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

Juan José Fernández Hernández

Grado de Ingeniería Informática

Base de Datos

Jordi Ferrer Duran

Xavier Baró Solé

Junio 2022

FICHA DEL TRABAJO FINAL

Título del trabajo:	*Diseño e implementación de la base de datos para una aplicación de control de procesos de seguridad informática*
Nombre del autor:	*Juan José Fernández Hernández*
Nombre del consultor/a:	*Jordi Ferrer Duran*
Nombre del PRA:	*Xavier Baró Solé*
Fecha de entrega (mm/aaaa):	06/2022
Titulación:	*Grado de Ingeniería Informática*
Área del Trabajo Final:	*Base de Datos*
Idioma del trabajo:	*Castellano*
Palabras clave	*Seguridad informática, vulnerabilidad abierta, ciberseguridad.*

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

El objetivo de este trabajo tiene como objetivo el diseño de una BD e implementación de esta para una aplicación de control de procesos de seguridad informática aplicada sobre una empresa automovilística.

Gestionar todos estos procesos hoy en día mediante procesos informáticos permite controlar las vulnerabilidades de la empresa englobados como es bien sabido dentro los procesos de ciberseguridad.

Nuestra BD analizará mediante una metodología en cascada, la implementación de los procedimientos necesarios y finales de la gestión y análisis de los datos almacenados en la misma. Se describirá con detalle los procedimientos de ABM e implementará (Alta + Baja + Modificación) de todas las clases creadas como relevantes. Se podrán ir incorporando de forma escalable y progresivamente todas aquellas necesidades relacionadas con la ciberseguridad de la empresa.

Finalmente se habrá conseguido los objetivos, en otras cosas, gracias a la buena fase de los requisitos, diseño y buena valoración de los datos estadísticos de los procedimientos aplicados en la ciberseguridad de la empresa.

Abstract (in English, 250 words or less):

The objective of this work is the design of a DB and its implementation for a computer security process control application applied to an automobile company.

Managing all these processes today through computer processes allows control of the company's vulnerabilities, encompassed as is well known within cybersecurity processes.

Our database will analyze, through a cascade methodology, the implementation of the necessary and final procedures, for the management and analysis of the data stored in it. ABM procedures will be described in detail and will implement (Add + Drop + Modification) of all the classes created as relevant. All those needs related to the company's cybersecurity can be incorporated in a scalable and progressive way.

Finally, the objectives will have been achieved, in other things, thanks to the good phase of the requirements, design and good evaluation of the statistical data of the procedures applied in the company's cybersecurity.

Índice

1. Introducción

1.1 Contexto y justificación del trabajo

Los datos estadísticos sobre ataques cibernéticos en el mundo revelan que el pasado año **2020**, fue uno de los más desafiantes de la historia; tanto a nivel individual como para la sociedad y para las empresas. Ante una pandemia mundial, la inestabilidad geopolítica mundial de los últimos años ha conllevado a trasladar estos problemas al mundo cibernético. Las amenazas en **2020** han batido todos los récords en cuanto a pérdida de datos y ciberataques en todo el mundo. Las estadísticas sobre ciberseguridad del año **2020** y anteriores indican que los ataques se han vuelto más sofisticados aumentando así el uso de nuevas tecnologías como el aprendizaje automático o la inteligencia artificial aplicada a ciberataques programados sobre empresas poco preparadas para ello.

Este proyecto nace como respuesta a la necesidad creada y planteada por una gran empresa del sector automovilístico, la cual necesita implantar un sistema de ciberseguridad.

Las reiteradas pérdidas de información y la excesiva vulnerabilidad a los ataques informáticos de la empresa le han conllevado a plantear una mejora en su plan de defensa contra el fraude informático y el robo de información.

La implantación de estos nuevos sistemas de ciberseguridad ha obligado a la creación, diseño e implantación de una Base de Datos **(BD)** que permita controlar de manera rápida y eficaz la situación de la empresa en términos de seguridad informática en cada momento.

Esta **BD** pretende analizar y monitorizar todas y cada una de las acciones que estan en curso durante el uso del sistema informático; asi como mitigar y evitar cualquier vulnerabilidad abierta que produciría una brecha de seguridad. Dicha **BD** también puede analizar y definir qué acciones son necesarias para evitar un ciberataque y una vez identificadas permitir su registro para posteriores usos.

Este proyecto tiene también la finalidad de controlar todas las restricciones de confidencialidad necesarias para la implantación de este sistema y para ello se desarrollará el registro del número total de incumplimientos de seguridad informática en todos y cada uno de los departamentos de la empresa.

Otro aspecto importante de este proyecto es llevar a cabo el registro y control de todas las sesiones de formación, tanto presenciales como telemáticas, que se realicen en todos los departamentos, para asi concienciar a sus propios empleados de la vulnerabilidad que existe a través de sus cuentas de correo personales, mediante técnicas de **"phishing"** [1].

Por último, este proyecto deberá hacer frente a la gestión y control de las diferentes auditorías de seguridad que se establezcan dentro de la empresa. Las futuras auditorias deberán permitir controlar todos los procesos de seguridad mediante políticas definidas y aprobadas por la misma.

1.2 Objetivos del Trabajo

Como primer objetivo se pretende crear y diseñar un **BD** para dar forma a las pretensiones de la empresa en la ciberseguridad. El diseño será escalable, relacional e integrable con otras **BD** que permitan dar información más global y datos estadísticos, con el fin de dar respuesta a los ataques informáticos como a posibles fallos de seguridad en el futuro.

El segundo objetivo de la **BD** estará relacionado con la expansión estructural de la misma, para que permita dar respuesta a cualquier caso de ataque cibernético que pueda tener la empresa; aportando así la información necesaria a tiempo real para que los indicadores requeridos sean los más fiables en cuanto a los datos con que se trabajan en las auditorias ya que deben de estar basados en datos reales y estudios fehacientes.

La **BD** deberá contar con los procedimientos almacenados para dar gestión y acceso a la información necesaria referente a los ataques cibernéticos.

[1] "phishing" Estafa que tiene como objetivo obtener a través de Internet datos privados de los usuarios, especialmente para acceder a cuentas bancarias y datos personales

1.3 Enfoque y método seguido

La estrategia por seguir en esta base de datos es que cuide la calidad de los **datos**, tenga los objetivos claros, segmente a sus clientes e incorpore los modelos predictos.

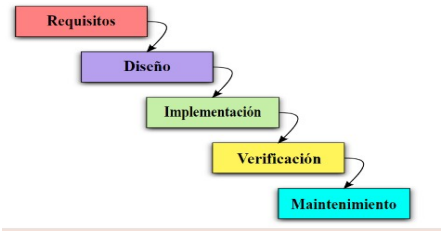
El diseño por crear en esta **BD** es un diseño basado en el modelo cascada, (también llamado secuencial o ciclo de vida de un programa).

Este enfoque metodológico requiere rigurosamente unas etapas en el proceso de diseño del software de tal forma que el inicio de cada etapa requiere esperar a la finalización de la etapa anterior.

Haciendo un poco de referencia histórica sobre este modelo de diseño, podemos referenciar a **Winston W. Royce que en 1970**[2] hizo una propuesta de este diseño como un método de aplicación de Base de Datos, que posteriormente sería revisado **Barry Boehm en 1980**[3].

deEste diseño sigue un patrón concreto cuya metodología se basa en unos términos generales los cuales son:

- Análisis de requisitos.
- Diseño del cuerpo de la **BD**.
- Diseño de la programación de la **BD**.
- Codificación de la **BD**.
- Pruebas **BD**.
- Mantenimiento de la **BD**



Fuente: https://es.wikipedia.org/wiki/Desarrollo_en_cascada

Por tanto, las etapas de este proyecto deben seguir esta metodología en cascada como queda definido en la planificación del proyecto.

- **Requisitos de la BD.** En esta etapa del proyecto se definirá todos los requisitos necesarios para crear la funcionalidad necesaria que va a necesitar el proyecto. Se analizan los requisitos que se piden en el enunciado del **TFG** y que previamente se ha proporcionado por la **UOC**.

[2]Winston W. Royce fué computólogo estadunidense director en el Centro de Tecnología de Software Lockheed en Austin, Texas. Pionero de la Ingeniería de software y conocido por su papel en el modelo de cascada en 1970.

[3] Barry Boehm es un ingeniero informático estadunidense y es profesor emérito de esta materia en el departamento de ciencias tecnológicas en la Universidad del Sur de California. Actualmente trabaja en la AIAA, en ACM, en IEEE y es miembro de la academia nacional de ingeniería.

- **Análisis y Diseño.** Después de analizar los requisitos necesarios y sugeridos por la **UOC**, se diseña lo que será el proyecto final y donde se definirá la estructura de este.

- **Implementación.** En esta etapa comenzaremos con la implementación de la **BD**. Ejecutaremos los scripts de la **BD** creados para la ejecución los requisitos requeridos por la **UOC**, necesarios para la realización del **TFG** y que deberán cumplir los procedimientos de gestión y acceso a la misma.

- **Pruebas.** Esta etapa nos permitirá conseguir y realizar resultados de éxito sobre nuestro proyecto, necesarios para conseguir la verificación de los requisitos requeridos en el **TFG**, mediante pruebas rutinarias que nos lleven a conseguir el objetivo.

- **Mantenimiento.** Normalmente en los proyectos reales se suele considerar esta etapa como una etapa más de cualquier proyecto diseñado con una metodología en cascada. En nuestro caso no se planifica ya que el proyecto final termina con la entrega final, memoria y presentación virtual del mismo.

1.4 Planificación del Trabajo

La planificación del trabajo es muy orientativa. Los hitos nos van a permitir hacer pequeñas entregas de la planificación de nuestro trabajo lo que supone una dedicación diaria y una entrega constante de esfuerzo.

El esfuerzo y la dedicación que he dedicado diariamente es de **2 horas** por día, así como **4 días** semanalmente, lo supone una dedicación semanal de **8 horas** totales.

He mantenido un margen de dedicación que utilizaré a posibles contingencias por retrasos debidos por cualquier circunstancia.

1.4.1 Tareas e hitos del trabajo

La planificación se ha dividido en dos partes o bloques importantes:

- Las tareas o entregas programadas en el proyecto obligatorias, que serán acompañadas de la documentación requerida con un tiempo previo a cada entrega:

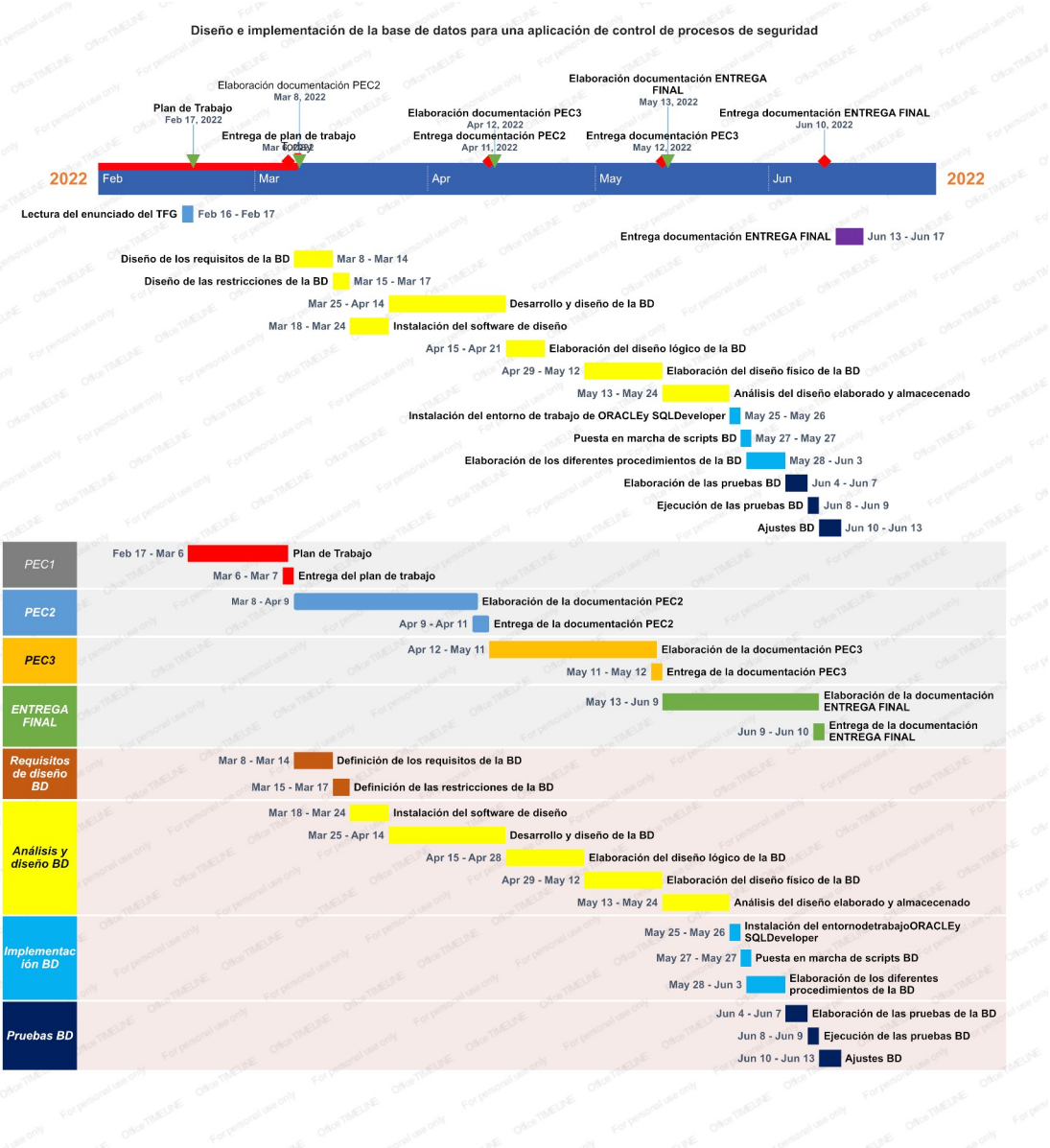
Nombre de la tarea	Tiempo duración	Comienzo tarea	Fin tarea
PEC1	**24 horas**	**Jue 07/02/22**	**Lun 07/03/22**
Plan de trabajo.	23 horas	Jue 17/02/22	Dom 06/03/22
Entrega Plan de trabajo.	1 hora	Dom 06/03/22	Lun 07/03/22
PEC2	**40 horas**	**Mar 08/03/22**	**Lun 11/04/22**
Elaboración de la documentación.	39 horas	Mar 08/03/22	Sáb 09/04/22
Entrega de la documentación.	4 horas	Sáb 09/04/22	Lun 11/04/22
PEC3	**40 horas**	**Mar 12/04/22**	**Mar 12/05/22**
Elaboración de la documentación.	39 horas	Mar 12/04/22	Lun 11/05/22
Entrega de la documentación.	4 horas	Lun 11/05/22	Mar 12/05/22
Entrega final	**40 horas**	**Mie 13/05/22**	**Jue 10/06/22**
Elaboración de la documentación.	39 horas	Mie 13/05/22	Lun 09/05/22
Entrega de la documentación.	4 horas	Lun 09/05/22	Mar 10/06/22
Presentación virtual TFG.	**5 días**	**Lun 13/06/22**	**Vie 17/06/22**

- El segundo bloque se dedica a las tareas y subtareas de la BD que se corresponden con su diseño, implementación y elaboración en su conjunto aparte de documentar el proyecto:

Nombre de la tarea	Tiempo duración	Comienzo tarea	Fin tarea
Requisitos BD	**12 horas**	**Mar 08/03/22**	**Jue 17/03/22**
Definición requisitos.	**10 horas**	**Mar 08/03/22**	**Lun 14/03/22**
Definición restricciones.	**2 horas**	**Mar 15/03/22**	**Jue 17/03/22**
Análisis y Diseño	**43 horas**	**Vie 18/03/22**	**Mar 24/05/22**
Instalación del diseño del software.	**2 horas**	**Vie 18/03/22**	**Jue 24/03/22**
Desarrollo y diseño.	**15 horas**	**Vie 25/03/22**	**Jue 14/04/22**
Elaboración del diseño lógico.	**7 horas**	**Vie 15/04/22**	**Jue 28/04/22**
Elaboración del diseño físico.	**9 horas**	**Vie 29/04/22**	**Jue 12/05/22**
Análisis del diseño elaborado y almacenado.	**10 horas**	**Vie 13/05/22**	**Mar 24/05/22**
Implementación	**20 horas**	**Mie 25/05/22**	**Vie 03/06/22**
Instalación del entorno PostgreSQL14.	**4 horas**	**Sáb 25/05/22**	**Dom 26/05/22**
Puesta en marcha de scripts.	**2 horas**	**Lun 27/05/22**	**Lun 27/05/22**
Elaboración de los diferentes procedimientos de la BD.	**14 horas**	**Mar 28/05/22**	**Vie 03/06/22**
Pruebas	**12 horas**	**Sáb 04/06/22**	**Lun 13/06/22**
Elaboración de las pruebas.	6 horas	Sáb 04/06/22	Mar 07/06/22
Ejecución de las pruebas.	2 horas	Mie 08/06/22	Jue 09/06/22
Ajustes de la BD.	4 horas	Vie 10/06/22	Lun 13/06/22

Las entregas del proyecto se tienen que corresponder tal y como dice el enunciado del **TFG** de la **UOC**, ya que concretamente para las entregas de la **PEC2** y **PEC3** serán básicamente verificaciones del producto final requerido alineado a la planificación de esta en cada plazo.

1.4.2 Diagrama de Gantt



1.4.3 Seguimiento periódico de la planificación del proyecto

- **PEC1:** Se elabora el plan de trabajo de todo el proyecto, así como toda su planificación. He tenido en cuenta el plan de contingencia y toda la valoración de la planificación del proyecto por fechas incluyendo horas. También he tenido que solicitar un poco más de tiempo (por circunstancias familiares) para poder finalizar esta parte del proyecto, que el tutor me concede dándonos un poco más de tiempo para su realización.

- **PEC2:** En esta etapa del proyecto realizo un seguimiento periódico de la planificación del proyecto. Realizo un diseño y una elaboración exhaustiva de los scripts necesarios para llevar a cabo el desarrollo de la **BD** necesarios en los requisitos planteados en el **TFG**. También finalizo el trabajo teniendo que solicitar al más de tiempo, tiempo que se me concede por parte del tutor.

  Elaboro el proyecto de acuerdo con la programación del proyecto en concreto al **Diagrama de Gantt** [4] que he diseñado.

- **PEC3:** En esta tarea del proyecto seguimos realizando un seguimiento periódico de la planificación del proyecto, vamos dando por finalizados muchos de los scripts empezados de la **BD** y comenzamos con los ajustes finales del proyecto. Queda poco para la entrega final por lo que tenemos que finalizar y terminar todos los ajustes finales para la prueba final de la **BD**.

  Llevo también acabo todas aquellas observaciones y recomendaciones que se me han transmitido por parte del tutor. Se elabora y finaliza esta parte del proyecto de acuerdo con el **Diagrama de Gantt** [4] que se ha diseñado.

1.5 Breve sumario de productos obtenidos

El objetivo de este proyecto nos lleva a enumerar un sumario de los productos obtenidos durante la duración de este:

- El desarrollo del script de la **BD** con sus diferentes esquemas, como motor de **BD PostgreSQL14**[5] y que deberá cubrir las necesidades que establecen los requisitos del enunciado del **TFG**.

[4] Diagrama de Gantt es una herramienta grafica cuyo objetivo es exponer el tiempo de dedicación previsto para diferentes tareas o actividades

- Memoria del trabajo del **TFG**, que se elaborará durante su tiempo de duración, incluirá todo el proyecto con sus detalles técnicos de diseño, de análisis, así como de construcción de este.

- Presentación en PowerPoint de todo el **TFG** que incluirá la elaboración y el funcionamiento de la **BD**. Nos permitirá dar una información global del proyecto de forma clara y concisa ya que incluirá datos importantes del mismo.

- El producto final de la **BD** recopilará todos los scripts de funcionamiento de este, nos permitirá realizar el plan de pruebas del proyecto y así como todas las pruebas finales de funcionamiento.

- Realizar todas aquellas consultas necesarias para poder conseguir todos los requisitos requeridos en el enunciado del proyecto.

.

1.6 Breve descripción de los otros capítulos de la memoria

Los siguientes capítulos forman parte del **TFG** que como bien se relacionan en el índice detallo una breve descripción de este a continuación:

- **Requisitos de la BD**

  Capítulo que recoge todos las directrices y necesidades para la recopilación de todos datos que son necesarios para la realización de las normas establecidas en el enunciado facilitado por la **UOC** para el **TFG** de **BD**.

  Se establecen los requisitos necesarios y básicamente las normas de evaluación de estas que servirán como base de nuestro proyecto.

Se establece también la planificación del **TFG**, el plan de contingencia y las condiciones de valoración de cada uno de los requisitos, que servirán como puntos a desarrollar a lo largo del proyecto, en etapas posteriores.

- **Análisis y Diseño BD**

  En este capítulo haremos un análisis de los requisitos necesarios en el **TFG**. Valoraremos los requisitos más importantes y de mayor importancia para su posterior desarrollo y diseño lógico, como físico. Desarrollaremos un diseño dentro de los requisitos requeridos por el **TFG** para almacenarlo después de analizarlo y diseñarlo. El diseño físico y lógico se elaborará a través de la instalación del entorno **PostgreSQL14**[5].

- **Implementación BD**

  Este capítulo desarrollará todos los scripts necesarios para el diseño y desarrollo dentro del entorno **PostgreSQL14**[5] de nuestra base de datos. Este entorno permitirá el acceso y el proceso de todos los procedimientos elaborados para su gestión.

- **Pruebas BD**

  Capítulo que establece todas y cada una de las pruebas contenidas en el plan de valoración de todos los datos de la **BD**. Permitirá dar por valido el **TFG**, diseñado dentro de los requisitos valorados en el proyecto.

[5]PostgreSQL14 es un sistema de gestión de bases de datos relacional orientado a objetos y de código abierto introduce la posibilidad de canalizar consultas hacia una base de datos, lo cual hace mejorar significativamente el rendimiento en las conexiones de alta latencia o para cargas de trabajo con un gran número de pequeñas operaciones de escritura (INSERT/ UPDATE/ DELETE).

1.7 Plan de Contingencia

El proyecto está expuesto a posibles riesgos durante toda la ejecución de este. Se establecen en el mismo las medidas para mitigarlos, asi como forma de analizar su impacto y las formas previstas de solucionarlos.

