PROYECTO DE TRABAJO DE GRADO

AUDITORÍA DE LA BASE DE DATOS DE SEGURIDAD SOCIAL DE LA EMPRESA INVERSIONES ALCABAMA S.A.

NIDIA STELLA BELTRAN CAMACHO

LUZ ADRIANA BAUTISTA CARDENAS

UNIVERSIDAD CATÓLICA DE COLOMBIA

FACULTAD DE INGENIERÍA

PROGRAMA DE ESPECIALIZACIÓN EN AUDITORIA DE SISTEMAS DE INFORMACIÓN

BOGOTÁ D.C _ JUNIO _ 2019

AUDITORÍA DE LA BASE DE DATOS DE SEGURIDAD SOCIAL DE LA EMPRESA INVERSIONES ALCABAMA S.A.

NIDIA STELLA BELTRAN CAMACHO

LUZ ADRIANA BAUTISTA CARDENAS

Trabajo de grado para obtener el título de especialista en Auditoría de Sistemas de Información.

Asesor: **ING. ESP. M.Eng. JAIRO ALEJANDRO BUITRAGO ROMERO**

UNIVERSIDAD CATÓLICA DE COLOMBIA

FACULTAD DE INGENIERÍA

PROGRAMA DE ESPECIALIZACIÓN EN AUDITORÍA DE SISTEMAS DE INFORMACIÓN

BOGOTÁ D.C, JUNIO 2019

Nota de aceptación

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

_____

Dedicatoria

Dedico este trabajo de grado a Dios en primera instancia. Agradezco inmensamente a mi hija, esposo, padres y hermanos por el apoyo y comprensión que me han brindado siempre para alcanzar mis metas, a los profesores gracias por compartir su experiencia, conocimiento y enseñanzas y a mis compañeros por los buenos momentos que caracterizaron la unión de un bonito grupo de especialización. Agradezco a la vida el permitirme alcanzar una meta más en pro de mi crecimiento profesional, mi bienestar y el de mi familia.

Ing. Nidia Stella Beltrán Camacho

Universidad Católica de Colombia

Este trabajo de grado se lo dedico en primera medida a Dios que me dio la fuerza para recorrer este camino y cumplir con el objetivo. Lo dedico también a mi familia que me apoyó incondicionalmente durante todo el proceso. A mis amigos que siempre me dieron ánimos para avanzar en el camino.

Ing. Luz Adriana Bautista Cárdenas

Universidad Católica de Colombia

Agradecimientos

Agradezco a Dios por permitirme alcanzar esta meta que años atrás me propuse realizar, dándome su bendición y rodeándome de personas especiales que me dieron ánimos y fuerza para continuar, a las personas que son mi razón, mi hija, mi esposo , mis padres y hermanos por su apoyo incondicional, por estar siempre hay con su comprensión. A mis compañeros por los momentos de alegría, y a los profesores que compartieron su conocimientos y experiencia.

Ingeniera Nidia Stella Beltrán Camacho

Universidad Católica de Colombia

Agradezco a Dios por darme la oportunidad de vivir esta experiencia y permitirme crecer profesionalmente dando un paso más en mi carrera. Agradezco a todos los ingenieros que hicieron parte del proceso compartiendo su amplio conocimiento y experiencia como auditores, por su esfuerzo y dedicación en hacer de nosotros parte de ese grupo de expertos. Agradezco inmensamente a mi amigo Cesar Cruz, quien me brindó todo su apoyo y colaboración durante este año para hacer que este proyecto fuera posible. A mis compañeros y ahora amigos, un grupo de increíbles personas que le dieron el toque alegre a cada sesión de clase.

Ing. Luz Adriana Bautista Cárdenas

Universidad Católica de Colombia

Tabla de Contenidos

Lista de Figuras

Lista de Tablas

Resumen

Las empresas en la actualidad independientemente sea su CORE de negocio, deben implementar en sus procesos la identificación y Gestión de Riesgo, esto ayuda en gran medida a que las compañías estén preparadas para las amenazas que pueden existir en el ambiente. Pero para las organizaciones protegerse de estas amenazas debe tener controles eficaces que mitiguen la materialización de estos riesgos. La auditoría se realiza como un mecanismo para evaluar la eficiencia y efectividad de estos controles. Los sistemas de información son los activos más valiosos para una compañía, de su correcta gestión depende en gran medida la información de sus trabajadores, proveedores y procesos.

Para el desarrollo de este proyecto se realizará un levantamiento de riesgos de la gestión de la BD, se evaluarán estos riesgos para detectar los más críticos y de este proceso, se realizará la auditoria para comprobar la efectividad de los controles aplicados a los riesgos detectados como críticos. Esto con el objetivo de mitigar estos riesgos y que no afecten la normal operación de la organización, en este caso de la BD de Seguridad Social de la empresa inversiones Alcabama S.A., para esto se basara la auditoria en las buenas prácticas de la Norma IIA.

Se llevara a cabo todo el proceso realizado en la auditoria basada en riesgos, para lo cual se realiza una Matriz de Riesgos, se evalúan estos de acuerdo al impacto y la probabilidad, y de acuerdo a su calificación se detectan los más críticos, en los cuales nos enfocaremos para realizar la auditoria de los controles aplicados a estos riesgos, para lo cual se realizaran pruebas a la efectividad de los controles, y se dará un informe de los hallazgos y recomendaciones realizadas para mejorar la efectividad de estos.

Palabras clave: Riesgos, Normas IIA, controles.

Abstract

Companies currently are their business CORE, they must implement in their processes the identification and Risk Management, this helps to a large extent as companies prepared for the responses that may exist in the environment. But for organizations protected from these threats they must have effective controls that mitigate the materialization of these risks. The audit is performed as a mechanism to evaluate the efficiency and effectiveness of these controls. The information of its workers, suppliers and processes.

For the development of this project, it is evaluated, evaluated, evaluated, evaluated, analyzed, analyzed, analyzed, analyzed, analyzed, analyzed, analyzed, analyzed, analyzed, critics This has the objective of mitigating these risks and not affecting the normal operation of the organization, in this case, the social security of the company Alcabama SA investments, for this the audit is based on the good practices of the Standard IIA.

The whole process was carried out, a risk audit was carried out, an assessment of the risks was carried out, these aspects were evaluated according to the impact and the probability, and according to the rating the most critical were detected, in the are the efforts to perform the audit of the controls applied to these risks, for which a test of the controls of the controls is carried out, and the report of the findings and the recommendations to improve the effectiveness of these.

Keywords: Risks, IIA Standards, controls.

Introducción

En la actualidad, la información que se produce alrededor del mundo crece exponencialmente, siendo generada por diversos medios como redes sociales, medios de comunicación, aplicaciones web entre otros; esta información se almacena en medios de almacenamiento, bases de datos alojadas en la nube o en servidores, pero ¿qué tan segura se encuentra la información? ¿Qué riesgos tiene esa información de ser consultada por terceros? son algunas de las preguntas que se generan, no solo dentro de una empresa, sino cualquier persona que genere datos confidenciales cada día.

Cuando el medio en el que se almacena la información no cuenta con los suficientes protocolos de seguridad, la confidencialidad, integridad y disponibilidad de la información queda expuesta, las vulnerabilidades de un sistema, abren puertas traseras a intrusos para que manipulen la información provocando daños irreparables a una organización.

Dado que la información es el activo más importante para una empresa, el medio en el que se encuentre almacenada debe garantizar total confidencialidad y disponibilidad al usuario; para esto es necesario realizar auditorías por medio las cuales se realice una evaluación de vulnerabilidades por medio de un procedimiento planeado, que detecte los riesgos a los que se encuentre expuesta y permitan mitigarlos a fin de protegerla.

Para este proyecto de investigación se presenta el procedimiento y los pasos que se llevarán a cabo para realizar la identificación y valoración de riesgos en la BD de seguridad social de la empresa Inversiones Alcabama S.A. La identificación de dichos riesgos se realizará mediante la aplicación de una entrevista al DBA que se elaborará basada en estándares, se presentarán las evidencias y se documentaran todas las pruebas y evaluaciones de controles aplicadas, los cuales

una vez detectados son el insumo para la construcción de un informe final de auditoria, en el cual se registran los hallazgos, riesgos detectados, evaluación de controles y recomendaciones.

Las recomendaciones se establecerán de acuerdo con el análisis de los datos obtenidos, mediante las evidencias recolectadas de las pruebas realizadas, dicho análisis se plasmará en un documento de recomendaciones para solucionar o reducir las vulnerabilidades de la BD.

Para describir el proceso de investigación, este documento está organizado de la siguiente manera: en el primer capítulo se realiza la descripción del problema a resolver, se dará una justificación de por qué se realiza este proyecto y se establecen los objetivos a cumplir con el desarrollo del mismo. En el segundo capítulo se hará una conceptualización de términos relacionados con BD a nivel general y específicamente Seguridad Social, términos que ayuden al lector a comprender el tema, dentro del marco teórico se explicará con mayor profundidad todo lo relacionado con Auditoria, pasando de lo general a lo específico, seguido a esto encontraremos las leyes y normatividad que rigen la auditoría y aquellas que estén estrechamente ligadas al tema del proyecto, y para cerrar el capítulo se encuentra el estado del arte. En el tercer capítulo se encontrará el planteamiento de la metodología de trabajo, en el cuarto capítulo se encontrarán los productos a entregar, el capítulo cinco se conformará de Resultados esperados e impactos del proyecto en donde se ejecutará toda la metodología y se documenta el informe de auditoría en el cual se plasmarán los hallazgos y recomendaciones el capítulo seis incluye las Nuevas Áreas De Estudio y para finalizar en el capítulo siete conclusiones de la investigación.

1 Generalidades

1.1 Línea de Investigación

De acuerdo al enfoque en el que se enmarca el presente proyecto y teniendo en cuenta la línea de investigación "**Software inteligente y convergencia tecnológica**" adscrita a la facultad de ingeniería y avalada por la Universidad Católica de Colombia, se toma esta como referencia, toda vez que permita indagar acerca del problema planteado y a su vez, dar solución a este evaluando los posibles escenarios tecnológicos que conlleven a generar una mejora en el proceso creando un resultado con calidad.

1.2 Planteamiento del Problema

En la actualidad las compañías se ven en la obligación de tener un correcto almacenamiento y protección de sus datos, esto implica que deban implementar auditorias periódicamente que les permitan garantizar que existen controles y procedimientos y que estos se utilizan correctamente, para de esta manera, tener los datos protegidos contra incidentes que afecten la triada de la seguridad de la información.

En las compañías, la información es la parte más sensible e involucra información de terceros la cual debe tener una correcta custodia en los sistemas de información, esto debido a que cuando una compañía no maneja procedimientos, políticas y controles adecuados, se ve expuesta a problemas de información errada, fuga de información confidencial o pérdida de información, como es el caso de Alcabama en dónde un ataque informático ocasionó no solo pérdidas de información sino también pérdidas económicas.

El ataque ocasionó la pérdida de los datos de proveedores del periodo comprendido entre

los años 2014 a 2017, el volumen de información perdida fue de aproximadamente 6 Gb comprendiendo archivos y cuentas bancarias. El servidor dedicado al almacenamiento de información comercial, contaba al momento con una capacidad de 2 Tb del cual se realizó un backup el día anterior, posterior al restablecimiento de este backup el resultado de la perdida de información fue de 500 Mb. Adicional se perdió toda la información almacenada en el servidor de correo electrónico.

El impacto económico generado a la compañía fue de $250’000.000 aproximadamente, cifra que comprende un día laboral de todo el personal de oficina (80 personas) y 30 horas continuas de trabajo del personal de IT (3 personas) en el restablecimiento de la operación normal del negocio.

La falta de actualización en el servidor de Windows Server y del antivirus, dejaron expuestas las bases de datos a cuantiosas pérdidas, lo que hace necesaria la aplicación de procedimientos, políticas y controles, los cuales deben ser verificados y se utiliza la auditoria como medio para realizar este análisis y a partir de estos dar recomendaciones para tener adecuados controles que permitan mitigar riesgos que afecten la confidencialidad, disponibilidad e integridad de la información.

1.2.1 Antecedentes del problema.

A través del tiempo las bases de datos (BD, por sus siglas en español) se han convertido en una herramienta indispensable para el almacenamiento de información, siendo un elemento fundamental para cualquier organización que desee salvaguardar sus datos y los de sus clientes. Desde el principio, las BD fueron pensadas dada la necesidad de almacenar grandes cantidades de

datos y con el propósito de permitir la consulta y generación de información relevante para las organizaciones, debido al volumen de los datos en mención. La anterior afirmación conlleva a analizar los posibles riesgos que se presentan al interior de una organización y que acarrean la perdida de información, u otros problemas que impactan directamente el negocio. Las bases de datos se han constituido como uno de los activos fijos más importantes de la organización, por tanto, se ha incrementado la necesidad de proteger tales repositorios ante cualquier eventualidad que pueda alterarlos.

En este punto se hace referencia a vulnerabilidades de seguridad, ataques o virus que comprometen los datos total o parcialmente. A nivel general se encuentran casos de ataques relacionados con pérdida de información vital para diversas compañías (Redacción APD, 2018); casos en los cuales se han comprometido temas económicos, de confiabilidad e imagen. Uno de los ataques recientes y que generó más de 1.445.000 víctimas a nivel mundial (20minutos, 2017) fue el Ransomware cuyo objetivo es secuestrar los datos de los usuarios y pedir un rescate por estos. Según informe generado por ESET, una compañía de ciberseguridad, algunas de las "familias" de Ransomware, afectaron en América Latina siendo Colombia el país más afectado con un 30% de amenazas detectadas. (Bilic, 2019)

Figura 1 Detecciones de FileCoder en Latinoamérica durante 2018

Nota: Tomado de internet. https://www.welivesecurity.com/la-es/2019/01/04/paises-mas-afectados-ransomware-latinoamerica-durante-2018/

En Colombia se reportaron aproximadamente 20 empresas, de las cuales no se conoce su nombre, infectadas por el virus WannaCry que se dio por el WanaCrypt0r que cifra archivos del disco duro y pide rescate. (El colombiano, 2017)

Indica la Dijin que este evento se da por no tener actualizado el sistema operativo y da algunas recomendaciones para evitar contagios de este tipo dentro de las empresas, estas recomendaciones incluyen: tener backups de la información, actualizar los sistemas operativos, evitar abrir archivos adjuntos o dar clic sobre links en correos de remitentes desconocidos y no compartir información personal o financiera por correo electrónico, teléfono, mensajes de texto o redes sociales (El colombiano, 2017). Un tipo especial de Ransomware tiene como objetivo principal atacar las Bases de Datos, el Cerber que trabaja del mismo modo que WannaCry, cifra la base de datos para después pedir un rescate por esta. Este tipo de virus aprovecha la falta de

actualización de los sistemas operativos para atacar y perjudicar a los usuarios. (Medina, 2016)

Dentro de la organización del caso de estudio de la presente investigación, en hechos recientes, se evidenció la falta de seguridad en la protección de los datos, la empresa fue víctima de un ataque por medio de la red al servidor. Este ataque fue de tipo ransomware el cual ocasionó pérdida de información sensible de las bases de datos de la compañía. Las medidas de prevención que se tomaron para mitigar ese ataque fueron:

- Apagar el servidor y desconectar todos los equipos en red para que el virus no se propague.
- Realizar análisis a todos los equipos con antivirus.
- Instalar parches de seguridad de Windows y adquirir una licencia de un antivirus que puede mitigar ese tipo de ataques

1.2.2 Pregunta de investigación.

¿Qué recomendaciones se realizaron a la entidad Inversiones Alcabama luego de una auditoria basada en riesgos?

1.3 Justificación

ALCABAMA S.A. es una empresa dedicada a la promoción, gerencia, construcción y venta de proyectos inmobiliarios, cuyo propósito es el de generar crecimiento, satisfacción y confiabilidad a sus clientes, al igual que a su equipo de colaboradores y accionistas. Cuidar de cada detalle relacionado con el negocio es parte fundamental de la organización, es por esto que

ALCABAMA cuida de los datos de sus clientes, colaboradores y asociados, basándose en la Ley 1581 de 2012 y el Decreto 1377 de 2013, para el tratamiento de la información de los datos personales, todo esto en busca de una mejora continua, implementando seguridad y controles para proteger toda su información. Es por esto que llevar un control estricto en cuanto al proceso, almacenamiento y seguridad de dicha información, se convierte en una tarea indispensable de realizar, llevando a cabo una revisión y evaluación de los sistemas que procesan la información de forma automática y no automática.

Debido al ataque presentado en el 2018, se decide realizar una auditoría basada en riesgos a la BD se seguridad social de la empresa ALCABAMA S.A., dado que esta BD maneja información sensible de los empleados, esta auditoria se realiza con el objetivo de identificar los riesgos que afectan la seguridad de los repositorios de información de la empresa, evaluar su nivel de impacto enfocado a aquellos que tienen mayor riesgo y de esta manera evaluar la efectividad de los controles establecidos, además de esto, dar a conocer a la compañía el estado actual de la seguridad que maneja la BD y dar recomendaciones que sean posibles de implementar para mejorar la seguridad y así disminuir la probabilidad de futuros ataques.

