las simulaciones y las políticas de empresa que se evalúan en ellas

COLUMNA	TIPO	PROPS.	DESCRIPCIÓN
IdSimul	integer	PK	Identificador de la simulación
IdPolSeg	integer	PK	Identificador de la política de seguridad
Observaciones	varchar2(1000)	null	Campo para anotaciones
FechaUltimaModif	date	null	Fecha de la última modificación del registro

## T\_VULNERAB\_PROCESOGEMPRESA

**Descripción:** Entidad que registra las vulnerabilidades que se detectan en cada proceso y el año de su detección

COLUMNA	TIPO	PROPS.	DESCRIPCIÓN
IdVulnerab	integer	PK	Identificador de la vulnerabilidad
IdProcesoGEmp	integer	PK	Identificador del proceso de gestión
Anyo	integer	PK	

### TABLAS COMPLEMENTARIAS

Las dos entidades que vemos a continuación no se incluyen dentro del listado de entidades fuertes ya que no son entidades creadas para el funcionamiento del sistema en sí. Estas dos entidades nacen para complementar a dicho sistema y a la futura aplicación con la idea de que la introducción de datos resulte una experiencia sencilla y sin errores para el futuro usuario:

## T\_POBLACION

**Descripción:** Tabla que guarda un registro de todas las poblaciones posibles a introducir. Se utilizará básicamente para facilitar la introducción de datos de cara a la futura aplicación sin necesidad de comprobar que los datos introducidos son correctos. Puesto que existen nombres de poblaciones repetidos al introducir los datos de un empleado se pedirá primero la información de la provincia y, de esta forma, solo se mostrarán los pueblos que pertenecen a esta (En caso de introducir primero el nombre de la población podría dar lugar a introducir mal la provincia a la que pertenece)\*

COLUMNA	TIPO	PROPS.	DESCRIPCIÓN
idPobl	integer	PK	Identificador de la población
Poblacion	varchar2(20)		Nombre de la población
CP	varchar2(5)		Código Postal correspondiente a la población
idProv	integer		Provincia a la que pertenece la población

Clave Alternativa: T\_POBLACION\_ak Columna: CP

## T\_PROVINCIA

**Descripción:** Tabla que guarda un registro de todas las provincias. Se utilizará básicamente para facilitar la introducción de datos de cara a la futura aplicación sin necesidad de comprobar que los datos introducidos son correctos. Puesto que existen nombres de poblaciones repetidos al introducir los datos de un empleado se pedirá primero la información de la provincia y, de esta forma, solo se mostrarán los pueblos que pertenecen a esta (En caso de introducir primero el nombre de la población podría dar lugar a introducir mal la provincia a la que pertenece)\*

COLUMNA	TIPO	PROPS.	DESCRIPCIÓN
idProv	varchar2(5)	PK	Identificador de la provincia
Provincia	varchar2(25)		Nombre de la provincia

Clave Alternativa: T\_PROVINCIA\_ak Columna: Provincia

\* Como nota comentaremos que, si introducimos los datos desde el SGBD el sistema no controla si la población y la provincia que introduces están relacionadas (Se entiende que quien haga las pruebas tendrá esto en cuenta) ya que será la futura aplicación la que una vez el usuario seleccione la provincia filtrará las poblaciones pertenecientes a dicha provincia por lo tanto, esta relación se mantendrá de forma consistente.

### *TABLAS REPOSITORIO ESTADÍSTICO*

Seguimos con el listado de tablas que formarán parte del Repositorio Estadístico. Tal y como sucede con las dos tablas que acabamos de ver, las que vienen a continuación no forman parte del sistema en sí, sino que lo complementan para dar respuesta en tiempo 1 a las consultas de dicho repositorio. Cabe señalar que muchas de las consultas se podrían agrupar de forma que una misma tabla diera respuesta a diferentes consultas, pero finalmente, se decidió crear tablas separadas por consultas ya que esto facilita su modificación en caso de que cambiaran los requerimientos del cliente.

Las tablas de las consultas C4, C5, C8, C10, C12 y C13, deberán ser inicializadas con el identificador a 1 y el resto de campos a 0 al arrancar el sistema y en concreto la T\_C8 deberá ser inicializada a 0 con cada comienzo de un nuevo año.

Dicho todo esto, no precisan de descripción ya que, además de lo dicho, su propio nombre lleva implícita la consulta a la que hacen referencia.

## DATA WAREHOUSE

Un *data warehouse (dwh)*<sup>13</sup> es un repositorio centralizado de datos que sirve de soporte en la gestión y toma de decisiones, y que se caracteriza por ser orientado a temas, integrado, no volátil y variable en el tiempo. El *dwh* almacena información, de múltiples fuentes, que se ha transformado para ofrecer un modelo común, eficiente y multidimensional para apoyar consulta y análisis y no se organizan de acuerdo con las aplicaciones que los usan, sino de acuerdo con su semántica.

El *dwh*<sup>14</sup> se ayuda de tablas de hechos que contienen observaciones sobre el hecho que se analiza a lo largo del tiempo. En estas tablas es aconsejable nunca incluir campos de más, solamente los necesario y medir el tamaño de cada campo y nunca añadir bits más allá de lo considerado necesario en cada caso.

Las tablas de hechos utilizadas en nuestro sistema son las siguientes:

### T\_CI\_SUMA

COLUMNA	TIPO	PROPS.
IdDepto	Integer	PK
Anyo	Integer	PK
Cant	Integer	

### T\_CI\_RESULT

COLUMNA	TIPO	PROPS.
IdDepto	Integer	PK
Anyo	Integer	PK
Cant	Integer	

### T\_C2\_SUMA

COLUMNA	TIPO	PROPS.
IdProceso	Integer	PK
Nombre	varchar2(100)	PK
Cant	Integer	

---

<sup>13</sup> Millán, M. E. (2012). Fundamentos de bases de datos. Cali, Colombia, Programa Editorial Universidad del Valle. Recuperado de <https://elibro.net/es/ereader/uoc/129060?page=114>.

<sup>14</sup> Millán, M. E. (2012). Fundamentos de bases de datos. Cali, Colombia, Programa Editorial Universidad del Valle. Recuperado de <https://elibro.net/es/ereader/uoc/129060?page=125>.

### T\_C2\_RESULT

COLUMNA	TIPO	PROPS.
IdProceso	Integer	PK
Nombre	varchar2(100)	PK
Cant	Integer	

### T\_C4

Al arrancar el sistema se deberá de inicializar con los datos de vulnerabilidades localizadas por la consultora exterior inicial.

COLUMNA	TIPO	PROPS.
Id	integer	PK
TotalVulnerabs	integer	
TotalVulnerabsMit	integer	
Porcentaje	number	

### T\_C5

COLUMNA	TIPO	PROPS.
Id	integer	PK
Cant	integer	

### T\_C6\_SUMA

COLUMNA	TIPO	PROPS.
IdPolSeg	integer	PK
Cant	integer	

### T\_C6\_RESULT

COLUMNA	TIPO	PROPS.
IdPolSeg	integer	PK
Cant	integer	

### T\_C7

COLUMNA	TIPO	PROPS.
IdDepto	integer	PK
TotalEmp	integer	
TotalEmpNoAcabado	integer	
Porcentaje	number	

## T\_C8

Hay que tener en cuenta que esta tabla deberá ser reiniciada a 0 con cada comienzo de un nuevo año, ya que su tratamiento será de los datos del año en curso.

COLUMNA	TIPO	PROPS.
Id	integer	PK
TotalEmp	integer	
TotalEmpIncumpAsig	integer	
PorcentajeIncumpAsig	number	
PorcentajeNOIncumpAsig	number	

## T\_C9\_SUMA

COLUMNA	TIPO	PROPS.
Anyo	integer	PK

## T\_C9\_RESULT

COLUMNA	TIPO	PROPS.
Anyo	integer	PK
Cant	integer	

## T\_C10

COLUMNA	TIPO	PROPS.
id	integer	PK
totalvulnerabsCrit	integer	
totalvulnerabsCritNoAcabada	integer	
Porcentaje	number	

## T\_C12

COLUMNA	TIPO	PROPS.
Id	integer	PK
Cant	integer	

## T\_C13

COLUMNA	TIPO	PROPS.
Id	integer	PK
TotalAM	integer	
TotalAMenProcOrRev	integer	
Porcentaje	number	



## TABLAS ENUMERACIONES

Finalizamos con las tablas Enumeraciones. Estas tablas, que tampoco forman parte del funcionamiento en sí de la BD, se crean con la finalidad de facilitar al usuario la inserción de datos en una futura aplicación de la misma manera que evita tener que realizar un control de inserción de errores en dicha aplicación. Ninguna de las tablas que siguen a continuación tienen procedimientos de alta, baja y/o modificación ya que se entiende que el usuario no tiene acceso a sus datos y vienen inicializadas con la implantación del sistema en cliente.

En la descripción de cada una de las tablas encontraremos a qué campo del sistema dan opciones de inserción cada una de ellas.

### T\_EstadoAccionMitigacion

**Descripción:** Tabla que registrará los posibles valores que podrá tomar el valor ACCIONMITIGACION.Estado

Se inicializará con los valores: {Definida, En proceso, Acabada, En revisión}

COLUMNA	TIPO	PROPIEDADES
idEAM	integer	PK
EstadoAccionMitigacion	varchar2(15)	

Clave Alternativa: T\_EstadoAccionMitigacion\_ak

Columna: EstadoAccionMitigacion

### T\_AfirmNeg

**Descripción:** Tabla que facilita la inserción correcta de los valores 'Sí', 'No' en una futura aplicación.

Se inicializará con los valores: {Sí, No}

COLUMNA	TIPO	PROPIEDADES
idAN	integer	PK
AfirmNeg	varchar2(5)	

Clave Alternativa: T\_AfirmNeg\_ak Columna: AfirmNeg

### T\_TipoSesionFormacion

**Descripción:** Tabla que registrará los posibles valores que podrá tomar el valor SESIONFORMACION.Tipo

Se inicializará con los valores: {Presencial, Telemática}

COLUMNA	TIPO	PROPIEDADES
idTSF	integer	PK
TipoSesionFormacion	varchar2(15)	

Clave Alternativa: T\_TipoSesionFormacion\_ak  
Columna: TipoSesionFormacion

### T\_TipoAuditoria

**Descripción:** Tabla que registrará los posibles valores que podrá tomar el valor AUDITORIA.Tipo

Se inicializará con los valores: {Externa, Interna}

COLUMNA	TIPO	PROPIEDADES
idTA	integer	PK
TipoAuditoria	varchar2(10)	

Clave Alternativa: T\_TipoAuditoria\_ak Columna: TipoAuditoria

### T\_TipoIncumplimiento

**Descripción:** Tabla que registrará los posibles valores que podrá tomar el valor EMPLEADO\_POLITICASEGURIDAD.Tipo

Se inicializará con los valores: {Auditoría, Simulación}

No se considera otro tipo de incumplimiento ya que para considerar que el incumplimiento ha sido efectivamente realizado debe “comprobarse” con una de estas dos opciones para así poder ser sancionado

COLUMNA	TIPO	PROPIEDADES
idTI	integer	PK
TipoIncumplimiento	varchar2(20)	

Clave Alternativa: T\_TipoIncumplimiento\_ak  
Columna: TipoIncumplimiento

### T\_TipoProcesoEmpresa

**Descripción** Tabla que registrará los posibles valores que podrá tomar el valor PROCESOGEMPRESA.Tipo

Se inicializará con los valores: {Admón., Comercial, Compras, Mixto, Seguridad, Ventas} Estos valores tienden a corresponder a cada uno de los departamentos excepto el Tipo “Mixto” que hace referencia a un tipo de proceso que combina varios departamentos.