Riesgo	Impacto del riesgo	Medidas a desarrollar
Conjunto de problemas que surgen durante el tiempo de diseño, elaboración del TFG. Trabajo, enfermedades, etc.	Retraso en las entregas, en la dedicación diaria al **TFG**.	Se preestablece un tiempo dedicado para mitigar este tipo de riesgos o contingencias. Resto horas semanales que no se utilizan como dedicación al desarrollo del **TFG**. Se coordinará siempre este tipo de contingencia con el profesor de este.
Problemas de software y de hardware del equipo informático que utilizamos para la elaboración del proyecto.	Problemas de retraso en la entrega del **TFG**, perdida de datos del proyecto y del entorno del **TFG**.	Utilizar la información y los datos en más de un equipo informático. Hacer varias copias de seguridad de las misma. Hacer uso de los servicios de la nube como **Google Drive**, donde podremos guardar

		copias del proyecto por duplicado.
Realizar un diseño equivocado y un análisis diferente a los requisitos iniciales del enunciado del TFG.	Retrasos en las entregas del **TFG**, rediseñar y replantear de nuevo el proyecto y su entorno.	Tener un guión claro en el momento de realizar el diseño del proyecto. Realizar un diagrama **UML** exacto y sin errores para poder desempeñar un buen diseño.

2. Resto de capítulos

2.1 Gestión de los requisitos

En este punto vamos a extraer del enunciado todos los requisitos necesarios que debe de cumplir el diseño de la **BD**, como también aquellos que se intuyan y pudierán ser interesantes en futuras revisiones del modelo. No se contemplarán las funcionalidades de las aplicaciones que finalmente pudiera utilizar la **BD**.

Se dispondrá del enunciado el cual explica lo que pretende almacenar la **BD** y lo que se solicita. Se exponen también las funcionalidades que dispondrán las aplicaciones que pueden hacer uso de esta **BD**.

2.1.1 Requisitos Funcionales

Código	Requisito
RQF-001	Se desea definir un conjunto de indicadores a monitorizar que permitan saber en cada momento la situación y cuáles son las acciones que están en curso para mitigar cualquier posible vulnerabilidad abierta.
RQF-002	Se desea implantar una **BD** para controlar todos los procesos de seguridad informática de una empresa del sector automovilístico.
RQF-003	Se registrarán en la **BD** todos los incumplimientos teniendo en cuenta todas las restricciones de confidencialidad que todas las acciones

	requieren. Para ello se deberán registrar el número total de incumplimientos por política en cada departamento de la empresa. La **BD** deberá tener un control y un registro exhaustivo de todas las sesiones de formación, tanto presenciales como telemáticas que se realicen en la empresa en temas referentes con la seguridad. Se deberán registrar sesiones formativas y los usuarios que participen en ellas.
RQF-004	Se deberá permitir la gestión de las diferentes auditorias definidas por la empresa. La auditoría estará ligada a las diferentes políticas definidas y aprobadas por la empresa. Serán realizadas por equipos externos e internos según se valoré en cada momento. Se guardarán los registros de los muestreos hechos durante la auditoria.
RQF-005	Se deberá permitir el control de los diferentes aspectos detallados a continuación: Ejecución de consultas necesarias para la correcta gestión y análisis de los datos almacenados en la **BD**. Visualización rápida del estado de los indicadores principales de monitorización del estado de seguridad de la empresa que se definan en cada momento.
RQF-006	Se deberá permitir guardar información: De todas las vulnerabilidades que se detecten. De las acciones de mitigación que se realicen. De las políticas de seguridad definidas. De las auditorias que se realicen.
RQF-007	Se deberá almacenar cada vulnerabilidad detectada en la **BD** en los siguientes estados: • Identificada. • No mitigada. • Parcialmente mitigada.

	• Totalmente mitigada. • También se deberán clasificar en: • Críticas. • No críticas.
RQF-008	Se deberán almacenar las acciones de mitigación según el estado en el que se encuentren: • Definida. • En proceso. • Acabada. • En revisión.
RQF-009	Se deberá poder almacenar cualquier volumen de datos, así como la gestión que se haga siguiendo las técnicas que se aplican a los mismos. **(Data Waterhouse)**. Se deberá poder consultar estadísticas de estos volúmenes de datos.
RQF-010	Se creará un repositorio estadístico que contenga los siguientes indicadores: • Departamentos de la empresa que, en un año, tienen el mayor número de incumplimientos de seguridad registrados en la **BD**. • Top5 de usuarios según el número de incumplimientos de seguridad asociados por departamentos, durante el año en curso. • Proceso de gestión interno, teniendo en cuenta toda la información de la **BD** que ha tenido un mayor nombre de vulnerabilidades detectadas. • Porcentaje de vulnerabilidades mitigadas en el momento de hacer la consulta. • Número total de acciones mitigadas que están acabadas en el momento de hacer la consulta. • Política de seguridad de la empresa teniendo en cuenta todos los departamentos, que en el momento de efectuar la consulta ha tenido más incumplimientos. • Porcentaje de usuarios de un departamento de la empresa que no han terminado todas las formaciones de seguridad asignadas.

	• Porcentaje de usuarios de la empresa que, en un año, no tienen ningún incumplimiento asignado. • Auditorías externas realizadas en el año, en el que se han detectado más incumplimientos. • Porcentaje de vulnerabilidades críticas que en el momento de ejecutar la consulta tienen alguna acción de mitigación abierta. • Sesiones de formación telemática que han tenido un porcentaje menor de participantes en total. • Número de vulnerabilidades críticas detectadas internamente teniendo en cuenta todos los datos de que se dispone en la **BD**. • Porcentaje de acciones de mitigación en el sistema que están en los estados de "**en proceso**" o "**en revisión**", en el momento de ejecutar la consulta. • Todas las acciones de mitigación en estado de "**en proceso**", de las personas de la empresa con más acciones asignadas. • Cada uno de estos indicadores se calculará y se almacenará mediante procedimientos automatizados dentro de la propia **BD**.
RQF-011	Se creará un log con todas las acciones realizadas con la **BD**. Se almacenarán todas las llamadas a los procedimientos ejecutados y los parámetros de entrada y salida.

2.1.2 Requisitos No Funcionales o Restricciones

	Requisito
RQNF-001	La Base de Datos deberá tener un diseño escalable.
RQNF-002	La Base de Datos tendrá un motor basado en **PostgreSQL14**.
RQNF-003	Toda la gestión y acceso a la información se hará mediante procedimientos de **BD**, siendo esta la única manera de acceder. Se implementarán procedimientos de **ABM (Alta+Baja+ Modificación)** de todas las clases relevantes.

	Se implementará un repositorio estadístico, registro de los logs y cualquier otro que se consideré necesario para el buen funcionamiento del sistema.
RQNF-004	Los procedimientos que se almacenen en la **BD** deberán cumplir: • Dispondrán como mínimo de un parámetro de salida llamado **RSP**, de tipo Sting, que indicará si la ejecución ha finalizado correctamente valor "**OK**" o si ha fracasado valor "**ERROR + TIPO DE ERROR**". • Dispondrán de tratamiento de excepciones.
RQNF-005	Todos los indicadores descritos y definidos en los requisitos funcionales (**RQF-010**) deberán poder ofrecer resultados en un tiempo constante **1**.
RQNF-006	El diseño deberá permitir guardar la información de las vulnerabilidades que se vayan detectando, de todas las políticas de seguridad definidas de los incumplimientos que se detecten, de las sesiones formativas realizadas y de las auditorias que se realicen.

2.2 Análisis y diseño

Para el análisis y diseño de la **BD**, procedemos al desarrollo conceptual de la misma mediante desarrollando su concepto a través de un *Diagrama UML* y *Diagrama ER*.

Una vez, lo tengamos procederemos a**l desarrollo lógico** de la misma para terminar con el **desarrollo físico e implementación**.

2.2.1 Modelo Conceptual

Diagrama UML

Para realizar el diseño de la **BD**, primero se realizará el modelo conceptual de la misma utilizando el diagrama **UML** o **E/R**, incluyendo todas las restricciones de integridad que se consideren relevantes, asi como todas las clases, atributos y relaciones de estas dentro de la **BD**.

El diagrama permitirá tener un concepto de la **BD** bastante amplio en sentido descendente combinando todos los requisitos funcionales de la misma, describiendo el contenido de información de esta y no las estructuras de almacenamiento que se necesitarán para manejar esta información.

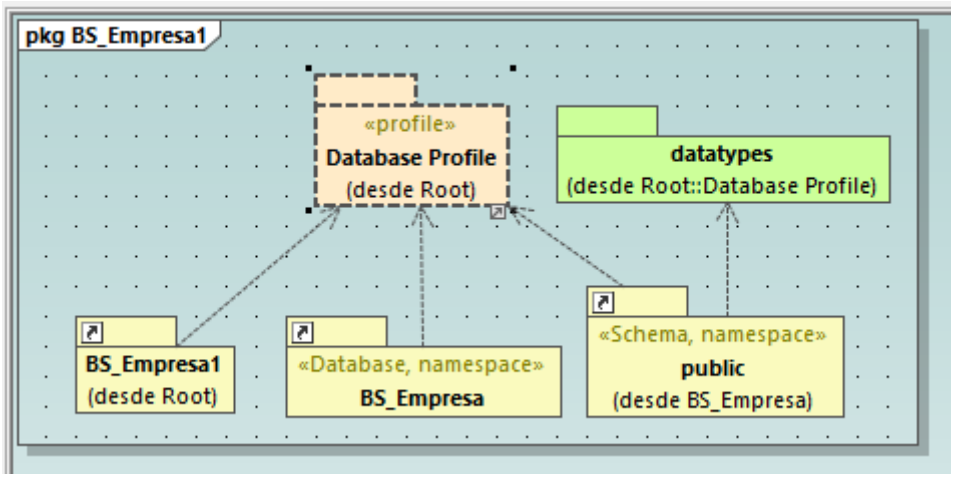
Para dar una explicación general del diseño conceptual de esta **BD** se ha preferido utilizar una visión parcial de cada una de las partes que la componen, para luego unirlas y relacionarlas entre sí. A continuación, se ofrece una visión del esquema final que servirá para dar un concepto global del diseño, que servirá como punto de partida y de referencia para la explicación de cada una de las partes.

Para distinguir cada una de estas partes más fácilmente, se relaciona cada una de las tablas explicatorias de la **BD** en función del paquete asignado.

La ***BD_Empresa*** está compuesta de varios paquetes importantes debido a la capacidad de datos con los que trabaja, en concreto el paquete ***public*** contiene todos las tablas más relevantes del proyecto dividas en estos bloques importantes:

- Login de perfiles.
- Gestión de Usuarios.
- Gestión de Incidencias.
- Gestión Equipos respuesta.
- Análisis de los procedimientos de seguridad.
- Auditoría externa.
- Log de procesos.

Principalmente la **BD** se compone de unos paquetes principales, principalmente ***public*** que es donde se encuentra las principales ***tables*** de la **BD**.



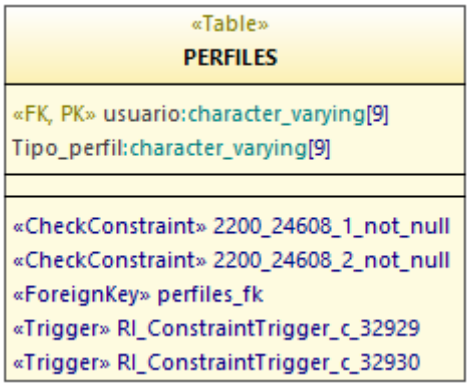
Paquete **public**

propietario	**BS_Empresa**
propiedades	nombre completo BS_Empresa::BS_Empresa::public

	nivel de acceso	Public
	«Database»	False
	«namespace»	True
	«Schema»	True
miembroPropio	AUDITORIA DATOS_AUDITADOSENTIDAD_AUDITORIAESQUEMA_NACIONAL_SEGURIDAD FunctionsGESTION_RESPUESTAINCIDENTESINCIDENTES_CRITICAL LOG_PROCESOSNOTIFICACIONESPERFILESSEVERITYSTATUS1STATUS2StoredProceduresUSUARIOSWORK_AREA	

LOGIN DE PERFILES

El Login de perfiles permitirá el acceso a la **BD**. La consultora externa a la empresa especializada en procedimientos de seguridad informática y el personal perteneciente a los recursos internos de la empresa podrán acceder a la **BD** a través del ***LOGIN DE PERFILES***. A través de este acceso se podrá acceder a las diferentes funcionalidades de la **BD** que permitirán el continuo trabajo de control de los diferentes procesos de seguridad cibernética llevados a cabo en la empresa.



Perfiles		
Atributo	***Tipo***	***Descripción***
Usuario	character_varing	Identificador de los usuarios que a través del Log de perfiles se podrán logar en la **BD**, pertenecientes a la consultora externa o a los propios usuarios de la empresa.
Tipo_perfil	character_varing	Identificador que permitirá distinguir al usuario al cual pertenece la persona que se loga en la **BD** de la empresa automovilística. Diferenciará a los

		usuarios si pertenecen a la estructura de la Consultora externa de la empresa o a la propia empresa.

Entidad 1 <Relación > Entidad 2	***Descripción***	***Cardinalidad*** **E1 : E2**
Perfil es *usuario*	Un perfil puede ser un usuario de la **BD** o no.	**1: 1...***
Perfil tiene *Tipo_perfil*	El Tipo_perfil tiene varios usuarios que corresponde a un perfil.	***: 1**

Tipo_Perfil		
Atributo	***Tipo***	***Descripción***
Id	Integer	Identificador del tipo de perfil. Va a poder identificar el tipo de perfil que se va a poder logar en la base de datos.
Tipo_perfil	character_varing	Identificador que permitirá distinguir al usuario al cual pertenece la persona que se loga en la **BD** de la empresa automovilística. Se va a diferenciar a los usuarios en Administradores, Consultores u Auditores.

Entidad 1 <Relación > Entidad 2	***Descripción***	***Cardinalidad*** **E1: E2**
Tipo_Perfil es *usuario*	Un perfil puede ser un usuario de la **BD** o no.	**1: 1... ***
Tipo_Perfil tiene *Perfiles*	El Tipo_perfil tiene varios perfiles de usuario que corresponde a un perfil.	***: 1**

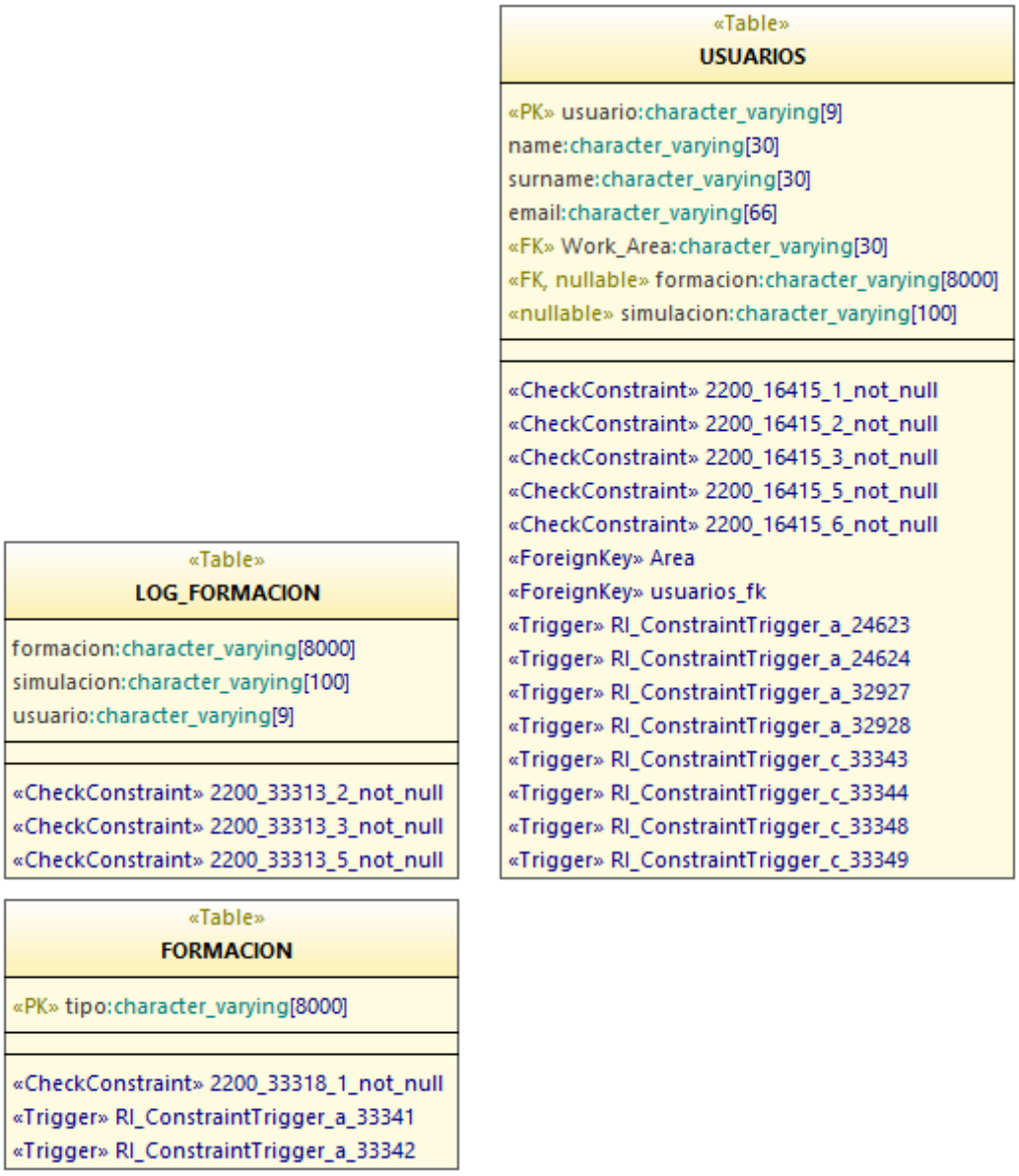
GESTION DE USUARIOS

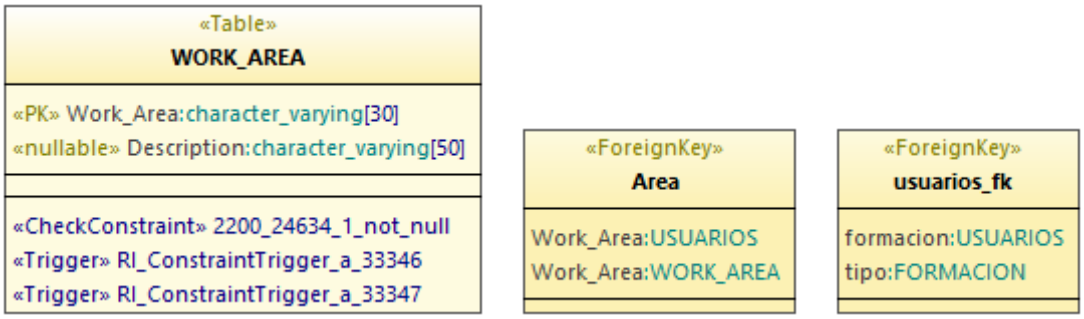
La **BD** permitirá controlar los diferentes procesos de seguridad informática aplicados sobre el personal de la empresa. Gestionará los datos principales del usuario que los cometa, así como el control de la formación de todo el personal de la misma vía presencial o telemática.

Permitirá verificar todos los protocolos de seguridad de la empresa, controlando todas las simulaciones de ataques cibernéticos.

A modo de estadística esta gestión intenta conocer que riesgos son más vulnerables en los usuarios y evitar que se produzcan. Por último, se guardará en un ***"Log_Formación"*** todos los registros realizados a los usuarios con respecto a la formación (telemática y presencial) y toda aquella otra formación a modo de

estadística para poder identificar la preparación de la empresa frente a los ataques y vulnerabilidades cibernéticas.





Usuarios		
Atributo	***Tipo***	***Descripción***
Usuario	character_varing	Identificador de los usuarios que a través del **Log** de perfiles se podrán logar en la **BD**, pertenecientes a los propios usuarios de la empresa.
Name	character_varing	Nombre de los usuarios.
surname	character_varing	Apellidos de los usuarios.
Email	character_varing	Cuenta de correo de los usuarios.
Work_Area	character_varing	Lugar de trabajo de los usuarios.
Formación	character_varing	Formación de los usuarios que podrá ser telemática o presencial con respecto a las vulnerabilidades de la empresa.
Simulación	character_varing	Simulaciones de ataques controlas para saber si los usuarios siguen las directrices definidas por la empresa en el tema de vulnerabilidades informáticas.

Entidad 1 <Relación > Entidad 2	***Descripción***	***Cardinalidad*** **E1: E2**
usuarios tiene *Work_Area*	El usuario tiene un área de trabajo concreta.	***: 1**
usuarios tiene *formación*	El usuario tiene una formación concreta.	***: 1**

Work_Area		
Atributo	***Tipo***	***Descripción***
Work_Area	character_varing	Identificador del área de trabajo de los usuarios que a través del Log de perfiles se podrán logar en la **BD**, pertenecientes a los propios usuarios de la empresa.

Description	character_varing	Identificador y descripción del lugar de trabajo de los usuarios donde trabajan dentro de la empresa.

Log_Formación

Atributo	***Tipo***	***Descripción***
usuario	character_varing	Identificador del usuario único y secuencial del registro del Log.
formación	character_varing	Identificador de la formación única y secuencial del registro del Log.
simulación	character_varing	Identificador de la simulación única y secuencial del registro del Log.

Formación

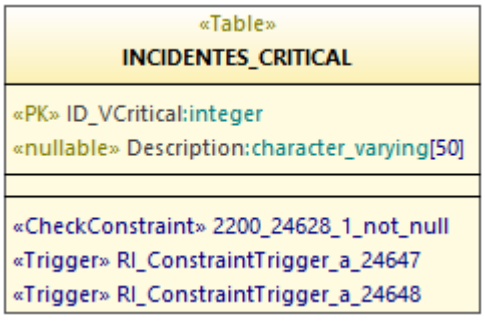
Atributo	***Tipo***	***Descripción***
Tipo	character_varing	Identificador del tipo de formación que recibirá cada usuario interno de la empresa. (Telemática o presencial). Será un identificador de control frente a las vulnerabilidades informáticas de la empresa.