La necesidad surge a partir del incidente de seguridad presentado en la organización, incidente en el cual se perdieron datos como información de proveedores y correos electrónicos. En términos de porcentajes, la información perdida corresponde a:

- Global (30%) "Todos los servidores"

- Local "Servidor" (70%)

En términos económicos se evalúa 1 día de trabajo por cada colaborador ya que, tras detectarse el incidente, todas las labores en oficina fueron suspendidas toda la jornada y el personal de sistemas se vio forzado a trabajar aproximadamente 30 horas consecutivas para restaurar la

operación normal de la empresa. La consecuencia de perder información de los proveedores fue tener que llamarlos uno a uno para recuperar datos personales, lo que también implicó tiempo de los trabajadores en realizar esta tarea.

Dentro de las pérdidas económicas se tiene en cuenta el valor de la BD de SS la cuál es objetivo de esta investigación, esta BD y su respectiva aplicación se encuentran avaluadas en $180 millones los cuales incluyen:

- Tiempo trabajado (Desarrollador)
- Tiempo trabajado (Administradores del sistema)
- Datos registrados
- Calidad de los datos registrados (Cedulas, Nombres, Direcciones, Correo, información familiar, ingresos de personal)
- 3 meses de desarrollo del sistema
- 2 meses de soporte
- 2 meses de corrección de Bugs (Desarrollador)
- Administrador del sistema 2 años ingresando la información
- La BD incluye información de trabajadores, contratistas, aportes a SS con documentos

1.4 Objetivos

1.4.1 Objetivo general.

Elaborar la auditoria a la base de datos de Seguridad Social de la empresa Inversiones Alcabama S.A.

1.4.2 Objetivos específicos.

- Identificar políticas y procedimientos establecidos en la compañía para el control de la base de datos de Seguridad Social de la empresa Inversiones ALCABAMA S.A.
- Reconocer el estado actual de la base de datos, identificando la aplicación de políticas y procedimientos de la compañía para el control de la base de datos de Seguridad Social de la empresa Inversiones ALCABAMA S.A.
- Determinar las pruebas que se van a realizar a los controles seleccionados.
- Probar la correcta aplicación de los controles identificados a la base de datos.
- Elaborar un reporte de auditoría en dónde se propongan recomendaciones para mejorar la seguridad de la base de datos de la organización ALCABAMA.

2 Marcos de referencia

2.1 Marco conceptual

En esta parte, se darán a conocer los conceptos relacionados al eje principal de esta investigación, para que el lector se familiarice con el tema y pueda comprender de la mejor manera lo que se pretende exponer.

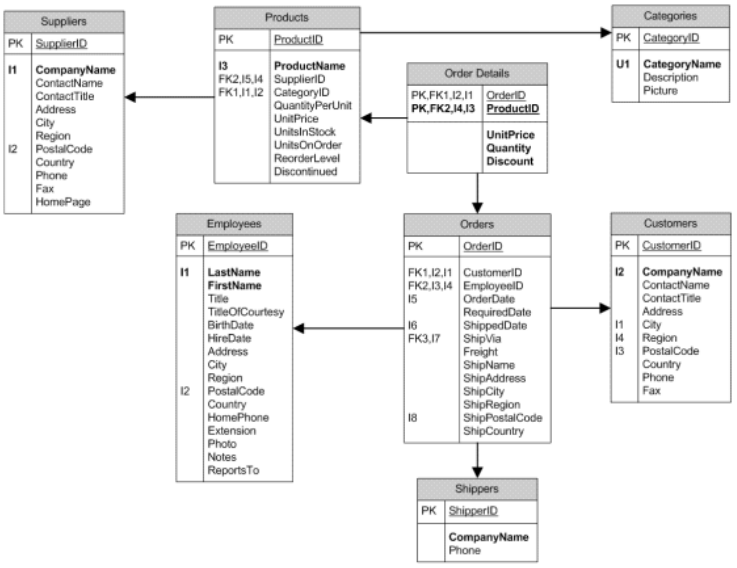
2.1.1 Base de Datos.

Como ya se había mencionado al inicio de este documento, se define Base de Datos como una colección de datos organizada de tal manera que permita la consulta y actualización de datos en el momento en que se requiera (Rouse, 2015).

Para Cisneros (1998), "Una BD es un recipiente en dónde se almacena la información" (p24).

Las BD se clasifican con base en diversos criterios como el tipo de contenido o el enfoque organizativo. En esta clasificación el más frecuente es la BD relacional, "una base de datos tabular en la que los datos se definen de manera que puede ser reorganizada y se accede en un número de maneras diferentes" (Rouse, 2015). En la figura 2 se ve la implementación de una BD relacional en un Diagrama Entidad/Relación o Modelo Conceptual, conformado por una serie de tablas y sus relaciones entre estas, conocido como Modelo Lógico.

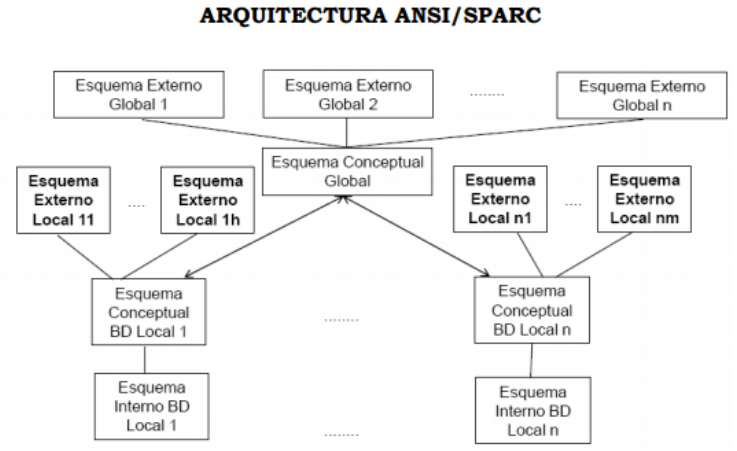
Figura 2 Diagrama Entidad/Relación



Nota: Tomado de internet. https://sites.google.com/site/alexanderchasit2/capitulo-1-diseno-de-base-de-datos-relacionales/1-3-elaboracion-de-modelos-relacionales-de-bases-de-datos-de-manera-tecnica-utilizando-una-herramienta-de-diseno-de-base-de-datos

Dentro del enfoque organizativo también se encuentran las BD Distribuidas, este tipo de BDs son dispersas o replicas entre diferentes puntos de una red.

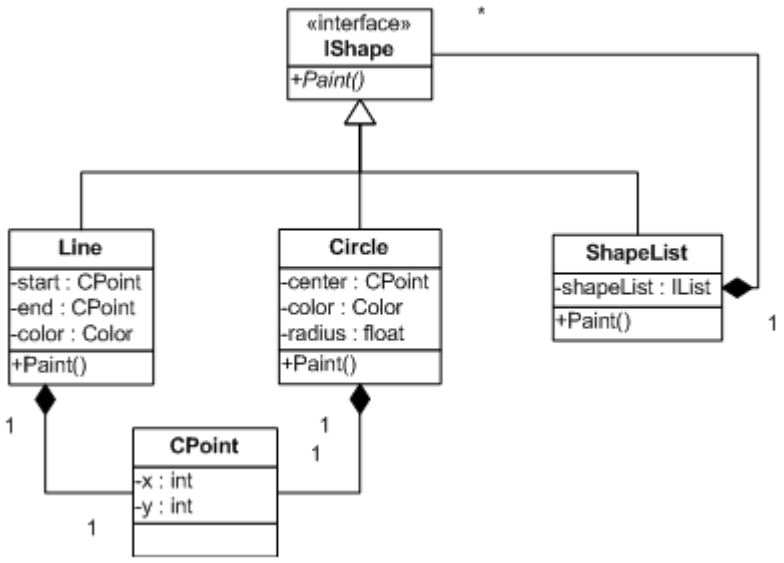
Figura 3 Arquitectura de una BD Distribuida



Nota: Tomado de internet. http://repositorio.utn.edu.ec/bitstream/123456789/522/6/04%20ISC%20151%20CAPITULO%20IV.pdf

Un tercer enfoque organizativo de las BD son las Orientadas a Objetos, las cuales son “congruentes con los datos definidos en clases y subclases de los objetos” (Rouse, 2015).

Figura 4 Modelo Orientado a Objetos



Nota: Tomado de internet. https://ferestrepoca.github.io/paradigmas-de-programacion/poo/poo_teoria/applications.html

2.1.2 Seguridad Social.

Son aquellas normas y procedimientos definidos por la ley y conformado por los regímenes generales establecidos para pensiones, salud, riesgos laborales, subsidio familiar y los servicios sociales complementarios que se definen en la ley (MINTRABAJO, 2019).

2.1.2.1 Sistema de seguridad social en Colombia.

Este sistema fue instituido por la Ley 100 de 1993, conformado por entidades, normas y procedimientos a los que tiene acceso toda la comunidad para garantizarles una

óptima calidad de vida. La Seguridad Social es un servicio obligatorio a cargo del estado y prestado por entidades públicas y privadas. (DNP, 2019)

El Sistema de Seguridad de acuerdo con la Ley 100, se compone de Sistema de Pensiones, salud, riesgos laborales y servicios sociales complementarios.

- **Sistema General de Pensiones:** "Garantiza a la población, el amparo contra las contingencias derivadas de la vejez, la invalidez y la muerte, mediante el reconocimiento de las pensiones y prestaciones determinadas en la Ley 100 de 1993" (DNP).
- **Sistema General de Seguridad Social en Salud: "**Regula el servicio público esencial de salud y crea condiciones de acceso al servicio a toda la población, en todos los niveles de atención. Es operado por las Entidades Promotoras de Salud (EPSs) y la prestación del servicio está a cargo de las Instituciones Prestadoras de Servicios de Salud (IPSs)" (DNP).
- **Sistema General de Riesgos Laborales:** "Conjunto de entidades públicas y privadas, normas y procedimientos, destinados a prevenir, proteger y atender a los trabajadores de los efectos de las enfermedades y los accidentes que puedan ocurrirles con ocasión o como consecuencia del trabajo que desarrollan" (DNP).
- Servicios **Sociales Complementarios. (Colombia mayor): "**Busca proteger a las personas de la tercera edad que se encuentran desamparadas, no cuentan con una pensión o viven en la indigencia y/o en extrema pobreza" (DNP).

2.1.2.2 *Sistema de seguridad social de la empresa Inversiones Alcabama.*

En la empresa inversiones Alcabama el sistema que maneja la seguridad social es el Sistema de Control de Afiliaciones el cual se encuentra enfocado en contratistas. Este

sistema se encuentra estructurado como muestra la Tabla 1:

Tabla 1 Estructura del sistema de Control de Afiliaciones

Módulos	Submódulos	Descripción
Registro y control	Información	Describe la función del módulo y una breve guía de como ingresar la información en este.
	Registrar Personal	Formulario de registro de nuevos trabajadores.
	Listado	Listado de personal activo e inactivo de las obras
	Documentos	Control de la documentación referente a afiliaciones
Traslados	información	Listado de personal activo e inactivo de las obras
	Contratista - obra	Contiene el formulario de traslados por contratista
Liquidador	Información	Describe la función del módulo y una breve guía de como ingresar la información en este.
	Archivo Planillas	Formulario para cargar los días a reconocer
	Planillas	Cargar y buscar planillas
	Planillas guardadas	Registro de planillas guardadas en el sistema
	Planillas Re liquidadas	Registro de planillas Re liquidadas
Informe	Informe general	Generador de informe general de liquidación
Director de obra	Información	Describe la función del módulo y una breve guía de como ingresar la información en este.
	Jornales	Control de planillas de jornales
Administración	Información	Describe la función del módulo y una breve guía de como ingresar la información en este.
	Beneficios contratistas	Permite mantener actualizada la información acerca de los beneficios que tiene cada contratista como son: por EPS, AFP, ARL, Caja de Compensación
	Actividades contratistas	Permite consultar, agregar y o modificar de forma rápida las actividades asociadas a los contratistas. Para editar un registro solo debe hacer clic en el nombre de la actividad.
	Frentes de trabajo	En esta opción puede consultar, agregar y o modificar de forma rápida frentes de trabajo. Para editar un registro solo debe hacer clic en el nombre del frente.

Usuarios	Información	Describe la función del módulo y una breve guía de como ingresar la información en este.
	Usuarios	Listado de usuarios registrados en el sistema
	Perfiles	Creación y listado de perfiles de usuario

Nota: Elaboración propia basado en los módulos de la aplicación de Seguridad Social de la empresa

El sistema no cuenta al momento con un manual técnico.

2.1.2.2.1 Perfiles y tipos de usuario.

Tabla 2 Perfiles y tipos de usuarios

Perfil	**Descripción**
Administración De Campos	Administración De Campos
Administrador	Permite Administrar Todos Los Módulo De La Aplicación
Contratista	Contratista
Director De Obra	Cargar Planillas De Jornales
Liquidación	Planillas
Registro Planillas	Registrar Planillas De Seguridad Social
Sst	Siso

Nota: Elaboración propia basada en la aplicación de Seguridad Social de la empresa

2.2 Marco teórico

Para comprender como detectar vulnerabilidades en una BD por medio de una auditoría, primero hay que entender el concepto de auditoría a BD, así como el funcionamiento de esta en un sistema de información. Al familiarizarse con los conceptos, el auditor puede evaluar de manera eficiente, la raíz del problema además de identificar los riesgos detectados y realizar recomendaciones para mitigar los mismos.

2.2.1 Auditoria de sistemas.

Una auditoría de sistemas, es un proceso que permite evaluar normas, controles, técnicas y procedimientos para garantizar la confiabilidad, oportunidad, seguridad y confidencialidad de la información almacenada y procesada en equipos de cómputo. (Alzate, 2001, pág. 9)

La auditoría informática debe evaluar tanto los equipos de cómputo en los que es almacenada la información sino también los sistemas de información y las operaciones que en estos se efectúan, como entradas, procedimientos, controles, archivos, seguridad y obtención de información. (Alzate, 2001, pág. 19)

Al realizar una auditoría de sistemas de información, el auditor debe considerar el efecto de los sistemas de información por computador, en una auditoría.

La auditoría informática cumple con los objetivos de una auditoria:

- Protección de activos e integridad de datos.
- Objetivos de gestión de protección de activos y eficacia y eficiencia

(Rodriguez, 2004).

2.2.1.1 Tipos de auditoria de sistemas.

La auditoría de sistemas se puede clasificar por tres tipos de criterios: Área de Aplicación Tabla3, Lugar de Origen Tabla 4 y Área de Especialización Tabla 5.

Tabla 3 Auditorías por Área de Aplicación

Área de Aplicación	
Financiera	Revisión de los estados financieros de una empresa o persona jurídica en base a unas normas establecidas (Pérez, 2018).
Administrativa	"Revisión analítica total o parcial de una organización con el propósito de precisar su nivel de desempeño y perfilar oportunidades de mejora para innovar valor y lograr una ventaja competitiva sustentable" (Franklin, 2007, pág. 20).
Operacional	"El auditor, por iniciativa propia, extiende su examen hacia aspectos que no tienen ya el propósito de verificar los estados financieros sino de darse una idea de la eficiencia con que se está administrando una o varias áreas de la empresa, a fin de ampliar su servicio y hace más útil su intervención" (Anguiano, 2005, pág. 20).
Integral	"Es el proceso de obtener y evaluar objetivamente, en un periodo determinado, evidencia relativa a la información financiera, la estructura del control interno financiero, el cumplimiento de las leyes y regulaciones pertinentes y la conducción ordenada en el logro de las metas y objetivos propuestos" (Luna Y. B., 2012, pág. 20).
Gubernamental	"Es el examen objetivo, sistemático y profesional de las operaciones financieras y/o administrativas, efectuando con posterioridad a su ejecución, en las entidades sujetas al Sistema Nacional de Control, elaborando el correspondiente informe" (Luna O. F., 2007, pág. 20).
Informática	Es el proceso de recoger, agrupar y evaluar evidencias para determinar si un sistema informatizado salvaguarda los activos, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización y utiliza eficientemente los recursos (Piattini & Pesso, 2001).

Nota: Elaboración propia adaptado de la información tomada de internet https://www.mindmeister.com/es/745044994/clasificaci-n-de-tipos-de-auditoria-en-sistemas?fullscreen=1

Tabla 4 Auditorías por Lugar de Origen

Lugar de Origen

Interna	"Una actividad independiente y objetiva de aseguramiento y consulta, concebida para agregar valor y mejorar las operaciones de una organización" (Iturriaga, Contreras, & Villavicencio, 2017, pág. 11).
Externa	"Es efectuada por personal externo a la empresa en donde examina y evalúan sus operaciones, para emitir una opinión veraz y técnica del sistema de control que se está desarrollando en esa área" (Lozano, 2014).