COLUMNA	TIPO	PROPIEDADES
idTPE	integer	PK
TipoProcesoEmpresa	varchar2(15)	

Clave Alternativa: T\_TipoProcesoEmpresa\_ak  
Columna: TipoProcesoEmpresa

### T\_DeteccionVulnerab

**Descripción:** Tabla que registrará los posibles valores que podrá tomar el valor VULNERABILIDAD.DetectadaPor

Se inicializará con los valores: {Cons. Externa Inicio, Empresa, Cons. Externa}

COLUMNA	TIPO	PROPIEDADES
idDV	integer	PK
DeteccionVulnerab	varchar2(20)	

Clave Alternativa: T\_DeteccionVulnerab\_ak  
Columna: DeteccionVulnerab

### T\_MotivoCausaBaja

**Descripción:** Tabla que registrará los posibles valores que podrá tomar el valor EMPLEADO.MotivoCausaBaja

Se inicializará con los valores: {Acuerdo, Despido, Rescisión, Voluntario, Otros}

COLUMNA	TIPO	PROPIEDADES
idMCB	integer	PK
MotivoCausaBaja	varchar2(15)	

Clave Alternativa: T\_MotivoCausaBaja\_ak  
Columna: MotivoCausaBaja

## T\_EstadoVulnerab

**Descripción:** Tabla que registrará los posibles valores que podrá tomar el valor VULNERABILIDAD.Estado

Se inicializará con los valores:

{Identificada, No mitigada, Parcialmente mit., Totalmente mit.}

COLUMNA	TIPO	PROPIEDADES
idEV	integer	PK
EstadoVulnerab	varchar2(20)	

Clave Alternativa: T\_EstadoVulnerab\_ak  
Columna: EstadoVulnerab

## REFERENCIAS

T_ACCIONMITIGACION	Responsable →	T_EMPLEADO
T_ACCIONMITIGACION	IdVulnerab →	T_VULNERABILIDAD
T_DEPARTAMENTO	Responsable →	T_EMPLEADO
T_EMPLEADO	IdPob →	T_POBLACION
T_EMPLEADO	IdProv →	T_PROVINCIA
T_EMPLEADO	IdDepto →	T_DEPARTAMENTO
T_POLITICASEGURIDAD	IdVulnerab →	T_VULNERABILIDAD
T_SIMULACION	Responsable →	T_EMPLEADO
T_AUDITORIA_POLITICASEGURIDAD	IdAudit →	T_AUDITORIA
T_AUDITORIA_POLITICASEGURIDAD	IdPolSeg →	T_POLITICASEGURIDAD
T_DEPARTAMENTO_PROCESOGEMPRESA	IdDepto →	T_DEPARTAMENTO
T_DEPARTAMENTO_PROCESOGEMPRESA	IdProcesoGEmp →	T_PROCESOGEMPRESA
T_EMPLEADO_SESSIONFORMACION	IdEmp →	T_EMPLEADO
T_EMPLEADO_SESSIONFORMACION	IdSesForm →	T_SESSIONFORMACION
T_EMPLEADO_SIMULACION	IdEmp →	T_EMPLEADO
T_EMPLEADO_SIMULACION	IdSimul →	T_SIMULACION

T_INCUMPLIMIENTO_DEPTO	IdDepto →	T_DEPARTAMENTO
T_INCUMPLIMIENTO_DEPTO	IdPolSeg →	T_POLITICASEGURIDAD
T_INCUMPLIMIENTO_EMP	IdEmp →	T_EMPLEADO
T_INCUMPLIMIENTO_EMP	IdPolSeg →	T_POLITICASEGURIDAD
T_INCUMPLIMIENTO_EMP	IdAudit →	T_AUDITORIA
T_INCUMPLIMIENTO_EMP	IdSimul →	T_SIMULACION
T_SIMULACION_POLITICASEGURIDAD	IdSimul →	T_SIMULACION
T_SIMULACION_POLITICASEGURIDAD	IdPolSeg →	T_POLITICASEGURIDAD
T_VULNERAB_PROCESOGEMPRESA	IdVulnerab →	T_VULNERABILIDAD
T_VULNERAB_PROCESOGEMPRESA	IdProcesoGEmp→	T_PROCESOGEMPRESA
T_POBLACION	IdProv →	T_PROVINCIA

#### 2.2.4. Análisis de los Procedimientos Almacenados y Disparadores

Tal y como se nos pide en el enunciado y por tanto, así se estima en las restricciones del proyecto (RNF-009) toda la gestión y acceso a la información se hará mediante procedimientos de BD, siendo esta la única manera de acceder.

Para ello implementaremos en primer lugar, todos aquellos procedimientos de alta, baja y modificación de todas las entidades principales y a continuación, de todos aquellos procedimientos y disparadores necesarios para mantener tanto el repositorio estadístico como para dar respuesta, como mínimo, a aquellas consultas que nos solicita el enunciado.

Antes de continuar cabe destacar ciertos aspectos...

- En ningún caso se hace un control de la duplicidad de las claves primarias ya que el sistema está diseñado para que el usuario no tenga que insertar/modificar estos campos de forma manual. (Sí que se controlan las claves alternativas, tales como DNI, nombre departamento, nombre vulnerabilidad...)
- El identificador de cada registro, a pesar de no poder ser nulo en ningún caso, tampoco se documenta como parámetro de entrada ya que, como se ha dicho anteriormente, en la futura aplicación del sistema, este no es un campo susceptible de ser introducido/modificado por los usuarios, sino

que el sistema lo calculará y lo incluirá en las sentencias de inserción directamente.

- La “no-introducción” de parámetros obligatorios, se entiende sobre todo para los casos de “Alta” no está controlada ya que será la futura aplicación la que no permita avanzar en el envío de datos si el usuario no ha introducido todos los obligatorios.

## PROCEDIMIENTOS ALMACENADOS

### Alta/Baja/Modif de Entidades

PROCEDIMIENTO	PR_ALTA_ACCIONMITIGACION
DESCRIPCIÓN	Proceso para crear una nueva acción de mitigación en el sistema
PARÁMETROS DE ENTRADA	<ul style="list-style-type: none"> <li>• PE_RESPONSABLE IN VARCHAR2</li> <li>• PE_FECHALIMITEIMPLANTACION IN VARCHAR2</li> <li>• PE_DESCRIPCION IN VARCHAR2</li> <li>• PE_IDVULNERAB IN NUMBER</li> <li>• PE_OBSERVACIONES IN VARCHAR2</li> </ul>
OPERATIVA	<p>Inserta una nueva acción de mitigación con los datos que se pasan como parámetros.</p> <p>En el campo FechaUltimaModif se guarda la fecha actual en el momento de insertar.</p> <p>Al insertar una acción mitigación tendrá Estado = ‘Definida’</p> <p>No se controla que la acción de mitigación a insertar ya exista en el sistema ya que este el que genera los identificadores.</p>
PARÁMETROS DE SALIDA	“OK” → Proceso finalizado correctamente

PROCEDIMIENTO	PR_BAJA_ACCIONMITIGACION
DESCRIPCIÓN	El sistema no permite el eliminado de registros de la tabla T_ACCIONMITIGACION

PROCEDIMIENTO	PR_MODIF_ACCIONMITIGACION
DESCRIPCIÓN	Proceso para modificar una acción de mitigación registrada en el sistema.
PARÁMETROS DE ENTRADA	<ul style="list-style-type: none"> <li>• PE_IDACCIONMIT IN NUMBER</li> <li>• PE_RESPONSABLE IN NUMBER</li> <li>• PE_FECHALIMITEIMPLANTACION IN DATE</li> <li>• PE_ESTADO IN VARCHAR2</li> <li>• PE_DESCRIPCION IN VARCHAR2</li> <li>• PE_OBSERVACIONES IN VARCHAR2</li> </ul>
OPERATIVA	<p>Solo permite modificar las acciones de mitigación que no estén acabadas.</p> <p>Solo pueden modificarse aquellos campos que se permite pasar por parámetro.</p> <p>El identificador no puede modificarse, se pasa como parámetro para localizar la acción de mitigación a modificar.</p>

	<p>Para la acción de mitigación cuyo identificador se pasa por parámetro, por cada parámetro que se le pasa al procedimiento si es diferente de NULL, lo modifica en el registro.</p> <p>La futura aplicación solo permitirá los cambios de estado de la siguiente manera:</p> <p>La futura aplicación solo permitirá los cambios de estado de la siguiente manera: Definida→En proceso→Acabada→En revisión</p> <p>Al insertar una acción mitigación tendrá Estado por defecto: ‘Definida’</p> <p>En caso de modificar las observaciones, no debe borrar las posibles observaciones anotadas anteriormente.</p> <p>El campo FechaUltimaModif será actualizado por el sistema con cada modificación</p> <p>No se controla si la acción de mitigación está o no acabada ya que la futura aplicación solo permitirá seleccionar para modificar aquellas acciones que aún no estén acabadas.</p>
PARÁMETROS DE SALIDA	<p>Proceso finalizado correctamente:</p> <ul style="list-style-type: none"> <li>• “El responsable ha sido modificado”</li> <li>• “La fecha límite de implantación ha sido modificada”</li> <li>• “El estado ha sido cambiado a: (valor del nuevo estado)”</li> <li>• “Descripción modificada”</li> <li>• “Observaciones modificadas”</li> </ul> <p>“Una acción de mitigación con estado acabada no se puede modificar”</p>

PROCEDIMIENTO	PR_ALTA_AUDITORIA
DESCRIPCIÓN	Proceso para crear una nueva auditoría en el sistema
PARÁMETROS DE ENTRADA	<ul style="list-style-type: none"> <li>• PE_TIPO VARCHAR2</li> <li>• PE_FECHA IN DATE</li> <li>• PE_OBSERVACIONES IN VARCHAR2</li> </ul>
OPERATIVA	<p>Inserta una nueva auditoría con los datos que se pasan como parámetros.</p> <p>Debido a la naturaleza de este proyecto por defecto se insertará con el campo TipoProcesoEmpresa = ‘Seguridad’</p> <p>En el campo FechaUltimaModif se guarda la fecha en el momento de insertar.</p> <p>No se controla que ya exista el identificador de la nueva Auditoría ya que es el propio sistema el que los asigna por secuencia.</p>
PARÁMETROS DE SALIDA	“OK” → Proceso finalizado correctamente

PROCEDIMIENTO	PR_BAJA_AUDITORIA
DESCRIPCIÓN	Elimina una Auditoría del sistema. Solo se permite si todavía no se ha llevado a cabo
PARÁMETROS DE ENTRADA	<ul style="list-style-type: none"> <li>• PE_IDAUDIT IN INTEGER</li> </ul>
OPERATIVA	Busca la auditoría cuyo identificador corresponde al valor que se pasa por parámetro y la elimina del sistema.