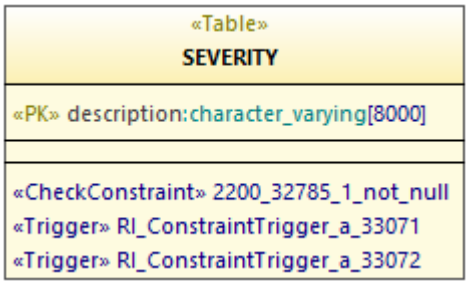
GESTIÓN DE INCIDENCIAS

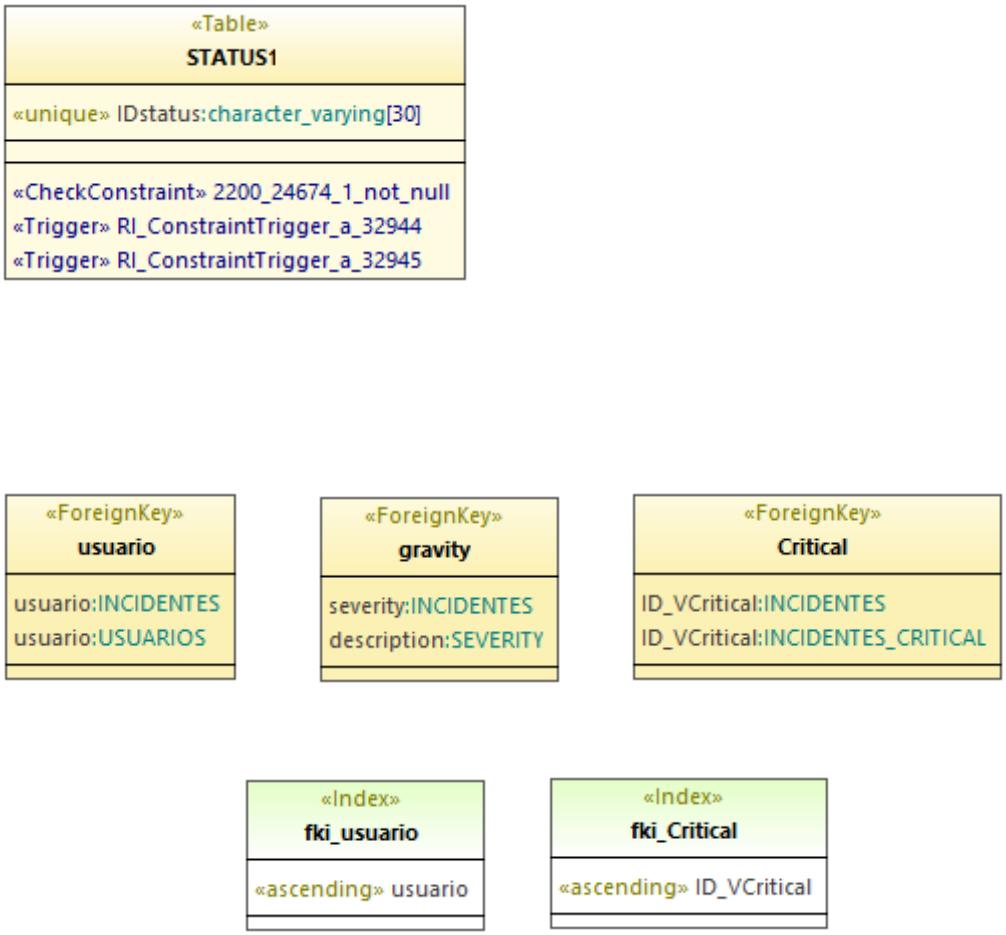
Este paquete gestionará el Alta, Baja y modificación de cualquier incidencia referente a las vulnerabilidades que surjan en la empresa automovilística.

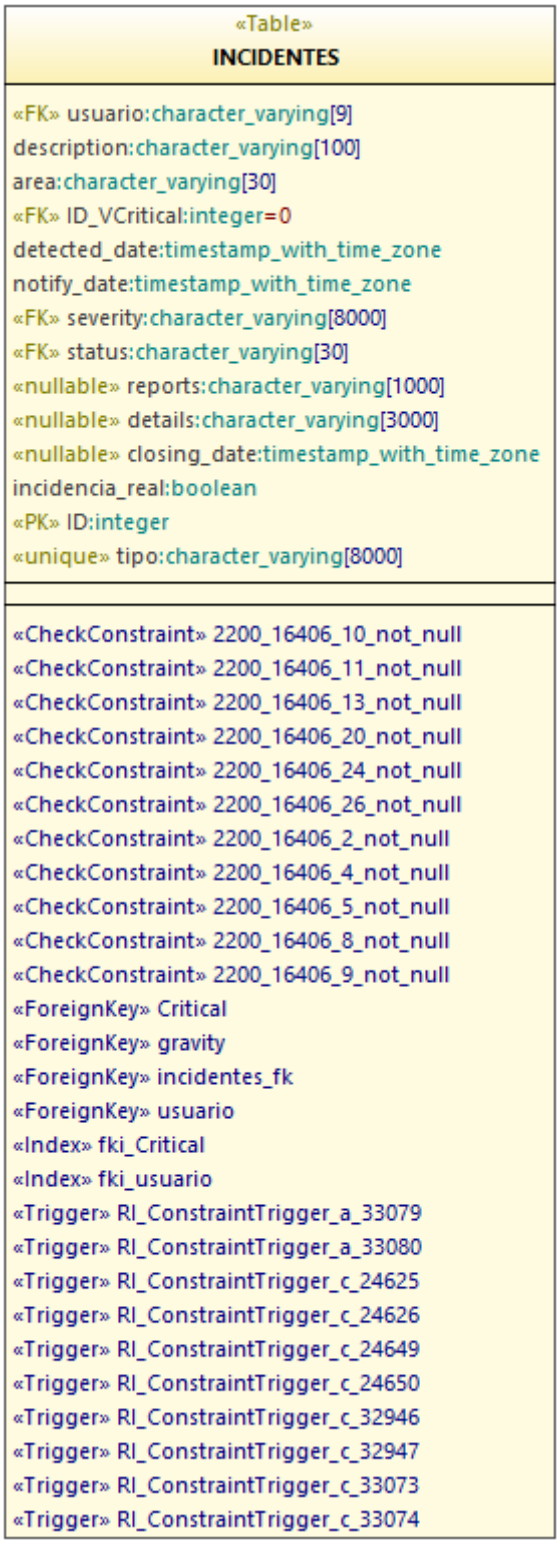
Dará la capacidad necesaria a la empresa para analizar y detectar las vulnerabilidades que se produzcan. Dará gestión mediante el registro de todas aquellas incidencias que se produzcan en la empresa, así como sus consultas.

Permitirá controlar y analizar las políticas de seguridad que se cumplen dentro de la empresa. Dichas políticas son de obligado cumplimiento por todos los departamentos de la empresa, así como todas las personas que la componen.






«Table»
STATUS1
«unique» IDstatus:character_varying[30]
«CheckConstraint» 2200_24674_1_not_null
«Trigger» RI_ConstraintTrigger_a_32944
«Trigger» RI_ConstraintTrigger_a_32945
«ForeignKey»
usuario
usuario:INCIDENTES
usuario:USUARIOS
«ForeignKey»
gravity
severity:INCIDENTES
description:SEVERITY
«ForeignKey»
Critical
ID_VCritical:INCIDENTES
ID_VCritical:INCIDENTES_CRITICAL
«Index»
fki_usuario
«ascending» usuario
«Index»
fki_Critical
«ascending» ID_VCritical


«Table»
INCIDENTES
«FK» usuario:character_varying[9]
description:character_varying[100]
area:character_varying[30]
«FK» ID_VCritical:integer=0
detected_date:timestamp_with_time_zone
notify_date:timestamp_with_time_zone
«FK» severity:character_varying[8000]
«FK» status:character_varying[30]
«nullable» reports:character_varying[1000]
«nullable» details:character_varying[3000]
«nullable» closing_date:timestamp_with_time_zone
incidencia_real:boolean
«PK» ID:integer
«unique» tipo:character_varying[8000]
«CheckConstraint» 2200_16406_10_not_null
«CheckConstraint» 2200_16406_11_not_null
«CheckConstraint» 2200_16406_13_not_null
«CheckConstraint» 2200_16406_20_not_null
«CheckConstraint» 2200_16406_24_not_null
«CheckConstraint» 2200_16406_26_not_null
«CheckConstraint» 2200_16406_2_not_null
«CheckConstraint» 2200_16406_4_not_null
«CheckConstraint» 2200_16406_5_not_null
«CheckConstraint» 2200_16406_8_not_null
«CheckConstraint» 2200_16406_9_not_null
«ForeignKey» Critical
«ForeignKey» gravity
«ForeignKey» incidentes_fk
«ForeignKey» usuario
«Index» fki_Critical
«Index» fki_usuario
«Trigger» RI_ConstraintTrigger_a_33079
«Trigger» RI_ConstraintTrigger_a_33080
«Trigger» RI_ConstraintTrigger_c_24625
«Trigger» RI_ConstraintTrigger_c_24626
«Trigger» RI_ConstraintTrigger_c_24649
«Trigger» RI_ConstraintTrigger_c_24650
«Trigger» RI_ConstraintTrigger_c_32946
«Trigger» RI_ConstraintTrigger_c_32947
«Trigger» RI_ConstraintTrigger_c_33073
«Trigger» RI_ConstraintTrigger_c_33074

Incidentes		
Atributo	***Tipo***	***Descripción***
ID	integer	Identificador único y secuencial del usuario de la BD
Usuario	character_varing	Identificador de los usuarios que han cometido la vulnerabilidad de seguridad informática.
Proceso	character_varing	Descripción del incidente de la vulnerabilidad producida en la empresa automovilística.
Área	character_varing	Área de trabajo de la empresa donde se ha producido y lugar donde se encuentra trabajando el usuario.
ID_VCritical	integer	Identificador de si la vulnerabilidad producida es crítica o no.
detected_date	timestamps_with_time_zone	Fecha y hora del día que se ha detectado la vulnerabilidad de seguridad informática en la empresa.
notify_date	timestamps_with_time_zone	Fecha y hora del día que se ha notificado la vulnerabilidad de seguridad informática a los sistemas de control de la empresa.
Severity	character_varing	Identificador que permite clasificar la vulnerabilidad en **MUY GRAVE**, **GRAVE**, **MEDIO**, **BAJA**, **MUY BAJA**.
Status	character_varing	Identificador que permite clasificar la incidencia de seguridad en acciones **IDENTIFICADAS**, **NO MITIGADAS**, **PARCIALMENTE MITIGADAS**, **TOTALMENTE MITIGADAS**.
Reports	character_varing	Identificador de todos los datos necesarios para el estudio y análisis de la vulnerabilidad producida.
Details	character_varing	Identificador de todos los detalles necesarios para que el estudio y análisis sea correctamente realizado por los servicios de control de la empresa.
closing_date	timestamps_with_time_zone	Fecha y hora que se da por terminada la incidencia de vulnerabilidad informática.
incidencia_real	boolean	Identificador que permite identificar si la incidencia es real o no lo es si en el estudio se evalúa que no cumple con las políticas definidas y aprobadas por la empresa.
Tipo	character_varing	Identificador del tipo de incidencia producida, que permita identificar claramente el tipo de vulnerabilidad informática producida que se encuentre dentro de los incumplimientos de seguridad definidos por la empresa automovilística.

Entidad 1 <Relación > Entidad 2	***Descripción***	***Cardinalidad*** **E1 : E2**
Incidentes tiene *usuarios*	Identificador del usuario que ha cometido el incidente. Varios incidentes pueden ser cometidos por el mismo usuario o relacionados con un mismo usuario.	***: 1**
Incidentes tiene *severity*	El incidente se podrá clasificar dependiendo de la gravedad de la vulnerabilidad en: **MUY GRAVE**, **GRAVE**, **MEDIO**, **BAJA**, **MUY BAJA**.	***: 1**
Incidentes tiene *status*	El incidente se podrá clasificar dependiendo del estado de las acciones tomadas con respecto a la vulnerabilidad en: **IDENTIFICADAS**, **NO MITIGADAS**, **PARCIALMENTE MITIGADAS**, **TOTALMENTE MITIGADAS.**	***: 1**
Incidentes tiene *ID_VCritical*	El incidente también se podrá clasificar: • Críticos • No críticos	***: 1**

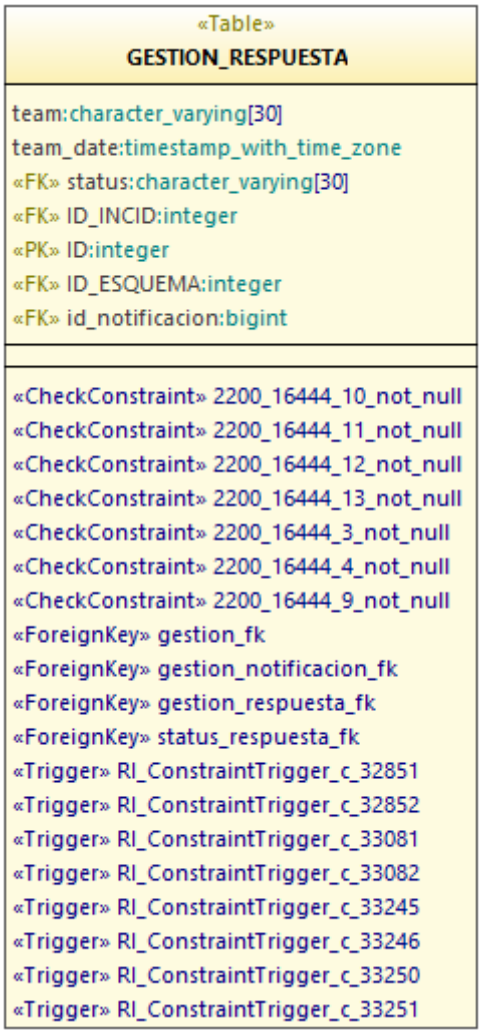
Severity		
Atributo	***Tipo***	***Descripción***
Description	character_varing	Identificador que permite clasificar la vulnerabilidad en **MUY GRAVE**, **GRAVE**, **MEDIO**, **BAJA**, **MUY BAJA**.
Status1		
Atributo	***Tipo***	***Descripción***
ID_Status	character_varing	Identificador que permite clasificar la incidencia de seguridad en acciones **IDENTIFICADAS**, **NO MITIGADAS**, **PARCIALMENTE MITIGADAS**, **TOTALMENTE MITIGADAS**.

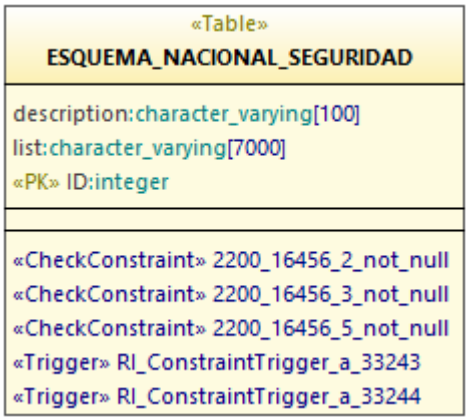
GESTIÓN DE EQUIPOS DE RESPUESTA

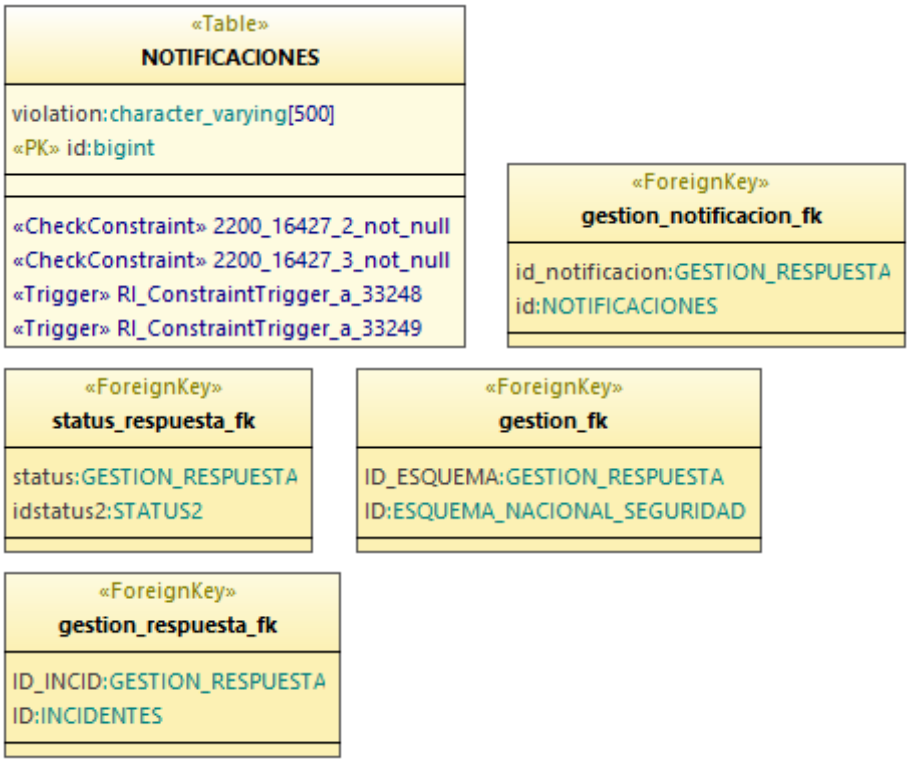
Este paquete de la **BD** gestiona el conjunto de las posibles soluciones a las diferentes vulnerabilidades informáticas de la empresa.

Todos los ataques producidos en la empresa serán analizados y gestionados por equipos especializados en procesos de seguridad informática.

Estas políticas de seguridad serán aprobadas por el departamento de **RRHH** de la empresa. Evaluarán mediante el reporte estadístico de la **BD** que protocolos de seguridad informática se cumplen por departamentos en la empresa y así que ataque es más vulnerable en la empresa.







Gestión_respuesta		
Atributo	***Tipo***	***Descripción***
ID	Integer	Identificador único y secuencial del incidente de la **BD**.
ID_INCID	Integer	Identificador del incidente que han cometido la vulnerabilidad de seguridad informática mediante un código generado aleatoriamente por la **BD**.
ID_ESQUEMA	Integer	Identificador del tipo de incidente de la vulnerabilidad producida en la empresa automovilística.
Id_notficacion	Bigint	Identificador de la notificación de la violación de la vulnerabilidad haciendo referencia a las políticas de seguridad aprobadas por la empresa.
Status	character_varing	Identificador del incidente clasificado según el estado en el que se encuentra el incidente: **DEFINIDA**, **EN PROCESO**, **EN REVISIÓN** y **ACABADA**.
team	character_varing	Equipo interno de la empresa que actualizará la lista de intrusiones o equipo de la consultora externa que durante dos meses se encargará de realizar dicho análisis de las vulnerabilidades de la empresa.
team_date	timestamps_with_time_zone	Fecha y hora del día que se ha notificado la vulnerabilidad de seguridad informática por los equipos internos u externos de la empresa que se encargan del análisis y control de dichas vulnerabilidades.

Entidad 1 <Relación > Entidad 2	***Descripción***	***Cardinalidad*** **E1 : E2**
Gestión_ respuesta tiene ID_INCID	Identificador del número de incidente a una sola gestión respuesta.	***: 1**
Gestión_respuesta tiene *Id_notificación*	Identificador de la notificación que la incidencia genera en respuesta a que tipo de violación ha generado la vulnerabilidad ocurrida en el incidente.	**1: 1**
Gestión_respuesta tiene *status*	La gestión de la respuesta está clasificada en varios estados: **DEFINIDA**, **EN PROCESO**, **EN REVISIÓN** y **ACABADA**.	***: 1**
Gestión_respuesta tiene *ID_ESQUEMA*	La gestión de la respuesta estará relacionada con una única vulnerabilidad.	***: 1**

Status2		
Atributo	***Tipo***	***Descripción***
ID_Status2	character_varing	Identificador de la gestión respuesta que está clasificada en varios estados: **DEFINIDA**, **EN PROCESO**, **EN REVISIÓN** y **ACABADA**.

Esquema_nacional_seguridad		
Atributo	***Tipo***	***Descripción***
ID	integer	Identificador del tipo de vulnerabilidad creada por los equipos de análisis de la propia empresa u externos.
Description	character_varing	Identificador y descripción del tipo de vulnerabilidad generada en la incidencia.
list	character_varing	Vulnerabilidades detectadas por los equipos propios de la empresa o por los equipos externos de la misma.

Notificaciones		
Atributo	***Tipo***	***Descripción***
ID	bigint	Identificador de la notificación generada que identifica la vulnerabilidad detectada.
violation	character_varing	Indica que vulnerabilidad ha sido detectada haciendo referencia a la lista de vulnerabilidades encontradas en la empresa.

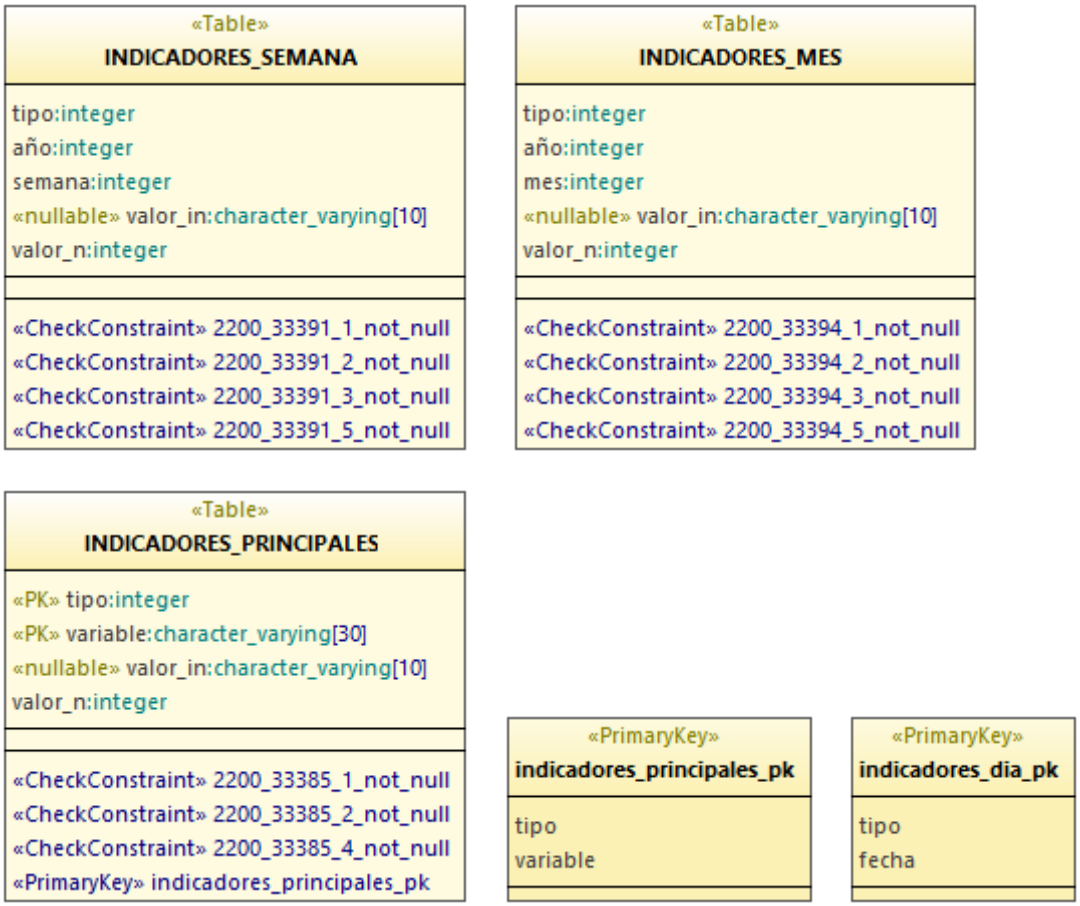
ANÁLISIS DE LOS PROCEDIMIENTOS DE SEGURIDAD (REPOSITORIO ESTADÍSTICO)

Las herramientas de análisis de que dispone la **BD** se podrán conocer a través de su repositorio estadístico o mediante consultas a la propia **BD** que luego serán analizadas e investigadas.