Nota: Elaboración propia adaptado de la información tomada de internet https://www.mindmeister.com/es/745044994/clasificaci-n-de-tipos-de-auditoria-en-sistemas?fullscreen=1

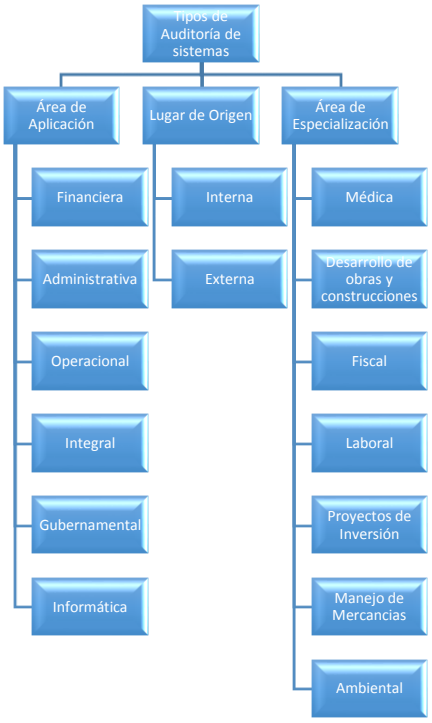
Tabla 5 Auditorías por área de Aplicación

Área de Especialización	
Médica	"Proceso de evaluación continuo, sistematizado y objetivo de la atención médica con base en el análisis crítico de la historia clínica, cuya finalidad es controlar la calidad de la atención en salud, contribuir de manera continua en la educación de los profesionales de la salud y emular la excelencia profesional" (Malagón-Londoño, Morera, & Laverde, 2003, pág. 167).
Desarrollo de obras y construcciones	"Conjunto de procedimientos técnicos que se aplican a un ente público o privado, con el fin de verificar el cumplimiento de la normatividad a que este se encuentra sujeto" (Estrada, 2003).
Fiscal	Auditoría realizada por la Administración Tributaria en orden a determinar las responsabilidades pecuniarias de los contribuyentes (Navarro, 2006, pág. 149).
Laboral	"Realizada por un profesional calificado e independiente, consistente en analizar, mediante la utilización de las técnicas de revisión y verificación idóneas, la adecuación de una empresa los principios y normas Socio Laborales que le son de aplicación a partir de los documentos examinados y la realidad de las conductas observadas" (Cañar, 2011).

Proyectos de Inversión	"Es la acumulación y examen objetivo, sistemático e independiente de evidencia con el propósito de expresar una opinión sobre el desempeño de todo o parte de un proyecto de inversión pública y/o de la entidad gestora del mismo" (Contraloría General de Estado Bolivia, 2006).
Manejo de Mercancías	Espinoza y Lozada (como citaron en (Delgado & Naranjo, 2015)) "Es un examen crítico e imparcial de la administración de una empresa, para determinar la eficacia con la que se logran sus objetivos establecidos y la eficiencia con la que utiliza y obtiene recursos".
Ambiental	"Conjunto de actividades coordinadas para dirigir y controlar una organización en lo relativo al medio ambiente" (ECA Instituto de Tecnología y Formación, S.A., 2007).

Nota: Elaboración propia adaptado de la información tomada de internet https://www.mindmeister.com/es/745044994/clasificaci-n-de-tipos-de-auditoria-en-sistemas?fullscreen=1

Figura 5 Tipos de Auditoría de Sistemas



Nota: Adaptado de la información tomada de internet https://www.mindmeister.com/es/745044994/clasificaci-n-de-tipos-de-auditoria-en-sistemas?fullscreen=1

2.2.2 Auditoria a bases de datos.

Una auditoría a BD consiste en realizar un seguimiento constante y detallado de los controles establecidos a los sistemas de BD para garantizar la seguridad y el correcto uso de los datos almacenados por los usuarios. El monitoreo y pruebas a los controles determinan la pertinencia y suficiencia de éstos, permitiendo entonces ajustar, eliminar o implementar nuevos controles para asegurar su adecuada utilización. (Murillo, 2006)

Una auditoría a BD permite determinar:

- Quién accede a los datos
- Cuando se accede a los datos
- Desde que tipo de dispositivo o aplicación se accede
- Desde que ubicación en la red
- Cuál fue la sentencia SQL ejecutada
- Cuál fue el efecto del acceso a la BD (Jhon Alexander López, 2013)

2.2.3 Seguridad en bases de datos.

La mayor parte de los datos sensibles alrededor del mundo se encuentran almacenados en BD, para un delincuente esto se convierte un objetivo a atacar. En 2009 los ataques externos por inyección SQL aumentaron un 345%, esto debido a que la mayoría de la información se encuentra almacenada en gestores de bases de datos comerciales. Actualmente cada vez más organizaciones se dedican a proteger las BD de accesos y cambios no autorizados. (Villalobos, 2012)

Existen muchas formas de proteger las BD de una organización. Dentro de los mecanismos de seguridad se encuentra el de la política de control de acceso, la cual se encuentra basada en la identidad del usuario, o la seguridad obligatoria que restringe el acceso a información confidencial. (Dominguez, 2015)

2.2.3.1 Principios básicos de seguridad en bd.

2.2.3.1.1 Identifique su seguridad.

"No se puede asegurar lo que no se conoce" (Villalobos, 2012).

En este punto es necesario identificar la información sensible de las BD, automatizando el proceso de identificación previendo que pueda cambiar dependiendo de diversos casos. Contar con herramientas de identificación que protejan las BD del Malware, colocando en la BD el resultado de los ataques de Inyección SQL. (Villalobos, 2012)

2.2.3.1.2 Evaluación de la vulnerabilidad y la configuración.

Se debe asegurar que no existen huecos de seguridad en la configuración de la BD, desde su instalación y al del sistema operativo, de la misma forma, los archivos con parámetros de configuración y programas ejecutables (Villalobos, 2012).

"Además, es necesario verificar que no se está ejecutando la base de datos con versiones que incluyen vulnerabilidades conocidas; así como impedir consultas SQL desde las aplicaciones o capa de usuarios. Para ello se pueden considerar (como administrador):

- Limitar el acceso a los procedimientos a ciertos usuarios.
- Delimitar el acceso a los datos para ciertos usuarios, procedimientos y/o datos.
- Declinar la coincidencia de horarios entre usuarios que coincidan" (Villalobos, 2012).

2.2.3.1.3 Endurecimiento.

Al finalizar la evaluación de la vulnerabilidad se realizan algunas

recomendaciones, lo que empieza a endurecer la BD. Para continuar con el endurecimiento es necesario eliminar las funciones y opciones que no sean utilizadas. Se debe crear una política clara en la que se establezca lo que es permitido o no hacer, además de mantener desactivado lo que no se necesita (Villalobos, 2012).

2.2.3.1.4 *Audite.*

El siguiente paso es realizar autoevaluaciones y seguimiento a las recomendaciones de auditoría para garantizar la seguridad de la BD. Se debe registrar cualquier cambio que se realice en la BD y generar una alerta cada vez que esto ocurra, para esto se debe automatizar el control de la configuración (Villalobos, 2012).

2.2.3.1.5 *Supervisión.*

Supervisar en tiempo real todas las actividades que se generen en la BD evita que esta quede expuesta, para ello es recomendable contar con agentes inteligentes de monitoreo, detección de intrusiones y uso indebido. La creación de alertas puede informar oportunamente sobre un acceso o cambio no autorizado, un ataque de inyección SQL, cambios en privilegios, etc. (Villalobos, 2012).

"El monitoreo dinámico es también un elemento esencial de la evaluación de vulnerabilidad, le permite ir más allá de evaluaciones estáticas o forenses" (Villalobos, 2012).

2.2.3.1.6 *Pistas de auditoría.*

"Aplique pistas de auditoría y genere trazabilidad de las actividades que afectan

la integridad de los datos, o la visualización los datos sensibles" (Villalobos, 2012).

2.2.3.1.7 Autenticación, control de acceso, y gestión de derechos.

> "No todos los datos y no todos los usuarios son creados iguales. Usted debe autenticar a los usuarios, garantizar la rendición de cuentas por usuario, y administrar los privilegios para de limitar el acceso a los datos. Implemente y revise periódicamente los informes sobre de derechos de usuarios, como parte de un proceso de formal de auditoría. Utilice el cifrado para hacer ilegibles los datos confidenciales, complique el trabajo a los atacantes, esto incluye el cifrado de los datos en tránsito, de modo que un atacante no puede escuchar en la capa de red y tener acceso a los datos cuando se envía al cliente de base de datos". (Villalobos, 2012)

2.2.4 Auditoría basada en riesgos.

Este modelo de auditoría cuenta con elementos de auditoría interna, por lo que es necesario que quién va a realizar la auditoría tenga conocimiento de la organización, esto para identificar fácilmente los riesgos. La auditoría basada en riesgos otorga valor a la organización ya que apoya el alcance de los objetivos empresariales, establecer primacía a los hallazgos además de las recomendaciones necesarias, se mitigan los riesgos y una utilización más objetiva de recursos. (Hernandez, 2018)

2.2.4.1 Características.

Deloitte propone algunas características:

2.2.4.1.1 Priorizar los riesgos relevantes.

- "Desarrolla las diferentes revisiones de conformidad con lo que la organización tiene identificado como riesgos relevantes.
- Todo riesgo relevante debe tener una política, estrategia, límites y estructura clara de cómo la organización lo administra.

- El equipo de auditoría debe concentrar sus horas, revisiones y entendimiento con las áreas de negocio o monitoreo de la entidad, pues en la medida que los riesgos más importantes tengan un mayor control es más probable que la entidad se encuentre entre los límites aceptados". (Actualicese, 2019)

2.2.4.1.2 *Enfoque en procesos.*

- "El mapeo de los procesos críticos de la organización es fundamental previo a la gestión del riesgo operativo.
- En los procesos críticos, desde el punto de vista de continuidad o de impacto, la auditoría debe focalizar sus revisiones, posibles errores o posibles mejoras en el proceso.
- Una auditoría preocupada por ir al detalle de las transacciones y generalmente vinculada a temas estrictamente financieros no es la que predomina". (Actualicese, 2019)

2.2.4.1.3 *Especialización en el negocio.*

- "Planes de auditoría efectivos entienden el funcionamiento de las líneas de negocio y evalúan la integridad de los riesgos, comprendiendo la especificidad y alcance de cada uno, donde la regulación es cada vez más extensa y detallada.
- El enfoque estándar de auditoría que aplicaba las mismas pruebas en cualquier industria dejó de ser efectivo, motivo por el cual los planes de capacitación de los auditores ahora deben estar diseñados para fortalecer el análisis cuantitativo y de datos, la evaluación de metodologías y modelos de gestión". (Actualicese, 2019)

2.2.4.1.4 *Es integral.*

- "Los planes de auditoría deben evaluar la gestión de cada riesgo, o bien de cada proceso crítico desde tres perspectivas: Gobierno, para asegurar que la estructura de roles y responsabilidades funciona; riesgo, para comprender si los tomadores de decisiones siguen la estrategia del riesgo de la organización; y control, para asegurar que las medidas preventivas o mitigadores forman parte de la cultura de todos los colaboradores". (Actualicese, 2019)

2.2.4.1.5 *Genera valor.*

- "El auditor moderno comprende que en sus revisiones el objetivo final no

es encontrar observaciones o darse por satisfecho en cuanto a si las actividades de los procesos están de acuerdo a los procedimientos.

- El auditor también debe preocuparse por entender el negocio para poder generar recomendaciones y valor de alternativas con las que podría mejorarse la gestión de la organización.
- Conservando su independencia, el auditor puede dar recomendaciones o sugerencias de acuerdo a su experiencia". (Actualicese, 2019)

2.2.5 Riesgo.

"El Riesgo, producto de la interrelación de amenazas y vulnerabilidades es, al final de cuentas, una construcción social, dinámica y cambiante, diferenciado en términos territoriales y sociales. Aun cuando los factores que explican su existencia pueden encontrar su origen en distintos procesos sociales y en distintos territorios, su expresión más nítida es en el nivel micro social y territorial o local. Es en estos niveles que el riesgo se concreta, se mide, se enfrenta y se sufre, al transformarse de una condición latente en una condición de pérdida, crisis o desastre". (Humboldt, 2004)

2.2.6 Riesgo tecnológico.

"El riesgo de origen tecnológico puede incidir sobre las metas y objetivos organizacionales y ser causa de otro tipo de riesgos al ser intrínseco al uso de tecnología. Por ello el daño, interrupción, alteración o falla derivada del uso de TI puede implicar pérdidas significativas en las organizaciones, pérdidas financieras, multas o acciones legales, afectación de la imagen de una organización y causar inconvenientes a nivel operativo y estratégico. Una situación que ejemplifica lo mencionado ocurrió en la entidad financiera colombiana Bancolombia, en febrero del año 2011; se presentó una caída de la red del banco lo cual produjo una suspensión en sus operaciones normales, que trajo como consecuencia caos en la atención a usuarios por aproximadamente una hora; lo anterior implicó pérdidas financieras significativas y afectación de la imagen para el banco." (Castro & Bayona, 2011)

2.2.7 Vulnerabilidades.

"La Vulnerabilidad es la condición en virtud de la cual un sujeto, sistema o población está o queda expuesta o en peligro, de resultar afectada por un fenómeno de origen natural, socio – natural o humano, llamado amenaza. También hace referencia a la capacidad de una comunidad para recuperarse de los efectos de un desastre. La vulnerabilidad, debe analizarse frente a las condiciones particulares de cada comunidad o ciudad, y a cada amenaza en particular. Además, la vulnerabilidad debe ser interpretada bajo un enfoque

multidimensional y de proceso (Causa - Efecto)". (Humboldt, 2004)

Las vulnerabilidades pueden ser agrupadas dependiendo del tipo de institución en:

Ambiental, Física, Económica, Social, Educativo, Institucional y Política

(Humboldt, 2004).

2.2.8 Hallazgo de auditoria.

"Resultados de la evaluación de las evidencias de la auditoría frente a los criterios de auditoría" (Pastor, pág. 274).

2.3 Marco jurídico

En este apartado se identifican algunas de las leyes y normas que se relacionan estrechamente con el desarrollo de este proyecto y que regulan las actividades de las personas que intervienen en el, tanto nosotras como ingenieras investigadoras, como la del usuario final del sistema.

2.3.1 Decreto 886 de 2014. Registro nacional de bases de datos.

Capítulo I

"Artículo 2°. Ámbito de aplicación. Serán objeto de inscripción en el Registro Nacional de Bases de Datos, las bases de datos que contengan datos personales cuyo Tratamiento automatizado o manual se realice por personas naturales o jurídicas, de naturaleza pública o privada, en el territorio colombiano o fuera de él, en este último caso, siempre que al responsable del Tratamiento o al Encargado del Tratamiento le sea aplicable la legislación colombiana en virtud de normas y tratados internacionales. Lo anterior sin perjuicio de las excepciones previstas en el artículo 2° de la Ley 1581 de 2012". (Ministerio de Comercio, Industria y Turismo, 2014)

“Artículo 3°. Deber de inscribir las bases de datos. El responsable del Tratamiento debe inscribir en el Registro Nacional de Bases de Datos, de manera independiente, cada una de las bases de datos que contengan datos personales sujetos a Tratamiento” (Ministerio de Comercio, Industria y Turismo, 2014).

2.3.2 Ministerio de comercio, industria y turismo decreto 886 de 2014(mayo 13 de 2014).

“Mediante la Ley 1266 de 2008 se dictaron normas generales sobre la protección del derecho al hábeas data. Posteriormente, mediante la Ley 1273 de 2009 se creó un nuevo bien jurídico tutelado denominado de la protección de la información y de los datos, tipificando penalmente las conductas contra la confidencialidad, la integridad y, la disponibilidad de los datos de los sistemas informativos” (GrupoEGS, 2017).

2.3.3 Ley de propiedad intelectual.

“Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia” (Universitat de Girona l'Institut de Dret Privat Europeu, 2014).

“Artículo 12. Colecciones. Bases de datos

> 1. También son objeto de propiedad intelectual, en los términos del Libro I de la presente Ley, las colecciones de obras ajenas, de datos o de otros elementos independientes como las antologías y las bases de datos que por la selección o disposición de sus contenidos constituyan creaciones intelectuales, sin perjuicio, en su caso, de los derechos que pudieran subsistir sobre dichos contenidos.
> La protección reconocida en el presente artículo a estas colecciones se refiere únicamente a su estructura en cuanto forma de expresión de la selección o

disposición de sus contenidos, no siendo extensiva a éstos.
2. A efectos de la presente Ley, y sin perjuicio de lo dispuesto en el apartado anterior, se consideran bases de datos las colecciones de obras, de datos, o de otros elementos independientes dispuestos de manera sistemática o metódica y accesibles individualmente por medios electrónicos o de otra forma.
3. La protección reconocida a las bases de datos en virtud del presente artículo no se aplicará a los programas de ordenador utilizados en la fabricación o en el funcionamiento de bases de datos accesibles por medios electrónicos". (Universitat de Girona l'Institut de Dret Privat Europeu, 2014)

2.4 Estado del arte

Para tener una guía en cuanto al desarrollo del tema, se toman algunos textos como referencia de trabajo metodológico e investigativo, analizando la profundidad del contenido y el método de desarrollo del problema formulado. En la siguiente tabla se resumen los trabajos realizados por otros autores.