	<p>No está permitido borrar Auditorias que ya se hayan realizado, pero no hay un control sobre esto ya que la futura aplicación solo permitirá seleccionar para borrar aquellas Auditorias que todavía no se hayan llevado a cabo.</p> <p>Al eliminarse, elimina también las posibles asignaciones a políticas de seguridad que pueda tener en T_AUDITORIA_POLITICASEGURIDAD (Se activa el disparador: TRIG7_ELIMINA_ASIGN_AUDIT)</p>
PARÁMETROS DE SALIDA	“OK” → Proceso finalizado correctamente

PROCEDIMIENTO	PR_MODIF_AUDITORIA
DESCRIPCIÓN	Proceso para modificar una auditoría registrada en el sistema.
PARÁMETROS DE ENTRADA	<ul style="list-style-type: none"> <li>• PE_AUDIT IN INTEGER</li> <li>• PE_TIPO VARCHAR2</li> <li>• PE_FECHA IN DATE</li> <li>• PE_TIPOPROCESOEMPRESA IN VARCHAR2</li> <li>• PE_RESULTADO IN VARCHAR2</li> <li>• PE_OBSERVACIONES IN VARCHAR2</li> </ul>
OPERATIVA	<p>Para la auditoría cuyo identificador se pasa por parámetro, por cada parámetro que se le pasa al procedimiento si es diferente de NULL, lo modifica en el registro.</p> <p>No debe borrar las posibles observaciones anotadas anteriormente.</p> <p>Actualización del campo FechaUltimaModif</p>
PARÁMETROS DE SALIDA	<p>Proceso finalizado correctamente:</p> <ul style="list-style-type: none"> <li>• “Tipo auditoría modificado”</li> <li>• “Fecha auditoría modificado”</li> <li>• “Tipo proceso empresa a auditar modificado”</li> <li>• “Observaciones modificadas”</li> </ul>

PROCEDIMIENTO	PR_ALTA_DEPARTAMENTO
DESCRIPCIÓN	Proceso para crear un nuevo departamento en el sistema
PARÁMETROS DE ENTRADA	<ul style="list-style-type: none"> <li>• PE_NOMBRE IN VARCHAR2</li> <li>• PE_RESPONSABLE IN VARCHAR2</li> <li>• PE_OBSERVACIONES IN VARCHAR2</li> </ul>
OPERATIVA	<p>Comprueba que el nombre del nuevo departamento no exista ya en el sistema y, si es así, inserta un nuevo departamento con los datos que se pasan como parámetros.</p> <p>Por defecto el campo CantEmpleados tendrá valor = 0</p> <p>En el campo FechaUltimaModif se guarda la fecha actual.</p>
PARÁMETROS DE SALIDA	<p>“OK” → Proceso finalizado correctamente</p> <p>“ERROR: El Nombre de departamento que quiere introducir ya existe en el sistema”</p>

PROCEDIMIENTO	PR_BAJA_DEPARTAMENTO
DESCRIPCIÓN	El sistema no permite el eliminado de registros de la tabla Departamento



PROCEDIMIENTO	PR MODIF DEPARTAMENTO
DESCRIPCIÓN	Proceso para modificar un departamento registrado en el sistema.
PARÁMETROS DE ENTRADA	<ul style="list-style-type: none"> <li>• PE_IDDEPTO IN INTEGER</li> <li>• PE_NOMBRE IN VARCHAR2</li> <li>• PE_RESPONSABLE IN INTEGER</li> <li>• PE_OBSERVACIONES IN VARCHAR2</li> </ul>
OPERATIVA	<p>Para el departamento cuyo identificador se pasa por parámetro, por cada parámetro que se le pasa al procedimiento si es diferente de NULL, lo modifica en el registro.</p> <p>El identificador no es modificable.</p> <p>No debe borrar las posibles observaciones anotadas anteriormente.</p> <p>Actualización del campo FechaUltimaModif</p>
PARÁMETROS DE SALIDA	<p>“OK” → Proceso finalizado correctamente</p> <p>“ERROR: El Nombre de departamento que quiere introducir ya existe en el sistema”</p>

PROCEDIMIENTO	PR ALTA EMPLEADO
DESCRIPCIÓN	Proceso para insertar un nuevo empleado en el sistema
PARÁMETROS DE ENTRADA	<ul style="list-style-type: none"> <li>• PE_DNI IN VARCHAR2</li> <li>• PE_NOMBRE IN VARCHAR2</li> <li>• PE_APELLIDO1 IN VARCHAR2</li> <li>• PE_APELLIDO2 IN VARCHAR2</li> <li>• PE_PROVINCIA IN VARCHAR2</li> <li>• PE_POBLACION IN VARCHAR2</li> <li>• PE_FECHANAINICIO VARCHAR2</li> <li>• PE_IDDEPTO IN NUMBER</li> <li>• PE_OBSERVACIONES IN VARCHAR2</li> </ul>
OPERATIVA	<p>Se comprueba que el DNI que se pasa como parámetro no exista ya en la BDD y, si es el caso, se inserta un nuevo empleado con los datos que se pasan como parámetros.</p> <p>Por defecto se da de alta como Activo = ‘Sí’ y con los campos FormacionesAsignadas e IncumpAsignados = ‘No’</p> <p>En el campo FechaUltimaModif se guarda la fecha actual</p>
PARÁMETROS DE SALIDA	<p>Proceso finalizado correctamente :</p> <ul style="list-style-type: none"> <li>• “Nombre modificado”</li> <li>• “Apellido 1 modificado”</li> <li>• “Apellido 2 modificado”</li> <li>• “Provincia modificada”</li> <li>• “Población modificada”</li> <li>• “Fecha Inicio modificada”</li> <li>• “Empleado activado”</li> <li>• “Empleado desactivado”</li> <li>• “Observaciones modificadas”</li> </ul> <p>“OK”</p> <p>“ERROR: El DNI que quiere introducir ya existe en el sistema”</p>

PROCEDIMIENTO	PR_BAJA_EMPLEADO
DESCRIPCIÓN	Proceso para dar de baja un empleado del sistema. Este procedimiento no elimina el registro del usuario del sistema, sino que lo modifica para indicar que ha causado baja en la empresa, por lo tanto, se tratará como una modificación
PARÁMETROS DE ENTRADA	<ul style="list-style-type: none"> <li>• PE_DNI IN VARCHAR2,</li> <li>• PE_FECHACAUSABAJA IN DATE</li> <li>• PE_MOTIVOCAUSABAJA IN VARCHAR2</li> <li>• PE_OBSERVACIONES IN VARCHAR2</li> </ul>
OPERATIVA	<p>Busca el empleado cuyo DNI corresponde al que se pasa por parámetro. Si Inactiva empleado...</p> <p>...marca como no activo modificando los parámetros que se pasan. Se lanza el disparador: TRIG1_INACTIVA_EMPLEADO</p> <p>Modifica las observaciones si a PE_OBSERVACIONES se le ha pasado valor (sin modificar las ya anteriores)</p> <p>Actualización del campo FechaUltimaModif</p> <p>No hay tratamiento de excepciones en la búsqueda del DNI introducido en el sistema ya que la futura aplicación mostrará un listado de los Empleados activos</p>
PARÁMETROS DE SALIDA	“OK” → Proceso finalizado correctamente

PROCEDIMIENTO	PR_MODIF_EMPLEADO
DESCRIPCIÓN	Proceso para modificar un empleado registrado en el sistema
PARÁMETROS DE ENTRADA	<ul style="list-style-type: none"> <li>• PE_DNI IN VARCHAR2</li> <li>• PE_NOMBRE IN VARCHAR2</li> <li>• PE_APELLIDO1 IN VARCHAR2</li> <li>• PE_APELLIDO2 IN VARCHAR2</li> <li>• PE_PROVINCIA IN NUMBER</li> <li>• PE_POBLACION IN NUMBER</li> <li>• PE_FECHAINICIO IN DATE</li> <li>• PE_ACTIVO IN VARCHAR2</li> <li>• PE_OBSERVACIONES IN VARCHAR2</li> </ul>
OPERATIVA	<p>Para el empleado cuyo DNI se pasa por parámetro, por cada parámetro que se le pasa al procedimiento si es diferente de NULL, lo modifica en el registro.</p> <p>Si Activa empleado ...marca como activo. FechaCausaBaja = NULL, MotivoCausaBaja = NULL.</p> <p>No debe borrar las posibles observaciones anotadas anteriormente.</p> <p>Actualización del campo FechaUltimaModif</p> <p>No hay tratamiento de excepciones en la búsqueda del DNI introducido en el sistema ya que la futura aplicación mostrará un listado de los Empleados ya introducidos para escoger uno a modificar.</p> <p>No se permite al usuario el cambio de departamento de los empleados.</p>
PARÁMETROS DE SALIDA	“OK” → Proceso finalizado correctamente

PROCEDIMIENTO	PR ALTA POLITICASEGURIDAD
DESCRIPCIÓN	Proceso para crear una nueva política de seguridad en el sistema. No será accesible para el usuario, se creará una política de seguridad por cada Vulnerabilidad creada. Una vez creada la Política de seguridad el usuario deberá modificar sus datos y Activarla (o no) según considere. Mientras el campo 'Activa' no tenga valor significará que aún no han modificado los datos (No se podrá guardar la información modificada si no le da valor al campo 'Activa')
PARÁMETROS DE ENTRADA	<ul style="list-style-type: none"> <li>PE_IDVULNERAB IN NUMBER</li> </ul>
OPERATIVA	<p>Inserta una nueva política de seguridad con los datos por defectos y asociada a la vulnerabilidad que se pasa por parámetro.</p> <p>En el campo FechaUltimaModif se guarda la fecha actual</p>
PARÁMETROS DE SALIDA	"Se ha creado una política de seguridad asociada a la vulnerabilidad" → Proceso finalizado con éxito

PROCEDIMIENTO	PR BAJA POLITICASEGURIDAD
DESCRIPCIÓN	Proceso para dar de baja una política de seguridad del sistema. Este procedimiento no elimina el registro del sistema, sino que lo modifica como no activa, por lo tanto, se tratará como una modificación
PARÁMETROS DE ENTRADA	<ul style="list-style-type: none"> <li>PE_IDPOLSEG IN INTEGER</li> </ul>
OPERATIVA	<p>Busca la política de seguridad cuyo identificador corresponde al valor que se pasa por parámetro y lo marca como no activo. El sistema también modificará el campo FechaBaja a la fecha en la que se inactiva la política de seguridad.</p> <p>No se puede desactivar una Política de Seguridad si tiene registros en la tabla AUDITORIA POLITICASEGURIDAD o SIMULACION POLITICASEGURIDAD Se llamará al disparador: TRIG2_INACTIVA_POLSEG</p> <p>Actualización del campo FechaUltimaModif</p> <p>No hay tratamiento de excepciones ya que la futura aplicación solo permitirá al usuario seleccionar una política de seguridad entre las que están activas</p>
PARÁMETROS DE SALIDA	"OK" → Proceso finalizado correctamente

PROCEDIMIENTO	PR MODIF POLITICASEGURIDAD
DESCRIPCIÓN	Proceso para modificar una política de seguridad del sistema.
PARÁMETROS DE ENTRADA	<ul style="list-style-type: none"> <li>PE_IDPOLSEG IN INTEGER</li> <li>PE_APROBADA IN VARCHAR2</li> <li>PE_DESCRIPCION IN VARCHAR2</li> <li>PE_CONSECUENCIAADMIN IN VARCHAR2</li> <li>PE_CONSECUENCIASIMUL IN VARCHAR2</li> <li>PE_ACTIVA IN VARCHAR2</li> <li>PE_OBSERVACIONES IN VARCHAR2</li> </ul>

OPERATIVA	<p>Para la política de seguridad cuyo identificador se pasa como parámetro, por cada parámetro que se le pasa al procedimiento si es diferente de NULL, lo modifica en el registro. En caso de modificar el campo 'Activa' el sistema también modificará los campos 'FechaactivaDesde'(a fecha actual) y 'FechaBaja' (NULL) No debe borrar las posibles observaciones anotadas anteriormente.</p> <p>Actualización del campo FechaUltimaModif</p> <p>No hay tratamiento de excepciones en la búsqueda de la política a modificar ya que la futura aplicación solo permitirá al usuario seleccionar una política de seguridad entre las existentes</p>
PARÁMETROS DE SALIDA	<p>Proceso finalizado correctamente:</p> <ul style="list-style-type: none"> <li>• “Política de Seguridad aprobada”</li> <li>• “Descripción modificada”</li> <li>• “Consecuencia Administrativa modificada”</li> <li>• “Consecuencia Simulación modificada”</li> <li>• “Política de Seguridad activada” / “Política de Seguridad desactivada”</li> <li>• “Observaciones modificadas”</li> </ul> <p>“Modificaciones OK”</p>

PROCEDIMIENTO	PR_ALTA_PROCESOGEMPRESA
DESCRIPCIÓN	Proceso para crear un nuevo proceso de gestión de empresa en el sistema
PARÁMETROS DE ENTRADA	<ul style="list-style-type: none"> <li>• PE_NOMBRE IN VARCHAR2</li> <li>• PE_TIPO IN VARCHAR2</li> <li>• PE_OBSERVACIONES IN VARCHAR2</li> </ul>
OPERATIVA	<p>Inserta un nuevo proceso de gestión de empresa con los datos que se pasan como parámetros.</p> <p>En el campo FechaUltimaModif se guarda la fecha actual</p> <p>No hay tratamiento de excepciones al insertar ya que es el sistema el que asigna el identificador del nuevo proceso de gestión de la empresa</p> <p>“OK” → Proceso finalizado correctamente</p>
PARÁMETROS DE SALIDA	“ERROR: El Nombre del proceso que quiere introducir ya existe en el sistema”

PROCEDIMIENTO	PR_BAJA_PROCESOGEMPRESA
DESCRIPCIÓN	El sistema no permite el eliminado de registros de la tabla ProcesoGEmpresa

PROCEDIMIENTO	PR_MODIF_PROCESOGEMPRESA
DESCRIPCIÓN	Proceso para modificar un proceso de gestión de empresa registrado en el sistema.
PARÁMETROS DE ENTRADA	<ul style="list-style-type: none"> <li>• PE_IDPROCESOGEMP IN INTEGER</li> <li>• PE_NOMBRE IN VARCHAR2</li> <li>• PE_TIPO IN VARCHAR2</li> <li>• PE_OBSERVACIONES IN VARCHAR2</li> </ul>
OPERATIVA	Para el proceso de gestión de empresa cuyo identificador se pasa por parámetro, por cada parámetro que se le pasa al procedimiento si es diferente de NULL, lo modifica en el registro.