Este repositorio estadísticos ofrecerá diferentes resultados que se definirán en tiempo constante **1**, es decir que solo haciendo una **SELECT** sobre un registro de una tabla se podrá obtener información muy importante para el análisis de todas las vulnerabilidades que se produzcan en la empresa.

Este repositorio estadístico permitirá dar cumplimiento a los siguientes indicadores:

- Número de incumplimientos se producen dentro de la empresa en cada departamento, que número de usuarios comenten más incumplimientos y que número de ellos incumplen menos.
- Saber qué porcentaje de vulnerabilidades críticas tienen alguna acción de mitigación abierta y que no esté acabada.
- Número de porcentaje de vulnerabilidades críticas detectadas internamente teniendo en cuenta todos los datos de que se disponen.
- Proceso de gestión interno, que teniendo en cuenta toda la información de que se dispone en la **BD**, ha tenido mayor nombre de vulnerabilidades detectadas.
- Porcentaje de vulnerabilidades que en el momento de ejecutar la consulta están totalmente mitigadas.
- Porcentaje de usuarios de la empresa que no tienen incumplimiento asignado.
- Porcentaje de usuarios de un departamento que no han acabado la formación de la empresa.
- Porcentaje de la sesión formativa telemática que ha tenido menor número de participantes.
- Porcentaje de acciones de mitigación que están en estado de **“en proceso”** o **“en revisión”**.
- Y por último todas aquellas acciones mitigadas que están en **“en proceso”**, porcentaje de personas responsables con más acciones asignadas.



La estructura de los indicadores de todas las entidades será similar y todas incorporarán la siguiente estructura:

Indicadores		
Atributo	***Tipo***	***Descripción***
tipo	integer	Tipo que hace referencia a un indicador.
Valor_in	character_varing	Este atributo no tendría sentido para la entidad ***Indicadores principales***, por ejemplo, pero se mantiene para facilitar la inclusión de futuros nuevos indicadores que podrían necesitarlo.
Valor_n	integer	Este indicador guardará el valor del indicador que será una media, un porcentaje, un contador, etc.

El atributo ***tipo*** podrá tomar posibles valores y no se referirá a ninguna entidad. Este atributo será ***numérico***. En la siguiente tabla se especifica el valor numérico, en que entidad se guarda y una descripción de este.

Valor	***Entidad***	***Descripción***
1	***Indicadores_año***	Número de incumplimientos se producen dentro de la empresa en cada departamento, que número de usuarios comenten más incumplimientos y que número de ellos incumplen menos, en un año en concreto.
2	***Indicadores_principales***	Saber qué porcentaje de vulnerabilidades críticas tienen alguna acción de mitigación abierta y que no esté acabada.
3	***Indicadores_principales***	Número de porcentaje de vulnerabilidades críticas detectadas internamente teniendo en cuenta todos los datos de que se disponen.
4	***Indicadores_principales***	Proceso de gestión interno, que teniendo en cuenta toda la información de que se dispone en la **BD**, ha tenido mayor nombre de vulnerabilidades detectadas.
5	***Indicadores_principales***	Porcentaje de vulnerabilidades que en el momento de ejecutar la consulta están totalmente mitigadas.
6	***Indicadores_año***	Porcentaje de usuarios de la empresa que, en el año en curso, no tienen incumplimiento asignado.
7	***Indicadores_principales***	Política de seguridad que, en el momento de ejecutar la consulta, ha tenido más incumplimientos (teniendo en cuenta todos los departamentos de la empresa).
8	***Indicadores_principales***	Dado un determinado departamento de la empresa, y teniendo en cuenta el momento de ejecutar la consulta, porcentaje de usuarios del departamento que no han acabado todas las formaciones de seguridad asignadas.
9	***Indicadores_principales***	Porcentaje de acciones de mitigación que están en estado de **“en proceso”** o **“en revisión”.**
10	***Indicadores_principales***	Número total de acciones de mitigación que, en el momento de ejecutar la consulta, no están totalmente acabadas.
11	***Indicadores_año***	Teniendo en cuenta el último año (el anterior al año en curso), título de sesión formativa telemática que ha tenido un porcentaje menor de participantes en total.
12	***Indicadores_año***	Teniendo en cuenta todas las auditorías externas realizadas, año en el cual se han detectado más incumplimientos (teniendo en cuenta sólo los detectados durante la auditoría).
		Porcentaje de usuarios de la empresa que, en el

13	***Indicadores_mes***	mes en curso, no tienen ningún incumplimiento asignado.
14	***Indicadores_principales***	Teniendo en cuenta todas las acciones de mitigación en estado "en proceso", persona responsable con más acciones asignadas.
15	***Indicadores_principales***	Top5 de usuarios por número de incumplimientos asociados directamente a ellos, o a su departamento, durante el año en curso.
16	***Indicadores_día***	Número total de acciones mitigadas, en el momento de efectuar la consulta, están **"en proceso"**.

Indicadores_principales

Atributo	***Tipo***	***Descripción***
tipo	integer	Tipo que hace referencia al indicador.
Variable	character_varing	Este atributo hace referencia al valor del indicador. Los posibles valores de este atributo dependen del tipo al que correspondan. • Tipo1: usuarios, media. • Tipo2: auditorias. • Tipo3:max_incumplimientos, min_incumplimientos. • Tipo4: por acciones mitigadas. • Tipo5: por variación. • Tipo6: vulnerabilidades.
Valor_in	character_varing	Valor del tipo String del indicador. Se usará para almacenar el incumplimiento (tipo3) o las acciones mitigadas (tipo4) y vulnerabilidades (tipo6).
Valor_n	integer	Este indicador guardará el valor del indicador que será una media, un porcentaje, un contador, etc.

Indicadores_día (Esta entidad albergará todos los indicadores del repositorio estadístico que se guardarán por día (tipo7). Esta entidad almacenará una tupla por tipo de indicador y día).

Atributo	***Tipo***	***Descripción***
tipo	integer	Tipo que hace referencia al indicador.
Fecha	timestamp_with_time_zone	Fecha en la que se produce el indicador.
Valor_in	character_varing	Valor del tipo String del indicador. Se usará para almacenar el incumplimiento (tipo 3) o las acciones mitigadas (tipo4) y vulnerabilidades (tipo6) para cálculos por día.
Valor_n	integer	Este indicador guardará el valor del indicador que será una media, un porcentaje, un contador, etc.

Indicadores_semana (Esta entidad albergará todos los indicadores del repositorio estadístico que se guardarán por día (tipo8-10). Esta entidad almacenará una tupla por tipo de indicador y semana).

Atributo	***Tipo***	***Descripción***
tipo	integer	Tipo que hace referencia al indicador.
año	integer	Año que hace referencia la semana.
semana	integer	Semana en que se calcula el indicador.
Valor_in	character_varing	Valor del tipo String del indicador. Se usará para almacenar el incumplimiento (tipo 3) o las acciones mitigadas (tipo4) y vulnerabilidades (tipo6) para cálculos por semana.
Valor_n	integer	Este indicador guardará el valor del indicador que será una media, un porcentaje, un contador, etc.

Indicadores_mes (Esta entidad albergará todos los indicadores del repositorio estadístico que se guardarán por día (tipo11). Esta entidad almacenará una tupla por tipo de indicador y mes).

Atributo	***Tipo***	***Descripción***
tipo	integer	Tipo que hace referencia al indicador.
año	integer	Año que hace referencia al mes.
mes	integer	Mes en que se calcula el indicador.
Valor_in	character_varing	Valor del tipo String del indicador. Se usará para almacenar el incumplimiento (tipo 3) o las acciones mitigadas (tipo4) y vulnerabilidades (tipo6) para cálculos por mes.
Valor_n	integer	Este indicador guardará el valor del indicador que será una media, un porcentaje, un contador, etc.

Indicadores_año (Esta entidad albergará todos los indicadores del repositorio estadístico que se guardarán por día (tipo12). Esta entidad almacenará una tupla por tipo de indicador y año).

Atributo	***Tipo***	***Descripción***
tipo	integer	Tipo que hace referencia al indicador.
año	integer	Año que hace referencia al año actual.
año1	integer	Año en que se calcula el indicador.
Valor_in	character_varing	Valor del tipo String del indicador. Se usará para almacenar el incumplimiento (tipo 3) o las acciones mitigadas (tipo4) y vulnerabilidades (tipo6) para cálculos por año.
Valor_n	integer	Este indicador guardará el valor del indicador que será una media, un porcentaje, un contador, etc.

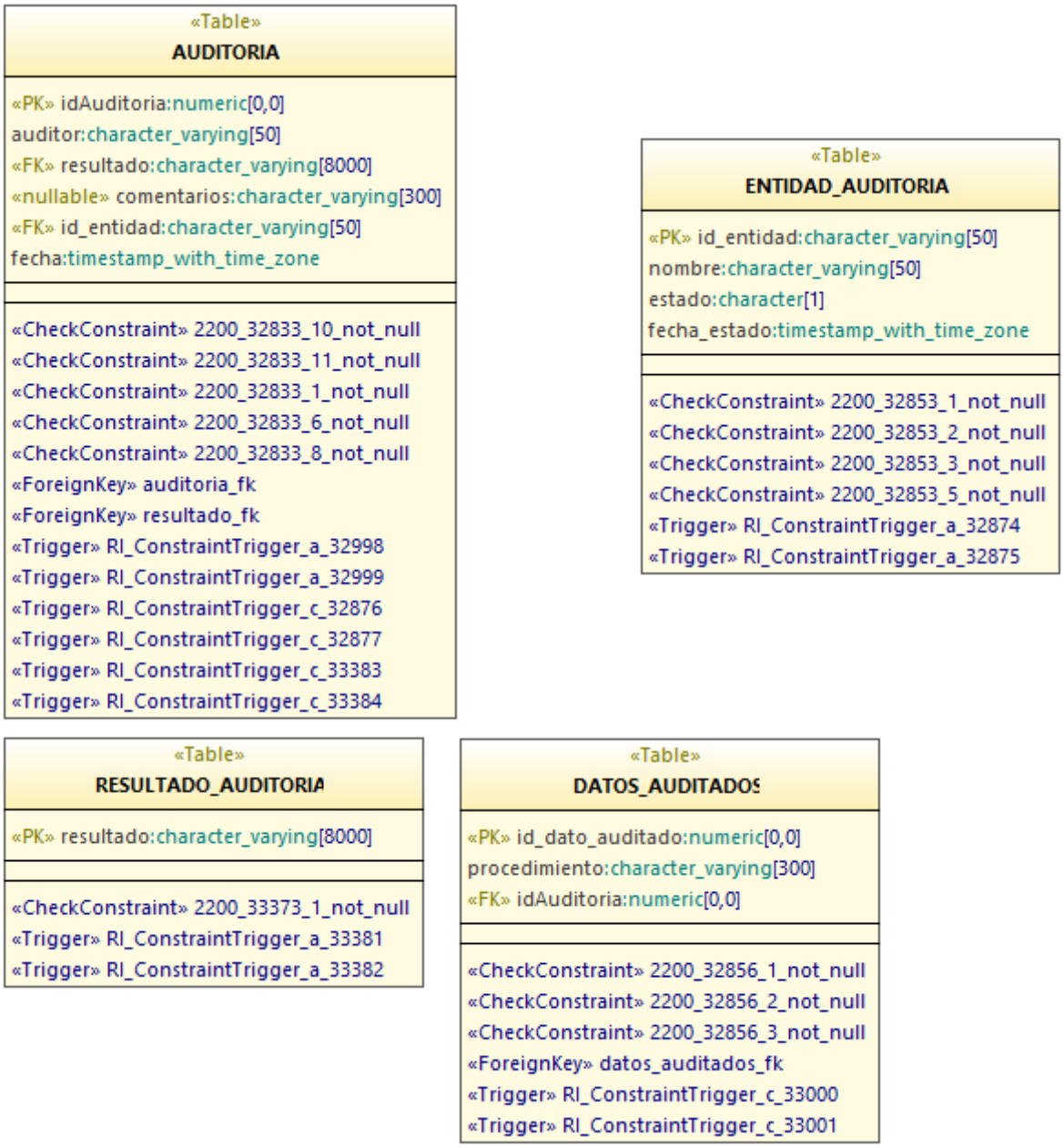
AUDITORIA EXTERNA

Este paquete de la **BD** se ocupará de la auditoria de todos los procesos de seguridad ligados a las diferentes políticas aprobadas por la empresa.

Esta auditoria será realizada por equipos externos e internos de la empresa. En el caso de los equipos externos existirá una consultora seleccionada por la propia empresa.

La **BD** contempla la creación de las tablas que permiten dicha consulta, analizando los diferentes procesos de gestión con el fin de buscar cualquier incumplimiento de las políticas de seguridad aprobadas por la empresa.

La **BD** guardará los datos analizados por la consultora externa, así como los analizados por los equipos internos de la empresa con fin estadístico y también para poder sacar conclusiones objetivas sobre las vulnerabilidades informáticas.


«Table»
AUDITORIA
«PK» idAuditoria:numeric[0,0]
auditor:character_varying[50]
«FK» resultado:character_varying[8000]
«nullable» comentarios:character_varying[300]
«FK» id_entidad:character_varying[50]
fecha:timestamp_with_time_zone
«CheckConstraint» 2200_32833_10_not_null
«CheckConstraint» 2200_32833_11_not_null
«CheckConstraint» 2200_32833_1_not_null
«CheckConstraint» 2200_32833_6_not_null
«CheckConstraint» 2200_32833_8_not_null
«ForeignKey» auditoria_fk
«ForeignKey» resultado_fk
«Trigger» RI_ConstraintTrigger_a_32998
«Trigger» RI_ConstraintTrigger_a_32999
«Trigger» RI_ConstraintTrigger_c_32876
«Trigger» RI_ConstraintTrigger_c_32877
«Trigger» RI_ConstraintTrigger_c_33383
«Trigger» RI_ConstraintTrigger_c_33384
«Table»
ENTIDAD_AUDITORIA
«PK» id_entidad:character_varying[50]
nombre:character_varying[50]
estado:character[1]
fecha_estado:timestamp_with_time_zone
«CheckConstraint» 2200_32853_1_not_null
«CheckConstraint» 2200_32853_2_not_null
«CheckConstraint» 2200_32853_3_not_null
«CheckConstraint» 2200_32853_5_not_null
«Trigger» RI_ConstraintTrigger_a_32874
«Trigger» RI_ConstraintTrigger_a_32875
«Table»
RESULTADO_AUDITORIA
«PK» resultado:character_varying[8000]
«CheckConstraint» 2200_33373_1_not_null
«Trigger» RI_ConstraintTrigger_a_33381
«Trigger» RI_ConstraintTrigger_a_33382
«Table»
DATOS_AUDITADOS
«PK» id_dato_auditado:numeric[0,0]
procedimiento:character_varying[300]
«FK» idAuditoria:numeric[0,0]
«CheckConstraint» 2200_32856_1_not_null
«CheckConstraint» 2200_32856_2_not_null
«CheckConstraint» 2200_32856_3_not_null
«ForeignKey» datos_auditados_fk
«Trigger» RI_ConstraintTrigger_c_33000
«Trigger» RI_ConstraintTrigger_c_33001

Auditoria		
Atributo	***Tipo***	***Descripción***
idAudioria	numeric	Identificador único y secuencial de la auditoria de la **BD**.
auditor	character_varing	Identificador del auditor.
Fecha	timestamps_with_time_zone	Identificador de la fecha que se efectúa la auditoria.
id_entidad	character_varing	Identificador de la entidad que realiza la auditoria.
resultado	character_varing	Identificador del resultado de la auditoria: • Superada. • Superada con comentarios. • No superada.
comentarios	character_varing	Identificador de las observaciones realizadas por el auditor. Este campo será opcional a discreción de este.

Entidad 1 <Relación > Entidad 2	***Descripción***	***Cardinalidad*** **E1: E2**
Auditoría es realizada *entidad_auditoria*	Cada una de las auditorías realizadas es realizada por una entidad_auditora.	***: 1**
Auditoria se obtiene *resultado*	En cada una de las auditorias se obtiene unos resultados.	***: 1**

Entidad_auditoria		
Atributo	***Tipo***	***Descripción***
id_entidad	character_varing	Identificador de la entidad que realiza la auditoria.
Nombre	character_varing	Identificador del auditor.
Estado	character_varing	Identificador que determinada el estado del registro.
fecha_estado	timestamps_with_time_zone	Identificador de la fecha que se establece el estado del registro.

Datos_Auditados		
Atributo	***Tipo***	***Descripción***
id_dato_auditado	numeric	Identificador único del registro de los datos auditados.
IdAuditoria	numeric	Identificador de la auditoria a la que corresponde.
procedimiento	character_varing	Identificador del procedimiento auditado.

Entidad 1 <Relación > Entidad 2	***Descripción***	***Cardinalidad*** **E1: E2**
Auditoria audita *Datos_auditados*	En cada una de las auditorias se auditan un número indeterminado de datos.	**1: ***

Resultado_auditoria		
Atributo	***Tipo***	***Descripción***
resultado	character_varing	Identificador único del resultado de la auditoría realizada. • Superada. • Superada con comentarios. • No superada.

LOG DE PROCESOS

Este paquete de la **BD** reunirá todas las llamadas a los procedimientos de seguridad de la empresa. Guardará todos los procedimientos aplicados mediante dos parámetros, uno de entrada y otro de salida.

La **BD** estandarizará los parámetros de salida mediante un parámetro de salida llamado **RSP**. La **BD** ejecutará un **"OK"** si el procedimiento se ha ejecutado correctamente o con un **"ERROR + TIPO DE ERROR"** si se ha ejecutado erróneamente.

Log_Procesos		
Atributo	***Tipo***	***Descripción***
idLog	numeric	Identificador único del registro del log del proceso.
Fecha	timestamps_with_time_zone	Identificador de la fecha y hora del registro del proceso del log.
procedimiento	character_varing	Identificador del procedimiento auditado.
ParámetroEntrada	character_varing	Identificador del parámetro de entrada para la ejecución

		del proceso.
ParámetroSalida	character_varing	Identificador del parámetro de salida para la ejecución del proceso.

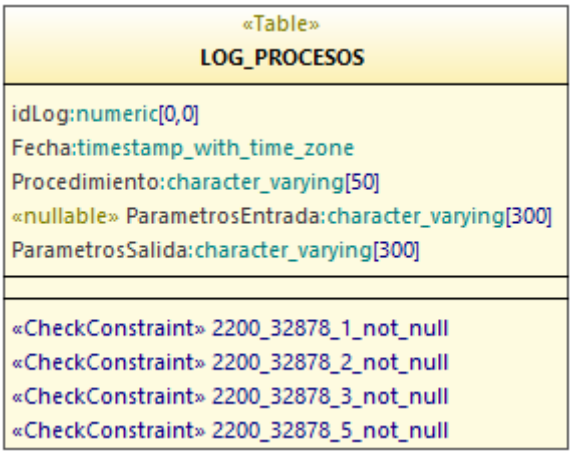
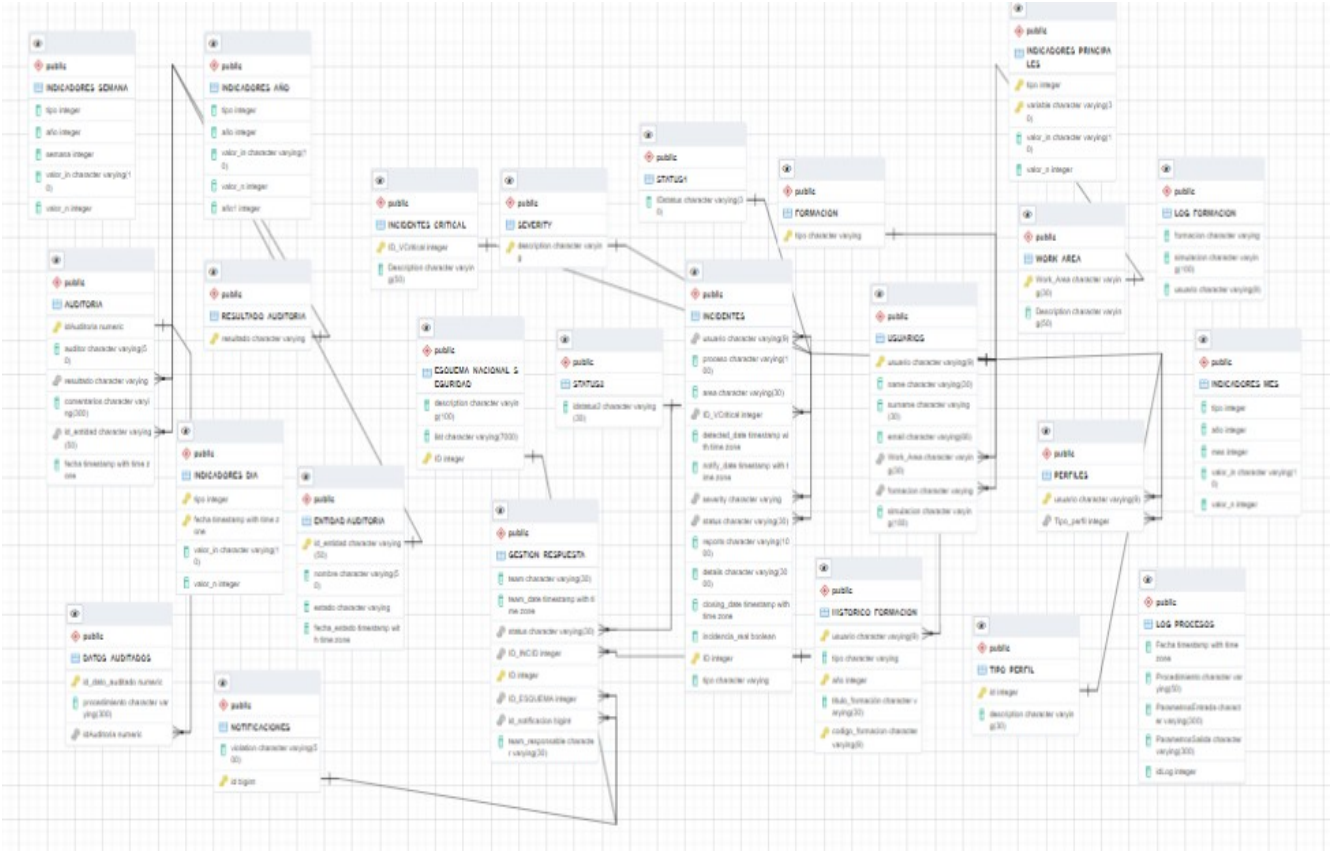


Diagrama ER



2.2.2 Diseño Lógico

Se transforma el modelo conceptual de la **BD** en un modelo lógico relacional. Este diseño se basa en todos los esquemas de relación que describen la **BD**.