Tabla 6 Trabajos de referencia de otros autores

Año	Título	Autor
2017	AUDITORÍA INFORMÁTICA USANDO LAS NORMAS COBIT EN EL CENTRO DE SISTEMAS DE INFORMACIÓN DEL HOSPITAL REGIONAL DOCENTE LAS MERCEDES DE CHICLAYO – 2016	Samillan, Giancarlo Rafael; Castillo Oviedo, Edwin
2015	AUDITORÍA EN SEGURIDAD INFORMÁTICA EN BASE DE DATOS DEL GRUPO DE TRABAJO DE INFRAESTRUCTURA Y SOPORTE DE TECNOLOGÍAS DE LA INFORMACIÓN DEL DEPARTAMENTO PARA LA PROSPERIDAD SOCIAL – DPS – DE BOGOTÁ, SEDE PRINCIPAL	LASSO URBANO, CLAUDIA ANDREA
2012	AUDITORÍA INFORMÁTICA EN EL ÁREA DE SISTEMAS E INDICADORES DE FUNCIONAMIENTO DEL HARDWARE EN LA EMPRESA SOLIDARIA DE SALUD EMSSANAR E.S.S. DEL DEPARTAMENTO DE NARIÑO	Noguera Quenguan, Laura Yaneth; Sanchez Perenguez, Edy Yanira
2010	AUDITORÍA A LA BASE DE DATOS SQL DEL SISTEMA DE "SEGURIDAD DE PRESAS" CONAGUA	Ramirez, Efren; Torres, Irais; Yañez, Judith; Mosqueda, Yasmin
2007	AUDITORIA DE BASES DE DATOS GAVA: SOPORTE PARA REGISTRACIÓN Y ANÁLISIS DE CAMBIOS EN LOS DATOS	Ingravallo, Héctor; Entraigas, Valeria

Nota: Elaboración propia, resumen de los trabajos de otros autores

2.4.1 "Auditoría informática usando las normas cobit en el centro de sistemas de información del hospital regional docente las mercedes de Chiclayo – 2016".

> "El objetivo de esta auditoría es análisis el de las tecnologías de la información, aplicada actualmente en el área del Centro de Sistemas de Información del HRDLM de Chiclayo. Debido a que el HRDLM de Chiclayo es una organización dedicada exclusivamente a garantizar la atención de las necesidades de salud con recurso humano competente, servicios de salud organizados y articulando diversos actores estratégicos, en concordancia con las prioridades regionales. Todo esto debe contribuir al desarrollo integral y sostenido de la Región Lambayeque. Para llegar a este nivel de servicio; cada área unas en mayor proporción que otras deben asegurarse de dar lo mejor de sí, de aquí que se identifican aquellos que para mantenerse en operación constante dependen del servicio que les brinda el Centro de Sistemas de Información. El análisis donde se identificarán las debilidades existentes y sus riesgos potenciales, se expondrán una serie de conclusiones sobre los actuales procedimientos en lo que refiere a TI, el cual nos ayudará a emitir recomendaciones para el mejoramiento de gestión TI". (Samillan & Castillo Oviedo, 2017)

2.4.2 "Auditoría en seguridad informática en base de datos del grupo de trabajo de infraestructura y soporte de tecnologías de la información del departamento para la prosperidad social – DPS – de Bogotá, sede principal".

> "Este trabajo tiene como fin refleja el resultado de una auditoría en seguridad informática realizada sobre las bases de datos del Departamento para la Prosperidad Social (DPS) cuyo principal activo es la información relacionada con la identificación de beneficiarios, así como la infraestructura que soporta los sistemas de información y demás servicios involucrados. El análisis de riesgos se fundamenta en la metodología Magerit, iniciando con un levantamiento de activos los cuales son valorados, se realiza la identificación de amenazas y la definición de salvaguardas, para finalmente realizar un informe con los hallazgos encontrados en cuanto a la efectividad de los controles existentes y las recomendaciones necesarias para la implementación de nuevos controles que garanticen la confiabilidad, disponibilidad y la integridad de la información". (LASSO URBANO, 2015)

2.4.3 "Auditoría informática en el área de sistemas e indicadores de funcionamiento del hardware en la empresa solidaria de salud EMSSANAR E.S.S. Del departamento de Nariño".

> "Este proyecto tiene como fin evaluar los procesos del área de sistemas de la entidad de salud EMSSANAR E.S.S buscando el mejoramiento, emprendimiento y crecimiento empresarial, teniendo como objetivo primordial, mejorar continuamente la calidad de atención y prestación del servicio de salud al usuario. Por otra parte, se realiza una auditoría con el fin de evaluar la eficiencia y eficacia del hardware de comunicaciones, los servidores e indicadores de funcionamiento, teniendo en cuenta que la administración de los recursos TIC es factor calve para el desempeño y funcionamiento de las diferentes actividades que se desarrollan dentro de los procesos pertenecientes a esta área, identificando vulnerabilidades que permitan obtener un diagnóstico para que por medio de este la entidad defina planes de mejoramiento a nivel de procesos y por ende a nivel empresarial". (Noguera Quenguan & Sanchez Perenguez, 2012)

2.4.4 "Auditoría a la base de datos SQL del sistema de "seguridad de presas" Conagua".

> "Con la presente auditoria se pretende llevar a cabo un análisis de riesgos para el "Sistema de Seguridad de Presas" de la CONAGUA que permita revisar la aplicación apegándonos a la metodología de COBIT y la relación con la política de la empresa. Se auditarán los controles de la Base de datos de la aplicación "Sistema de Seguridad de Presas", se realizará un análisis de riesgos conforme a las buenas prácticas de la metodología COBIT. Debido a que el "sistema de seguridad de presas" se implementó por primera vez el 1o de marzo de 2010 en la CONAGUA, es necesario llevar a cabo el proceso de auditoría para minimizar los riesgos de que la aplicación no funcione adecuadamente y determinar si cumple con las buenas prácticas". (Ramirez, Torres, Yañez, & Mosqueda, 2010)

2.4.5 "Auditoria de bases de datos GAVA: Soporte para registración y análisis de cambios en los datos".

"Este trabajo presenta una introducción teórica a la Auditoria Informática como marco

general describiendo los diferentes conceptos de los objetos que la integran tanto como sus componentes y el marco legal argentino en el que se halla inmerso. Y como resultado práctico final se ofrece una herramienta que permite en forma sencilla, intuitiva y sobre todo centralizada mantener una registración sobre el cambio de los datos y su posterior análisis. Tal herramienta tiene la capacidad de interactuar con cualquier DBMS y Base de Datos desarrollada siempre que esté previamente configurada". (Ingravallo & Entraigas, 2007)

3 Metodología

El presente proyecto se enmarca en un paradigma de investigación positivista ya que esta permite la generación de una hipótesis, además de su verificación y predicción, con un enfoque cuantitativo que permite el uso de métodos estadísticos para tratar la información, un alcance exploratorio y un diseño experimental.

3.1 Fases del proyecto

Para el desarrollo de este trabajo de investigación, se opta por aplicar una metodología basada en las etapas que componen el proceso de la auditoría en donde se plantean 4 fases de trabajo que comprenden desde el conocimiento de la organización hasta la generación de un informe de auditoría. Adicional se tiene en cuenta la Norma IIA 2200 Planificación del trabajo en donde se establece que es deber de un auditor, establecer un plan de trabajo que contemple alcance, objetivos, tiempo y asignación de recursos, por consiguiente, las fases del trabajo se describen de la siguiente manera:

Fases de la metodología de trabajo

Figura 6 Fases de la metodología

Nota: Elaboración propia (2019)

- **Fase 1 Inicio**

En esta primera fase se realiza familiarización tanto de la organización como del sistema, conociendo a que se dedica la organización, que información tiene en sus bases de datos, exploración de procesos de la organización en el manejo de sus bases de datos, de tal forma que permita conocer los procedimientos que manejan, en donde están instaladas y su estructura. Para esto se llevará a cabo una entrevista de familiarización.

- **Fase 2 Planeación**

En esta fase se realizará el cronograma a seguir para cumplir los objetivos de la auditoria en el tiempo establecido, se detectarán las actividades que se realizan en la BD y en la aplicación que la utiliza. A partir de estas actividades se realizará la identificación de los riesgos con los cuales se crearán las Matrices de riesgos, las cuales

nos permitirán conocer los controles existentes a evaluar. Para evaluar estos controles se realizará en esta fase el diseño de las pruebas a ejecutar.

- **Fase 3 Ejecución**

En esta fase se realizará la ejecución de las pruebas diseñadas en la fase de planeación.

- **Fase 4 Cierre**

Revisión de las pruebas realizadas, conclusiones de estas, análisis de cuestionarios, identificar las causas de las debilidades, determinar la probabilidad y el impacto que tendrá cada debilidad en el sistema de información. Identificar los hallazgos de tipo preventivo, detectivo y correctivo de las debilidades encontradas. Identificar los recursos afectados por las debilidades encontradas.

3.2 Instrumentos o herramientas utilizadas

3.2.1 Entrevista a DBA.

Con la entrevista aplicada al DBA se pretende conocer el estado actual de la BD a fin de identificar los posibles riesgos existentes y de esta manera generar una serie de recomendaciones para mejorar el estado de la misma. A continuación, se presenta el modelo de la entrevista que se aplicará al DBA, en seguida, la ficha técnica en donde se establecen los requisitos del sistema para su correcto funcionamiento.

Tabla 7 Modelo entrevista a DBA

CARACTERÍSTICAS DE LA ENTREVISTA	
Fecha de aplicación	15/04/2019

Tipo de entrevista	Estructurada
Enfoque	Sujeto-Objeto
Objetivos	Identificar algunas características importantes del estado actual de la base de datos de Seguridad Social y la aplicación que la aloja.
Quién realiza la entrevista	
Nombre Entrevistado	
Edad	
Ocupación	
Nivel de educación	
Relación con el proyecto	

Formulario Preparado

A. Introducción
Como proyecto investigativo se planea realizar una auditoría a una base de datos de la empresa Inversiones Alcabama S.A., la Base de Datos seleccionada es la de Seguridad Social que se encuentra enfocada a Contratistas y a la cual se le evaluará el nivel de seguridad a fin de detectar posibles vulnerabilidades que pongan en riesgo la información de los colaboradores de la compañía.
B. Identificar entrevistados y participantes
Cesar Camilo Cruz: Tecnólogo en Análisis y Desarrollo de Sistemas de Información, desarrollador Backend y Frontend, diseñador de Bases de Datos.

Nota: Elaboración propia (2019)

Tabla 8 Preguntas de familiarización de la BD

c. Preguntas de familiarización de la BD	
Seguridad lógica y pistas de auditoría	
c 1	¿Se cuenta con una política o estándar que haya sido definida por el área de TI para el control de acceso a las BDs?
c 2	¿Se cuenta con una lista de usuarios de la BD?
c 3	¿El dueño de la base de datos realiza certificación de usuarios?
c 4	¿Existe un proceso formal para la solicitud de creación de nuevos usuarios?

c 5	¿El proceso de solicitud de usuarios nuevos se encuentra documentado?
c 6	¿Existen diferentes estados de usuario como Activo, Inactivo, bloqueado?
c 7	¿Se realizan validaciones para que no existan campos nulos?
c 8	¿Existe una Matriz de Roles y Perfiles de la base de datos?
c 9	¿Se cuenta con un estándar definido que permita aplicar controles que garanticen la adecuada asignación de privilegios y roles?
c 10	¿Existen usuarios que tengan acceso directo a la BD, diferente a los del DBA?
Integridad	
c 11	¿El sistema cuenta con un MER?
c 12	¿Hay un responsable de mantener el MER?
c 13	¿Existe un Diccionario de datos?
c 14	¿El DD se actualiza con cada modificación en la BD?
c 15	¿Quién actualiza las BD?
c 16	¿Con qué periodicidad se actualiza la BD?
c 17	¿El DBA puede modificar información de la BD?
c 18	¿Se cuenta con documentación de la BD?
c 19	¿Todos los cambios o actualizaciones en BD son registrados por escrito?
c 20	¿Solo el DBA tiene acceso a las claves de la aplicación?
Continuidad - backup y restauración	
c 21	¿Realiza copias de seguridad de la BD?
c 22	¿Existe un procedimiento documentado para realizar las copias de seguridad?
c 23	¿Realiza copias de seguridad a diario?
c 24	¿Existe un responsable del procedimiento para realizar copias de seguridad?
c 25	¿Lleva un control / planilla para registro de las copias de seguridad?
c 26	¿Revisa las copias de seguridad? Que hayan sido efectivas, que contengan la información respaldada.
c 27	¿Revisa el log de la copia de seguridad?
c 28	¿Deja evidencia (informe/registro novedades/bitácora) de la revisión de este log? ¿Cuál?
c 29	¿Guarda bajo llave las copias de seguridad?
Seguridad en el ambiente	
c 30	¿Ud. es la única persona encargada de salvaguardar las copias de seguridad en la organización?

c 31	¿Controlan el acceso al centro de cómputo a través de guarda de seguridad?
c 32	¿Controlan el acceso al centro de cómputo a través de identificación dactilar?
c 33	¿Controlan el acceso al centro de cómputo a través de tarjeta electrónica?
c 34	¿Controlan el acceso al centro de cómputo a través de clave?
c 35	¿Controlan el acceso al centro de cómputo a través de identificación biométrica?
c 36	¿Se lleva registro del ingreso al centro de cómputo?
c 37	¿El centro de cómputo es vigilado a través de cámaras?
c 38	¿Se cuenta con UPS en el centro de cómputo?
c 39	¿Se realiza monitoreo a la UPS?
c 40	¿Se monitorea la temperatura del centro de cómputo?

Nota: Elaboración propia (2019)

Tabla 9 Ficha técnica de la BD

FICHA TÉCNICA DE LA BD			
OBJETIVO:			
ESTADO:			
USUARIOS:			
PLATAFORMA TECNOLÓGICA			
SERVIDORES:			
	PROCESADOR	**MEMORIA**	**DISCO**
HW:			
SW:			
PC'S:			
	PROCESADOR	**MEMORIA**	**DISCO**
HW:			
SW:			
REDES:			
FW:			
PX:			
MÓDULOS			
MANUALES			
PROCEDIMIENTOS DE BACKUP			

Nota: Elaboración propia (2019)

3.2.2 Diseño de pruebas de cumplimiento.

Para la creación y posterior aplicación de las pruebas a la BD se seleccionaron las pruebas de cumplimiento, las cuales buscan controlar los riesgos internos y externos de la organización a su vez que busca verificar el cumplimiento de los procedimientos y estándares establecidos en la organización. Adicionalmente se verifica que tan efectivos son los controles que se aplican en los sistemas.

Figura 7 Diseño de la prueba

PT - Nombre de la prueba	
Objetivo de la prueba:	
Descripción de la prueba:	
Desarrollo de la prueba:	
Resultados de la prueba:	
Convenciones:	

Nota: Elaboración propia (2019)

3.2.3 Diseño matriz de riegos.

Se diseña la matriz de riesgos a fin de valorar los riesgos identificados en la

aplicación de la entrevista de familiarización, una vez obtenidos se valora el impacto y la probabilidad de estos para identificar los controles y evaluar su eficacia.

Tabla 10 Modelo Matriz de Riesgos

Empresa: Inversiones Alcabama S.A. Análisis de Riesgos Identificación de Riesgos									
Escenario	**Actividad**	**Código**	**Nombre**	**Descripción**	**IMPACTO**		**PROBABILIDAD**		**Control**
					Categoría	**Peso**	**Categoría**	**Peso**	
SEGURIDAD LÓGICA									
INTEGRIDAD									
CONTINUIDAD - BACKUP Y RESTAURACIÓN									
SEGURIDAD EN EL AMBIENTE									

Nota: Elaboración propia (2019)

3.3 Análisis de los datos

3.3.1 Plan de auditoría.

La auditoría interna para la evaluación de los controles que la organización ha establecido sobre las aplicaciones y repositorios de información a fin de mitigar los riesgos existentes, se desarrolla de acuerdo a la norma IIA 2200 que hace referencia a la planificación del trabajo en el cual deben considerarse tiempo, objetivos, alcance y recursos. En esta primera fase se aplica entrevista de

familiarización (Ver anexo 9.2 Entrevista de familiarización, Tablas 27, 28 29, 30 y 31) la cual servirá como guía para identificar los escenarios y las actividades que en la fase 2 se tomarán como base para el levantamiento de los riesgos asociados a la BD, la aplicación que la aloja y la infraestructura física del Data Center.

Ejecución metodológica:

Inicio

- Definir objetivo de auditoría
- Definir el alcance de la auditoría
- Recursos necesarios: entrevista de familiarización

Planeación

- Cronograma
- Levantamiento de riesgos
- Metodología

Análisis de matriz de riesgos

- Evaluación de riesgos
- Identificación de controles
- Evaluación de controles

Informe de auditoría

- Hallazgos
- Recomendaciones

3.3.2 Marco de referencia ISO 31000.

Analizar los riegos, da un acceso a su evaluación y análisis del tratamiento que se les debe aplicar. Para realizar este análisis se deben tener en cuenta las causas y fuentes de riesgos, las consecuencias que estos puedan tener, así como el impacto que pueden generar y la probabilidad de que sucedan en un determinado periodo de tiempo. La evaluación de riesgos también implica la revisión de los controles establecidos y la eficacia y eficiencia de estos.

Impacto

El impacto de un riesgo es el nivel de afectación que puede generar un evento en la organización relacionado con el funcionamiento de las BD.

La valoración del impacto está dada en 5 niveles (Ver anexo 9.4 Evaluación del Impacto Tabla 33).

Peso 1 (Insignificante): No genera ningún impacto en la organización.

Peso 2 (Menor): El impacto no genera mayor afectación en la organización.

Peso 3 (Moderado): Tiene un impacto medio y debe empezar a ser tenido en cuenta.

Peso 4 (Mayor): Su impacto puede generar consecuencias considerables en la organización, requiere de acciones específicas.

Peso 5 (Catastrófico): Su impacto puede generar consecuencias irreversibles para la empresa, los servicios se detienen y puede haber consecuencias económicas y reputacionales para la empresa. Requiere acciones inmediatas.