	<p>No debe borra las posibles observaciones anotadas anteriormente.</p> <p>Actualización del campo FechaUltimaModif</p> <p>No hay tratamiento de excepciones en la búsqueda del proceso a modificar ya que la futura aplicación solo permitirá al usuario seleccionar un proceso entre los existentes</p>
PARÁMETROS DE SALIDA	“OK” → Proceso finalizado correctamente

PROCEDIMIENTO	PR_ALTA_SESIONFORMACION
DESCRIPCIÓN	Proceso para crear una nueva sesión de formación en el sistema
PARÁMETROS DE ENTRADA	<ul style="list-style-type: none"> <li>• PE_TIPO IN VARCHAR2</li> <li>• PE_TITULO IN VARCHAR2</li> <li>• PE_DESCRIPCION IN VARCHAR2</li> <li>• PE_FECHAINICIOSESIONFORMACION IN DATE</li> <li>• PE_FECHAFINSESIONFORMACION IN DATE</li> <li>• PE_OBSERVACIONES IN VARCHAR2</li> </ul>
OPERATIVA	<p>Inserta una nueva sesión de formación con los datos que se pasan como parámetros.</p> <p>En el campo FechaUltimaModif se guarda la fecha actual</p>
PARÁMETROS DE SALIDA	<p>“OK” → Proceso finalizado correctamente</p> <p>“ERROR: El TÍTULO que quiere introducir ya existe en el sistema”</p>

PROCEDIMIENTO	PR_BAJA_SESIONFORMACION
DESCRIPCIÓN	Elimina una sesión de formación del sistema.
PARÁMETROS DE ENTRADA	<ul style="list-style-type: none"> <li>• PE_SESFORM IN NUMBER</li> </ul>
OPERATIVA	<p>Solo se permite si todavía no se ha iniciado. Busca la sesión de formación que se pasa por parámetro y la elimina del sistema</p> <p>Al eliminarse elimina también las posibles asignaciones a empleados que pueda tener en T_EMPLEADO_SESOINFORMACION (Se activa el disparador: TRIG5_ELIMINA_ASIGNACIONES_SESIONFORMACION)</p> <p>No hay tratamiento de excepciones en la búsqueda de la sesión de formación a dar de baja ya que la futura aplicación solo permitirá seleccionar para dar de baja aquellas que cumplen con la condición descrita.</p>
PARÁMETROS DE SALIDA	“OK” → Proceso finalizado correctamente

PROCEDIMIENTO	PR_MODIF_SESIONFORMACION
DESCRIPCIÓN	Proceso para modificar una sesión de formación registrada en el sistema.
PARÁMETROS DE ENTRADA	<ul style="list-style-type: none"> <li>• PE_IDSESIONFORM IN NUMBER</li> <li>• PE_TIPO IN VARCHAR2</li> <li>• PE_TITULO IN VARCHAR2</li> <li>• PE_DESCRIPCION IN VARCHAR2</li> <li>• PE_FECHAINICIOSESIONFORMACION IN DATE</li> </ul>

	<ul style="list-style-type: none"> <li>• PE_FECHAFINSESIONFORMACION IN DATE</li> <li>• PE_OBSERVACIONES IN VARCHAR2</li> </ul>
OPERATIVA	<p>Para la sesión de formación cuyo identificador se pasa por parámetro, por cada parámetro que se le pasa al procedimiento si es diferente de NULL, lo modifica en el registro.</p> <p>No debe borrar las posibles observaciones anotadas anteriormente.</p> <p>Actualización del campo FechaUltimaModif</p> <p>No hay tratamiento de excepciones en la búsqueda de la sesión de formación a modificar ya que la futura aplicación solo permitirá seleccionar para modificar aquellas sesiones de formación ya existentes.</p>
PARÁMETROS DE SALIDA	“OK” → Proceso finalizado correctamente

PROCEDIMIENTO	<b>PR_ALTA_SIMULACION</b>
DESCRIPCIÓN	Proceso para crear una nueva simulación en el sistema
PARÁMETROS DE ENTRADA	<ul style="list-style-type: none"> <li>• PE_RESPONSABLE IN INTEGER</li> <li>• PE_DESCRIPCION IN VARCHAR2</li> <li>• PE_FECHA IN DATE</li> <li>• PE_OBSERVACIONES IN VARCHAR2</li> </ul>
OPERATIVA	<p>Inserta una nueva simulación con los datos que se pasan como parámetros.</p> <p>En el campo FechaUltimaModif se guarda la fecha actual</p> <p>No hay tratamiento de excepciones en la inserción de las simulaciones ya que es el propio sistema el que asigna el identificador de la nueva Simulación.</p>
PARÁMETROS DE SALIDA	“OK” → Proceso finalizado correctamente

PROCEDIMIENTO	<b>PR_BAJA_SIMULACION</b>
DESCRIPCIÓN	Elimina una simulación del sistema.
PARÁMETROS DE ENTRADA	<ul style="list-style-type: none"> <li>• PE_IDSIMUL IN INTEGER</li> </ul>
OPERATIVA	<p>Solo se permite si la simulación todavía no se ha llevado a cabo. Busca la simulación que se pasa por parámetro y la elimina del sistema</p> <p>Al eliminarse elimina también las posibles asignaciones que pueda tener en: T_EMPELADO_SIMULACION (Se activa el disparador: TRIG6_ELIMINA_ASIGN_SIMUL)</p> <p>No hay tratamiento de excepciones en la búsqueda de la simulación a dar de baja ya que la futura aplicación solo permitirá seleccionar para dar de baja aquellas que cumplen con la condición descrita.</p>
PARÁMETROS DE SALIDA	“OK” → Proceso finalizado correctamente

PROCEDIMIENTO	<b>PR_MODIF_SIMULACION</b>
DESCRIPCIÓN	Proceso para modificar una simulación registrada en el sistema.

PARÁMETROS DE ENTRADA	<ul style="list-style-type: none"> <li>• PE_IDSIMUL IN NUMBER,</li> <li>• PE_RESPONSABLE IN INTEGER,</li> <li>• PE_DESCRIPCION IN VARCHAR2,</li> <li>• PE_FECHA IN DATE,</li> <li>• PE_OBSERVACIONES IN VARCHAR2</li> </ul>
OPERATIVA	<p>Para la simulación cuyo identificador se pasa por parámetro, por cada parámetro que se le pasa al procedimiento si es diferente de NULL, lo modifica en el registro.</p> <p>No debe borrar las posibles observaciones anotadas anteriormente.</p> <p>Actualización del campo FechaUltimaModif</p> <p>No hay tratamiento de excepciones en la búsqueda de la simulación a modificar ya que la futura aplicación solo permitirá seleccionar para modificar aquellas simulaciones ya existentes.</p>
PARÁMETROS DE SALIDA	<p>Proceso finalizado correctamente:</p> <ul style="list-style-type: none"> <li>• “Responsable modificado”</li> <li>• “Descripción modificada”</li> <li>• “Fecha modificada”</li> <li>• “Observaciones modificadas”</li> </ul> <p>“OK”</p>

PROCEDIMIENTO	PR_ALTA_VULNERABILIDAD
DESCRIPCIÓN	Proceso para crear una nueva vulnerabilidad en el sistema
PARÁMETROS DE ENTRADA	<ul style="list-style-type: none"> <li>• PE_NOMBRE IN VARCHAR2</li> <li>• PE_CRITICA IN VARCHAR2</li> <li>• PE_DESCRIPCION IN VARCHAR2</li> <li>• PE_FECHADETECCION IN DATE</li> <li>• PE_DETECTADAPOR IN VARCHAR2</li> <li>• PE_OBSERVACIONES IN VARCHAR2</li> </ul>
OPERATIVA	<p>Comprueba que no existe otra vulnerabilidad con el mismo nombre. Si no la hay, inserta una nueva vulnerabilidad con los datos que se pasan como parámetros.</p> <p>Al campo: “Estado” se le asignará por defecto el valor: “Identificada”</p> <p>En el campo FechaUltimaModif se guarda la fecha actual.</p> <p>Crearé, por defecto, la Política de seguridad que le corresponde a dicha Vulnerabilidad y el sistema enviará un mail al usuario que corresponda para recordarle que debe modificar esta Política de seguridad. (Proceso de mail a implantar en segunda fase)</p>
PARÁMETROS DE SALIDA	<p>“OK” → Proceso finalizado correctamente</p> <p>“ERROR: El NOMBRE que quiere introducir ya existe en el sistema”</p>

PROCEDIMIENTO	PR_BAJA_VULNERABILIDAD
DESCRIPCIÓN	El sistema no permite el eliminado de registros de la tabla Vulnerabilidad

PROCEDIMIENTO	PR_MODIF_VULNERABILIDAD
DESCRIPCIÓN	Proceso para modificar una vulnerabilidad registrada en el sistema.