La *relación* es la unidad básica del modelo relacional y las *relaciones* entre las diferentes entidades del modelo conceptual la BD, que son instancias de los diferentes tipos de relación.

Si definimos *relación* del modelo lógico, hacemos referencia al conjunto de atributos, con un dominio concreto en el que uno de ellos es la clave primaria.

Para transformar las entidades y las relaciones del diseño conceptual se utilizan varias estrategias que se irán utilizando y utilizando, así como justificando en cada parte del diseño.

Algunas de estas estrategias serán las siguientes:

- Si tomamos el diseño conceptual, dispondremos de un inventario de entidades **(E_1, E_2, E_3…)** que representarán una relación en el diseño lógico **(R_1, R_2, R_3…).** La estructura que hemos diseñado permitirá que los atributos ya especificados, donde uno o varios de ellos, conformarán la clave primaria que identificará cada tupla de forma inequívoca.

- Todas las relaciones del diseño conceptual, entre entidades **E_1** y **E_2** que tengan multiplicidad del tipo **1: *,** incluirán atributos en la relación R_2 que hagan relevancia a la clave primaria de la relación R_1 que es la clave foránea.

- Todas las relaciones del diseño conceptual, entre entidades como **E_1** y **E_2** que tengan una multiplicidad **1: 1**, podrían seguir siendo relaciones independientes con atributos referenciados o fusionando ambas relaciones en una sola relación.

- Cuando establezcamos relaciones de entidades **$E_2 \rightarrow E_1$** y **$E_3 \rightarrow E_1$** se decidirá en cada caso sí:

    - Se generará las relaciones **R_2** y **R_3** basadas en las entidades **E_2** y **E_3**, cada una de ellas combinada con los atributos de la entidad general **E_1**.

    - Se generará una sola relación **R** con la suma de los atributos de las entidades **E_1, E_2** y **E_3.**

Todos los esquemas relacionales del diseño lógico utilizarán las siguientes notaciones:

- Todas las relaciones serán identificadas con el nombre, seguido de la lista de atributos entre paréntesis y separados por comas.

- Todos los atributos que formen parte de la clave primaria irán subrayados con línea continua.

- Todos los atributos que formen parte de la clave alternativa irán subrayados con línea discontinua.

- Todos los atributos **NOT NULL** irán en negrita.

- Todas las claves foráneas se deberán especificar de forma textual con la siguiente nomenclatura, es decir *is foreing key to Relation.* Estas claves estarán representadas por flechas que van desde la clave foránea a la clave primaria de la relación a la que hace referencia.

De esta misma forma el diseño lógico también se explicará de la misma forma que el diseño conceptual atendiendo a cada parte del proyecto.

2.2.2.1 Sistema de Login de perfiles

Relación	Resultado
Usuario	Relación que se obtiene directamente de las entidades ***perfiles*** y ***usuarios*** dentro del Diseño Conceptual. La fusión con la entidad ***usuarios*** es porque sirve para identificar al usuario que se loga en la **BD** en una relación (**1:1...***). Se han añadido atributos para poder referenciar las relaciones de ambas entidades mediante los atributos ***email, surname, name, Work_Area, formación, simulación.***

2.2.2.2 Sistema de Gestión de Usuarios

Relación	Resultado
Work_Area	Relación que se obtiene directamente de las entidades **usuarios** y **Work_Area** dentro del Diseño Conceptual. La fusión con la entidad **usuarios** es porque sirve para identificar el área de trabajo del usuario que se loga en la **BD** en una relación (***:1**). Se han añadido atributos para poder referenciar las relaciones entre ambas entidades mediante **Work_Area** y **Description**.
Formación	Relación que se obtiene directamente de las entidades **usuarios** y **formación** dentro del Diseño Conceptual. La fusión con la entidad **usuarios** es porque sirve para identificar la formación en el trabajo respecto a la seguridad cibernética dentro de la empresa, en una relación (***:1**). Se han añadido atributos para poder referenciar las relaciones entre ambas entidades a través del atributo **tipo.**
Log_Formación	Relación que se obtiene directamente de la entidad **Log_Formación** dentro del Diseño Conceptual. Sus valores hacen referencia a los atributos que componen la entidad y no hacen referencia a ninguna clave foránea porque adoptan datos genéricos.

2.2.3 Sistema de Gestión de Incidencias

Relación	Resultado
Usuario	Relación que se obtiene directamente de las entidades ***usuarios*** e ***incidentes*** dentro del Diseño Conceptual. La fusión con la entidad ***usuarios*** es porque sirve para identificar la incidencia relacionada con el usuario dentro de la empresa, en una relación (***:1**). A esta relación se le añaden los atributos que hacen referencia a esta relación y a las entidades ***severity, incidentes_critical, status1 y usuarios.***
severity	Relación que se obtiene directamente de las entidades ***severity*** e ***incidentes*** dentro del Diseño Conceptual. La fusión con la entidad ***severity*** es porque sirve para identificar el tipo de gravedad de la incidencia relacionada con el usuario dentro de la empresa, en una relación (***:1**). A esta relación se le añaden los atributos que hacen referencia a esta relación y a la entidad ***severity.***
status	Relación que se obtiene directamente de las entidades ***status1*** e ***incidentes*** dentro del Diseño Conceptual. La fusión con la entidad ***status1*** es porque sirve para identificar el estado de la incidencia relacionada con el usuario dentro de la empresa, en una relación (***:1**). A esta relación se le añaden los atributos que hacen referencia a esta relación y a la entidad ***status1.***
ID_VCritical	Relación que se obtiene directamente de las entidades ***Incidentes_Critical*** e ***incidentes*** dentro del Diseño Conceptual. La fusión con la entidad ***Incidentes_Critical*** es porque sirve para identificar el estado crítico de la incidencia relacionada con el usuario dentro de la empresa, en una relación (***:1**). A esta relación se le añaden los atributos que hacen referencia a esta relación y a la entidad ***Incidentes_Critical.***

2.2.2.4 Sistema de Gestión Equipos de Respuesta

Relación	Resultado
ID_INCID	Relación que se obtiene directamente de las entidades ***Gestión_Respuesta*** e ***Incidentes*** dentro del Diseño Conceptual. La fusión con la entidad ***Incidentes*** es porque sirve para identificar el número de identificador del incidente relacionado con el usuario que se loga en la **BD** en una relación (***:1**). A esta relación se le añaden los atributos que hace referencia a esta relación y a la entidad ***Incidentes.***
Id_notificacion	Relación que se obtiene directamente de las entidades ***Gestión_Respuesta*** y ***Notificaciones*** dentro del Diseño Conceptual. La fusión con la entidad ***Notificaciones*** es porque sirve para identificar el número de identificador de la notificación que se genera al tipo de incidente relacionado con el usuario que se loga en la **BD** en una relación (**1:1**). A esta relación se le añaden los atributos que hace referencia a esta relación y a la entidad ***Notificaciones.***
status	Relación que se obtiene directamente de las entidades ***Gestión_Respuesta*** y ***Status2*** dentro del Diseño Conceptual. La fusión con la entidad ***Status2*** es porque sirve para identificar el estado del incidente relacionado con el usuario que se loga en la **BD** en una relación (***:1**). A esta relación se le añaden los atributos que hace referencia a esta relación y a la entidad ***Status2.***
ID_ESQUEMA	Relación que se obtiene directamente de las entidades ***Gestión_Respuesta*** y ***Esquema_Nacional_Seguridad*** dentro del Diseño Conceptual. La fusión con la entidad ***Esquema_Nacional_Seguridad*** es porque sirve para identificar el tipo de incidentes relacionado con el usuario que se loga en la **BD** en una relación (***:1**) y con la entidad **Esquema_Nacional_seguridad**. A esta relación se le añaden los atributos que hace referencia a esta relación y a la entidad ***Incidentes.***

2.2.2.5 Sistema de Análisis de los procedimientos de seguridad

Relación	Resultado
Indicadores_principales	Relación que se obtiene directamente de la entidad ***indicadores_principales*** del Diseño Conceptual. Aunque el ***valor_in*** puede hacer referencia a cualquier tipo de indicador, no se crea ninguna clave foránea porque es un dato muy genérico.
Indicadores_día	Relación que se obtiene directamente de la entidad ***indicadores día*** del Diseño Conceptual. El ***valor_in*** puede hacer referencia a cualquier tipo de indicador, por esa razón no se crea ninguna clave foránea porque es un dato muy genérico. El ***valor_in*** se mantiene para facilitar la inclusión de futuros nuevos indicadores que podrían necesitarlo.
Indicadores_semana	Relación que se obtiene directamente de la entidad ***indicadores semana*** del Diseño Conceptual. El ***valor_in*** puede hacer referencia a cualquier tipo de indicador, por esta razón no se crea ninguna clave foránea porque es un dato muy genérico.
Indicadores_mes	Relación que se obtiene directamente de la entidad ***indicadores mes*** del Diseño Conceptual. El ***valor_in*** puede hacer referencia a cualquier tipo de indicador, por esta razón no se crea ninguna clave foránea porque es un dato muy genérico.
Indicadores_año	Relación que se obtiene directamente de la entidad ***indicadores año*** del Diseño Conceptual. El ***valor_in*** puede hacer referencia a cualquier tipo de indicador, por esta razón no se crea ninguna clave foránea porque es un dato muy genérico.

2.2.2.6 Sistema de Auditoría Externa

Relación	Resultado
Id_entidad	Relación que se obtiene directamente de las entidades ***Entidad auditoría*** y ***Auditoría*** dentro del Diseño Conceptual. La fusión con la entidad ***Auditoría*** es porque sirve para identificar el número de identificador de la entidad auditora relacionado con la auditoría que se realiza a la empresa en una relación (***:1**). A esta relación se le añaden los atributos que hace referencia a esta relación y a la entidad ***auditoría*** y ***auditoría.***
resultado	Relación que se obtiene directamente de las entidades ***resultado auditoría*** y ***Auditoría*** dentro del Diseño Conceptual. La fusión con la entidad ***resultado auditoría*** es porque sirve para identificar el resultado de cada una de las auditorías que se realizan a la empresa en una relación (***:1**). A esta relación se le añaden los atributos que hace referencia a esta relación y a la entidad ***resultado auditoría.***
IdAuditoría	Relación que se obtiene directamente de las entidades ***datos auditados*** y ***Auditoría*** dentro del Diseño Conceptual. La fusión con la entidad ***datos auditados*** es porque sirve para identificar los datos auditados de cada una de las auditorías que se realizan a la empresa en una relación (**1:***). A esta relación se le añaden los atributos que hace referencia a esta relación y a la entidad ***datos auditados.***

2.2.2.7 Sistema de Log_Procesos

Relación	Resultado
Log_Procesos	Relación que se obtiene directamente de la entidad ***Log_Procesos*** dentro del Diseño Conceptual. Sus valores hacen referencia a los atributos que componen la entidad y no hacen referencia a ninguna clave foránea porque adoptan datos genéricos.

2.2.3 Diseño Físico

En esta parte, vamos a dar forma al diseño físico transformando el modelo lógico que nos permitirá posteriormente implementar ese modelo lógico en un sistema de gestión de base de datos, basado en el **motor SQL,** concretamente en ***PostgreSQL14*.** Su implementación se hará a través de su herramienta de gestión y de administración ***pgAdmin4****.*

2.2.3.1 Tipos de Datos

PostgreSQL14 maneja una gran cantidad de datos, a pesar de ello, dentro del proyecto solo se usarán unos tipos de datos en concreto, para ello en la siguiente tabla hacemos una relación de los diferentes tipos de datos más importantes que utilizamos.

2.2.3.2 Diccionario

El siguiente diagrama **ER** es una representación del diseño físico de la ***BD_Empresa*** creada con **PostgreSQL14**. Incluye todos los campos, variables y tablas de la **BD** usando **PostgreSQL** como motor de esta.

2.2.3.3 Sistema de Login de perfiles

Tabla: **Perfiles**				Esta tabla representa el conjunto de todos los perfiles de los usuarios que pueden utilizar la BD_Empresa. Esta entidad debe definir una persona que pueda identificarse de forma inequívoca dentro de la BD_Empresa. A través de este acceso se podrá acceder a las diferentes funcionalidades de la BD que permitirán el continuo trabajo de control de los diferentes procesos de seguridad cibernética llevados a cabo en la empresa.
	Campo	Tipo	Nulo	Descripción
PK FK	usuario	character varing (9)	**NO**	Identificador del usuario que se loga en la BD. Podrán pertenecer a la consultora externa o a los propios usuarios de la empresa.
	Tipo_perfil	character varing (9)	**NO**	Identificador que permitirá distinguir al usuario al cual pertenece la persona que se loga en la BD externa o la propia empresa. Podrán pertenecer a la consultora externa o a la estructura de la propia empresa.
FOREING KEY (usuario) REFERENCES USUARIOS (usuario) FOREING KEY (Tipo_perfil) REFERENCES TIPO_PERFIL (id)				

Tipo	**Características**	**Observaciones**
VARCHAR	Cadena de caracteres alfanuméricos de longitud fija.	**VARCHAR** (Bytes) Entre 1 hasta 7000 bytes como máximo.
INT	Cantidad entera de datos numéricos.	**INT** (Bytes) Entre 2 y 8 bytes Cantidad máxima.
TIMESTAMP TZ	Fecha y hora.	Almacena día, mes, año, semana, horas, minutos y segundos (después de medianoche).
BOOL	Representa los valores de lógica binaría, verdadero o falso.	Almacena los valores **TRUE or FALSE.**
NUMERIC	Representa valores numéricos como decimal, siendo la precisión restringida y exactamente la declarada.	**NUMERIC** (Precisión, escala) Si no se indica la precisión se tomará en función del número a guardar, sino se indica la escala se tomará la escala cero

Tabla: ***Tipo_Perfil***				Esta tabla representa el conjunto de todos los perfiles de los usuarios que pueden utilizar la ***BD_Empresa.*** Esta entidad debe definir una persona que pueda identificarse de forma inequívoca dentro de la ***BD_Empresa.*** A través de este acceso se podrá acceder a las diferentes funcionalidades de la **BD** que permitirán el continuo trabajo de control de los diferentes procesos de seguridad cibernética llevados a cabo en la empresa. Engloba tres tipos diferentes de perfiles ***ADMINISTRADOR, AUDITOR, CONSULTOR.***
	Campo	Tipo	Nulo	Descripción
PK	*id*	integer (4)	**NO**	Identificador del tipo de perfil que se loga en la **BD**. Podrán pertenecer a la **consultora** externa o a los propios usuarios de la empresa, al **auditor**, y al **administrador** de la **BD**.
	Tipo_perfil	character_varing (30)	**NO**	Identificador que permitirá distinguir al usuario al cual pertenece la persona que se loga en la **BD** de la empresa. Podrán pertenecer a la consultora externa o a la estructura de la propia empresa.
FOREING KEY (***usuario***) *REFERENCES USUARIOS* (***usuario***) FOREING KEY (***Tipo_perfil***) *REFERENCES* TIPO_PERFIL ***(id***)				

2.2.3.4 Sistema de Gestión de Usuarios

Tabla: ***Usuarios***				Esta tabla representa el conjunto de usuarios que van a utilizar la ***BD_Empresa.*** Esta entidad gestionará todos los datos necesarios de los usuarios para poder identificarlos a nivel estadísticos del Log de Formación, así como para aquellas otras estadísticas necesarias para la lucha contra ataques cibernéticos. .
	Campo	Tipo	Nulo	Descripción

PK	*usuario*	character_varing (9)	**NO**	Identificador del usuario que se loga en la **BD**. Pertenecerán a los propios usuarios de la empresa.
	name	character_varing (30)	**NO**	Nombre del usuario.
	email	character_varing (66)	**NO**	Email del usuario.
	surname	character_varing (30)	**NO**	Apellidos del usuario.
FK	*Work_Area*	character_varing (30)	**NO**	Área de trabajo del usuario.
FK	*Formación*	character_varing (8000)		Formación del usuario en seguridad informática.
	Simulación	character_varing (100)		Simulaciones realizadas en seguridad informática.
FOREING KEY (***Work_Area***) *REFERENCES WORK*_AREA (***Work_Area***) FOREING KEY (***formacion***) *REFERENCES* FORMACION (***tipo***)				
Tabla: **formación**			Esta tabla representa la formación del usuario en seguridad y vulnerabilidades informáticas, dentro de la **BD_Empresa**. Esta entidad gestiona todos los datos referentes a la formación que debe dar la empresa a sus usuarios en relación con la ciberseguridad.	
	Campo	Tipo	Nulo	Descripción
PK	*tipo*	character_varing (8000)	**NO**	Identificador del tipo de formación que debe de tener el usuario con respecto a la ciberseguridad en la empresa de automovilismo.

Tabla: **Work_Area**			Esta tabla representa el área de trabajo de los usuarios, dentro de la BD_Empresa. Esta entidad gestiona el lugar de trabajo de los usuarios de la empresa.	
	Campo	Tipo	Nulo	Descripción
PK	Work_Area	character_varing (30)	**NO**	Identificador del área de trabajo de los usuarios de la empresa.
	Description	character_varing (50)	**SI**	Identificador y descripción del lugar de trabajo de los usuarios donde trabajan dentro de la empresa.
Tabla: **Log_formacion**			Esta tabla es para albergar el Log de consultas de la formación y de la simulación con respecto a la seguridad cibernética de cada usuario de la empresa.	
	Campo	Tipo	Nulo	Descripción
	usuario	character_varing (9)	**NO**	Identificador del usuario único y secuencial del registro del Log.
	Formación	character_varing (8000)	**NO**	Identificador del usuario único y secuencial del registro del Log.

	Simulación	character_varing (100)	**NO**	Identificador del usuario único y secuencial del registro del Log.

2.2.3.5 Sistema de Gestión de Incidencias

Tabla: **Incidentes**				Esta tabla gestionará el Alta, Baja y modificación de cualquier incidencia referente a las vulnerabilidades que surjan en la empresa automovilística. Permitirá controlar y analizar las políticas de seguridad que se cumplen dentro de la empresa. Dichas políticas son de obligado cumplimiento por todos los departamentos de la empresa, así como todas las personas que la componen.
	Campo	Tipo	Nulo	Descripción
PK	ID	integer (4)	**NO**	Identificador único y secuencial del usuario de la BD.
FK	usuario	character_varing (9)	**NO**	Identificador de los usuarios que han cometido la vulnerabilidad de seguridad informática.
	proceso	character_varing (100)	**NO**	Descripción del incidente de la vulnerabilidad producida en la empresa automovilística.
	area	character_varing (30)	**NO**	Área de trabajo de la empresa donde se ha producido y lugar donde se encuentra trabajando el usuario.
FK	ID_VCritical	integer (4)	**NO**	Identificador de si la vulnerabilidad producida es crítica o no.
	detected_date	timestamps_with_time_zone	**NO**	Fecha y hora del día que se ha detectado la vulnerabilidad de seguridad informática en la empresa.
	notify_date	timestamps_with_time_zone	**NO**	Fecha y hora del día que se ha notificado la vulnerabilidad de seguridad informática a los sistemas de control de la empresa.
FK	*severity*	character_varing	**NO**	Identificador que permite clasificar la vulnerabilidad en **MUY GRAVE**, **GRAVE**, **MEDIO**, **BAJA**, **MUY BAJA**.
				Identificador que permite clasificar la incidencia de

FK	*status*	character_varing (30)	**NO**	seguridad en acciones **IDENTIFICADAS**, **NO MITIGADAS**, **PARCIALMENTE MITIGADAS**, **TOTALMENTE MITIGADAS**.
	reports	character_varing (1000)	**SI**	Identificador de todos los datos necesarios para el estudio y análisis de la vulnerabilidad producida.
	details	character_varing (3000)	**SI**	Identificador de todos los detalles necesarios para que el estudio y análisis sea correctamente realizado por los servicios de control de la empresa.
	closing_date	timestamps_with_time_zone	**NO**	Fecha y hora que se da por terminada la incidencia de vulnerabilidad informática.
	incidencia_real	boolean	**NO**	Identificador que permite identificar si la incidencia es real o no lo es si en el estudio se evalúa que no cumple con las políticas definidas y aprobadas por la empresa.
UK	*tipo*	character_varing	**NO**	Identificador del tipo de incidencia producida, que permita identificar claramente el tipo de vulnerabilidad informática producida que se encuentre dentro de los incumplimientos de seguridad definidos por la empresa automovilística.

FOREING KEY (***Usuario***) *REFERENCES USUARIOS* (***Usuario***)
FOREING KEY (***ID_Critical***) *REFERENCES* INCIDENTES_CRITICAL(***ID_VCritical***)
FOREING KEY (***severity***) *REFERENCES* SEVERITY(***Description***)
FOREING KEY (***status***) *REFERENCES* STATUS1(***ID_Status***)

Tabla: ***ID_VCritical*** — Esta tabla representa si la vulnerabilidad es crítica o no.