Probabilidad:

La probabilidad de que un evento ocurra en la organización se establece de acuerdo al nivel de experiencia de esta. Se clasificaron en 5 niveles (Ver anexo 9.5 Evaluación de Probabilidad, Tabla 34).

Peso 1 (Raro): Tiene una ocurrencia de 1 cada 10 años.

Peso 2 (Improbable): Tiene una ocurrencia de 1 cada 5 años.

Peso 3 (Posible): Tiene una ocurrencia de 1 cada 2 años.

Peso 4 (Probable): Tiene una ocurrencia de 1 cada año.

Peso 5 (Casi seguro): Tiene una ocurrencia de más de 2 veces al año.

3.4 Alcance y limitaciones

3.4.1 Alcance.

Se desarrolla la metodología con el fin de generar un informe de auditoría, en el cual se validen los controles existentes aplicados a la BD, los cuales surgen a partir de la aplicación de los cuestionarios de familiarización, y verificar que estos se estén aplicando de forma correcta, no obstante se tomarán en cuenta aquellos controles que no se aplican y se realizarán las recomendaciones pertinentes para la mejora del proceso y así garantizar la integridad y confiabilidad de los datos almacenados en la BD.

3.4.2 Limitaciones.

Las siguientes limitaciones restringen el proceso investigativo y el desarrollo del proyecto:

- Falta de documentación de procesos que permitan validar que se sigue un procedimiento estándar en la gestión, operación y manipulación de la BD y sus aplicaciones.
- El periodo de tiempo para el desarrollo del proyecto comprende 3 meses.
- El tiempo del DBA y director de TI para responder los cuestionarios.
- El acceso a información confidencial de la empresa.

4 Productos a entregar

A continuación, se presenta la lista de entregables generados durante el desarrollo del proyecto.

Tabla 11 Lista de productos a entregar

PRODUCTOS A ENTREGAR PROYECTO DE GRADO		
TIPO PRODUCTO	**DESCRIPCIÓN DEL PRODUCTO**	**FECHA DE ENTREGA**
Matriz de riesgos	Auditoria basada en riesgos.	30 de mayo de 2019
	Tablas:	
	- Se identifican actividades del proceso de seguridad y de integridad.	
	- Una vez identificadas las actividades, se identifican los riesgos.	
	- Criterios de probabilidad e impacto	
	- Matriz de riesgos	
	- Riesgos críticos	
Documentos de auditoria	Lineamientos a seguir a través del ciclo de Deming o PHVA: El modelo aplica:	30 de mayo de 2019
	- Diseño de las pruebas	
	- Papeles de trabajo	
	- Marcas de auditoria	
	- Documento de hallazgos.	
	- Informe de auditoría.	
	- Documentos de Mejoras propuestas.	

Nota: Elaboración propia (2019)

5 Entrega de resultados esperados e impactos

5.1 Desarrollo de la metodología

5.1.1 Fase 1 inicio.

Como fase de inicio se realizará una contextualización acerca de la organización Inversiones Alcabama S.A.

5.1.1.1 Familiarización.

- **"Misión:** ALCABAMA S.A. es una empresa dedicada a la promoción, gerencia, construcción y venta de proyectos inmobiliarios, cuyo propósito es el de generar crecimiento, satisfacción y confiabilidad a sus clientes, al igual que a su equipo de colaboradores y accionistas". (Inversiones Alcabama S.A., 2016)

- **"Visión:** Ser una empresa sólida, que se reconozca por la calidad de sus proyectos, su compromiso, innovación, servicio al cliente y la búsqueda del mejoramiento continuo" (Inversiones Alcabama S.A., 2016).

- **"Compromiso social:** Como parte de nuestro constante aporte a la familia colombiana, ALCABAMA se ha convertido en uno de los principales benefactores de la FUNDACIÓN SANTA ISABEL, entidad sin ánimo de lucro que fomenta el bienestar y desarrollo de las personas a través de cinco líneas de trabajo. En dichas líneas se enmarcan diversos programas tales como, grandes ciudadanos, por una familia mejor, tiempo para aprender y disfrutar; además del ofrecimiento

de espacios para la formación permanente en alianza con el SENA, entre otras entidades. De los programas de la Fundación se benefician niños, niñas, jóvenes y adultos mediante un modelo de intervención que promueve la inclusión, la formación en valores, la conciencia ciudadana y la construcción de proyectos de vida". (Inversiones Alcabama S.A., 2016)

- **"Experiencia:** Aunque la actividad constructora de Inversiones Alcabama S.A. inicia en el año 1993, desde 1983 el mismo grupo de socios a través de otras sociedades ha desarrollado un número importante de proyectos inmobiliarios. En estos 32 años de experiencia, el grupo empresarial ha desarrollado más de 25.200 unidades inmobiliarias que equivalen aproximadamente a 2.200.000 m2 de área construida". (Inversiones Alcabama S.A., 2016)

- **"Servicios**
    - Comercial
        - Dudas e inquietudes acerca de los proyectos
        - Ayuda en la legalización del negocio
        - Inquietudes sobre el proceso de escrituración o estado de cuenta de su inmueble
    - Mi inmueble
        - Urgencias
            - Suspensión o fallas en los servicios públicos
            - Suspensión o fallas en ascensores, motobombas o planta eléctrica
            - Contingencias dentro del conjunto

- Postventa". (Inversiones Alcabama S.A., 2016)

Alcabama posee diferentes BD para el almacenamiento de la información de la organización, las cuales conforman uno de los activos más importantes para la organización. A continuación, se relacionan estas BD con una breve descripción.

Tabla 12 Sistemas y Bases de datos de la empresa

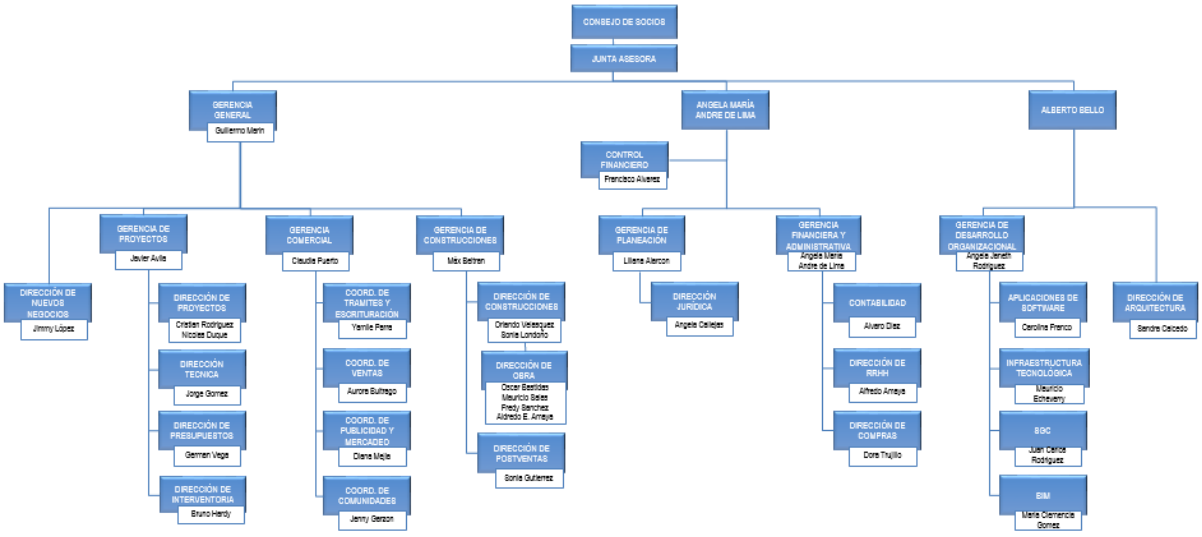
Sistemas y Bases de datos de la empresa		
Sistema	**Nombre Base de Datos**	**Función**
SACCO	BD de cortes de obra	Sistema Administrativo de Cortes Contratistas en Obra.
Control Afiliaciones	BD de contratistas	Sistemas control de afiliaciones enfocado a contratistas
Kardex	BD de insumos	Gestiona el inventario de almacén por obras
Control Patios	BD de pedidos de obra	Sistema para el control de pedidos de materiales de obra
Control Equipos	BD de maquinaria y equipos	Monitoreo de maquinaria y equipos
Sagef	BD de facturas	Sistema de Administración y gestión de facturas enfocado a proveedores
Gestión comercial	BD de clientes y contactos	Da una vista de 360 grados de clientes potenciales, contactos y ofertas. Pronostica o informa sobre el flujo de ventas.

Nota: Elaboración propia basada en los sistemas de la organización (2019)

- **Organigrama Empresarial**

La figura 6 representa la estructura organizacional de la empresa Inversiones Alcabama S. A.

Figura 8 Organigrama Alcabama



Nota: Elaboración propia basada en el organigrama de la empresa (2019)

Para complementar el proceso de familiarización y conocer el estado de la BD, el sistema que la aloja y conocer el estado del Datacenter, se aplicó una entrevista de familiarización al DBA en la cual se identifican claramente los controles aplicados a los repositorios de información de la empresa los cuales serán evaluados para medir su eficacia y eficiencia, así como los controles faltantes los cuales son los que mayor riesgo implican (Ver anexo 9.2 Entrevista de Familiarización, Tablas 27 a 31). Para conocer el estado del Datacenter y la aplicación, se creó una ficha técnica en la cual se consignan los datos de la plataforma tecnológica, los módulos del sistema, los manuales existentes y los procedimientos de backup que se realizan (Ver anexo 9.1 Ficha técnica del sistema, Tabla 26).

5.1.2 Fase 2 Planeación.

La creación de un plan de trabajo genera que una visión clara de las actividades a realizar, así como la secuencia de ejecución de cada una de estas. El cronograma de actividades es parte de la gestión del proyecto y le permite a la organización establecer el tiempo que le va a tomar llevar a cabo un proceso, así como llevar un control detallado del avance del proyecto y del cumplimiento de los objetivos. El cronograma permite, a medida que avanza el tiempo, ir ajustando costos y

recurso de ser necesario. Un plan de trabajo claro permite identificar las actividades que la empresa necesita para alcanzar sus objetivos, el tiempo que tomará la ejecución de cada actividad, los recursos necesarios para llevarlas a cabo y determinar la relación existente entre actividades (Vilá, 2014). El cronograma de trabajo de este proyecto se divide en cuatro actividades: Inicio, Planeación, Ejecución y Cierre. Se parte de la generación del EDT el cual muestra la visión general de cada actividad y los procesos que la componen (Ver Figura 8 EDT). El cronograma representa una visión más detallada del trabajo a realizar, en este se desglosan los procesos que compone cada actividad y los tiempos que tomará la ejecución de cada proceso (Ver Tabla 13 Cronograma). Por último, se crea el diagrama de Gantt el cual muestra gráficamente el avance del proceso que se está ejecutando (Ver Tabla 14 Diagrama de Gantt).

La identificación de las actividades que se establecieron para el levantamiento de los riesgos, se realiza teniendo en cuenta la entrevista de familiarización aplicada al DBA, en donde se clasifican las preguntas de acuerdo a su relación con un tema específico. En una categoría superior a las actividades se encuentran los ambientes en los cuales se divide la entrevista para darle un enfoque más preciso al tipo de preguntas que se realizan. Se establecieron 4 ambientes para la creación de la entrevista: Seguridad Lógica y Pistas de Auditoría, Integridad, Continuidad - Backup Y Restauración y Seguridad en el Ambiente (Ver anexo 9.3 Matriz de Riesgos, Tabla 22). Una vez identificadas las actividades se establecen los riesgos asociados a cada una; para cada actividad se pueden asociar varios riesgos. A cada riesgo le fue asignado un código para su fácil identificación, así como la descripción de cada uno (Ver anexo 9.3 Matriz de Riesgos, Tabla 32). Luego de identificar los riesgos se valora cada uno asignándoles un peso de acuerdo a su impacto y probabilidad, valores establecidos previamente (Ver anexos 9.4 Evaluación de Impacto, Tabla 33, 9.5 Evaluación de Probabilidad, Tabla 34). Finalmente se identifican los controles que se aplican a cada riesgo teniendo en cuenta las respuestas suministradas por el DBA en la entrevista de familiarización. La matriz de riesgos es el compendio de identificar: ambientes, actividades, riesgos y controles, y permite al lector una fácil lectura de la información y evaluación de cada riesgo. La prueba de los controles se hace teniendo en cuenta la valoración dada a cada riesgo, en donde se evaluará la efectividad de los controles cuyos riesgos tienen mayor calificación, es decir, los que se encuentran en la escala de color rojo, naranja y amarillo ya que estos representan una

probabilidad más alta de materializarse.

Las pruebas a los controles tienen como objetivo evaluar la eficiencia, eficacia y desarrollo de los controles, los cuales evitan que el riesgo se materialice. Se ejecuta una prueba por cada controla evaluar; el formato de la prueba incluye un objetivo para esa prueba, la descripción paso a paso de la prueba, el desarrollo de la prueba en el cual se presentan imágenes y gráficas que dan evidencia del proceso y finalmente se documenta el resultado obtenido (Ver Figura 6 Diseño de pruebas de cumplimiento).

5.1.2.1 EDT.

Figura 9 EDT

Nota: Elaboración propia (2019)

5.1.2.2 Cronograma.

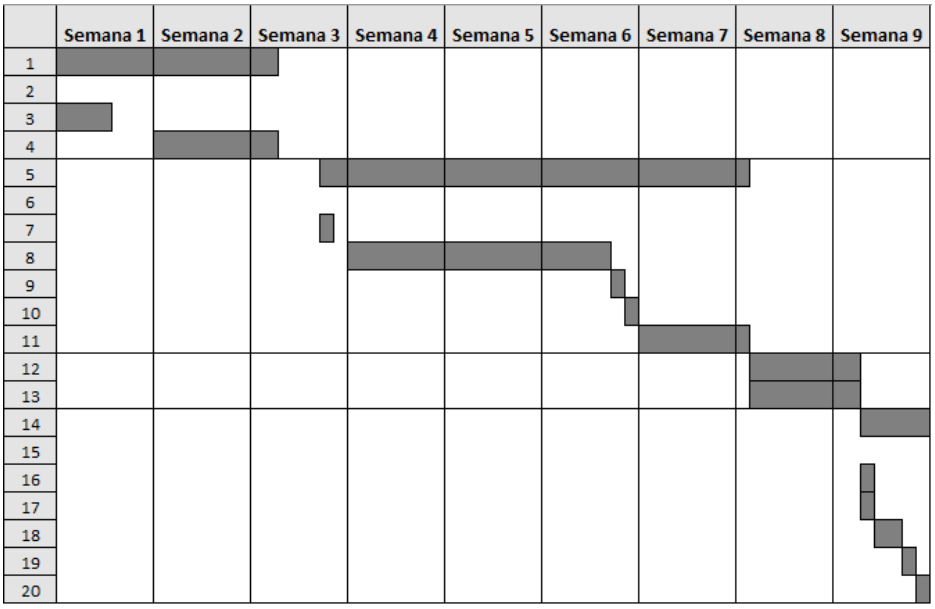
Tabla 13 Cronograma de actividades

	Nombre	Duración	Inicio	Fin
1	**Inicio**	**12 días**	**01/04/2019**	**12/04/2019**
2	**Familiarización**	12 días	01/04/2019	12/04/2019
3	Creación de cuestionarios	4 días	01/04/2019	04/04/2019
4	Aplicación de cuestionarios	6 días	08/04/2019	12/04/2019
5	**Planeación**	**12 días**	**20/04/2019**	**01/05/2019**
6	**Levantamiento de riesgos**	12 dias	20/04/2019	01/05/2019
7	Identificación de actividades	2 días	20/04/2019	21/04/2019
8	Identificación de riesgos	2 días	22/04/2019	23/04/2019
9	Evaluación de matriz de riesgos	1 día	24/04/2019	24/04/2019
10	Cálculo de criticidad de riesgos	1 día	24/04/2019	24/04/2019
11	Diseño de pruebas	3 días	29/04/2019	01/05/2019
12	**Ejecución**	**2 días**	**07/05/2019**	**08/09/2019**
13	Aplicación de pruebas	2 días	07/05/2019	08/09/2019
14	**Cierre**	**4 días**	**09/04/2019**	**12/04/2019**
15	**Generación de informe de auditoría**	4 días	09/04/2019	12/04/2019
16	Revisión de pruebas	1 día	09/04/2019	09/04/2019
17	Análisis de cuestionarios	1 día	09/04/2019	09/04/2019
18	Identificación de debilidades	2 días	10/04/2019	11/04/2019
19	Identificación de hallazgos	1 día	12/04/2019	12/04/2019
20	Recomendaciones	1 día	12/04/2019	12/04/2019

Nota: Elaboración propia (2019)

5.1.2.3 Diagrama de Gantt.

Tabla 14 Diagrama de Gantt



Nota: Elaboración propia (2019)

5.1.3 Fase 3 ejecución.

Evaluados los riegos y controles presentes, se diseñaron y programaron 10 pruebas (Ver tabla) las cuales permiten evaluar la efectividad de los controles