PARÁMETROS DE ENTRADA	<ul style="list-style-type: none"> <li>• PE_IDVULNERAB IN NUMBER</li> <li>• PE_NOMBRE IN VARCHAR2</li> <li>• PE_ESTADO IN VARCHAR2</li> <li>• PE_DESCRIPCION IN VARCHAR2</li> <li>• PE_FECHADETECCION IN VARCHAR2</li> <li>• PE_OBSERVACIONES IN VARCHAR2</li> </ul>
OPERATIVA	<p>Para la vulnerabilidad cuyo identificador se pasa por parámetro, por cada parámetro que se le pasa al procedimiento si es diferente de NULL, lo modifica en el registro.</p> <p>El campo “Critica” no es modificable.</p> <p>El campo “DetectadaPor” no será modificable para el usuario (Salvo que se vuelva a contar con una consultoría externa para localizar nuevas vulnerabilidades)</p> <p>No debe borrar las posibles observaciones anotadas anteriormente.</p> <p>El campo “Estado” solo es editable para los usuarios para cambiarlo de Identificada a No mitigada, el resto solo es modificable por el propio sistema. Será la futura aplicación quien controlará que se pueda modificar este campo o no según su valor actual en el momento.</p> <p>Actualización del campo FechaUltimaModif</p>
PARÁMETROS DE SALIDA	<p>Proceso finalizado correctamente:</p> <ul style="list-style-type: none"> <li>• “OK, Nombre Modificado”</li> <li>• “OK, Estado Modificado”</li> <li>• “OK, Descripción Modificada”</li> <li>• “OK, Fecha Detección Modificada”</li> <li>• “OK, Observaciones Modificadas”</li> </ul> <p>“ERROR: El NOMBRE que quiere introducir ya existe en el sistema”</p>

PROCEDIMIENTO	<b>PR_ALTA_AUDITORIA_POLITICASEGURIDAD</b>
DESCRIPCIÓN	Proceso para asignar una política de seguridad a una auditoría
PARÁMETROS DE ENTRADA	<ul style="list-style-type: none"> <li>• PE_IDAUDIT IN INTEGER</li> <li>• PE_POLSEG IN INTEGER</li> <li>• PE_SUPERADA IN VARCHAR2</li> <li>• PE_OBSERVACIONES IN VARCHAR2</li> </ul>
OPERATIVA	<p>No tiene que comprobar que la política de seguridad está, previamente, aprobada por la empresa ya que la futura aplicación solo permitirá escoger al usuario entre las políticas de seguridad ya aprobadas por la empresa (y que estén activas)</p> <p>Inserta el registro con los datos que se pasan por parámetro. El campo Anyo lo toma el propio sistema de la fecha de la Auditoría.</p> <p>En el campo FechaUltimaModif se guarda la fecha actual</p>
PARÁMETROS DE SALIDA	“OK” → Proceso finalizado correctamente

PROCEDIMIENTO	<b>PR_BAJA_AUDITORIA_POLITICASEGURIDAD</b>
DESCRIPCIÓN	Proceso para dar de baja la asignación de una auditoría a una política de seguridad.
PARÁMETROS DE ENTRADA	<ul style="list-style-type: none"> <li>• PE_IDAUDIT IN NUMBER,</li> <li>• PE_IDPOLSEG IN NUMBER</li> </ul>



OPERATIVA	<p>Solo permite borrar aquellos registros en los que todavía no se ha llevado a cabo la auditoría. Pero el sistema no controla esto ya que la futura aplicación filtrará al usuario únicamente aquellas asignaciones en las que la auditoría aún no se haya realizado para que el usuario escoja una para eliminar.</p> <p>Por lo tanto, el sistema únicamente tendrá que borrar el registro que se le pase por parámetro</p>
PARÁMETROS DE SALIDA	“OK” → Proceso finalizado correctamente

PROCEDIMIENTO	<b>PR_MODIF_AUDITORIA_POLITICASEGURIDAD</b>
DESCRIPCIÓN	Proceso para modificar la asignación de una auditoría a una política de seguridad.
PARÁMETROS DE ENTRADA	<ul style="list-style-type: none"> <li>• PE_IDAUDIT IN NUMBER</li> <li>• PE_IDPOLSEG IN NUMBER</li> <li>• PE_SUPERADA IN VARCHAR2</li> <li>• PE_OBSERVACIONES IN VARCHAR2</li> </ul>
OPERATIVA	<p>Solo se permite modificar los campos ‘Superada’ y ‘Observaciones’</p> <p>Actualización del campo FechaUltimaModif</p>
PARÁMETROS DE SALIDA	<p>Proceso finalizado correctamente:</p> <p>“OK, Campo: Superada, Modificado”</p> <p>“OK, Campo: Observaciones, Modificado”</p>

PROCEDIMIENTO	<b>PR_ALTA_DEPARTAMENTO_PROCESOGEMPRESA</b>
DESCRIPCIÓN	Procedimiento que asigna un proceso de gestión de la empresa a un departamento.
PARÁMETROS DE ENTRADA	<ul style="list-style-type: none"> <li>• PE_IDDEPTO IN NUMBER</li> <li>• PE_IDPROCESOGEMP IN NUMBER</li> <li>• PE_OBSERVACIONES IN VARCHAR2</li> </ul>
OPERATIVA	<p>Crea un registro nuevo con aquellos parámetros que se le pasan por parámetros.</p> <p>No hay tratamiento de excepciones ya que la futura aplicación no permitirá seleccionar un proceso a un departamento que ya lo tenga asignado.</p>
PARÁMETROS DE SALIDA	“OK” → Proceso finalizado correctamente

PROCEDIMIENTO	<b>PR_BAJA_DEPARTAMENTO_PROCESOGEMPRESA</b>
DESCRIPCIÓN	Procedimiento que elimina el registro que corresponde con los campos que se le pasan por parámetro.
PARÁMETROS DE ENTRADA	<ul style="list-style-type: none"> <li>• PE_IDDEPTO IN NUMBER</li> <li>• PE_IDPROCESOGEMP IN NUMBER</li> </ul>
OPERATIVA	El sistema borra directamente el registro que corresponde al proceso y al departamento pasados por parámetro.
PARÁMETROS DE SALIDA	“OK” → Proceso finalizado correctamente

PROCEDIMIENTO	<b>PR_MODIF_DEPARTAMENTO_PROCESOGEMPRESA</b>
DESCRIPCIÓN	Procedimiento que permite modificar las Observaciones del proceso de gestión de la empresa asociado a un departamento

PARÁMETROS DE ENTRADA	<ul style="list-style-type: none"> <li>• PE_IDDEPTO IN NUMBER</li> <li>• PE_IDPROCESOGEMP IN NUMBER</li> <li>• PE_OBSERVACIONES IN VARCHAR2</li> </ul>
OPERATIVA	El sistema modifica las observaciones y actualiza la fecha de última modificación
PARÁMETROS DE SALIDA	“OK” → Proceso finalizado correctamente

PROCEDIMIENTO	<b>PR_ALTA_EMPLEADO_SESIONFORMACION</b>
DESCRIPCIÓN	Procedimiento que asigna una sesión de formación a un empleado.
PARÁMETROS DE ENTRADA	<ul style="list-style-type: none"> <li>• PE_IDEMP IN NUMBER</li> <li>• PE_IDSESFORM IN NUMBER</li> <li>• PE_OBSERVACIONES IN VARCHAR2</li> </ul>
OPERATIVA	<p>El sistema creará un registro asignando una sesión de formación a un empleado.</p> <p>No hay tratamiento de excepciones ya que la futura aplicación solo permitirá asignar a un empleado aquellas sesiones que todavía no tenga asignadas y que no hayan empezado.</p> <p>En vista de una segunda fase de implementación se estudiará la posibilidad de enviar un mail al usuario cada vez que le asignen una sesión de formación.</p>
PARÁMETROS DE SALIDA	“OK” → Proceso finalizado correctamente

PROCEDIMIENTO	<b>PR_BAJA_EMPLEADO_SESIONFORMACION</b>
DESCRIPCIÓN	Procedimiento que elimina la asignación de una sesión de formación a un empleado.
PARÁMETROS DE ENTRADA	<ul style="list-style-type: none"> <li>• PE_IDSESFORM IN NUMBER</li> <li>• PE_IDEMP IN NUMBER</li> </ul>
OPERATIVA	El sistema no permite que se elimine un registro si la sesión de formación ya ha comenzado, pero no hay tratamiento de excepciones ya que será la futura aplicación la que controlará mediante un desplegable que el usuario solo pueda seleccionar para eliminar aquellas formaciones asignadas al usuario que todavía no se hayan realizado.
PARÁMETROS DE SALIDA	“OK” → Proceso finalizado correctamente

PROCEDIMIENTO	<b>PR_MODIF_EMPLEADO_SESIONFORMACION</b>
DESCRIPCIÓN	Procedimiento que permite modificar las fechas y observaciones de la asignación de una sesión de formación a un empleado.
PARÁMETROS DE ENTRADA	<ul style="list-style-type: none"> <li>• PE_IDEMP IN NUMBER,</li> <li>• PE_IDSESFORM IN NUMBER,</li> <li>• PE_FECHAINICIOFORMACION IN VARCHAR2,</li> <li>• PE_FECHAFINFORMACION IN VARCHAR2,</li> <li>• PE_OBSERVACIONES IN VARCHAR2</li> </ul>
OPERATIVA	<p>El sistema comprueba los valores que se van a modificar (parámetros no nulos) y los modifica en el registro.</p> <p>Actualización de FechaUltimaModif</p>

PARÁMETROS DE SALIDA	Proceso finalizado correctamente: “OK, Campo: FechaInicioFormacion, Modificado” “OK, Campo: FechaFinFormacion, Modificado” “OK, Campo: Observaciones, Modificado”
----------------------	--

PROCEDIMIENTO	PR ALTA EMPLEADO SIMULACION
DESCRIPCIÓN	Proceso para registrar la inclusión de un empleado en una simulación
PARÁMETROS DE ENTRADA	<ul style="list-style-type: none"> <li>• PE_EMP IN INTEGER</li> <li>• PE_IDSIMUL IN INTEGER</li> <li>• PE_OBSERVACIONES IN VARCHAR2</li> </ul>
OPERATIVA	<p>Inserta un registro nuevo en la tabla T_EMPLEADO_SIMULACION con los datos que se pasan como parámetros.</p> <p>En el campo FechaUltimaModif se guarda la fecha actual</p> <p>No hay tratamiento de excepciones ya que la futura aplicación solo permitirá asignar a un empleado aquellas simulaciones que todavía no tenga asignadas y que no hayan empezado.</p>
PARÁMETROS DE SALIDA	“OK” → Proceso finalizado correctamente

PROCEDIMIENTO	PR BAJA EMPLEADO SIMULACION
DESCRIPCIÓN	Elimina un registro de la tabla EMPLEADO_SIMULACION. Solo permite eliminar el registro si la simulación aún no se ha llevado a cabo
PARÁMETROS DE ENTRADA	<ul style="list-style-type: none"> <li>• PE_EMP IN INTEGER</li> <li>• PE_IDSIMUL IN INTEGER</li> </ul>
OPERATIVA	<p>Elimina el registro de la tabla T_EMPLEADO_SIMULACION cuyos IDEMP e IDSIMUL se pasan como parámetros.</p> <p>El sistema no permite que se elimine un registro si la simulación ya ha comenzado, pero no hay tratamiento de excepciones ya que será la futura aplicación la que controlará mediante un desplegable que el usuario solo pueda seleccionar para eliminar aquellas simulaciones asignadas al usuario que todavía no se hayan realizado.</p>
PARÁMETROS DE SALIDA	“OK” → Proceso finalizado correctamente

PROCEDIMIENTO	PR MODIF EMPLEADO SIMULACION
DESCRIPCIÓN	Proceso para modificar las observaciones de la asignación de una simulación a un empleado.
PARÁMETROS DE ENTRADA	<ul style="list-style-type: none"> <li>• PE_IDEMP IN NUMBER</li> <li>• PE_IDSIMUL IN NUMBER</li> <li>• PE_OBSERVACIONES IN VARCHAR2</li> </ul>
OPERATIVA	<p>Para el empleado y la simulación que se pasan como parámetros se modifican las observaciones.</p> <p>No debe borrar las posibles observaciones anotadas anteriormente.</p> <p>Actualización del campo FechaUltimaModif</p>
PARÁMETROS DE SALIDA	Proceso finalizado correctamente: <ul style="list-style-type: none"> <li>• “OK, Campo: Observaciones, Modificado”</li> </ul>

PROCEDIMIENTO	PR ALTA INCUMPLIMIENTO DEPTO
DESCRIPCIÓN	Procedimiento para dar de alta o modificar la cantidad de incumplimientos que tiene asignados un departamento durante un año.
PARÁMETROS DE ENTRADA	<ul style="list-style-type: none"> <li>• PE_IDDEPTO IN NUMBER</li> <li>• PE_IDPOLSEG IN NUMBER</li> <li>• PE_ANYO IN NUMBER</li> </ul>
OPERATIVA	<p>Por cada incumplimiento de empleado se actualiza esta tabla modificando o dando de alta un registro.</p> <p>Si ya existe un registro con el departamento, política de seguridad y año que se pasan por parámetros lo modifica aumentando en 1 la Cantidad. Si el registro no existe, lo crea.</p>
PARÁMETROS DE SALIDA	<p>Proceso finalizado correctamente:</p> <ul style="list-style-type: none"> <li>• “OK, incumplimiento depto. modificado”</li> <li>• “OK, incumplimiento depto creado”</li> </ul>