	Campo	Tipo	Nulo	Descripción
PK	*ID_VCritical*	Integer (4)	**NO**	Identificador de la vulnerabilidad detectada es declarada como crítica o no.
	Description	character_varing (50)	**SI**	Descripción de la vulnerabilidad crítica o no crítica declarada previamente.

Tabla: ***Status1*** — Esta tabla representa las incidencias de seguridad en acciones **IDENTIFICADAS**, **NO MITIGADAS**,

				PARCIALMENTE MITIGADAS, **TOTALMENTE MITIGADAS**.
	Campo	Tipo	Nulo	Descripción
U K	*IDstatus*	character_varing (30)	**NO**	Identificador de la incidencia de seguridad en acciones como: **IDENTIFICADAS**, **NO MITIGADAS**, **PARCIALMENTE MITIGADAS**, **TOTALMENTE MITIGADAS**.

Tabla: ***Severity***			Esta tabla representa las vulnerabilidades en **MUY GRAVES, GRAVES, MEDIAS, BAJAS y MUY BAJAS**.
Campo	Tipo	Nulo	Descripción
PK	*Description*	character_varing	**NO**	Identificador que permite clasificar la vulnerabilidad en **MUY GRAVE**, **GRAVE**, **MEDIO**, **BAJA**, **MUY BAJA**.

2.2.3.6 Sistema de Gestión Equipos de Respuesta

Tabla: ***Gestión_respuesta***				Esta tabla gestionará el conjunto de las posibles soluciones a las diferentes vulnerabilidades informáticas de la empresa. Esta tabla gestionará todos los ataques producidos en la empresa siendo analizados y gestionados por equipos especializados en procesos de seguridad informática. Las políticas de seguridad serán aprobadas por el departamento de **RRHH** de la empresa. Esta tabla guardará los datos necesarios para hacer el reporte estadístico de los protocolos de seguridad informática que cumplirán los diferentes departamentos de la empresa para determinar que ataque es más vulnerable en la empresa.
	Campo	Tipo	Nulo	Descripción
PK	*ID*	integer (4)	**NO**	Identificador único y secuencial del usuario de la **BD**.
FK	*ID_ESQUEMA*	Integer (4)	**NO**	Identificador del tipo de incidente de la vulnerabilidad producida en la empresa automovilística.
FK	*ID_INCID*	Integer (4)	**NO**	Identificador del incidente que han cometido la vulnerabilidad de seguridad informática mediante un código generado aleatoriamente por la **BD**.
FK	*Id_notificacion*	Integer (8)	**NO**	Identificador de la notificación de la violación de la vulnerabilidad haciendo referencia a las políticas de seguridad aprobadas por la empresa.
FK	*status*	character_varing (30)	**NO**	Identificador del incidente clasificado según el estado en el que se encuentra el incidente: **DEFINIDA**, **EN PROCESO**, **EN REVISIÓN** y **ACABADA**.
	team	character_varing (30)	**NO**	Equipo interno de la empresa que actualizará la lista de intrusiones o equipo de la consultora externa que durante dos meses se

				encargará de realizar dicho análisis de las vulnerabilidades de la empresa.
	team_date	timestamps_with_time_zone	**NO**	Fecha y hora del día que se ha notificado la vulnerabilidad de seguridad informática por los equipos internos o externos de la empresa que se encargan del análisis y control de dichas vulnerabilidades.
FOREINGKEY (***ID_ESQUEMA***) *REFERENCES ESQUEMA*_NACIONAL_SEGURIDAD(***ID***) FOREING KEY (***ID_INCID***) *REFERENCES* INCIDENTES(***ID***) FOREING KEY (***status***) *REFERENCES* STATUS2(***idstatus2***) FOREING KEY (***id_notificacion***) *REFERENCES* NOTIFICACIONES (***id***)				

Tabla: ***Esquema_Nacional_Seguridad***				Esta tabla representa la descripción y la lista de todas las vulnerabilidades detectadas por los equipos propios de la expresa o por los externos.
	Campo	Tipo	Nulo	Descripción
PK	*ID*	Integer (4)	**NO**	Identificador del tipo de vulnerabilidad creada por los equipos de análisis de la propia empresa u externos.
	Description	character_varing (100)	**NO**	Identificador y descripción del tipo de vulnerabilidad generada en la incidencia.
	list	character_varing (7000)	**NO**	Vulnerabilidades detectadas por los equipos propios de la empresa o por los equipos externos de la misma.

Tabla: ***Notificaciones***				Esta tabla representa la descripción y la lista de todas las vulnerabilidades detectadas por los equipos propios de la expresa o por los externos.
	Campo	Tipo	Nulo	Descripción
PK	*id*	Integer (8)	**NO**	Identificador de la notificación generada que identifica la vulnerabilidad detectada.
	violation	character_varing (500)	**NO**	Indica que vulnerabilidad ha sido detectada haciendo referencia a la lista de vulnerabilidades encontradas en la empresa.

Tabla: ***Status2***				Esta tabla representa el estado de la gestión respuesta de las incidencias detectadas en la empresa.
	Campo	Tipo	Nulo	Descripción

UK	*Id_status2*	character_varing (30)	**NO**	Identificador de la gestión respuesta que está clasificada en varios estados: **DEFINIDA**, **EN PROCESO**, **EN REVISIÓN** y **ACABADA**.

2.2.3.7 Sistema de Análisis de los procedimientos de seguridad

Tabla: ***Indicadores Principales***				Esta tabla representa los indicadores principales del repositorio estadístico de la **BD.** Esta tabla almacenará una tupla por tipo de indicador y variable que se almacenará para este indicador concreto.
	Campo	Tipo	Nulo	Descripción
PK	*tipo*	integer (4)	**NO**	Tipo que hace referencia al indicador.
PK	*Variable*	character_varing (30)	**NO**	Este atributo hace referencia al valor del indicador. Los posibles valores de este atributo dependen del tipo al que correspondan. Tipo1: usuarios, media. Tipo2: auditorias. Tipo3:max_incumplimientos, min_incumplimientos. Tipo4: por acciones mitigadas. Tipo5: por variación. Tipo6: vulnerabilidades.
	Valor_in	character_varing (10)	**SI**	Valor del tipo String del indicador. Se usará para almacenar el incumplimiento (tipo3) o las acciones mitigadas (tipo4) y vulnerabilidades (tipo6).
	Valor_n	integer (4)	**NO**	Este indicador guardará el valor del indicador que será una media, un porcentaje, un contador, etc.

Tabla: ***Indicadores día***				Esta tabla representa los indicadores del repositorio estadístico de la **BD** que se guardan cada día**.** Esta tabla almacenará una tupla por tipo de indicador y variable cada día.
	Campo	Tipo	Nulo	Descripción

PK	*tipo*	integer (4)	**NO**	Tipo que hace referencia al indicador.
PK	*fecha*	timestamps_with_time_zone	**NO**	Fecha en la que se produce el indicador.
	Valor_in	character_varing (10)	**SI**	Valor del tipo String del indicador. Se usará para almacenar el incumplimiento (tipo 3) o las acciones mitigadas (tipo4) y vulnerabilidades (tipo6) para cálculos por día.
	Valor_n	integer (4)	**NO**	Este indicador guardará el valor del indicador que será una media, un porcentaje, un contador, etc.

Tabla: ***Indicadores semana***			Esta tabla representa los indicadores del repositorio estadístico de la **BD** que se guardan cada semana**.** Esta tabla almacenará una tupla por tipo de indicador y variable cada semana.
Campo	Tipo	Nulo	Descripción
tipo	integer (4)	**NO**	Tipo que hace referencia al indicador.
año	integer (4)	**NO**	Año que hace referencia la semana.
semana	integer (4)	**NO**	Semana en que se calcula el indicador.
Valor_in	character_varing (10)	**SI**	Valor del tipo String del indicador. Se usará para almacenar el incumplimiento (tipo 3) o las acciones mitigadas (tipo4) y vulnerabilidades (tipo6) para cálculos por semana.
Valor_n	integer (4)	**NO**	Este indicador guardará el valor del indicador que será una media, un porcentaje, un contador, etc.

Tabla: ***Indicadores mes***			Esta tabla representa los indicadores del repositorio estadístico de la **BD** que se guardan cada mes**.** Esta tabla almacenará una tupla por tipo de indicador y variable cada mes.
Campo	Tipo	Nulo	Descripción
tipo	integer (4)	**NO**	Tipo que hace referencia al indicador.
mes	integer (4)	**NO**	Mes en que se calcula el indicador.
año	integer (4)	**NO**	Año que hace referencia al mes.
			Valor del tipo String del indicador. Se

	Valor_in	character_varing (10)	**SI**	usará para almacenar el incumplimiento (tipo 3) o las acciones mitigadas (tipo4) y vulnerabilidades (tipo6) para cálculos por mes.
	Valor_n	integer (4)	**NO**	Este indicador guardará el valor del indicador que será una media, un porcentaje, un contador, etc.

Tabla: ***Indicadores año***				Esta tabla representa los indicadores del repositorio estadístico de la **BD** que se guardan cada año**.** Esta tabla almacenará una tupla por tipo de indicador y variable cada año.
	Campo	Tipo	Nulo	Descripción
	tipo	integer (4)	**NO**	Tipo que hace referencia al indicador.
	año	integer (4)	**NO**	Año que hace referencia al año actual.
	año1	integer (4)	**NO**	Año en que se calcula el indicador.
	Valor_in	character_varing (10)	**SI**	Valor del tipo String del indicador. Se usará para almacenar el incumplimiento (tipo 3) o las acciones mitigadas (tipo4) y vulnerabilidades (tipo6) para cálculos por año.
	Valor_n	integer (4)	**NO**	Este indicador guardará el valor del indicador que será una media, un porcentaje, un contador, etc.

2.2.3.8 Sistema de Auditoría Externa

Tabla: ***Auditoría***				Esta tabla representa la consultora externa contratada por la empresa automovilística con el fin de combatir las vulnerabilidades generadas en la empresa en seguridad informática, generando una lista de vulnerabilidades asociadas a cada uno de los procesos de gestión de la misma.
	Campo	Tipo	Nulo	Descripción
PK	*idAuditoria*	numeric	**NO**	Identificador único y secuencial de la auditoria de la **BD**.
	auditor	character_varing (50)	**NO**	Nombre del auditor de la consultora externa.
	comentarios	character_varing (300)	**SI**	Identificador de las observaciones realizadas por el auditor. Este

				campo será opcional a discrepción del mismo.
	fecha	timestamps_with_time_zone	**NO**	Identificador de la fecha que se efectúa la auditoria.
FK	*id_entidad*	character_varing (50)	**NO**	Identificador de la entidad que realiza la auditoria.
FK	*resultado*	character_varing (30)	**NO**	Identificador del resultado de la auditoria: Superada. Superada con comentarios. No superada.
FOREING KEY (***id_entidad***) *REFERENCES ENTIDADA* AUDITORIA (***id_entidad***) FOREING KEY (***resultado***) *REFERENCES* RESULTADO_AUDITORIA (***resultado***)				

Tabla: ***Entidad_auditoria***				Esta tabla representa a la entidad auditora que realiza la consulta externa relacionando el estado de la detección con el nombre de la persona que realiza la auditoría externa, así como la fecha en el que se establece el estado del registro.
	Campo	Tipo	Nulo	Descripción
PK	*id_entidad*	character_varing (50)	**NO**	Identificador de la entidad que realiza la auditoria.
	estado	character_varing	**NO**	Identificador que determinada el estado del registro.
	nombre	character_varing (50)	**NO**	Identificador del auditor.
	fecha_estado	timestamps_with_time_zone	**NO**	Identificador de la fecha que se establece el estado del registro.

Tabla: Resultado_auditoria				Esta tabla representa el resultado final de la auditoría de la consulta externa realizada por la empresa automovilística.
	Campo	Tipo	Nulo	Descripción
PK	resultado	character_varing	**NO**	Identificador único del resultado de la auditoría realizada. Superada. Superada con comentarios. No superada.

Tabla: Datos_auditados				Esta tabla representa los registros de las vulnerabilidades encontradas de manera externa en la empresa automovilística.
	Campo	Tipo	Nulo	Descripción
PK	id_dato_auditado	numeric	**NO**	Identificador único del registro de los datos auditados.

FK	idAuditoria	numeric	**NO**	Identificador de la auditoria a la que corresponde.
	procedimiento	character_varing (300)	**NO**	Identificador del procedimiento auditado.
FOREING KEY (idAuditoría) REFERENCES AUDITORIA (idAuditoría)				

2.2.3.9 Sistema de Log_Procesos

Tabla: ***Log_Procesos***				Esta tabla almacena todas las llamadas a procedimientos que se hagan en la tabla log_procesos. Almacenando el nombre del procedimiento, la fecha y los parámetros de entrada y salida.
	Campo	Tipo	Nulo	Descripción
	idLog	numeric	**NO**	Identificador único del registro del log del proceso.
	fecha	numeric	**NO**	Identificador de la fecha y hora del registro del proceso del log.
	procedimiento	character_varing (50)	**NO**	Identificador del procedimiento auditado.
	ParámetroEntrada	character_varing (300)	**SI**	Identificador del parámetro de entrada para la ejecución del proceso.
	ParámetroSalida	character_varing (300)	**NO**	Identificador del parámetro de salida para la ejecución del proceso.

2.2.4 Análisis del diseño elaborado y almacenado.

En los requerimientos (**RQNF-003 y RQNF-004**) se solicita que toda la gestión y acceso a la información se hará mediante procedimientos de la **BD**.

Se implementarán los procedimientos de alta, baja y modificación de todas las entidades relevantes y todos los procedimientos y disparadores para el mantenimiento del repositorio estadístico, registro de logs y cualquier otro que se considere necesario para el funcionamiento de la **BD** y del sistema.

Los procedimientos que se incluyan en el sistema tendrán tratamiento de excepciones, disponiendo de al menos de un parámetro, tipo String, de salida llamado **RSP**, que indicará si la ejecución ha finalizado correctamente **(valor 'OK')** o si ha fracasado **(valor 'ERROR+ TIPO ERROR')**.

2.2.4.1 Procedimientos Almacenados

Procedimiento	**Alta_Perfil**
Descripción	Proceso para crear un nuevo perfil en el sistema de la **BD**.
Parámetro de entrada	**p_usuario** in VARCHAR (9). **p_Tipo_perfil** in VARCHAR (9).
Operativa	Se comprueba que: El identificador **usuario** no exista en la tabla usuario. El **tipo de perfil** o corresponda a un usuario perteneciente a la propia empresa o la consultora externa. Si todo es correcto, se insertará en la tabla **Usuario** un nuevo registro dependiendo si el usuario pertenece a la empresa o a la consultora externa de la empresa.
Parámetro de Salida	**"OK"** → *si todo es correcto y concluye con éxito.* **"ERROR"** → *El Usuario ya existe o la persona está asociada a otro usuario.* **"ERROR"** → *El Tipo_perfil no es válido.* **"ERROR"** → *La clave del usuario está vacía.* **"ERROR"** → *El usuario no existe.* **"ERROR"** → *Autorización no válida.*
Procedimiento	**Alta_Usuario**
Descripción	Proceso para crear un nuevo usuario en el sistema de la **BD**.
Parámetro de entrada	**p_usuario** in VARCHAR (9). **p_email** in VARCHAR (66). **p_formacion** in VARCHAR. **p_name** in VARCHAR (30). **p_simulacion** in VARCHAR (100). **p_surname** in VARCHAR (30). **p_Work_Area** in VARCHAR (30).
Operativa	Se comprueba que:

	El identificador **usuario** no exista en la tabla usuario. El **email** no esté vacío. La **formación** sea telemática o presencial. El **name** no esté vacío. El **surname** no esté vacío. El **Work_Area** no esté vacío y corresponda a las áreas de trabajo de la empresa. Si todo es correcto, se insertará en la tabla **Usuario** un nuevo registro.
Parámetro de Salida	**"OK"** → *si todo es correcto y concluye con éxito.* **"ERROR"** → *El Usuario ya existe o la persona está asociada a otro usuario.* **"ERROR"** → *El email no es válido.* **"ERROR"** → *La clave del usuario está vacía.* **"ERROR"** → *El usuario no existe.* **"ERROR"** → *Autorización no válida.* **"ERROR"** → *El name no corresponde a ese usuario.* **"ERROR"** → *El Work_Area no corresponde a ningún área de la empresa.* **"ERROR"** → *El surname no corresponde a ningún usuario.* **"ERROR"** → *El email no corresponde a ningún usuario.* **"ERROR"** → *El name no corresponde a ningún usuario.*

Procedimiento	**Modificar_Usuario**
Descripción	Proceso para modificar un usuario en el sistema de la **BD**.
Parámetro de entrada	**p_usuario** in VARCHAR (9). **p_email** in VARCHAR (66). **p_formacion** in VARCHAR. **p_name** in VARCHAR (30). **p_simulacion** in VARCHAR (100).

	p_surname in VARCHAR (30). **p_Work_Area** in VARCHAR (30).
Operativa	Se comprueba que: El identificador **usuario** exista en la tabla usuario. El **email** no esté vacío. La **formación** sea telemática o presencial. El **name** no esté vacío. El **surname** no esté vacío. El **Work_Area** no esté vacío y corresponda a las áreas de trabajo de la empresa. Si todo es correcto, se insertará en la tabla **Usuario** la modificación del registro.
Parámetro de Salida	**"OK"** → *si todo es correcto y concluye con éxito.* **"ERROR"** → *El Usuario ya existe o la persona está asociada a otro usuario.* **"ERROR"** → *El email no es válido.* **"ERROR"** → *La clave del usuario está vacía.* **"ERROR"** → *El usuario no existe.* **"ERROR"** → *Autorización no válida.* **"ERROR"** → *El name no corresponde a ese usuario.* **"ERROR"** → *El Work_Area no corresponde a ningún área de la empresa.* **"ERROR"** → *El surname no corresponde a ningún usuario.* **"ERROR"** → *El email no corresponde a ningún usuario.* **"ERROR"** → *El name no corresponde a ningún usuario.*
Procedimiento	***Activar_Usuario***
Descripción	Proceso para activar un usuario que ha sido de baja en el sistema de la **BD**. La activación implica que se modifique el estado y su fecha.
Parámetro de entrada	**p_usuario** in VARCHAR (9).
Operativa	Se comprueba que:

	El identificador **usuario** exista en la tabla usuario y que se haya dado de baja. Si todo es correcto, se actualizará el estado del usuario en la tabla **Usuario** y la fecha de alta será la misma que tome del sistema.
Parámetro de Salida	**"OK"** → *si todo es correcto y concluye con éxito.* **"ERROR"** → *El Usuario ya no existe o el usuario ya está activo.*
Procedimiento	**Baja_Usuario**
Descripción	Proceso para dar de baja un usuario en el sistema de la **BD**. La baja NO implica que se eliminen todos los datos del usuario, sino que se establece un estado de baja y la fecha de la misma.
Parámetro de entrada	• **p_usuario** in VARCHAR(9).
Operativa	Se comprueba que: El identificador usuario exista en la tabla usuario y que no se haya dado de baja. Si todo es correcto, se eliminará en la tabla Usuario la identificación del usuario y la fecha será la que tome del sistema.
Parámetro de Salida	**"OK"**→ *si todo es correcto y concluye con éxito.* **"ERROR"**→ *El Usuario ya no existe o el usuario se ha dado de baja.*
Procedimiento	**Alta_Incidente**
Descripción	Proceso para crear un nuevo incidente en el sistema de la **BD**.
Parámetro de entrada	**p_ID** in INT (4). **p_area** in VARCHAR (30). **p_closing_date** in TIMESTAMPTZ. **p_proceso** in VARCHAR (100). **p_details** in VARCHAR (3000). **p_detected_date** in TIMESTAMPTZ. **p_ID_VCritical** in INT (4). **p_incidencia_real** in BOOL. **p_notify_date** in TIMESTAMPTZ. **p_reports** in VARCHAR (1000).

	p_severity in VARCHAR. **p_status** in VARCHAR (30). **p_tipo** in VARCHAR. **p_usuario** in VARCHAR (9).
Operativa	Se comprueba que: El identificador **usuario** no exista en la tabla **usuario** y no esté vacío. El **area** no esté vacío. El **closing_date** que no esté vacío. El **proceso** que no esté vacío. El **details** que no esté vació. El **detected_date** que no esté vacío. El **ID_VCritical** que corresponda a uno de los tipos de incidencia crítica según su gravedad. La **incidencia_real** que no esté vacía. La **notify_date** que no esté vacía. El **reports** que no esté vacío. El **severity** que corresponda a uno de los tipos de gravedad según el tipo de incidencia y no se encuentre vacío. El **status** que se encuentre clasificada la incidencia en los diferentes tipos y no se encuentre vacía. El **tipo** que no este vacío. Si todo es correcto, se insertará en la tabla **Incidentes** un nuevo registro.
Parámetro de Salida	**"OK"** → *si todo es correcto y concluye con éxito.* "**ERROR"** → *El Usuario ya existe o la persona está asociada a otro usuario.* **"ERROR"** → *La incidencia_real está vacía.* **"ERROR"** → *El area está vacía.* **"ERROR"** → *El usuario no existe.* **"ERROR"** → *Autorización no válida.*

	“ERROR” → *El status no corresponde a ningún tipo.* **“ERROR”** → *El tipo está vacío.* **“ERROR”** → *El severity no corresponde a ningún a ninguno de los establecidos.* **“ERROR”** → *El reports está vacío*. **“ERROR”** → *El notify_date está vacío.* **“ERROR”** → *El closing_date está vacío*. **“ERROR”** → *El proceso está vacío.* **“ERROR”** → *El details está vacío.* **“ERROR”** → *El detected_date está vacío.* **“ERROR”** → *El notify_date está vacío.* **“ERROR”** → *El ID_VCritical no corresponde a ningún tipo establecido.*
Procedimiento	***Baja_Incidente***
Descripción	Proceso para dar de baja un incidente en el sistema de la **BD**. La baja NO implica que se eliminen todos los datos del incidente, sino que se establece un estado de baja y la fecha de esta.
Parámetro de entrada	**p_ID** in INT (4). **p_usuario** in VARCHAR (9).
Operativa	Se comprueba que: El identificador **usuario** exista en la tabla usuario y que no se haya dado de baja. El identificador del **incidente** exista en la tabla incidentes y que no se haya dado de baja. Si todo es correcto, se eliminará en la tabla **Usuario** la identificación del **usuario** y la fecha será la que tome del sistema, así como el identificador del **incidente** asociado al usuario.
Parámetro de Salida	***“OK”*** *→ si todo es correcto y concluye con éxito.* ***“ERROR”*** *→ El Usuario ya no existe o el usuario se ha dado de baja.* ***“ERROR”*** *→ El incidente ya no existe o el incidente se ha dado de*

	baja.
Procedimiento	**Modificar_Incidente**
Descripción	Proceso para modificar un incidente en el sistema de la **BD**.
Parámetro de entrada	**p_ID** in INT (4). **p_area** in VARCHAR (30). **p_closing_date** in TIMESTAMPTZ. **p_proceso** in VARCHAR (100). **p_details** in VARCHAR (3000). **p_detected_date** in TIMESTAMPTZ. **p_ID_VCritical** in INT (4). **p_incidencia_real** in BOOL. **p_notify_date** in TIMESTAMPTZ. **p_reports** in VARCHAR (1000). **p_severity** in VARCHAR. **p_status** in VARCHAR (30). **p_tipo** in VARCHAR. **p_usuario** in VARCHAR (9).
Operativa	Se comprueba que: El identificador **usuario** exista en la tabla **usuario** y no este vacío. El **area** no este vacío. El **closing_date** que no este vacío. El **proceso** que no este vacío. El **details** que no este vacío. El **detected_date** que no este vacío. El **ID_VCritical** que corresponda a uno de los tipos de incidencia crítica según su gravedad. La **incidencia_real** que no esté vacía. La **notify_date** que no esté vacía. El **reports** que no este vacío. El **severity** que corresponda a uno de los tipos de gravedad según

	el tipo de incidencia y no se encuentre vacío. El **status** que se encuentre clasificada la incidencia en los diferentes tipos y no se encuentre vacía. El **tipo** que no este vacío. Si todo es correcto, se insertará en la tabla **Incidentes** la modificación del registro.
Parámetro de Salida	**"OK"** → *si todo es correcto y concluye con éxito.* "**ERROR"** → *El Usuario ya existe o la persona está asociada a otro usuario.* **"ERROR"** → *La incidencia_real está vacía.* **"ERROR"** → *El area está vacía.* **"ERROR"** → *El usuario no existe.* **"ERROR"** → *Autorización no válida.* **"ERROR"** → *El status no corresponde a ningún tipo.* **"ERROR"** → *El tipo está vacío.* **"ERROR"** → *El severity no corresponde a ningún a ninguno de los establecidos.* **"ERROR"** → *El reports está vacío.* **"ERROR"** → *El notify_date está vacío.* **"ERROR"** → *El closing_date está vacío.* **"ERROR"** → *El proceso está vacío.* **"ERROR"** → *El details está vacío.* **"ERROR"** → *El detected_date está vacío.* **"ERROR"** → *El notify_date está vacío.* **"ERROR"** → *El ID_VCritical no corresponde a ningún tipo establecido.*
Procedimiento	**Alta_Entidad_Auditoria**
Descripción	Proceso para crear una nueva entidad auditora.
Parámetro de entrada	**p_id_identidad** in VARCHAR (50). **p_nombre** in VARCHAR (50).