Tabla 15 Programación de pruebas de auditoría

Programación de pruebas de auditoría	
Código	**Descripción**
P01	Verificar Configuración de permisos de usuarios
P02	Bloqueo de Sesión de usuarios por inactividad
P03	Verificar mantenimiento de los servidores donde se encuentra alojada la BD y la Aplicación
P04	Verificación de permisos de usuarios administrador
P05	Verificación de documentación del procedimiento de restablecimiento de backups
P06	Verificación del correcto restablecimiento de backups en un ambiente de pruebas
P07	Validación del Plan de Continuidad del Negocio
P08	Validar el control de Acceso al datacenter
P09	Verificación de medidas de seguridad en data center
P10	Verificación de medidas de seguridad en los equipos del datacenter

Nota: Elaboración propia (2019)

5.1.3.1 Pruebas.

- **P01- Verificar Configuración de permisos de usuarios**

Tabla 16 P01-Verificar Configuración de permisos de usuarios

P01- Verificar Configuración de permisos de usuarios
Objetivo de la prueba: Verificar que los permisos de los usuarios se encuentren asignados de acuerdo a la matriz de roles y perfiles
Descripción de la prueba: 1. Verificar la matriz de roles y perfiles 2. Verificar los permisos asignados en el sistema y en la Base de datos que se encuentren de acuerdo con la matriz

3. Verificar que la matriz se encuentre asignado de acuerdo al cargo.

Desarrollo de la prueba:

1. Se solicita la matriz de roles y perfiles al DBA h1

2. Se ejecuta el Query SELECT * FROM ssocial.perfiles; para listar los perfiles de usuario

3. Se verifica en la BD, en la tabla usuarios, la asignación de permisos de acuerdo al perfil de usuario

id	nombre	descripcion	modulos	created_at	updated_at	entry_by
1	Administrador	Permite administrar todos los módulo de la aplic...	1,2,3,4,5,6,8	2016-10-11 10:34:14	2018-08-14 09:46:58	1
2	Director De Obra	Cargar planillas de jornales	2,8	2016-10-11 10:50:16	2018-08-14 09:47:21	1
3	Registro planillas	Registrar planillas de seguridad social	5,6	2016-10-13 18:35:12	2017-01-17 14:39:06	1
4	Liquidación	Planillas	1,6,8	2016-11-16 10:29:50	2017-01-12 11:03:27	1
5	Administración de campos	Administración de campos	3	2016-12-16 09:54:29	2016-12-16 09:54:29	1
6	Contratista	Contratista	7	2017-04-07 08:37:04	2017-04-07 08:37:05	1
7	SST	Siso	7,6	2017-05-17 14:41:40	2017-05-17 14:41:40	1
NULL	NULL	NULL	NULL	NULL	NULL	NULL

4. Se ejecuta el Query SELECT * FROM ssocial.modulos; para listar los módulos

5. Se compara el listado de perfiles con los módulos que tiene asignados

id	nombre	descripcion	created_at	updated_at	entry_by
1	Liquidador	Relizar liquidaciones	2016-10-11 09:41:30	2016-10-11 09:41:40	1
2	Planilla Jornales	Cargar las planillas de jornales (Director de obra)	2016-10-11 09:42:19	2016-10-11 09:42:24	1
3	Administracion	Administrar variables de entorno	2016-10-11 09:42:49	2016-10-11 09:42:55	1
4	Usuarios	Administrar usuarios	2016-10-11 09:43:12	2016-10-11 09:43:19	1
5	Registro Control	Administrar ingreso de los trabajadores	2016-10-11 09:43:46	2016-10-11 09:43:48	1
6	Traslados	Traslados entre contratistas y obras	2017-01-10 15:21:26	2017-01-10 15:21:29	1
7	Contratistas	Contratistas	2017-04-07 08:36:37	2017-04-07 08:36:38	1
8	Informes	Generar Informes	2018-08-14 09:46:07	2018-08-14 09:46:07	1
NULL	NULL	NULL	NULL	NULL	NULL

6. Se ejecuta el Query SELECT * FROM ssocial.users; para listar los usuarios

id	name	email	password	remembe	status	projects	profiles	user_type	created_	updated_a	entry_by
1	César Camilo Cruz Cáceres	adri@adri.com	$2y$10$f...	0gxLF...	1	79,87	1	NULL	2016-...	2019-06...	NULL
2	Soporte Pagos	soporte@alcabama.com.co	$2y$10$l...	H3We...	1	1,2,7,9,1...	2	NULL	2016-...	2018-08...	NULL
3	Carolina Franco	carolina.franco@alcabama.com.co	$2y$10$...	9h5id...	1	87	1	NULL	2016-...	2017-03...	NULL
4	Juan Camilo Gonzalez	programacion2@alcabama.com.co	$2y$10$...	NULL	1			NULL	2016-...	2017-01...	NULL
5	Andres Larrotta	programacion3@alcabama.com.co	$2y$10$...	NULL	1	79			2016-...	2016-10...	NULL
6	Jazmin Lopez Ortega	asdfasdf	$2y$10$...	HcIq5...	1	1,2,7,9,1...	2	NULL	2016-...	2016-10...	NULL
7	victor	victor@victor.com	$2y$10$...	NULL	0	79,87,21,...		Global	2016-...	2016-10...	1
8	Alejandra Garzon	alejandra.garzon@alcabama.com.co	$2y$10$...	vGBy...	1		3,4,5	NULL	2016-...	2018-10...	1
9	Dayan Pinzon	asistente.gestion@alcabama.com.co	$2y$10$r...	LB6W...	1	1,2,7,9,1...	2	Global	2016-...	2018-07...	1
10	Magdalena Gomez	magdalena.gomez@alcabama.com.co	$2y$10$...	kgvD...	1	1,2,7,9,1...	2,3,4,5	Global	2016-...	2018-10...	1
11	Gustavo Salamanca Lopez	auxiliar.archivo@alcabama.com.co	$2y$10$z...	AOD6...	1	79,87,21,...	3,5	Global	2016-...	2018-06...	1
12	Jazmin Lopez Ortega	jazmin.lopez@alcabama.com.co	$2y$10$j...	CjWiI...	1	NULL	1,2	NULL	2016-...	2018-09...	1
13	Victor Manuel	administrador.bm@alcabama.com.co	$2y$10$...	NULL	1	1,2,7,9,1...	2	Global	2016-...	2016-12...	1
14	Jeimy Andrea Minota Alva...	jeimy.minota@alcabama.com.co	$2y$10$...	NULL	1	NULL	3	NULL	2016-...	2016-12...	1
15	Juan Carlos Morera	auxarchivo@alcabama.com.co	$2y$10$f...	FO1kj...	1	1,2,7,9,1...	2,3,4,5	Global	2016-...	2018-04...	1
21	James Cruz	james.cruz@alcabama.com.co	$2y$10$...	g74p...	1	NULL	NULL	NULL	2017-...	2017-04...	1
22	Yazmin Correa	yazmin.correa@alcabama.com.co	$2y$10$k...	u4mj...	1	NULL	NULL	NULL	2017-...	2017-01...	1
23	Jhon Saavedra	jhon.saavedra@alcabama.com.co	$2y$10$...	uFH4...	1	NULL	NULL	NULL	2017-...	2017-12...	1
24	Natalia Ramirez	natalia.ramirez@alcabama.com.co	$2y$10$i...	NULL	1	NULL	NULL	NULL	2017-...	2017-02...	1
25	Hugo Guzman	hugo.guzman@alcabama.com.co	$2y$10$...	Qc4O...	1	NULL	NULL	NULL	2017-...	2017-05...	1
26	Hernan Dario Muñoz	hernan.postventas@alcabama.com.co	$2y$10$...	NULL	1	NULL	NULL	NULL	2017-...	2017-03...	1
27	Oscar Rojas	oscar.rojas@alcabama.com.co	$2y$10$...	JTy1S...	1	NULL	NULL	NULL	2017-...	2017-04...	1
28	Katherin Paola Bustos	programador.php@alcabama.com.co	$2y$10$...	Rd9A...	1	79	1,6	NULL	2017-...	2017-10...	1
29	Victor	victor.robayo@alcabama.com.co	$2y$10$l...	NULL	1	1,2,7,9,1...	7	Global	2017-...	2017-05...	1
30	Astrid Palma	astrid.palma@alcabama.com.co	$2y$10$j...	NULL	1	NULL	NULL	NULL	2017-...	2018-01...	1
31	Sala Ventas Hacienda la Q...	sventas.hlaquinta@alcabama.com.co	$2y$10$...	NULL	1	NULL	NULL	NULL	2017-...	2017-10...	1
32	Dayan Pinzon	dayan.pinzon@alcabama.com.co	$2y$10$...	tqf1R...	1	97,79,87,...	1,2,3,...	Global	2018-...	2018-10...	1
33	Juan Carlos Murcia	carlos.murcia@alcabama.com.co	$2y$10$...	NULL	1	1,2,7,9,1...	2	NULL	2018-...	2018-04...	1
34	Paola Torres	paola.torres@alcabama.com.co	$2y$10$...	sdyiT...	1	1,2,7,9,1...	2	NULL	2018-...	2018-04...	1
35	Sala ventas Argami	salaventas.argami@alcabama.com.co	$2y$10$...	NULL	1	1,2,7,9,1...	2	NULL	2018-...	2018-05...	1
36	Almacen Aqualina Orange	almacen.orange@alcabama.com.co	$2y$10$...	NULL	1	1,2,7,9,1...	2	NULL	2018-...	2018-08...	1
37	Oscar Bastidas	oscar.bastidas@alcabama.com.co	$2y$10$...	XpF37...	1	1,2,7,9,1...	2	Global	2018-...	2018-09...	1
38	Brayant Echeverria	Residente.Alborada2@alcabama.co...	$2y$10$...	NULL	1	1,2,7,9,1...	2	Global	2018-...	2018-08...	32
39	Auxiliar Residente Alborada	Auxresidente.alborada@alcabama.c...	$2y$10$k...	NULL	1	1,2,7,9,1...	2	Global	2018-...	2018-08...	32
40	Sonia Londono	Sonia.Londono@alcabama.com.co	$2y$10$...	NULL	1	1,2,7,9,1...	2	Global	2018-...	2018-08...	32
41	Rosa Elena Sarabria Rozo	Rosa.Sarabria@alcabama.com.co	$2y$10$...	NULL	1	1,2,7,9,1...	2	Global	2018-...	2018-08...	32
42	Yesica Mendez	Yesica.Mendez@alcabama.com.co	$2y$10$...	NULL	1	1,2,7,9,1...	2	Global	2018-...	2018-08...	32
43	Lina Rivera	Lina.Rivera@alcabama.com.co	$2y$10$...	qwiY...	1	1,2,7,9,1...	2	Global	2018-...	2018-09...	32
44	Enrique Amaya	Enrique.amaya@alcabama.com.co	$2y$10$s...	NULL	1	1,2,7,9,1...	2	Global	2018-...	2018-08...	32
45	Edison Ramirez	Edison.Ramirez@alcabama.com.co	$2y$10$...	tpiZQ...	1	1,2,7,9,1...	2	Global	2018-...	2018-09...	32
46	Cristhian Cardenas	Cristhian.Cardenas@alcabama.com.co	$2y$10$j...	NULL	1	1,2,7,9,1...	2	Global	2018-...	2018-08...	32
47	Mauricio Salas	Mauricio.Salas@alcabama.com.co	$2y$10$...	NULL	1	1,2,7,9,1...	2	Global	2018-...	2018-08...	32
48	Residente San Rafael	Residente.Sanrafael@alcabama.com...	$2y$10$...	o04D...	1	1,2,7,9,1...	2	Global	2018-...	2018-08...	32
49	Clemencia Gomez	Clemencia.Gomez@alcabama.com.co	$2y$10$...	NULL	1	1,2,7,9,1...	2	Global	2018-...	2018-08...	32
50	Wilian Enriquez	Wilian.enriquez@alcabama.com.co	$2y$10$...	NULL	1	1,2,7,9,1...	2	Global	2018-...	2018-08...	32
51	Wilson Ruiz	Wilson.Ruiz@alcabama.com.co	$2y$10$...	NULL	1	1,2,7,9,1...	2	Global	2018-...	2018-09...	32
52	Fredy Sanchez	FredySanchez@alcabama.com.co	$2y$10$t...	ZOGF...	1	1,2,7,9,1...	2	Global	2018-...	2018-09...	32
53	Luis Casallas	Luis.casallas@alcabama.com.co	$2y$10$...	9tLBt...	1	1,2,7,9,1...	2	Global	2018-...	2018-09...	32
54	Manuel Rodriguez	Residente.Zapan@alcabama.com.co	$2y$10$...	NULL	1	1,2,7,9,1...	2	Global	2018-...	2018-09...	32
55	Alejandro Reio	Aleiandro.Reio@alcabama.com.co	$2y$10$...	NULL	1	1,2,7,9,1...	2	Global	2018-...	2018-08...	32
56	Carolina Luna	Carolina.Luna@alcabama.com.co	$2y$10$...	XnCVt...	1	1,2,7,9,1...	2	Global	2018-...	2018-09...	32
57	Laura Lopez	Laura.Lopez@alcabama.com.co	$2y$10$...	NULL	1	1,2,7,9,1...	2	Global	2018-...	2018-08...	32
58	David Buitrago	Residente.Madelena@alcabama.com...	$2y$10$...	79kae...	1	1,2,7,9,1...	2	Global	2018-...	2018-08...	32
59	Miguel Garcia	Miguel.Garcia@alcabama.com.co	$2y$10$i...	B4jn0...	1	1,2,7,9,1...	2	Global	2018-...	2018-09...	32
60	Julio Torres	Julio.Torres@alcabama.com.co	$2y$10$l...	NULL	1	1,2,7,9,1...	2	Global	2018-...	2018-08...	32
61	Antonio Alvarez	Jose.Alvarez@alcabama.com.co	$2y$10$...	VcvlF...	1	1,2,7,9,1...	2	Global	2018-...	2018-09...	32
62	Orlando Velasquez	Orlando.Velasquez@alcabama.com.co	$2y$10$...	NULL	1	1,2,7,9,1...	2	Global	2018-...	2018-08...	32
63	Bruno Hardy	Bruno.Hardy@alcabama.com.co	$2y$10$...	NULL	1	1,2,7,9,1...	2	Global	2018-...	2018-08...	32
64	Ender Ramirez	Ender.Ramirez@alcabama.com.co	$2y$10$...	NULL	1	1,2,7,9,1...	2	Global	2018-...	2018-08...	32
65	Sonia Gutierrez	sonia.gutierrez@alcabama.com.co	$2y$10$...	NULL	1	1,2,7,9,1...	2	Global	2018-...	2018-09...	1
66	Adriana Pardo	administrador.seguimiento@alcabam...	$2y$10$...	q4EL...	1	1,2,7,9,1...	2,3,4,5	Global	2016-...	2018-10...	1
NULL	NULL	NULL	NULL	NULL	NULL	NULL	NULL	NULL	NULL	NULL	NULL

Resultados de la prueba:

Se evidencia que no se cuenta con una matriz de roles y perfiles establecida contra la cual se pueda realizar la comparación de perfiles asignados en el sistema

Convenciones:

hn: Corresponde a un hallazgo identificado

Nota: Elaboración propia (2019)

- **P02 - Bloqueo de Sesión de usuarios por inactividad**

Tabla 17 P02-Bloqueo de Sesión de usuarios por inactividad

P02 - Bloqueo de Sesión de usuarios por inactividad

Objetivo de la prueba:

Verificar que este configurado el bloqueo de sesión de usuarios por inactividad

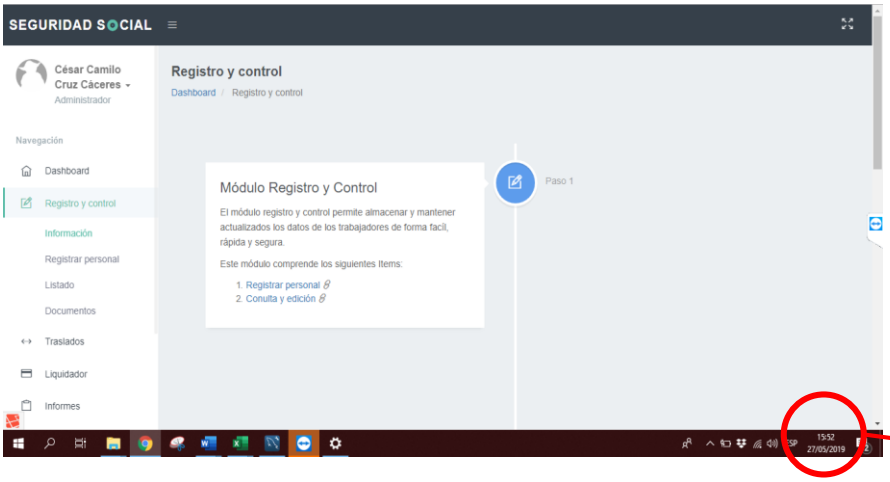
Descripción de la prueba:

1. Valide las políticas de Seguridad de SI
2. Verificar si está configurado en el servidor las políticas de bloqueo de sesión de forma automática
3. Verifique en un pc que esto esté sucediendo

Desarrollo de la prueba:

1. Se solicita al DBA la política de bloqueo de sesión de usuario de forma automática h1
2. En un pc de usuario se realiza el ingreso al sistema

3. El usuario permanece inactivo en la aplicación durante 45 minutos e ingresa de manera normal a la aplicación



Resultados de la prueba:

1. Se evidencia que no existe una política de bloqueo de sesión de usuario documentada

2. Se evidencia que la aplicación no se bloquea por inactividad prolongada del usuario

Convenciones:

hn: Corresponde a un hallazgo identificado

Nota: Elaboración propia (2019)