PROCEDIMIENTO	PR BAJA INCUMPLIMIENTO DEPTO
DESCRIPCIÓN	El usuario no tiene acceso a la baja y/o modificación de estos registros

PROCEDIMIENTO	PR MODIF INCUMPLIMIENTO DEPTO
DESCRIPCIÓN	Las únicas modificaciones que se pueden realizar se hacen en el procedimiento: PR_ALTA_INCUMPLIMIENTO_DEPTO

PROCEDIMIENTO	PR ALTA INCUMPLIMIENTO EMP
DESCRIPCIÓN	Proceso para registrar el incumplimiento de un empleado
PARÁMETROS DE ENTRADA	<ul style="list-style-type: none"> <li>• PE_IDEMP IN INTEGER</li> <li>• PE_POLSEG IN INTEGER</li> <li>• PE_TIPO IN VARCHAR2</li> <li>• PE_OBSERVACIOES IN VARCHAR2</li> <li>• PE_IDAUDIT IN NUMBER,</li> <li>• PE_IDSIMUL IN NUMBER</li> </ul>
OPERATIVA	<p>Dependiendo de si el tipo de Incumplimiento es por Simulación o por Política de seguridad el sistema extraerá los valores de los campos: “Consecuencia*” y el año correspondiente.</p> <p>Se guarda un registro del incumplimiento del empleado con los datos que se pasan como parámetros y con la variable var_consecuencia como valor del campo Consecuencia del nuevo registro.</p> <p>En el campo FechaUltimaModif se guarda la fecha actual.</p> <p>Por cada registro nuevo se llamará al proceso: PR_ALTA_INCUMPLIMIENTO_DEPTO</p>
PARÁMETROS DE SALIDA	“OK” → Proceso finalizado correctamente

PROCEDIMIENTO	PR BAJA INCUMPLIMIENTO EMP
DESCRIPCIÓN	El sistema no permite la eliminación de registros de la tabla INCUMPLIMIENTO_EMP

PROCEDIMIENTO	PR_MODIF_INCUMPLIMIENTO_EMP
DESCRIPCIÓN	Proceso para modificar las observaciones del incumplimiento de un empleado.
PARÁMETROS DE ENTRADA	<ul style="list-style-type: none"> <li>PE_IDINCUMP IN INTEGER</li> <li>PE_OBSERVACIONES IN VARCHAR2</li> </ul>
OPERATIVA	<p>Para el incumplimiento que se pasa como parámetro, modifica las observaciones del registro.</p> <p>No debe borrar las posibles observaciones anotadas anteriormente.</p> <p>Actualización del campo FechaUltimaModif</p>
PARÁMETROS DE SALIDA	“OK” → Proceso finalizado correctamente

PROCEDIMIENTO	PR_ALTA_SIMULACION_POLITICASEGURIDAD
DESCRIPCIÓN	Proceso para asignar una política de seguridad a una simulación
PARÁMETROS DE ENTRADA	<ul style="list-style-type: none"> <li>PE_IDSIMUL IN NUMBER,</li> <li>PE_IDPOLSEG IN NUMBER,</li> <li>E_OBSERVACIONES IN VARCHAR2</li> </ul>
OPERATIVA	<p>Inserta un registro nuevo en la tabla SIMULACION_POLITICASEGURIDAD con los datos que se pasan como parámetros.</p> <p>No comprueba que ya exista esta asignación ya que la futura aplicación solo permitirá asignar a una simulación políticas de seguridad que aún no se le hayan asignado.</p> <p>En el campo FechaUltimaModif se guarda la fecha actual</p>
PARÁMETROS DE SALIDA	“OK” → Proceso finalizado correctamente

PROCEDIMIENTO	PR_BAJA_SIMULACION_POLITICASEGURIDAD
DESCRIPCIÓN	Elimina un registro de la tabla: T_SIMULACION_POLITICASEGURIDAD.
PARÁMETROS DE ENTRADA	<ul style="list-style-type: none"> <li>PE_IDSIMUL IN INTEGER</li> <li>PE_POLSEG IN INTEGER</li> </ul>
OPERATIVA	<p>Solo permite eliminar el registro si la simulación aún no se ha llevado a cabo aunque no se hace tratamiento de esto ya que la futura aplicación mostrará un desplegable únicamente con las asignaciones que todavía no hayan llevado a cabo su simulación.</p> <p>Elimina el registro de la tabla T_SIMULACION_POLITICASEGURIDAD cuyos IDSIMUL e IDPOLSEG se pasan como parámetros.</p>
PARÁMETROS DE SALIDA	“OK” → Proceso finalizado correctamente

PROCEDIMIENTO	PR_MODIF_SIMULACION_POLITICASEGURIDAD
DESCRIPCIÓN	Proceso para modificar las observaciones de la asignación de una política de seguridad a una simulación.
PARÁMETROS DE ENTRADA	<ul style="list-style-type: none"> <li>PE_IDSIMUL IN INTEGER</li> <li>PE_IDPOLSEG IN INTEGER</li> <li>PE_OBSERVACIONES IN VARCHAR2</li> </ul>

OPERATIVA	<p>Para la simulación y la política de seguridad que se pasan como parámetros se modifican las observaciones.</p> <p>No debe borrar las posibles observaciones anotadas anteriormente.</p> <p>Actualización del campo FechaUltimaModif</p> <p>La futura aplicación solo permitirá asignar a una simulación, mediante listado, aquellas políticas de seguridad que en ese momento estén activas y aprobadas por la empresa</p>
PARÁMETROS DE SALIDA	“OK” → Proceso finalizado correctamente

PROCEDIMIENTO	<b>PR_ALTA_VULNERAB_PROCESOGEMP</b>
DESCRIPCIÓN	Procedimiento que asigna una vulnerabilidad a un proceso de gestión de la empresa junto con el año en el que asigna.
PARÁMETROS DE ENTRADA	<ul style="list-style-type: none"> <li>• PE_IDVULNERAB IN NUMBER,</li> <li>• PE_IDPROCESOGEMP IN NUMBER,</li> <li>• PE_ANYO IN NUMBER</li> </ul>
OPERATIVA	<p>Busca si ya existe esta asignación (No importa el año en el que se asignara, importa que ya existe la asignación en sí)</p> <p>Si existe lanza un mensaje de error.</p> <p>Si no existe crea la asignación</p>
PARÁMETROS DE SALIDA	<p>“ERROR: Esta vulnerabilidad ya fue asignada a este proceso en: (Año en el que se asignó)”</p> <p>“OK” → Proceso finalizado correctamente</p>

PROCEDIMIENTO	<b>PR_BAJA_VULNERABILIDAD_PROCESOGEMPRESA</b>
DESCRIPCIÓN	Procedimiento que da de baja la asignación de una vulnerabilidad a un proceso de gestión de la empresa.
PARÁMETROS DE ENTRADA	<ul style="list-style-type: none"> <li>• PE_IDVULNERAB IN NUMBER</li> <li>• PE_IDPROCESOGEMP IN NUMBER</li> </ul>
OPERATIVA	<p>El usuario selecciona un proceso de gestión de la empresa y, la futura aplicación, mostrará un desplegable con las vulnerabilidades que tiene asignadas.</p> <p>El proceso eliminará este registro</p>
PARÁMETROS DE SALIDA	“OK” → Proceso finalizado correctamente

PROCEDIMIENTO	<b>PR_MODIF_VULNERAB_PROCESOGEMP</b>
DESCRIPCIÓN	El sistema no permite modificar las asociaciones entre los procesos de gestión de la empresa y sus vulnerabilidades detectadas

## Otros Procedimientos

PROCEDIMIENTO	PR_ESTADOSVULNERAB
DESCRIPCIÓN	Modifica el campo Estado de la tabla T_VULNERABILIDAD según se modifiquen los valores de los T_ACCIONMITIGACION.
PARÁMETROS DE ENTRADA	<ul style="list-style-type: none"> <li>PE_IDVULNERAB IN NUMBER</li> </ul>
OPERATIVA	Cuando se modifica el Estado de la Acción de Mitigación se analizan todos los estados del resto de Acciones de mitigación y selecciona un Estado para la vulnerabilidad según corresponda.
PARÁMETROS DE SALIDA	“OK” → Proceso finalizado correctamente

## DISPARADORES

Los disparadores, también llamados Triggers, son scripts que contienen una serie de reglas predefinidas asociadas a una tabla al realizarse determinadas operaciones tales como insertar, actualizar o eliminar registros.<sup>15</sup>

En nuestro caso concreto los disparadores que utilizaremos serán los siguientes:

TABLA	EVENTO	ACCIÓN
T_EMPLEADO	AFTER UPDATE	Si campo Activo pasa a ser='No': TRIG1_INACTIVA_EMPLEADO_RESP
T_EMPLEADO	AFTER INSERT UPDATE (ACTIVO, IDDEPTO)	TRIG2_ACTUALIZA_CANTEMPLEADOS
T_SESIONFORMACION	BEFORE DELETE	TRIG5_ELIMINA_ASIGN_SESFORM
T_SIMULACION	BEFORE DELETE	TRIG6_ELIMINA_ASIGN_SIMUL
T_AUDITORIA	BEFORE DELETE	TRIG7_ELIMINA_ASIGN_AUDIT
T_INCUMPLIMIENTO_DEPTO	AFTER INSERT UPDATE	TRIG_C1_SUMA
T_C1_SUMA	AFTER INSERT UPDATE	TRIG_C1_RESULT
T_VULNERAB_PROCESOGEMPRESA	AFTER INSERT UPDATE	TRIG_C2_SUMA
T_C2_SUMA	AFTER INSERT UPDATE	TRIG_C2_RESULT
T_VULNERABILIDAD	AFTER DELETE INSERT UPDATE	TRIG_C4
T_ACCIONMITIGACION	AFTER INSERT UPDATE (ESTADO)	TRIG_C5
T_INCUMPLIMIENTO_EMP	AFTER INSERT	TRIG_C6_SUMA
T_C6_SUMA	AFTER INSERT UPDATE	TRIG_C6_RESULT
T_EMPLEADO_SESIONFORMACION	AFTER INSERT	TRIG_C7
T_INCUMPLIMIENTO_EMP	AFTER INSERT	TRIG_C8
T_INCUMPLIMIENTO_EMP	AFTER INSERT UPDATE (IDAUDIT)	TRIG_C9_SUMA
T_C9_SUMA	AFTER INSERT UPDATE	TRIG_C9_RESULT
T_VULNERABILIDAD	AFTER DELETE INSERT UPDATE	TRIG_C10

<sup>15</sup> <https://www.tutorialesprogramacionya.com/oracleya/temarios/descripcion.php?cod=261&punto=1&inicio=>

	(ESTADO)	
T_VULNERABILIDAD	AFTER INSERT	TRIG_C12
T_ACCIONMITIGACION	AFTER DELETE INSERT UPDATE (ESTADO)	TRIG_C13

## 2.3. Implementación

### 2.3.1. SGBD

Un sistema de gestión de bases de datos (SGBD) es una capa de software necesaria para crear, manipular y recuperar datos desde una base de datos<sup>16</sup>. Este proyecto se ha desarrollado con el SGBD relacional de Oracle en su versión “21.4.3.063” de SQLDeveloper.

El lenguaje utilizado ha sido tanto SQL, (para las propias sentencias de creación en sí) como PL/SQL para procedimientos, disparadores....