Operativa	Se comprueba que: El identificador de la **identidad** no exista en la tabla **Entidad Auditoria**. El **nombre** no esté vacío y no exista en la tabla **Entidad Auditoria**. Si todo es correcto, se insertará en la tabla **Entidad Auditoria** un nuevo registro.
Parámetro de Salida	***"OK"*** *→ si todo es correcto y concluye con éxito.* ***"ERROR"*** *→ El nombre de la entidad está vacía o ya existe para otra entidad.* ***"ERROR"*** *→ La entidad está vacía o ya existe previamente.*
Procedimiento	**Modificar_Entidad_Auditoria**
Descripción	Proceso para modificar una entidad auditora que ya existe. Se podrá modificar el nombre de la entidad.
Parámetro de entrada	**p_id_identidad** in VARCHAR (50). **p_nombre** in VARCHAR (50).
Operativa	Se comprueba que: El identificador de la **identidad** exista en la tabla **Entidad Auditoria**. El **nombre** no esté vacío y no exista en la tabla **Entidad Auditoria**. Si todo es correcto, se modificará en la tabla **Entidad Auditoria** el nuevo registro.
Parámetro de Salida	***"OK"*** *→ si todo es correcto y concluye con éxito.* ***"ERROR"*** *→ El nombre de la entidad está vacía o existe para otra entidad.* ***"ERROR"*** *→ La entidad no existe.*
Procedimiento	**Baja_Entidad_Auditoria**
Descripción	Proceso para dar de baja una entidad auditora que ya existe. La baja no implica que se eliminen los datos de la entidad en el sistema, sino que se establece un estado de baja y la fecha de esta.

Parámetro de entrada	**p_id_identidad** in VARCHAR (50).
Operativa	Se comprueba que: El identificador de la **identidad** exista en la tabla **Entidad Auditoria**. La entidad no está referenciada en la tabla **Auditoría**. Si todo es correcto, se actualizaría el estado y la fecha en la tabla **Entidad Auditoria** del nuevo registro.
Parámetro de Salida	***"OK"*** *→ si todo es correcto y concluye con éxito.* ***"ERROR"*** *→ La entidad está referenciada en la tabla Auditoría.* ***"ERROR"*** *→ La entidad no existe.*
Procedimiento	**Activar_Entidad_Auditoria**
Descripción	Proceso para activar una entidad auditora que, ya existido, es decir que se encuentra de baja. La activación implica la modificación del estado y su fecha.
Parámetro de entrada	**p_id_identidad** in VARCHAR (50).
Operativa	Se comprueba que: El identificador de la **identidad** exista en la tabla **Entidad Auditoria** y se encuentre en el estado de baja. Si todo es correcto, se modificará el estado de la entidad en la tabla **Entidad Auditoria** y la fecha de alta será la del sistema.
Parámetro de Salida	***"OK"*** *→ si todo es correcto y concluye con éxito.* ***"ERROR"*** *→ La entidad no existe o ya se ha dado de alta.*
Procedimiento	**Alta_Auditoria**
Descripción	Proceso para crear una nueva auditoría externa
Parámetro de entrada	**p_id_identidad** in VARCHAR (50). **p_auditidor** in VARCHAR (50). **p_fecha** in TIMESTAMPTZ. **p_resultado** in VARCHAR. **p_comentarios** in VARCHAR (300).

Operativa	Se comprueba que: El identificador de la **identidad** exista en la tabla **Entidad Auditoria** y se encuentre activada. El nombre del **auditor** no se encuentre vacío. La **fecha** no esté vacía. El **resultado** de la auditoría debe ser Superada, No superada o Superada con comentarios. Si el resultado de la auditoría es superado con comentarios, los comentarios no deben de estar vacíos. Si todo es correcto, se insertará el alta en la tabla **Auditoria** del nuevo registro. Utilizará un disparador y una tabla de secuencias para poder asignar automáticamente el identificador secuencial del registro.
Parámetro de Salida	**"OK"** → *si todo es correcto y concluye con éxito.* **"ERROR"** → *La entidad no existe o ya se ha dado de baja.* **"ERROR"** → *El auditor está vacío.* **"ERROR"** → *La fecha está vacía.* **"ERROR"** → *El valor del resultado es incorrecto.* **"ERROR"** → *Los comentarios del resultado están vacíos.*
Procedimiento	**Modificar_Auditoria**
Descripción	Proceso para modificar una auditoría externa que ya existe.
Parámetro de entrada	**p_id_identidad** in VARCHAR (50). **p_auditidor** in VARCHAR (50). **p_fecha** in TIMESTAMPTZ. **p_resultado** in VARCHAR. **p_comentarios** in VARCHAR (300). **p_idAuditoria** in NUMERIC.
Operativa	Se comprueba que: El identificador de la **identidad** exista en la tabla **Entidad Auditoria** y se encuentre activada.

	El identificador de la **Auditoria** existe en la tabla **Auditoria**. El nombre del **auditor** no se encuentre vacío. La **fecha** no esté vacía. El **resultado** de la auditoría debe ser Superada, No superada o Superada con comentarios. Si el resultado de la auditoría es superado con comentarios, los comentarios no deben de estar vacíos. Si todo es correcto, se modificará todo el registro en la tabla **Auditoria**.
Parámetro de Salida	**"OK"** → *si todo es correcto y concluye con éxito.* **"ERROR"** → *La entidad no existe o ya se ha dado de baja.* **"ERROR"** → *El auditor está vacío.* **"ERROR"** → *La fecha está vacía.* **"ERROR"** → *El valor del resultado es incorrecto.* **"ERROR"** → *Los comentarios del resultado están vacíos.* **"ERROR"** → *La auditoría no existe.*
Procedimiento	**Baja_Auditoria**
Descripción	Proceso para dar de baja una auditoría externa
Parámetro de entrada	**p_idAuditoria** in NUMERIC.
Operativa	Se comprueba que: El identificador de la Auditoria debe de existir en la tabla **Auditoría**. Si todo es correcto, se dará de baja y se eliminará en la tabla **Auditoria** el registro, así como todos los datos referentes a los **datos_auditados** relacionados con esta auditoría correspondientes a la tabla **Datos_Auditados**.
Parámetro de Salida	***"OK"*** *→ si todo es correcto y concluye con éxito.* ***"ERROR"*** *→ La auditoría no existe.*
Procedimiento	**Alta_Datos_Auditados**
Descripción	Proceso para dar de alta un dato auditado a una auditoría externa existente.

Parámetro de entrada	**p_idAuditoria** in NUMERIC. **p_id_dato_auditado** in NUMERIC.
Operativa	Se comprueba que: El identificador de la **Auditoria** debe de existir en la tabla **Auditoría**. El **dato_auditado** no debe de estar vacío. Si todo es correcto, se dará de alta el dato_auditado en la tabla **datos_auditados** como un nuevo registro. Se utilizará un disparador y una tabla de secuencias para poder asignar automáticamente el identificador secuencial del registro.
Parámetro de Salida	**"OK"** → *si todo es correcto y concluye con éxito.* **"ERROR"** → *La auditoría no existe.* **"ERROR"** → *El dato_auditado se encuentra vacío.*
Procedimiento	**Alta_Log_Procesos**
Descripción	Proceso para crear un registro de log cuando se ejecuta un procedimiento interno de la **BD**.
Parámetro de entrada	**p_procedimiento** in VARCHAR (50). **p_paramentroEntrada** in VARCHAR (300). **p_paramentroSalida** in VARCHAR (300). **p_fecha** in TIMESTAMPTZ.
Operativa	Se comprueba que: El nombre del **procedimiento** no este vacío. Los **parámetros de salida** no deben de estar vacíos. La **fecha** no debe de estar vacía. Si todo es correcto, se dará de alta el registro de los datos de entrada en la tabla de **Log_Procesos** con la fecha introducida previamente con los parámetros de entrada. Esta tabla utilizará un disparador, así como una tabla de secuencias para asignar automáticamente el identificador secuencial del registro del Log.

Parámetro de Salida	***"OK"*** *→ si todo es correcto y concluye con éxito.* ***"ERROR"*** *→ El procedimiento está vacío.* ***"ERROR"*** *→ Los parámetros de salida están vacíos.*
Procedimiento	**Alta_Log_Formación**
Descripción	Proceso para crear un registro de log de formación cuando se ejecuta un procedimiento interno de la **BD**.
Parámetro de entrada	**p_formación** in VARCHAR. **p_simulación** in VARCHAR (100). **p_usuario** in VARCHAR (9).
Operativa	Se comprueba que: La **formación** no debe de estar vacío, debe de ser telemática o presencial. Debe de existir el registro en la tabla **usuarios**. La **simulación** no debe de estar vacía. Debe de existir el registro en la tabla **usuarios**. El identificador del usuario debe de existir en la tabla **usuarios**. Si todo es correcto, se dará de alta el registro de los datos de entrada en la tabla de **Log_Formación.** Esta tabla utilizará un disparador, así como una tabla de secuencias para asignar automáticamente el identificador secuencial del registro del usuario en la tabla del **Log_Formación**.
Parámetro de Salida	***"OK"*** *→ si todo es correcto y concluye con éxito.* ***"ERROR"*** *→ La formación está vacío.* ***"ERROR"*** *→ La simulación está vacía.* ***"ERROR"*** *→ El usuario no debe ser vacío. Debe corresponder a un usuario dado de alta en la tabla usuarios.*
Procedimiento	**Consulta_Gestión_Respuesta**
Descripción	Proceso para consultar los registros de la tabla Gestión_Respuesta cuando se ejecuta un procedimiento interno de la **BD**.
Parámetro de entrada	**p_formación** in VARCHAR. **p_simulación** in VARCHAR (100). **p_usuario** in VARCHAR (9).
Operativa	Se comprueba que:

	La **formación** no debe de estar vacío, debe de ser telemática o presencial. Debe de existir el registro en la tabla **usuarios**. La **simulación** no debe de estar vacía. Debe de existir el registro en la tabla **usuarios**. El identificador del usuario debe de existir en la tabla **usuarios**. Si todo es correcto, se dará de alta el registro de los datos de entrada en la tabla de **Log_Formación.** Esta tabla utilizará un disparador, así como una tabla de secuencias para asignar automáticamente el identificador secuencial del registro del usuario en la tabla del **Log_Formación**.
Parámetro de Salida	***"OK"*** *→ si todo es correcto y concluye con éxito.* ***"ERROR"*** *→ La formación está vacío.* ***"ERROR"*** *→ La simulación está vacía.* ***"ERROR"*** *→ El usuario no debe ser vacío. Debe corresponder a un usuario dado de alta en la tabla usuarios.*

A modo de representación adjunto algunas de las consultas de la **BD**, que la misma debería realizar correctamente. Estas consultas se apoyan sobre las tablas de los indicadores de la **BD**, mediante la creación de unas tuplas donde guardaremos todas estas consultas en función de los parámetros de entrada y salida, así como de los resultados que pretendamos conseguir:

- **Indicadores Principales**
- **Indicadores Día**
- **Indicadores Año**
- **Indicadores Semana**
- **Indicadores Mes**

Procedimiento	**Calculo_Indicador_Consulta01**
Descripción	Proceso que obtiene el departamento que, en un año concreto, tiene un número mayor de incumplimientos de seguridad registrados en la **BD**.
Parámetro de entrada	
Operativa	Suma de las incidencias ocurridas en la (**tabla INCIDENTES**) por áreas de trabajo, en un año concreto. Guarda el primer registro con más incumplimientos por departamento en un año concreto en el que se hace la consulta.

<table>
<tr><td>Resultado</td><td>Este indicador se representa con el tipo 1 y se guarda en la tabla indicadores_Año en 1 tupla:

<table><tr><th>Tipo</th><th>año</th><th>Año1</th><th>Valor_in</th><th>Valor_n</th></tr><tr><td>1</td><td>Año actual.</td><td>Año concreto del estudio.</td><td>Departamento con más incidencias en un año concreto.</td><td>Incidentes del departamento.</td></tr></table></td></tr>
<tr><td>Parámetro de Salida</td><td>“OK” → si todo es correcto y concluye con éxito.
“ERROR” → Indefinido.</td></tr>
</table>

<table>
<tr><th>Procedimiento</th><th>Calculo_Indicador_Consulta08</th></tr>
<tr><td>Descripción</td><td>Porcentaje de usuarios de la empresa que, en el año en curso, no tienen ningún incumplimiento asignado.</td></tr>
<tr><td>Parámetro de entrada</td><td></td></tr>
<tr><td>Operativa</td><td>Suma de todas las incidencias cometidas por el usuario en la (tabla USUARIOS).
Guarda el registro dentro de la variable n.
Calcular el porcentaje de los usuarios que no han cometido ningún incidente de seguridad.</td></tr>
<tr><td>Resultado</td><td>Este indicador se representa con el tipo 6 y se guarda en la tabla indicadores_Año en 1 tupla:

<table><tr><th>Tipo</th><th>año</th><th>Año1</th><th>Valor_in</th><th>Valor_n</th></tr><tr><td>6</td><td>Año actual.</td><td>Año concreto del estudio.</td><td>Usuarios de la empresa en el año actual.</td><td>Porcentaje = (Número total de usuarios que no han cometido ningún incidente * 100) / Número total de usuarios.</td></tr></table></td></tr>
<tr><td>Parámetro de Salida</td><td>“OK” → si todo es correcto y concluye con éxito.
“ERROR” → Indefinido.</td></tr>
</table>

2.3 Implementación

2.3.1 Tipo de SGBD

El proyecto ha sido desarrollado sobre un Sistema de Gestión de Base de Datos (**SGBD)** relacional **PostgreSQL**, cuya implementación se realizará sobre la versión **PostgreSQL14**.

2.3.2 TableSpace de la BD

Este mecanismo va a permitir decidir donde podremos almacenar las tablas o cada fragmento de ellas. De la misma manera esto va a permitir elegir en que máquina, disco, o trozo de este tendremos los diferentes datos de la base de datos.

- Existirá un TableSpace donde se ubiquen todos los objetos permanentes del proyecto.
- Existirá un TableSpace temporal donde no se podrán ubicar objetos permanentemente. Es muy recomendable poder disponer de un espacio temporal para poder optimizar operaciones de ordenaciones.

2.3.3 Usuarios

Para el mantenimiento y explotación de la **BD** se crearán una serie de usuarios con una serie de privilegios. Estos usuarios se podrán logar en la misma con tres tipos diferentes que dependiendo del usuario la **BD** le asignará unos privilegios u otros.

- **ADMINISTRADOR**
- **CONSULTOR**
- **AUDITOR**

USUARIOS	PRIVILEGIOS
ADMINISTRADOR	**Entre otras cosas podrá iniciar y parar la instancia de la BD, crear modificar, y borrar la base de datos.** **Este usuario que se empleará para la construcción e implementación de la BD.** **Podrá utilizar los TableSpace disponibles de la BD.**
CONSULTOR	**Podrán conectarse a la BD.** **Podrán seleccionar, modificar y borrar datos de la BD en tablas de otros**

	usuarios. **Este usuario se utilizará para lanzar consultas sobre la BD, procedimientos, etc.** **Utilizará igualmente todos los TableSpace de la BD.** **Acciones permitidas para este usuario:** • **CREATE SESION** • **SELECT ANY TABLE** • **UPDATE ANY TABLE** • **DELETE ANY TABLE**
AUDITOR	**Podrán conectarse a la BD.** **Podrán seleccionar, modificar y borrar datos de la BD en tablas de otros usuarios.** **Este usuario se utilizará para lanzar consultas sobre la BD, procedimientos, etc.** **Utilizará igualmente todos los TableSpace de la BD.** **Acciones permitidas para este usuario:** • **CREATE SESION** • **SELECT ANY TABLE** • **UPDATE ANY TABLE** **DELETE ANY TABLE**

2.3.4 Scripts de la BD

Se detallan a continuación los scripts creados para este proyecto, principalmente para la implementación de la BD en el orden que se han ido creando:

- Tablas
- Secuencias
- Índices
- Procedimientos
- Disparadores
- Funciones, etc.

Script	Contenido de la BD
Creación BS_Empresa	Se crearán los diferentes scripts correspondientes a la **BD** en sus diferentes secciones: • Creación del **TableSpace**. • Creación de las tablas que albergarán los usuarios de la misma **BD,** así como de los Tipos de **Perfil y los Perfiles**. • Creación de la tabla **Usuarios**. • Creación de la tabla **Incidentes**. • Creación de la tabla **Gestión de Respuesta**. • Creación de los objetos de la tabla **Usuarios** que albergará: Tablas Índices Secuencias Disparadores para las claves primarias • Creación de los objetos del **Repositorio Estadístico.** • Creación de los objetos de la **Auditoría Externa** a la empresa. • Asignar privilegios a los usuarios de la **BD**. • Creación de los objetos de **formación** de los empleados de la empresa donde se realiza el estudio de las vulnerabilidades informáticas.
Procedimientos. SQL	Este Script implementa: • Se aplicarán los procedimientos descritos en esta memoria correspondiente al **Análisis del diseño elaborado y almacenado.** Concretamente a los **procedimientos almacenados.** • Se implementarán los disparadores necesarios para el mantenimiento del Repositorio Estadístico de este documento.

2.3.5 Repositorio Estadístico

Este apartado se especificarán todas las consultas a la BD que permitirán obtener todos los indicadores solicitados y relacionados con el Repositorio Estadístico.