- **P03 - Verificar mantenimiento de los servidores donde se encuentra alojada la BD y la Aplicación**

Tabla 18 P03-Verificar mantenimiento de los servidores

P03 - Verificar mantenimiento de los servidores donde se encuentra alojada la BD y la Aplicación

Objetivo de la prueba:

Verificar que se esté realizando mantenimiento a los servidores donde se encuentra la Bd y la aplicación

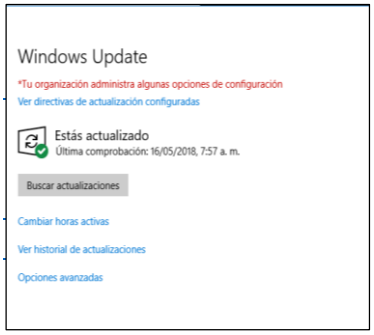
Descripción de la prueba:

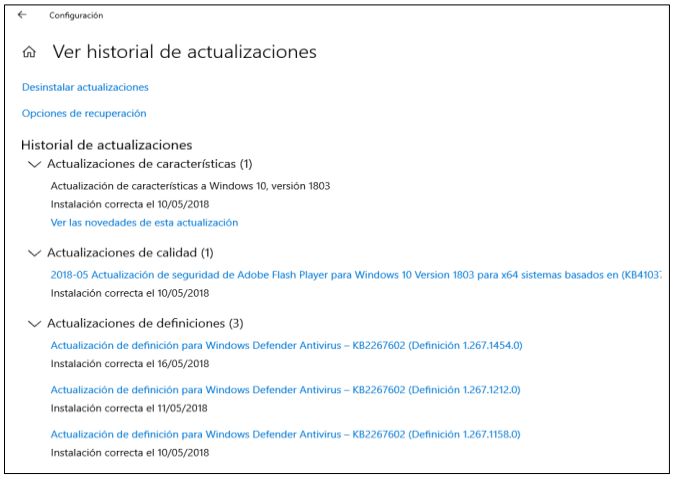
1. Solicitar programas de mantenimiento h1
2. Solicitar los registros de estos mantenimientos h2

3. Verificar que se realicen instalación de parches, mantenimiento de antivirus
4. Verificar en el servidor fecha de última actualización

Desarrollo de la prueba:

1. Se verifica que el antivirus se encuentra actualizado observando la fecha de la última actualización





2. Servidor Linux 16.04 actualizado a la versión 16.08
3. Antivirus ClamAV actualizado de versión 2 a 3

Resultados de la prueba:

1. Como resultado de la prueba, se identifica que no se cuenta con programas de mantenimiento de los servidores, por lo cual no se puede tener evidencia del mantenimiento realizado a estos

2. Se verifica que el sistema cuenta con el último parche de antivirus actualizado
3. No se aporta evidencia de actualización de servidor y antivirus de servidor, solo se encuentra registro de actualizaciones en equipo de usuario

Convenciones:

hn: Corresponde a un hallazgo identificado

Nota: Elaboración propia (2019)

- **P04 - Verificación de permisos de usuarios administrador**

Tabla 19 P04-Verificación de permisos de usuarios administrador

P04 - Verificación de permisos de usuarios administrador

Objetivo de la prueba:

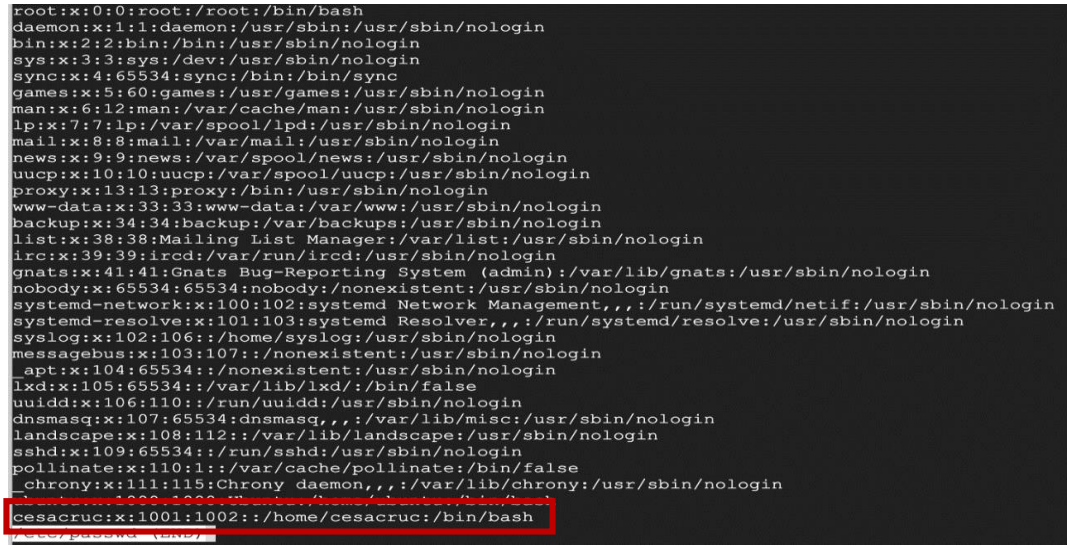
Verificar que los usuarios que se encuentren como administrador en el directorio activo no ingresen a la BD con permisos de administrador

Descripción de la prueba:

1. Consultar con el administrador de base de datos para asegurarse de cómo se gestiona la base de datos.
2. Verificar listado de usuarios con permiso de administrador en directorio activo
3. Verificar que los usuarios relacionados en el listado no cuenten con permiso de ingreso a la BD.

Desarrollo de la prueba:

1. Se verifican los usuarios administradores en el server



2. En la BD se ejecuta la consulta SELECT * FROM ssocial.perfiles; para obtener el listado de perfiles y verificar el id del perfil Administrador

id	nombre	descripcion	modulos	created_at	updated_at	entry_by
1	Administrador	Permite administrar todos los módulo de la aplic...	1,2,3,4,5,6,8	2016-10-11 10:34:14	2018-08-14 09:46:58	1
2	Director De Obra	Cargar planillas de jornales	2,8	2016-10-11 10:50:16	2018-08-14 09:47:21	1
3	Registro planillas	Registrar planillas de seguridad social	5,6	2016-10-13 18:35:12	2017-01-17 14:39:06	1
4	Liquidación	Planillas	1,6,8	2016-11-16 10:29:50	2017-01-12 11:03:27	1
5	Administración de campos	Administración de campos	3	2016-12-16 09:54:29	2016-12-16 09:54:29	1
6	Contratista	Contratista	7	2017-04-07 08:37:04	2017-04-07 08:37:05	1
7	SST	Siso	7,6	2017-05-17 14:41:40	2017-05-17 14:41:40	1
NULL	NULL	NULL	NULL	NULL	NULL	NULL

3. En la BD se ejecuta la consulta SELECT * FROM ssocial.users WHERE profiles = 1; para validar que usuarios cuentan con perfil Administrador

id	name	email	password	remember_token	status	projects	profiles
1	César Camilo Cruz Cáceres	adri@adri.com	$2y$10$fifcem7NVJR6XjdLPH7KUePP1XPh0o1G...	0gxLFq5j6ksL3DH3Nx3W5oKpyU7xWvtx2XMRf...	1	79,87	1
3	Carolina Franco	carolina.franco@alcabama.com.co	$2y$10$dYOiPePNE.2SPGHOqgtg8ed2J4WzhrQ...	5hSiDZzEpd3g1T56cZwFTCfJmY4wB63agRItvK...	1	87	1
12	Jazmin Lopez Ortega	jazmin.lopez@alcabama.com.co	$2y$10$j6M0HsLsF6u2j7rBR4OxQ..MNXMkc2hR...	QjWlINRZ8VZia50PQwHkLCZThNaZSaJ49qfoFH...	1	NULL	1,2
28	Katherin Paola Bustos	programador.php@alcabama.com.co	$2y$10$PX3YSBafk4TXXYslxtePLegYslp2FIMbu...	Rd9AKsyApAxiLvMQtxdcqErVC5oQAiD3KEdMbV...	1	79	1,6
32	Dayan Pinzon	dayan.pinzon@alcabama.com.co	$2y$10$St8/or7.bNK9a3jrAwLEx.bd28B//nZ/Hb...	tqf1RUPUR6WQeFg93UNvYMSbVUsDsq1u6uzoI...	1	97,79,87,21,102,98,83,82,95,78,70,88,54,55,...	1,2,3,4,5,6,7
NULL	NULL	NULL	NULL	NULL	NULL	NULL	NULL

Resultados de la prueba:
1. Se evidencia que en el server solo existe un usuario administrador y que es diferente de los usuarios Administradores de la BD

Convenciones:
hn: Corresponde a un hallazgo identificado

Nota: Elaboración propia (2019)

- **P05 - Verificación de documentación del procedimiento de restablecimiento de backups**

Tabla 20 P05-Verificación de documentación backups

P05 - Verificación de documentación del procedimiento de restablecimiento de backups
Objetivo de la prueba: Validar que el procedimiento documentado muestre el paso a paso del restablecimiento de la BD en caso de presentarse una caída del sistema **Descripción de la prueba:** 1. Solicitar documentación de la BD al DBA 2. Validar que el procedimiento documentado corresponde con la actividad mencionada 3. Verificar que el procedimiento realizado cumple con los parámetros establecido en la documentación 4. Tomando como muestra los logs de la BD, validar que el procedimiento se realizó conforme a lo establecido en la documentación 5. Concluir y documentar las situaciones identificadas **Desarrollo de la prueba:** 1. Se validó que el procedimiento esté descrito en pasos claros 2. El procedimiento para el restablecimiento de backups es el siguiente: - Se deben detener los servidores - Realizar el restablecimiento de forma controlada - Habilitar los servidores para uso **Resultados de la prueba:**

1. Se identificó que no se cuenta con documentación del proceso que se sigue para restablecer backups.
2. El procedimiento fue aportado por el DBA con base en su conocimiento y experiencia
3. Se identificó que no se cuenta con logs que validen el restablecimiento satisfactorio del backup lo que implica que la correcta realización del proceso se realiza por comprobación visual.

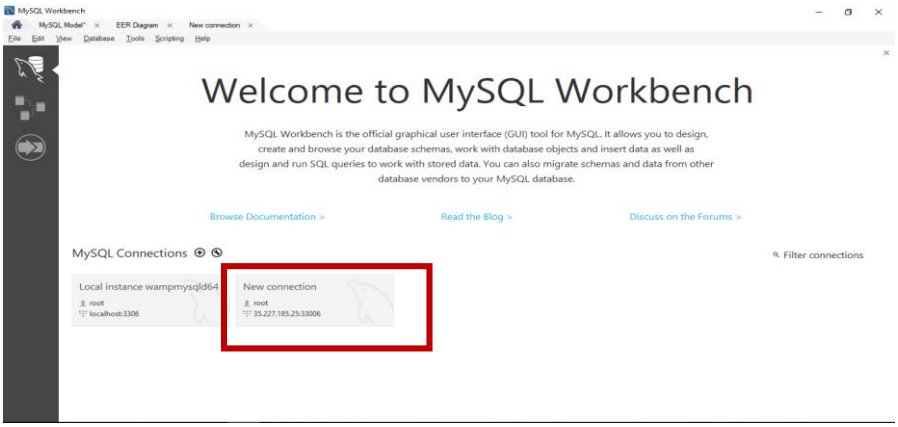
Convenciones:
hn: Corresponde a un hallazgo identificado

Nota: Elaboración propia (2019)

- **P06 - Verificación del correcto restablecimiento de backups en un ambiente de pruebas**

Tabla 21 P06-Verificación del correcto restablecimiento de backups

P06 - Verificación del correcto restablecimiento de backups en un ambiente de pruebas
Objetivo de la prueba: Contar con un ambiente de pruebas para verificar que el restablecimiento de backups es correcto
Descripción de la prueba: 1. Solicitar al DBA el acceso al ambiente de pruebas de la BD 2. Solicitar al DBA el último backup realizado a la BD 3. Realizar el restablecimiento del backup en el ambiente de pruebas 4. Validar que la información restablecida sea correcta 5. Validar el log generado por el procedimiento y verificar que este finalizó de manera satisfactoria h1 6. Concluir y documentar las situaciones identificadas
Desarrollo de la prueba: 1. Se habilita acceso al ambiente de pruebas de la BD



2. Se realiza el restablecimiento del backup aportado por el DBA

Resultados de la prueba:

Se evidencia que no es posible comprobar que el restablecimiento del backup fue exitoso ya que no se guardan registros de los ejercicios de restablecimiento que se realizan, no se generan logs del procedimiento.

Convenciones:

hn: Corresponde a un hallazgo identificado

Nota: Elaboración propia (2019)

- **P07 - Validación del Plan de Continuidad del Negocio**

Tabla 22 P07-Validación del Plan de Continuidad del Negocio

P07 - Validación del Plan de Continuidad del Negocio

Objetivo de la prueba:

Documentar y divulgar el plan de continuidad del negocio al personal de TI

Descripción de la prueba:

1. Solicitar al director de TI la documentación del Plan de Continuidad del negocio h1

2. Validar que el procedimiento documentado corresponde con la actividad mencionada

3. Verificar que el Plan de Continuidad incluye las BD como proceso critico
4. Verificar que el Plan de Continuidad incluye todos los procesos misionales de la organización
5. Concluir y documentar las situaciones identificadas

Desarrollo de la prueba:
1. Se solicita la documentación del Plan de Continuidad del Negocio
2. Director de TI confirma que las BD cuentan cómo proceso crítico dentro del plan de continuidad
3. Director de TI conforma que todos los procesos misionales hacen parte del plan de continuidad

Resultados de la prueba:
Se evidencia que no se cuenta con documentación del Plan de Continuidad del Negocio
La información suministrada por el director de TI fue de carácter verbal de acuerdo a su experiencia, por lo que no es posible comprobar que sus afirmaciones sean ciertas

Convenciones:
hn: Corresponde a un hallazgo identificado

Nota: Elaboración propia (2019)

- **P08 - Validar el control de acceso al Datacenter**

Tabla 23 P08-Validar el control de acceso al Datacenter

P08 - Validar el control de Acceso al datacenter

Objetivo de la prueba:
Validar el sistema de control de acceso al datacenter

Descripción de la prueba:
1. Verificar por medio de la observación, con qué mecanismos de control de acceso se cuenta para el ingreso al datacenter
2. Validar el registro de ingreso al datacenter
3. Verificar el listado de usuarios del área de TI con autorización de acceso al datacenter
4. Concluir y documentar las situaciones identificadas

Desarrollo de la prueba:

1. Se verifica por medio de la observación los mecanismos de control de acceso y se registra fotográficamente

2. En el listado de usuarios del área de TI se encuentran: h3

- Mauricio Echeverry - director de TI
- David Gutiérrez - Técnico de sistemas
- Iván Torres - Ing. De Sistemas

Resultados de la prueba:

1. Se evidencia que para el acceso al datacenter no se cuenta con los suficientes mecanismos de control de acceso

2. Se evidencia que la cámara de seguridad enfoca la salida de emergencia y no la entrada al datacenter, no obstante, la cámara captura el ingreso de personal al datacenter.

3. No se evidencia un registro formal de accesos al datacenter

4. No se aportó un listado formal de usuarios con ingreso autorizado al datacenter, el listado fue suministrado verbalmente

Convenciones:

hn: Corresponde a un hallazgo identificado

Nota: Elaboración propia (2019)

- **P09 - Verificación de medidas de seguridad en Datacenter**

Tabla 24 P09-Verificación de medidas de seguridad en Datacenter

P09 - Verificación de medidas de seguridad en data center

Objetivo de la prueba:
Verificar que el data center cuenta con pisos falsos para evitar daños en los equipos

Descripción de la prueba:
1. Solicitar acceso al datacenter
2. Verificar por medio de la observación que el data center cuenta con pisos falsos
3. Concluir y documentar las situaciones identificadas

Desarrollo de la prueba:
1. Se autoriza acceso al datacenter
2. Se toma registro fotográfico en donde se puede observar el entorno del datacenter h1

Sin piso falso
h1

Resultados de la prueba:
Se observa que el datacenter no cuenta con pisos fasos lo que puede ocasionar daño en los equipos en caso de una sobrecarga eléctrica, poniendo en riesgo la información de la empresa

Convenciones:
hn: Corresponde a un hallazgo identificado

Nota: Elaboración propia (2019)

- **P10 - Verificación de medidas de seguridad en los equipos del datacenter**

Tabla 25 P10-Verificación de medidas de seguridad en los equipos del datacenter

P10 - Verificación de medidas de seguridad en los equipos del datacenter

Objetivo de la prueba:
Verificar que el data center cuenta con UPS para regular las sobrecargas de voltaje

Descripción de la prueba:
1. Solicitar acceso al datacenter
2. Verificar por medio de la observación que en el datacenter se cuenta con UPS para controlar los fallos de energía
3. Verificar por medio de la observación que el circuito de protección de las UPS no se encuentre deteriorado
4. Concluir y documentar las situaciones identificadas

Desarrollo de la prueba:
1. Se autoriza acceso al datacenter
2. Se toma registro fotográfico en donde se puede observar el entorno del datacenter

Resultados de la prueba:
Se observa que el datacenter cuenta con UPS para el control de fallos de energía y que funcionan correctamente

Convenciones:

hn: Corresponde a un hallazgo identificado

Nota: Elaboración propia (2019)

5.1.4 Fase 4 cierre.

5.1.4.1 Informe detallado.

Durante el periodo comprendido entre el 1 de abril y el 15 de mayo de 2019 se realizó auditoría a la base de datos de seguridad social de la empresa Inversiones Alcabama S.A en los componentes de seguridad lógica, integridad, continuidad y ambiente, enmarcados en buenas prácticas de las normas IIA de auditores internos. Se detectó que el ambiente de control de la base de datos no cuenta con procedimientos ni políticas documentadas, se realiza la auditoria a los controles de los riesgos cuya calificación obtuvo un peso de 3, 4 y 5.