El lenguaje de Consulta Estructurado (SQL; Structured Query Language) es un sublenguaje estándar de base de datos.<sup>17</sup>

PL/SQL es un lenguaje de programación desarrollado por Oracle como extensión de SQL. La principal característica de PL/SQL es su capacidad para integrar construcciones de procedimientos con SQL<sup>18</sup>

### 2.3.2. Scripts para la BD

Se muestra, a continuación, tanto el listado de los scripts creados para la implementación de la BD como su correspondiente contenido:

SCRIPT	CONTENIDO
BD_create.sql	Script con el contenido necesario para la creación de la BD: <ul style="list-style-type: none"> <li>• Creación de tablas, relaciones...</li> <li>• Creación de secuencias</li> </ul>
PR_ABM.sql	Procedimientos de Alta/Baja/Modif de registros
PR_ESTADOSVULNERAB.sql	Procedimiento de actualización de los estados de las vulnerabilidades
TRIG_BD.sql	Disparadores varios que actualizan la BD
TRIG_RE.sql	Disparadores que actualizan las tablas de Repositorio Estadístico
Inicializa.sql	Script que inicializa el sistema con los valores necesarios para poder empezar a trabajar.

<sup>16</sup> Millán, M. E. (2012). Fundamentos de bases de datos. Cali, Colombia, Programa Editorial Universidad del Valle. Recuperado de <https://elibro.net/es/ereader/uoc/129060?page=1>.

<sup>17</sup> Beynon-Davies, P. (2018). *Sistemas de bases de datos*. Editorial Reverté.

<sup>18</sup> (01/06/2022) <https://www.unir.net/ingenieria/revista/que-es-plsql/>



### 2.3.3. Repositorio Estadístico

A continuación, se detallan las consultas que se realizarán al sistema para la obtención en tiempo de las consultas que ofrecerá el Repositorio Estadístico.

CÓDIGO	CONSULTA
C1	<p>Departamento que, en un año concreto, tiene un número mayor de incumplimientos registrados en la BD</p> <p><b>SELECT IdDepto FROM T_C1_RESULT WHERE Anyo = (Año a consultar);</b></p> <p>Para que mostrara toda la info.:</p> <p><b>SELECT * FROM T_C1_RESULT WHERE Anyo = (Año a consultar);</b></p>
C2	<p>Proceso de gestión interno que ha tenido mayor número de vulnerabilidades detectadas</p> <p><b>SELECT * FROM T_C2_RESULT;</b></p>
C4	<p>Porcentaje de vulnerabilidades que, en el momento de ejecutar la consulta, están totalmente mitigadas</p> <p><b>SELECT Porcentaje FROM T_C4;</b></p>
C5	<p>Número total de acciones de mitigación que , en el momento de ejecutar la consulta, no están totalmente acabadas</p> <p><b>SELECT Cant FROM T_C5;</b></p>
C6	<p>Política de seguridad que, en el momento de ejecutar la consulta, ha tenido más incumplimientos</p> <p><b>SELECT * FROM T_C6_RESULT;</b></p>
C7	<p>Dado un determinado departamento, 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.</p> <p><b>SELECT Porcentaje FROM T_C7 WHERE IdDepto = (Depto a consultar);</b></p>
C8	<p>Porcentaje de usuarios de la empresa que, en el año en curso, no tienen ningún incumplimiento asignado.</p> <p><b>SELECT PorcentyakeNOImcumpAsig FROM T_C8;</b></p>
C9	<p>Teniendo en cuenta todas las auditorías externas realizadas, año en el cual se han detectado más incumplimientos.</p> <p><b>SELECT * FROM T_C9_RESULT;</b></p>
C10	<p>Porcentaje de vulnerabilidades críticas que, en el momento de ejecutar la consulta, tienen alguna acción de mitigación abierta</p> <p><b>SELECT Porcentaje FROM T_C10;</b></p>
C12	<p>Número de vulnerabilidades críticas detectadas internamente teniendo en cuenta todos los datos de que se dispone.</p> <p><b>SELECT Cant FROM T_C12;</b></p>

C13	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”
	<code>SELECT Porcentaje FROM T_C13;</code>

## 2.4. Pruebas

A lo largo del documento se ha ido detallando algunos de los controles que se dejan a cargo de la futura aplicación con respecto al funcionamiento del sistema. Pues bien, llegado este punto es importante recordar que esos controles al ser parte de una aplicación todavía inexistente (y que queda fuera del alcance de este trabajo) no lo tenemos ahora en la realización de las pruebas (aunque en la mayoría de los casos sí que lo encontramos como código comentado en los scripts de procedimientos). Por ejemplo, ya se ha comentado que solo se podrán borrar sesiones de formación que aún no se hayan realizado, pues bien, si ahora intentásemos borrar una sesión ya realizada el sistema no lo estaría controlando ya que está diseñado para que sea la futura aplicación la que filtre al usuario qué sesiones son las que puede, o no, eliminar.

Con esto quiero decir que las pruebas que se van a llevar a cabo tienen esto en cuenta y no se hace ninguna “trampa para pillar” al sistema en este control. Dicho esto, procedemos a la fase de pruebas comenzando por detallar el plan de pruebas.

### 2.4.1. Plan de pruebas

Las fases que se van a seguir para las pruebas serán las siguientes: (Cuando no se especifica lo contrario se entiende que los datos que se introducen son “correctos”, es decir, la respuesta del sistema debería de ser, “OK” o mensaje similar)

1. Insertar 5 departamentos con Responsable = NULL
2. Insertar 7 empleados (Asignarles Provincia y Población)
3. Insertar 1 empleado con DNI ya introducido en el sistema → Error
4. Modificar 4 departamentos asignándoles un Responsable
5. Comprobar situación; Valor de los campos:
  - T\_EMPLEADO: Provincia, Población
  - T\_DEPARTAMENTO.CantEmpleados
6. Insertar 3 sesiones de formación
7. Insertar 3 Simulaciones
8. Insertar 3 Auditoria
9. Insertar las Vulnerabilidades (2) detectadas por la Consultora externa de inicio
10. Insertar las Vulnerabilidades (3) detectadas por la propia empresa.
11. Comprobar situación; Valores tablas (Modificadas por medio de disparadores tras inserción de Vulnerabilidades):
  - T\_C4
  - T\_C10
  - T\_C12
12. Se asignan acciones de mitigación a cada una de las diferentes vulnerabilidades.
13. Revisión de las tablas:

- T\_C5
  - T\_C13
14. Se modifican, activan y aprueban las políticas de seguridad 1, 2 y 3.
  15. Se modifica la Auditoría con Identificador = 2 (Modificación de campos: Fecha, TipoProcesoEmpresa, Observaciones)
  16. Modificación de los estados de las acciones de mitigación (y por tanto, modificación de los Estados de las Vulnerabilidades que correspondan por parte del sistema)
  17. Se intenta modificar el estado de una acción de mitigación ya acabada
  18. Modificación del estado de la vulnerabilidad 3 a: “No mitigada” y Descripción: “La mitigación queda aplazada
  19. Revisión de las tablas tras modificaciones en T\_ACCIONMITIGACION
  20. Modificación de datos del Empleado 1
  21. Modificación de datos de Simulación 1
  22. Se crean 4 procesos de gestión de la empresa.
  23. Modificación de proceso de gestión
  24. Se intenta crear un proceso de gestión con un nombre ya existente
  25. Se asignan las sesiones de formación a los empleados.
  26. El empleado 1 ha acabado la sesión de formación 1

#### **2.4.2. Elaboración del Juego de Pruebas**

El juego de pruebas que se ejecuta para la elaboración de pruebas de este proyecto queda especificado en el script: “JuegoDePruebas.txt” que se adjunta con este documento.

#### **2.4.3. Realización de las Pruebas y Resultado**

Junto con este documento de memoria principal adjunto el Anexo II donde se puede encontrar las capturas de pantalla de las salidas que da el sistema

### **2.5. Mejoras**

Una vez el producto se da por finalizado toca hacer autoevaluación del propio trabajo de cada uno y valorar de forma crítica el resultado obtenido. Si este fuera un trabajo real a implementar en cliente ya se le hubiera explicado a este que, de primeras, se le iba a implantar el módulo básico para ir haciéndose con el sistema y, una vez esto controlado se realizaría una segunda fase de implementación en la que no solo se incluirían las mejoras demandadas por el cliente tras su primera toma de contacto sino además las posibles mejoras que han ido surgiendo a lo largo de las fases de creación consensuadas con el cliente.

En este caso, se detallan a continuación, algunas de las mejoras que estarían pendientes de evaluar con el cliente para valorar, o no, su implementación en el sistema:

- El sistema podría dar a elegir al usuario si, al modificar los campos Descripción y/o Observaciones se borra la anterior o se escribe a continuación. También se podría valorar la opción de que el usuario eligiese en el momento cómo debe actuar el sistema mediante un check a marcar, o no, durante su ejecución.
- Envío de mail: Hay varios momentos en el sistema en los que se podría plantear al cliente la opción de que dicho sistema enviara un mail a la persona acordada sobre diferentes estados de la BD, por ejemplo: Cuando un empleado que es responsable en varias situaciones y es desactivado, este campo “Responsable” se quedaría a NULL. Por lo que el sistema enviaría un mail a esta persona seleccionada para recordarle la nueva situación de esta tabla.
- En las tablas encargadas del repositorio estadístico no siempre se almacena el nombre de la entidad a la que se refiere, por ejemplo, en T\_C1\_SUMA se almacena el identificador del departamento, pero no el nombre de este.
- Algunas tablas como la T\_C2 y la T\_C6, se podrían mejorar permitiendo que se pudiera filtrar por año, de la misma manera que T\_C8 podría guardar la información de cada año.
- Otro de los aspectos a mejorar del sistema actual es la continuidad de las secuencias en caso de error en el proceso. Esto es, actualmente los identificadores los asigna el sistema por medio de secuencias, en caso de producirse un error, dicha secuencia reconoce que ya ha asignado ese número (que en realidad no) y a la siguiente inserción asignará un número más, por lo que se queda un salto de numeración que puede resultar molesto y/o confuso para el cliente. En vista a unas mejoras del sistema se debería de analizar de qué manera programar el sistema para responder ante estos casos.
- Los procesos de actualización del repositorio estadístico actualmente se hacen desde disparadores; esto con un aumento de procesos a actualizar podría provocar una sobrecarga en el SGBD. Para evitar esto lo que se podría hacer llegado el caso, sería realizar las llamadas del Rep. Estadístico desde los procedimientos de A/B/M
- En el repositorio estadístico hay ciertas consultas, como por ejemplo C1, C6... que , al valorar los casos de comparaciones no contempla la opción de que dos registros puedan tener la misma cantidad y no uno más que el otro. Si se da el caso de que dos registros tienen la misma cantidad implica que no se puede dar respuesta a “¿cuál de los dos tiene un mayor número de...?” Teniendo en cuenta que esto fuera un hipotético caso real estaríamos ante un caso de tener que hablar con el cliente y decidir qué hacer en estos casos para optimizar la respuesta del sistema lo máximo posible.

- Actualmente el sistema registra una política de seguridad por cada vulnerabilidad, estaría bien establecer una reunión con el cliente por consensuar si resulta más interesante el crear una política de seguridad por cada acción de mitigación o, simplemente permitir que se puedan crear varias políticas de seguridad por vulnerabilidad (ahora mismo no se permite ya que el empleado no tiene acceso al procedimiento de creación de políticas de seguridad)
- Para la siguiente fase de implementación se debería de preparar un disparador que en las modificaciones de T\_Poblacion y T\_Provincia actualice todos los campos en lo que aparecen o hacen referencia los actualice.
- Es importante decir que, actualmente, el sistema no cuenta ni con detalle de usuarios ni con vistas. Estos sería un aspecto importante a tener en cuenta para la siguiente fase de implantación.
- De la misma forma, para la siguiente fase también se debería de considerar la creación de índices con los que no cuenta ahora
- Actualmente el sistema no permite que los usuarios cambien de forma manual el departamento de un empleado. Quedaría en manos del cliente decidir si quiere que esto continúe así o que el sistema permita a los usuarios establecidos esta modificación

### 3. CONCLUSIONES

De este trabajo me llevo varias conclusiones; por un lado, algo que ya tenía muy claro: en estos temas cuando se trabaja PARA un cliente, se trabaja CON el cliente. Con esto a lo que me refiero es que cuando estás diseñando, en este caso, una BD para un cliente hay decisiones que no puedes (debes) tomar por ti misma. Es cierto que teníamos un amplio enunciado con las explicaciones, pero, aun así, como desarrollador tienes que tomar unas decisiones a sabiendas que quien podría tomar las decisiones más acertadas es el cliente o, al menos, el cliente junto con el desarrollador.