Indicador	Descripción de la consulta

1	Departamento que tiene un número mayor de incumplimientos de seguridad registrados.
	
	`CREATE OR REPLACE FUNCTION public. incidencias_departamento("año1" integer)`
	` RETURNS integer`
	` LANGUAGE plpgsql`
	`AS $function$`
	
	`declare`

	r varchar; begin r:= (select COUNT(u."Work_Area") AS incidencias FROM "INCIDENTES" i2 left join "USUARIOS" u on u. usuario = i2. usuario where date_part('year', i2.detected_date::date)=año1); return r; end $function$;
2	Proceso de gestión interno, ha tenido un mayor nombre de vulnerabilidades detectadas. select i. proceso from "INCIDENTES" i group by i. proceso having count (*) = (select count (distinct i2. proceso) from "INCIDENTES" i2);
3	Top5 de usuarios por número de incumplimientos asociados directamente a ellos, o a su departamento durante el año en curso. select count (i. usuario), i2. usuario AS incidencias FROM "INCIDENTES" i2,"INCIDENTES" i where date_part ('year', i2. detected_date::date)=2022 and i2.usuario = i.usuario group by i2.usuario, i2.area order by max(distinct i2.usuario),count(distinct i2.usuario) limit 5;
4	Porcentaje de vulnerabilidades que, en el momento de ejecutar la consulta, están TOTALMENTE MITIGADAS. select i. status, 100 *(select COUNT (i2. status) from "INCIDENTES" i2 where i2. status ='TOTALMENTE MITIGADA') / (select COUNT (*) from "INCIDENTES" i3) as "PORCENTAJE" from "INCIDENTES" i where i. status ='TOTALMENTE MITIGADA' group by i. status;
5	Número total de acciones de mitigación que, en el momento de ejecutar la consulta, no están totalmente acabadas. select count (*) as "ACCIONES DE MITIGACION" from "GESTION_RESPUESTA" gr where status<>'ACABADA';
6	Política de seguridad que, en el momento de ejecutar la consulta, ha tenido más incumplimientos. select n. violation from "GESTION_RESPUESTA" gr, "NOTIFICACIONES" n where gr.id_notificacion = n.id group by n. violation having count(*) = (select max(id_notificacion) from "GESTION_RESPUESTA");
7	Dado un determinado departamento de la empresa, y teniendo en cuenta el momento de ejecutar la consulta, porcentaje de usuarios del departamento que no han acabado todas las formaciones de seguridad asignadas. select u2."Work_Area", 100 *(select COUNT(*) from "USUARIOS" u where u.simulacion = 'NO' and u."Work_Area" = 'DIRECCIÓN')/ (Select COUNT(*)from "USUARIOS" u where u."Work_Area" ='DIRECCIÓN') as "PORCENTAJE" from "USUARIOS" u2 where u2."Work_Area" = 'DIRECCIÓN' group by u2."Work_Area" ;
8	Porcentaje de usuarios de la empresa que, en el año en curso, no tienen ningún

	incumplimiento asignado. `select distinct i2. usuario, 100 *(select e2.total - e1.total from (select count(*) as total from "USUARIOS") as e1, (select distinct COUNT(u.usuario) as total from "USUARIOS" u left join "INCIDENTES" i on u.usuario = i.usuario) as e2)/(Select COUNT(*)from "USUARIOS" u) as "PORCENTAJE" from "INCIDENTES" i2 group by i2. usuario;`
9	Teniendo todas las auditorias externar realizadas, año en el que se han detectado más incumplimientos (teniendo en cuenta sólo los detectados durante la auditoría). `select extract (year from team_date) from "GESTION_RESPUESTA" gr group by gr.team_date having count(*) = (select count(gr."ID_INCID") from "GESTION_RESPUESTA" gr left join "PERFILES" p on gr.team_responsable = p.usuario where gr.team_responsable = p.usuario and p."Tipo_perfil" = 2);`
10	Porcentaje de vulnerabilidades críticas que, en el momento de ejecutar la consulta, tienen una alguna acción de mitigación abierta (que no esté en estado “acabada”) `select i2."ID",i2."ID_VCritical", 100 *(select COUNT(gr.status) from "GESTION_RESPUESTA" gr, "INCIDENTES" i where gr."ID_INCID" = i."ID" and gr.status <> 'ACABADA' and i."ID_VCritical"<3)/(Select COUNT(*)from "INCIDENTES" i, "GESTION_RESPUESTA" gr where i."ID_VCritical" <3 and i."ID"= gr."ID_INCID") as "PORCENTAJE" from "INCIDENTES" i2 where i2."ID_VCritical" < 3 group by i2."ID_VCritical”, i2."ID";`
11	Teniendo en cuenta el último año (año anterior al actual), título de la sesión formativa telemática que ha tenido un porcentaje menor de participantes total. `select hf.titulo_formación from "HISTORICO_FORMACION" hf group by hf.titulo_formación having count(*) = (select count (*) from "HISTORICO_FORMACION" where año = extract (year from now())-1);`
12	Número de vulnerabilidades críticas detectadas internamente teniendo en cuenta todos los datos de que se dispone. `select count(gr."ID_INCID") from "GESTION_RESPUESTA" gr left join "PERFILES" p on gr.team_responsable = p.usuario left join "INCIDENTES" i ON gr."ID_INCID" = i."ID" where gr.team_responsable = p.usuario and p."Tipo_perfil" = 1 and i."ID_VCritical" < 3;`
13	En el momento de ejecutar la consulta, porcentaje de acciones de mitigación en el sistema que están en los estados de “en proceso” o “en revisión”. `select distinct 100 *(select count (*) from "GESTION_RESPUESTA" gr where gr. status = 'EN PROCESO' or gr. status = 'EN REVISION’) /(Select COUNT(*)from "GESTION_RESPUESTA") as "PORCENTAJE" from “GESTION_RESPUESTA" gr2 group by gr2.status;`
14	Teniendo en cuenta todas las acciones de mitigación en estado “en proceso”, persona responsable con más acciones asignadas.

	select max (t2. responsable2), gr2.team_responsable from (select count (t1. responsable) as responsable2, t1. responsable as nombre from (select (gr. team_responsable) as responsable from "GESTION_RESPUESTA" gr where gr. status ='EN PROCESO') as t1 group by responsable) as t2 left join "GESTION_RESPUESTA" gr2 on gr2.team_responsable = t2. nombre group by gr2.team_responsable, t2. responsable2 order by (t2. responsable2) desc limit 1;

2.4 Pruebas

2.4.1 Scripts de preparación de los set de datos

Antes de realizar las pruebas, se preparan los **SET** de datos de datos que permitirán la realización de estas. Concretamente se crean los siguientes scripts:

Scripts	¿Qué engloba?
Datos_principales_BD.sql__	Este script crea un paquete de unos **100** datos de personas que inserta en las tablas de integración para poder probar el funcionamiento de esta.
Datos_Estadísticos.BD.sql	Este script borra los datos anteriores y crea unos datos para poder llevar a cabo las pruebas del repositorio estadístico.

2.4.2 Documento de pruebas

En la tabla siguiente se lleva a cabo las pruebas finales sobre la **BD,** se procede a llevar a cabo los procedimientos de la **BD** almacenados con todos sus posibles resultados. Esta se implementa en un script de prueba, para ellos utilizaremos los scripts de datos de integración antes comentados, probando los procedimientos de integración de la propia **BD** como los estadísticos, a través de los datos de integración del **repositorio estadístico**.

Procedimiento	Id_Prueba	Descripción	Resultado
Integración de datos	PR000.01	Procedimiento que engloba la integración de los datos de los scripts de datos principales y estadísticos. Su resultado recoge la información: • **INSERT** datos de integración. • **UPDATE** datos que son actualizados. _	Correcto

Alta_Perfil	**PR001.01**	**"OK"** → *si todo es correcto y concluye con éxito.*	Correcto
	PR001.02	**"ERROR"** → *El Usuario ya existe o la persona está asociada a otro usuario.*	Correcto
	PR001.03	**"ERROR"** → *El Tipo_perfil no es válido.*	Correcto
	PR001.04	**"ERROR"** → *La clave del usuario está vacía.*	Correcto
	PR001.05	**"ERROR"** → *El usuario no existe.*	Correcto
	PR001.06	**"ERROR"** → *Autorización no válida.*	Correcto
Alta_Usuario	**PR002.01**	**"OK"** → *si todo es correcto y concluye con éxito.*	Correcto
	PR002.02	**"ERROR"** → *El Usuario ya existe o la persona está asociada a otro usuario.*	Correcto
	PR002.03	**"ERROR"** → *El email no es válido.*	Correcto
	PR002.04	**"ERROR"** → *La clave del usuario está vacía.*	Correcto
	PR002.05	**"ERROR"** → *El usuario no existe.*	Correcto
	PR002.06	**"ERROR"** → *Autorización no válida.*	Correcto
	PR002.07	**"ERROR"** → *El name no corresponde a ese usuario.*	Correcto
	PR002.08	**"ERROR"** → *El Work_Area no corresponde a ningún área de la empresa.*	Correcto
	PR002.09	**"ERROR"** → *El surname no corresponde a ningún usuario.*	Correcto
	PR002.10	**"ERROR"** → *El email no corresponde a ningún usuario.*	Correcto
	PR002.11	**"ERROR"** → *El name no corresponde a ningún usuario.*	Correcto
Modificar_Usuario	**PR003.01**	**"OK"** → *si todo es correcto y concluye con éxito.*	Correcto
	PR003.02	**"ERROR"** → *El Usuario ya existe o la persona está asociada a otro usuario.*	Correcto
	PR003.03	**"ERROR"** → *El email no es válido.*	Correcto
	PR003.04	**"ERROR"** → *La clave del usuario está vacía.*	Correcto
	PR003.05	**"ERROR"** → *El usuario no existe.*	Correcto
	PR003.06	**"ERROR"** → *Autorización no válida.*	Correcto
	PR003.07	**"ERROR"** → *El name no corresponde a ese usuario.*	Correcto
	PR003.08	**"ERROR"** → *El Work_Area no corresponde a ningún área de la empresa.*	Correcto
	PR003.09	**"ERROR"** → *El surname no corresponde a ningún usuario.*	Correcto
	PR003.10	**"ERROR"** → *El email no corresponde a ningún usuario.*	Correcto
	PR003.11	**"ERROR"** → *El name no corresponde a ningún usuario.*	Correcto

Activar_Usuario	**PR004.01**	**“OK”** → *si todo es correcto y concluye con éxito.*	Correcto
	PR004.02	**“ERROR”** → *El Usuario ya no existe o el usuario ya está activo.*	Correcto
Baja_Usuario	**PR005.01**	**“OK”**→ *si todo es correcto y concluye con éxito.*	Correcto
	PR005.02	**“ERROR”**→ *El Usuario ya no existe o el usuario se ha dado de baja.*	Correcto
Alta_Incidente	**PR006.01**	**“OK”** → *si todo es correcto y concluye con éxito.*	Correcto
	PR006.02	“**ERROR”** → *El Usuario ya existe o la persona está asociada a otro usuario.*	Correcto
	PR006.03	**“ERROR”** → *La incidencia_real está vacía.*	Correcto
	PR006.04	**“ERROR”** → *El area está vacía.*	Correcto
	PR006.05	**“ERROR”** → *El usuario no existe.*	Correcto
	PR006.06	**“ERROR”** → *Autorización no válida.*	Correcto
	PR006.07	**“ERROR”** → *El status no corresponde a ningún tipo.*	Correcto
	PR006.08	**“ERROR”** → *El tipo está vacío.*	Correcto
	PR006.09	**“ERROR”** → *El severity no corresponde a ningún a ninguno de los establecidos.*	Correcto
	PR006.10	**“ERROR”** → *El reports está vacío*.	Correcto
	PR006.11	**“ERROR”** → *El notify_date está vacío.*	Correcto
	PR006.12	**“ERROR”** → *El closing_date está vacío*.	Correcto
	PR006.13	**“ERROR”** → *El proceso está vacío.*	Correcto
	PR006.14	**“ERROR”** → *El details está vacío.*	Correcto
	PR006.15	**“ERROR”** → *El detected_date está vacío.*	Correcto
	PR006.16	**“ERROR”** → *El notify_date está vacío.*	Correcto
	PR006.17	**“ERROR”** → *El ID_VCritical no corresponde a ningún tipo establecido.*	Correcto
Baja_Incidente	**PR007.01**	***“OK”*** → *si todo es correcto y concluye con éxito.*	Correcto
	PR007.02	***“ERROR”*** → *El Usuario ya no existe o el usuario se ha dado de baja.*	Correcto
	PR007.03	***“ERROR”*** → *El incidente ya no existe o el incidente se ha dado de baja.*	Correcto
	PR008.01	**“OK”** → *si todo es correcto y concluye con éxito.*	Correcto
	PR008.02	“**ERROR”** → *El Usuario ya existe o la persona está asociada a otro usuario.*	Correcto
	PR008.03	**“ERROR”** → *La incidencia_real está vacía.*	Correcto
	PR008.04	**“ERROR”** → *El area está vacía.*	Correcto

Modificar_Incidente	**PR008.05**	**“ERROR”** → *El usuario no existe.*	Correcto
	PR008.06	**“ERROR”** → *Autorización no válida.*	Correcto
	PR008.09	**“ERROR”** → *El status no corresponde a ningún tipo.*	Correcto
	PR008.10	**“ERROR”** → *El tipo está vacío.*	Correcto
	PR008.11	**“ERROR”** → *El severity no corresponde a ningún a ninguno de los establecidos.*	Correcto
	PR008.12	**“ERROR”** → *El reports está vacío.*	Correcto
	PR008.13	**“ERROR”** → *El notify_date está vacío.*	Correcto
	PR008.14	**“ERROR”** → *El closing_date está vacío.*	Correcto
	PR008.15	**“ERROR”** → *El proceso está vacío.*	Correcto
	PR008.16	**“ERROR”** → *El details está vacío.*	Correcto
	PR008.17	**“ERROR”** → *El detected_date está vacío.*	Correcto
	PR008.18	**“ERROR”** → *El notify_date está vacío.*	Correcto
	PR008.19	**“ERROR”** → *El ID_VCritical no corresponde a ningún tipo establecido.*	Correcto
Alta_Entidad Auditora	**PR009.01**	***“OK”*** → *si todo es correcto y concluye con éxito.*	Correcto
	PR009.02	***“ERROR”*** → *El nombre de la entidad está vacía o ya existe para otra entidad.*	Correcto
	PR009.03	***“ERROR”*** → *La entidad está vacía o ya existe previamente.*	Correcto
Modificar_Entidad Auditora	**PR010.01**	***“OK”*** → *si todo es correcto y concluye con éxito.*	Correcto
	PR010.02	***“ERROR”*** → *El nombre de la entidad está vacía o existe para otra entidad.*	Correcto
	PR011.03	***“ERROR”*** → *La entidad no existe.*	Correcto
Baja_Entidad Auditora	**PR012.01**	***“OK”*** → *si todo es correcto y concluye con éxito.*	Correcto
	PR012.02	***“ERROR”*** → *La entidad está referenciada en la tabla Auditoría.*	Correcto
	PR012.03	***“ERROR”*** → *La entidad no existe.*	Correcto
Activar_Entidad Auditora	**PR013.01**	***“OK”*** → *si todo es correcto y concluye con éxito.*	Correcto
	PR013.02	***“ERROR”*** → *La entidad no existe o ya se ha dado de alta.*	Correcto
Alta_Auditoría	**PR014.01**	**“OK”** → *si todo es correcto y concluye con éxito.*	Correcto
	PR014.02	**“ERROR”** → *La entidad no existe o ya se ha dado de baja.*	Correcto
	PR014.03	**“ERROR”** → *El auditor está vacío.*	Correcto
	PR014.04	**“ERROR”** → *La fecha está vacía.*	Correcto
	PR014.05	**“ERROR”** → *El valor del resultado es*	Correcto

		incorrecto.	
	PR014.06	**"ERROR"** → *Los comentarios del resultado están vacíos.*	Correcto
Modificar_Auditoría	**PR015.01**	**"OK"** → *si todo es correcto y concluye con éxito.*	Correcto
	PR015.02	**"ERROR"** → *La entidad no existe o ya se ha dado de baja.*	Correcto
	PR015.03	**"ERROR"** → *El auditor está vacío.*	Correcto
	PR015.04	**"ERROR"** → *La fecha está vacía.*	Correcto
	PR015.05	**"ERROR"** → *El valor del resultado es incorrecto.*	Correcto
	PR015.06	**"ERROR"** → *Los comentarios del resultado están vacíos.*	Correcto
	PR015.07	**"ERROR"** → *La auditoría no existe.*	Correcto
Baja_Auditoría	**PR016.01**	***"OK"*** → *si todo es correcto y concluye con éxito.*	Correcto
	PR016.02	***"ERROR"*** → *La auditoría no existe.*	Correcto
Alta_Datos_ Auditados	**PR017.01**	**"OK"** → *si todo es correcto y concluye con éxito.*	Correcto
	PR017.02	**"ERROR"** → *La auditoría no existe.*	Correcto
	PR017.03	**"ERROR"** → *El dato_auditado se encuentra vacío.*	Correcto
Alta_Log_Procesos	**PR018.01**	***"OK"*** → *si todo es correcto y concluye con éxito.*	Correcto
	PR018.02	***"ERROR"*** → *El procedimiento está vacío.*	Correcto
	PR018.03	***"ERROR"*** → *Los parámetros de salida están vacíos.*	Correcto
Alta_Log_Formacion	**PR019.01**	***"OK"*** → *si todo es correcto y concluye con éxito.*	Correcto
	PR019.02	***"ERROR"*** → *La formación está vacío.*	Correcto
	PR019.03		Correcto
	PR019.04	***"ERROR"*** → *La simulación está vacía.*	Correcto
		"ERROR" → *El usuario no debe ser vacío. Debe corresponder a un usuario dado de alta en la tabla usuarios.*	
Consulta_Gestion Respuesta	**PR020.01**	***"OK"*** → *si todo es correcto y concluye con éxito.*	Correcto
	PR020.02	***"ERROR"*** → *La formación está vacío.*	Correcto
	PR020.03		Correcto
	PR020.04	***"ERROR"*** → *La simulación está vacía.*	Correcto
		"ERROR" → *El usuario no debe ser vacío. Debe corresponder a un usuario dado de alta en la tabla usuarios*	
Calculo_Indicador	**PR021.01**	**"OK"** → *si todo es correcto y*	Correcto

Consulta01		*concluye con éxito.*	
	PR021.02	**"ERROR"** → *Indefinido.*	Correcto
Calculo_Indicador Consulta08	**PR022.01**	**"OK"** → *si todo es correcto y concluye con éxito.*	Correcto
	PR022.02	**"ERROR"** → *Indefinido.*	Correcto

3. Conclusiones

La finalización de este proyecto ha conllevado un gran esfuerzo y tener que sacar mucho tiempo de trabajo sobre todo en aquellos momentos donde los he tenido. La planificación y el desarrollo junto con el esfuerzo ha permitido llegar a conseguir el objetivo.

Ha sido una gran experiencia personal de las cuales he sacado un gran gratificación final, gracias a haber llevado a cabo correctamente lo cual ha permitido enormemente a la consecución de los objetivos programados:

- Se ha querido dar mucha importancia a los detalles a la definición de los requisitos ya que el método utilizado ha sido el de cascada, cualquier error en la interpretación de estos habría supuesto que se hubiera propagado en las siguientes fases del proyecto, lo cual solucionarlo habría supuesto mucho trabajo y tiempo mal invertido y aprovechado.

  Cada requisito se ha referenciado a cada punto del enunciado con la finalidad de poder facilitar al cliente la validación de estos más rápidamente y generar en el cliente la sensación de que el proyecto cumple con los objetivos.

- El diseño conceptual forma una parte importante del proyecto ya que ha permitido dar la forma final a esta memoria y en definitiva a esta **BD** que desde el punto de vista informático cubre con las expectativas requeridas en el dosier entrega inicialmente y a su vez con los requisitos esperados.

  Todas las decisiones que se han ido tomando han permitido poder llegar finalmente al diseño lógico y físico que en general considero que son los dos diseños muy estándar y no han cambiado mucho en exceso el modelo final.

El problema de los retrasos que he tenido con respecto a la planificación ha sido el excesivo trabajo que he tenido y sobre todo a una optimista planificación.

Por último, creo que he cumplido con todos los objetivos del proyecto, el diseño del repositorio estadístico creo que permite incluir nuevos indicadores, de iguales

características a los actuales, sin tener que modificar en exceso el diseño de la estructura de este.

He tenido que aplazar algunas de las entregas programadas y gracias a la paciencia de mi tutor de sus observaciones que ha realizado en ellas, me ha permitido a mi juicio realizar un buen trabajo ya que creo que cumple con las expectativas requeridas. He aplicado los consejos que me ha dado mi tutor durante todo este tiempo y creo que ese objetivo se ha conseguido.

Toda la metodología utilizada ha seguido el programa inicial del proyecto. El concepto inicial ha sido el adecuado y el diseño creo que acertado ya que gracias a la validación inicial de los requisitos del proyecto el diseño conceptual ha sido fiel reflejo de estos, los cambios que se han realizado se han intentado que fueran los mínimos y creo que atienden, fundamentalmente a todas las sugerencias de mi tutor.

4. Glosario

BD: Abreviatura de **"Base de Datos".**

Primary Key: Conjunto de atributos que identifican unívocamente cada tupla de cada tabla.

Foreing Key: Atributos que coinciden y se identifican con una clave primaria de otra tabla la cual tiene relación.

Atributo: Aquella unidad básica de información que se encuentra dentro de una entidad o relación.

Campo: Es equivalente al atributo. Forma parte del diseño físico de la **BD**. Constituye una propiedad de la tabla de la **BD**.

Entidad: Es la representación del concepto sobre los que se almacena información. Diseño conceptual.

Disparador: (Trigger) Es un objeto que se asocia con tablas y se almacena en la base de datos.

Procedimiento almacenado: Corresponde a un programa almacenado físicamente en la base de datos. Su ventaja es que, al ser ejecutado, en repuesta de una petición de usuario, es que es ejecutado directamente en el motor de la base de datos, el cual usualmente corre en un servidor separado.

Relación (diseño conceptual): Se consideran a todas las relaciones establecidas entre entidades dentro del diseño conceptual.

Relación (diseño físico): A toda la estructura formada por filas y columnas que almacenan toda la información referente a una entidad o relación conceptual.

Tabla: Toda estructura formada por filas y columnas que permiten sintetizar, comparar e interpretar de forma sencilla, un conjunto de características que describen el comportamiento de una o más variables.

Tupla: Representa un objeto único de datos implícitamente estructurados en una tabla.

SQL: Abreviatura de lenguaje de consulta de base de datos.

PostgreSQL 14: Es un servidor de base de datos objeto relacional libre, que incluye características de la orientación de objetos, como puede ser la herencia, tipos de datos, funciones, disparadores, bajo la licencia **BSD**.

UML: Fue creado para forjar un lenguaje de modelado visual común y semántica y sintácticamente rico para la arquitectura, el diseño y la implementación de sistemas de software complejos, tanto en estructura como en comportamiento.

SGBD: Abreviatura de Sistema de Gestión de Bases de Datos.

RRHH: Abreviatura del departamento de cualquier empresa de Recursos Humanos.

5. Bibliografía

- Libro: Jordi Casas Roma, Introducción al diseño de la base de datos, material de la UOC.

- Libro: Jordi Casas Roma, Diseño conceptual de las bases de datos, material de la UOC.

- Libro: Xavier Burgués Illa, Diseño Lógico de las bases de datos, material de la UOC.

- Web:https://techexpert.tips/es/windows-es/instalacion-de-postgresql-en-windows/ está Web fue visitada el 19/02/22.

- Web:https://elbauldelprogramador.com/bases-de-datos/ esta Web fue visitada 29/05/22.

- Web:https://www.tutorialesprogramacionya.com/postgresqlya/ esta Web fue visitada 24/04/22.

- Web:https://es.wikipedia.org/wiki/Desarrollo_en_cascada esta Web fue visitada en 25/03/22.

- Web:https://es.wikipedia.org/wiki/Modelo_conceptual#:~:text=Un%20modelo%20conceptual%20es%20una,es%20un%20conjunto%20de%20conceptos esta Web fue visitada en 04/05/22.

- Web:https://es.wikipedia.org/wiki/Modelo_de_base_de_datos esta Web fue visitada en 15/04/22.

- Web:https://ayudaleyprotecciondatos.es/bases-de-datos/modelos/ esta Web fue visitada en 18/03/22.