Por otro lado, me llama muchísimo la atención las modificaciones que sufre el diseño de la base de datos durante todo su proceso de creación. Prácticamente todas las decisiones que se tomaban pasaban por realizar algún cambio en el diseño y realmente me parece maravilloso ya que eso te hace ver que el proyecto está “vivo” y se está adaptando a los requerimientos del cliente en cada momento.

Para responder sobre el logro de los objetivos planteados tengo varios matices... por un lado, he diseñado e implementado una BD que almacena la información que pide el enunciado, con unos procesos para llevar a cabo su mantenimiento y la resolución de prácticamente todas las consultas que se piden para el repositorio estadístico (así, dicho todo de forma muy sintetizada), por lo tanto si se me preguntan si esto cumple con los objetivos iniciales diría que sí, a más o menos nivel, pero lo cumple. En cambio, si me pregunto a mí misma si he cumplido los objetivos puede ser que la respuesta sea diferente... Obviamente no me puedo decir que el sistema no funcione, pero la verdad es que me hubiera gustado tratar con más detalle muchos de los puntos de trabajo o haber llegado a mucho más de lo que he hecho... ¿Podría haber acabado de hacer todas las consultas? Sí. ¿Podría haber hecho un plan de pruebas más exhaustivo? También. Es más, esa era la idea que llevaba, pero al final entre todas las decisiones que se tienen que ir tomando también están las de decidir cuándo parar en un punto para poder llegar a todos los demás y, aunque me “moleste” entregar algo a un nivel que no es el que me gustaría también debo ser sincera y reconocerme a mí misma que si esto no se ha conseguido no ha sido ni por falta de ganas ni por falta de trabajo. Ser docente en activo, mamá en solitario de una bebé de 21 meses y estudiante del grado después de más de 10 años fuera del mundo de la informática, ha supuesto un esfuerzo extra y muchas (demasiadas) horas sin dormir y viéndolo desde esta perspectiva creo que mis objetivos, sobre todo los personales, pueden considerarse más que cubiertos.

Lo dicho, una respuesta con muchos matices que no intentan ser una justificación de nada, sino una valoración de la realidad que da respuesta a por qué no se ha conseguido llegar a todo si la idea era presentar un muy buen trabajo.

Es posible que sobre la metodología y planificación lo tenga algo más claro. Si bien es cierto que la planificación ha sufrido modificaciones considero que todas han sido positivas de cara a la consecución del trabajo. Por un lado, un error mío en la comprensión del enunciado me hizo perder toda una semana de trabajo y por otro creo que fui demasiado optimista en la asignación de horas. Al final, ambas

se solucionan de la misma forma, sacar horas de donde no las hay y dedicarlas al proyecto, aunque no estén planificadas dentro de su plan de trabajo.

Como he dicho anteriormente, hay varios aspectos del sistema que se me han quedado “en el tintero”. Por un lado, tendríamos los aspectos funcionales de la base de datos que se han tratado como segunda fase de implementación teniendo en cuenta que esto fuera un caso “real”. Por otro lado, entrar al detalle en la fase de pruebas sería algo que se podría cubrir realizando estas pruebas con el cliente de forma que aprovecharíamos esto para introducir al cliente en el funcionamiento del sistema y además valorar si se está en la línea de lo que este esperaba.

Así pues, para finalizar con esto, solo me queda decir que, aunque esto no es un proyecto real, los imprevistos, los malentendidos y las horas de esfuerzo y trabajo también forman parte de nuestro día a día en el mundo laboral, pero teniendo una buena base de planificación y organización no se puede permitir que “las horas malas” puedan a las buenas ya que es en estas, en las buenas, en las que vas a conseguir que tu proyecto salga, o no, adelante.

## 4. GLOSARIO

- **ATRIBUTO**→ Los nombres que identifican propiedades, cualidades, identificadores o características de entidades o de relaciones.
- **BASE DE DATOS (BD)**→ Conjunto de datos almacenado en memoria externa organizados mediante una estructura de datos.  
BD, abreviatura de Base de Datos
- **CAMPO**→ Propiedad que posee una tabla. Equivalente al atributo
- **CIBERATAQUE**→Conjunto de acciones dirigidas contra sistemas de información con el objetivo de perjudicar a personas, Instituciones o empresas
- **CLAVE PRIMARIA (PRIMARY KEY)**→Clave candidata que se escoge para identificar sus tuplas de modo único.
- **CLAVE AJENA (FOREIGN KEY)**→ Atributo o un conjunto de atributos de una relación cuyos valores coinciden con los valores de la clave primaria de alguna otra relación (puede ser la misma)
- **DISPARADOR (Trigger)**→Programa que se asocia a una tabla y se ejecuta cuando, en esta, se produce un evento determinado.
- **DISEÑO CONCEPTUAL**→Parte de las especificaciones de requisitos de los usuarios y su resultado es el esquema conceptual de la BD
- **DISEÑO LÓGICO**→Proceso de construir un esquema de la información que utiliza la empresa, basándose en un modelo de base de datos específico e independiente del SGBD concreto que se vaya a utilizar, así como de cualquier otra consideración física.
- **DISEÑO FÍSICO**→ Proceso de producir la descripción de la implementación de la BD en memoria secundaria, a partir del esquema lógico.
- **ENTIDAD**→Representación de un concepto del mundo real
- **FAKE (NEWS)**→ Falso. FAKE NEWS: Noticias falsas.
- **IMPLEMENTAR**→Poner en funcionamiento métodos o medidas para llevar algo a cabo.
- **SCRIPT**→ Documento que contiene instrucciones, escritas en Código de programación



- **SGBD**→Abreviatura de Sistema de Gestión de Base de Datos. Aplicación que permite a los usuarios definir, crear y mantener la base de datos además de proporcionar un acceso controlado a la misma.
- **PL/SQL**→(*Procedural Language/Strctured Query Lenguaje*)Es un lenguaje de procedimiento diseñado específicamente para abarcar sentencias SQL dentro de su sintaxis.
- **SQL**→Siglas que corresponden a *Structured Query Lenguaje*. Lenguaje estándar que permite manejar los datos de una BD relacional.
- **RANSOMWARE**→Un tipo de malware que impide a los usuarios acceder a su sistema o a sus archivos personales y que exige el pago de un rescate para poder acceder de nuevo a ellos.
- **TABLA**→ Estructura similar a la relación del diseño lógico
- **TUPLA**→Cada una de las filas de una relación lógica o tabla

## 5. BIBLIOGRAFÍA

### 5.1. Libros

- Date, C.J., Introducción a los sistemas de bases de datos (7a ed.). Prentice-Hall. (2001)
- Beynon-Davies, P. Sistemas de bases de datos. Editorial Reverté. (2018).
- Mercedes Marqués, Bases de Datos, Universitat Jaume I, 1ª Edición Col·lecció Sapientia, 18, Castellón, 2011
- Millán, M. E. Fundamentos de bases de datos. Cali, Colombia, Programa Editorial Universidad del Valle. (2012)

### 5.2. Webs

- 25 marzo 2022
  - <https://www.tutorialesprogramacionya.com/oracleya/temarios/descripcion.php?cod=193>
  - <https://magicplsql.blogspot.com/2016/08/las-variables-de-plsql.html>
- 2 abril, 2022
  - <https://www.youtube.com/watch?v=8YMUIJIxZZQ>
  - <https://docs.microsoft.com/es-es/sql/relational-databases/sequence-numbers/sequence-numbers?view=sql-server-ver15>
  - <https://elbauldelprogramador.com/plsql-procedimientos-y-funciones/>
  - <https://www.desarrollo-web-br-bd.com/es/sql/como-pasar-el-parametro-de-fecha-dentro-del-procedimiento-de-oracle/1056539817/>
  - <https://www.firebirdsql.org/manual/es/nullguide-es-comprobacion.html>
- 15 abril 2022
  - <http://www.editorialox.com/provinciasdeespana.htm>
  - <https://www.dataprix.com/es/forum/oracle-database/concatenar-cadenas-oracle>
- 3 mayo 2022
  - <https://datos.gob.es/es/blog/que-es-un-diccionario-de-datos-y-por-que-es-importante>
  - <https://www.magicplsql.com/pl-sql/itemlist/tag/IF%20ELSE%20THEN>
  - <https://ayudaleyprotecciondatos.es/bases-de-datos/trigger/>
  - <http://profesionghh.blogspot.com/2015/01/triggers-o-disparadores-de-base-de-datos.html>
  - <https://www.tutorialesprogramacionya.com/oracleya/temarios/descripcion.php?cod=261&punto=1&inicio=>
  - <https://elbauldelprogramador.com/plsql-disparadores-o-triggers/>
  - <https://es.stackoverflow.com/questions/306092/comparar-una-fecha-string-con-sysdate-o-current-date>
  - <https://www.tutorialesprogramacionya.com/oracleya/temarios/descripcion.php?cod=167&punto=1&inicio=>

- 16 mayo 2022
  - <https://www.tutorialesprogramacionya.com/oracleya/temarios/descripcion.php?cod=255&punto=1&inicio=>
  - <https://codigolite.com/crear-ejecutar-y-eliminar-una-funcion-en-oracle/>
  - <https://www.oracle.com/es/tools/technologies/howto-sql-worksheet-basic-syntax.html>
  
- 18 mayo 2022
  - <https://elbauldelprogramador.com/plsql-declaracion-de-variables/>
  - <https://www.discoduroderoer.es/pedir-datos-al-usuario-en-pl-sql/>
  
- 19 mayo 2022
  - <https://docs.oracle.com/database/121/DWHSG/concept.htm#DWHSG-GUID-452FBA23-6976-4590-AA41-1369647AD14D>
  - <https://docs.oracle.com/en/database/oracle/oracle-database/19/lnpls/static-sql.html#GUID-25917214-FD91-499D-AB39-CE21484AB167>
  - <https://elbauldelprogramador.com/plsql-cursores/>
  - <https://docs.oracle.com/en/database/oracle/oracle-database/19/lnpls/static-sql.html#GUID-BCCE0985-AB78-48B8-A453-F44FCC4DA595>
  
- 20 mayo 2022
  - <https://www.optical.pe/blog/tipos-de-ataques-informaticos-y-previsiones-para-el-2022/>
  - <https://www.ibm.com/resources/guides/cyber-resilient-organization-study/>
  - [https://www.redseguridad.com/actualidad/informes-ciberseguridad/que-ciberamenazas-seran-tendencia-en-2022\\_20211103.html](https://www.redseguridad.com/actualidad/informes-ciberseguridad/que-ciberamenazas-seran-tendencia-en-2022_20211103.html)
  - <https://www.infobae.com/america/peru/2021/12/08/cuales-son-las-predicciones-de-ciberseguridad-global-para-el-2022/>
  
- 25 mayo 2022
  - <https://elbauldelprogramador.com/plsql-excepciones/>
  - <https://www.lawebdelprogramador.com/foros/Oracle/693959-Saber-si-retorna-o-no-valor-el-select.html>
  - <https://www.tutorialesprogramacionya.com/oracleya/temarios/descripcion.php?cod=269&punto=1&inicio=>
  - <https://www.tutorialesprogramacionya.com/oracleya/temarios/descripcion.php?cod=181&punto=1&inicio=>

## 6. ANEXOS

A continuación, se incluye un listado de los anexos a la entrega final de la memoria y una breve explicación de su contenido:

- Anexo1: Documento que contiene el Modelo Lógico en mayor tamaño que en el documento para facilitar su visualización
- Anexo2: Ejecución del plan de pruebas con capturas de pantalla de los resultados obtenidos

NOTA: No se incluyen los archivos que son parte de la propia entrega del trabajo.