A continuación, se presentan los puntos a mejorar:

- Se evidenció que existe Matriz de roles y perfiles y se encuentra adecuadamente asignados a los usuarios de la BD los roles y perfiles según lo establecido para su perfil.
- Se evidencia que no existen políticas de bloqueo de usuarios documentadas, y se evidencia que en la aplicación no existen control de bloqueo de sesión de usuarios cuando hay inactividad, se recomienda implementar políticas de

bloqueo de sesión de usuarios por inactividad, ya que esto permite tener un mayor control sobre la seguridad de la información.

- Se recomienda contar con un programa de mantenimiento documentado que se realice semestralmente, es decir es recomendable que se realice 2 veces al año. La realización de estos mantenimientos debe quedar documentado.
- Se evidenció que se realizan los mantenimientos e instalación de parches en los pc, en los servidores no se encontraron evidencias de estas actualizaciones y mantenimientos.
- Se recomienda documentar el proceso que se sigue para el reestablecer la BD en caso de tener una caída, se evidencia que no cuentan con procesos documentados para el restablecimiento de backups de la BD.
- Se evidenció la falta de logs que indiquen el correcto restablecimiento del backup, esta comprobación la deben realizar de forma visual, se recomienda implementar logs para poder comprobar adecuadamente la correcta ejecución de este proceso.
- Se recomienda realizar ejercicios de restauración de la BD en ambiente de pruebas periódicamente, para comprobar que los backups están siendo realizados correctamente.
- Se evidencia que no existe manejo de logs para comprobar el restablecimiento del backup de la BD sea realizado correctamente, no existen registros de si estos ejercicios de restauración en ambiente de pruebas se realizan periódicamente, se recomienda al realizar estos ejercicios documentarlos.

- Se evidencia que no se cuenta con un plan documentado de plan de continuidad de negocio, por lo tanto, se recomienda documentar este plan y los procesos que tiene en cuenta.
- Se evidencia que para e ingreso al datacenter no se cuenta con un adecuado control de acceso, se recomienda implementar accesos electrónicos como tarjetas o un sistema biométrico para mayor seguridad.
- Se recomienda implementar otra cámara de vigilancia o una cámara con mayor cobertura, ya que se evidencia que la existente no abarca la totalidad del área.
- Se recomienda llevar una bitácora de ingreso de personal al datacenter, ya que se evidencia que no se maneja ningún registro de control a este.
- Se evidencia que no existe un comunicado formal de personal autorizado para ingreso al datacenter, se recomienda que exista señal de que es una zona a la que solo se puede ingresar con autorización y que exista un listado formal de personal autorizado.
- Se evidencia que no se cuenta con pisos falsos en el data center, se recomienda la instalación de pisos falsos para evitar daños por sobrecarga de energía.
- Se recomienda realizar ejercicios en horario no laboral del funcionamiento correcto de la UPS, además de realizar los mantenimientos periódicos para garantizar que en caso de una falla eléctrica funcionara correctamente.

5.2 ¿Cómo se responde a la pregunta de investigación con los resultados?

¿Qué recomendaciones se realizaron a la entidad Inversiones Alcabama luego de una auditoria basada en riesgos?

Las recomendaciones realizadas a la organización se hicieron tomando como base las evidencias obtenidas en la etapa de ejecución de pruebas, en donde se detectaron las falencias en los controles establecidos, además de evidenciar la ausencia de controles en varios de los procesos y la ausencia de documentación en el 90% de los procesos relacionados con la protección de información.

Las recomendaciones van enfocadas a la mejora en la gestión de la calidad de los procesos misionales de la empresa, con un enfoque basado en riesgos que le permita a la organización tener una toma de decisiones asertiva en la gestión de riesgos.

6 Nuevas áreas de estudio

Durante el desarrollo y ejecución de este proyecto, quedan a la luz diversas líneas de investigación, que, al ser evaluadas y ejecutadas, generarán un valor adicional al rendimiento de la organización. El alcance de este trabajo no abarcaba todos los frentes que pueden ser trabajados para alcanzar de una manera óptima, los objetivos del negocio.

A continuación, se presentan algunos trabajos futuros que pueden ser objeto de investigaciones futuras y que contribuirán al alcance de las metas estratégicas de la organización.

- Desde cada área de trabajo y a cargo de cada líder, realizar el levantamiento de los riesgos que puede generar cada proceso ejecutado, ya que al tener una visión clara de estos se contribuye a un mejoramiento en la planeación y ejecución del trabajo del equipo.
- Contando con el área de calidad, realizar el levantamiento y documentación de los procesos de cada área de trabajo, esto con el fin de tener una clara segregación de funciones y evitar la concentración de funciones en un solo cargo. Este proceso además permite que el personal nuevo de la compañía pueda realizar una ejecución de proceso con forme a unos parámetros establecidos por la empresa.
- Como sugerencia, la empresa puede certificarse en una norma de Gestión de la Calidad como la ISO 9001, que le permite a la organización tener un enfoque basado en riesgos y de esta manera generar acciones preventivas, además

la organización puede asegurar que su gestión de la calidad se encuentre alineada con los objetivos de la organización.

7 Conclusiones

Las herramientas utilizadas para el levantamiento de información en el proceso de familiarización, permitieron llevar a cabo la identificación de los riesgos asociados a la Base de Datos de Seguridad Social y su entorno, además de poder identificar los controles establecidos por la organización en el manejo y protección de la información. Con esta identificación se creó la matriz de riesgos en donde se realizó la valoración de impacto y probabilidad de ocurrencia de los riesgos, cuyo criterio de ponderación fue establecido por las autoras.

Con base en los resultados obtenidos en la fase de ejecución, se sugiere a la organización implementar controles que mitiguen la ocurrencia de eventos inesperados que afecten la confiabilidad, disponibilidad e integridad de los repositorios de información, además de la infraestructura física que los salvaguarda.

Es necesario para la empresa implementar monitoreo a los riesgos que se encuentran en calificación menores a tres en la matriz, con el fin de no permitir que estos suban de calificación y se conviertan en posibles riesgos críticos.

Al realizar la evaluación de los riesgos que se encuentran con calificación mayor a tres, se toman como enfoque para auditoria con el fin de evaluar la efectividad de los controles aplicados, para poder realizar recomendaciones que faciliten la mitigación de los riesgos y permitan a la organización tener una mayor seguridad de la información.

8 Bibliografía

20minutos. (27 de 06 de 2017). *20 minutos*. Obtenido de https://www.20minutos.es/noticia/3035545/0/que-es-ransomware-ciberataque-mundial/

Actualicese. (14 de 02 de 2019). *Actualicese*. Obtenido de https://actualicese.com/actualidad/2019/02/14/auditoria-basada-en-riesgos-caracteristicas-que-auditores-deben-tener-en-cuenta-para-su-aplicacion/

Agudo, S. (17 de 3 de 2017). *GENBETA*. Obtenido de https://www.genbeta.com/seguridad/el-fbi-explica-como-fue-hackeado-yahoo-mediante-un-ataque-de-spear-phishing

Alzate, A. T. (2001). *AUDITORÍA DE SISTEMAS Una visión práctica.* Manizales: Centro de Publicaciones Universidad Nacional de Colombia.

Anguiano, J. Á. (2005). *Auditoría Administrativa.* México: Facultad de Contaduría y Administración, UNAM.

Bilic, D. G. (15 de Marzo de 2019). *welivesecurity*. Obtenido de welivesecurity web site: https://www.welivesecurity.com/la-es/2019/01/04/paises-mas-afectados-ransomware-latinoamerica-durante-2018/

Cañar, J. V. (05 de 2011). *Universidad Politécnica Salesiana Ecuador Repositorio Institucional.* Obtenido de https://dspace.ups.edu.ec/bitstream/123456789/1447/13/UPS-QT01864.pdf

Castro, A. R., & Bayona, Z. O. (15 de Agosto de 2011). *Dialnet.* Obtenido de https://dialnet.unirioja.es/descarga/articulo/4797252.pdf

Contraloría General de Estado Bolivia. (2006). *Contraloría General de Estado Bolivia*. Obtenido

de https://www.contraloria.gob.bo/portal/Auditor%C3%ADa/Auditor%C3%ADasdeProyectosdeInversi%C3%B3nP%C3%BAblica.aspx

Delgado, J. J., & Naranjo, J. E. (02| de 2015). *Universidad politécnica Salesiana Repositorio Institucional.* Obtenido de https://dspace.ups.edu.ec/bitstream/123456789/9942/1/UPS-GT000922.pdf

DNP. (10 de 04 de 2019). *Departamento Nacional de Planeación*. Obtenido de https://www.dnp.gov.co/programas/desarrollo-social/subdireccion-de-empleo-y-seguridad-social/Paginas/Seguridad-Social-Integral.aspx

Dominguez, J. (2015). Principios Básicos de Seguridad en Bases de Datos. *Universidad Politécnica Regional de Estado de Aconcagua*, 7.

ECA Instituto de Tecnología y Formación, S.A. (2007). *Auditorías Ambientales.* España: FUNDACIÓN CONFEMETAL.

El colombiano. (15 de 05 de 2017). *El colombiano*. Obtenido de https://www.elcolombiano.com/tecnologia/wannacry-afecta-a-20-empresas-colombianas-NF6531294

Estrada, A. A. (10 de 2003). *Centro de Información Documental Biblioteca del INFONAVIT.* Obtenido de https://infonavit.janium.net/janium/TESIS/Maestria/Arizmendi_Estrada_Alfredo_45142.pdf

Franklin, E. B. (2007). *Auditoría Administrativa Gestión Estratégica del Cambio.* México: Pearson Educación.

Gonzalez, J. L. (1998). *Panorama sobre bases de datos (Un enfoque práctico).* Mexicali, Baja California: Universidad Autónoma de Baja California.

GrupoEGS. (1 de 08 de 2017). *Leyex.Info*. Obtenido de https://ucatolica-leyex-info.ucatolica.basesdedatosezproxy.com/noticias/detalle/se-implementan-las-politica-de-tratamiento-de-datos-personales-21033

Hernandez, C. (31 de 10 de 2018). *Instituto Nacional de Contadores Públicos*. Obtenido de https://www.incp.org.co/la-auditoria-basada-riesgos-cuales-ventajas/

Humboldt. (2004). *El ABC de la Gestión de Riesgos.* Humboldt.

Ingravallo, H., & Entraigas, V. (19 de Marzo de 2007). *Departamento de Informática sede Trelew.* Obtenido de http://www.dit.ing.unp.edu.ar/graduate/bitstream/123456789/208/1/ActivityLogGava.pdf

Inversiones Alcabama S.A. (04 de 2016). *ALCABAMA*. Obtenido de Alcabama Web site: http://alcabama.com/mision-vision

Inversiones Alcabama S.A. (04 de 2016). *ALCABAMA*. Obtenido de Alcabama Web Site: http://alcabama.com/compromiso-social

Inversiones Alcabama S.A. (04 de 2016). *ALCABAMA*. Obtenido de Alcabama Web Site: http://alcabama.com/nuestra-experiencia

Inversiones Alcabama S.A. (04 de 2016). *ALCABAMA*. Obtenido de Alcabama Web Site: http://alcabama.com/nuestros-servicios

Iturriaga, C. K., Contreras, R. S., & Villavicencio, R. A. (2017). *Auditoría Interna Perspectivas*

de vanguardia. México: Instituto Mexicano de Contadores Públicos.

Jhon Alexander López, A. F. (2013). *Desarrollo de una metodología para el control de reisgos para auditoría a Bases de Datos.* Pereira.

Jimenez, R. (20 de 1 de 2014). *qore*. Obtenido de http://www.qore.com/articulos/14763/Como-se-llevo-a-cabo-el-ataque-a-Target

LASSO URBANO, C. A. (2015). *Universidad Nacional Abierta y a Distancia - UNAD.* Obtenido de https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/3717/1/27149612.pdf

Lozano, L. C. (2014). *Universidad Militar.* Obtenido de https://repository.unimilitar.edu.co/bitstream/handle/10654/13537/Importancia%20de%20las%20Auditorias.pdf;jsessionid=E9CD93FFAA43918FD2CE2863277D477F?sequence=1

Luna, O. F. (2007). *Auditoría Gubernamental Moderna.* Lima: IICO.

Luna, Y. B. (2012). *Auditoría Integral normas y procedimientos.* Bogotá: ECOE.

Malagón-Londoño, G., Morera, R. G., & Laverde, G. P. (2003). *Auditoría en Salud Para una Gestión Eficiente.* Bogotá: Editorial Médica Panamericana.

Medina, E. (3 de 6 de 2016). *Muy Seguridad*. Obtenido de https://www.muyseguridad.net/2016/06/03/myspace-robo-427-millones-contrasenas/

Ministerio de Comercio, Industria y Turismo. (13 de 05 de 2014). Decreto 886 de 2014. *Decreto*

886 de 2014, Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, relativo al Registro Nacional de Bases de Datos. Colombia. Obtenido de https://ucatolica-leyex-info.ucatolica.basesdedatosezproxy.com/normativa/detalle/decreto-886-de-2014-36452/txt

MINTRABAJO. (20 de 04 de 2019). *Ministerio del Trabajo*. Obtenido de http://www.mintrabajo.gov.co/empleo-y-pensiones/empleo/subdireccion-de-formalizacion-y-proteccion-del-empleo/que-es-la-seguridad-social

Murillo, J. V. (30 de 11 de 2006). *Dialnet.* Obtenido de https://dialnet.unirioja.es/descarga/articulo/5381374.pdf

Navarro, J. C. (2006). *Apuntes de Auditoría.* España: LaTex.

Noguera Quenguan, L. Y., & Sanchez Perenguez, E. Y. (2012). *Biblioteca Alberto Quijano Guerrero.* Obtenido de http://biblioteca.udenar.edu.co:8085/atenea/biblioteca/85139.pdf

Pastor, J. R. (s.f.). *Implantación del Plan de Prevención de Riesgos Laborales en la Empresa. Gestión Integrada y Auditoría.* Madrid: Editorial Vision Net.

Pérez, A. B. (24 de 03 de 2018). *Enciclopedia Financiera*. Obtenido de https://www.enciclopediafinanciera.com/auditoria-financiera.htm

Piattini, M. G., & Pesso, E. d. (2001). *Auditoría Informática Un enfoque práctico.* México: ALFAOMEGA GRUPO EDITOR.

Ramirez, E., Torres, I., Yañez, J., & Mosqueda, Y. (Agosto de 2010). *DOCPLAYER.* Obtenido de https://docplayer.es/1918307-Auditoria-a-la-base-de-datos-sql-del-sistema-de-seguridad-de-presas-conagua.html

Redacción APD. (06 de 07 de 2018). *APD*. Obtenido de https://www.apd.es/empresas-afectadas-por-ciberataques/

Rodriguez, O. J. (2004). *La Auditoría de Sistemas de Información como elemento de control.* Palmira: Universidad del Valle.

Rouse, M. (15 de 1 de 2015). *Search Datacenter*. Obtenido de https://searchdatacenter.techtarget.com/es/definicion/Base-de-datos

Samillan, G. R., & Castillo Oviedo, E. (2017). *Repositorio Institucional Universidad Nacional Pedro Luis Gallo.* Obtenido de http://repositorio.unprg.edu.pe/bitstream/handle/UNPRG/1221/BC-TES-5923.pdf?sequence=1&isAllowed=y

Saucedo, S., Gutiérrez, L. A., Ayala, A., & Lozoya, J. (s.f.). *International Institute of Informatics and Systemics.* Obtenido de http://www.iiis.org/CDs2014/CD2014SCI/CISCI_2014/PapersPdf/CA899MY.pdf

Universidad Javeriana. (s.f.). *Pontificia Universidad Javeriana.* Obtenido de http://pegasus.javeriana.edu.co/~CIS1210IS02/news/Gu%C3%ADa%20Metodol%C3%B3gica%20para%20COBIT%204.1.pdf

Universitat de Girona l'Institut de Dret Privat Europeu. (4 de 06 de 2014). *Universitat de Girona*. Obtenido de http://civil.udg.es/normacivil/estatal/reals/Lpi.html

Vilá, J. (11 de Septiembre de 2014). *EAE Business School Harvard Deustoi*. Obtenido de EAE Business School web site: https://retos-directivos.eae.es/el-cronograma-de-actividades-y-la-dinamica-del-proyecto/

Villalobos, J. (13 de 01 de 2012). *Principios Básicos de Seguridad en Bases de Datos*. Obtenido de Revista .Seguridad: https://revista.seguridad.unam.mx/numero-12/principios-basicos-de-seguridad-en-bases-de-datos

9 Anexos

9.1 Ficha técnica del sistema

Anexo 1 Ficha técnica

FICHA TÉCNICA			
OBJETIVO:	Seguridad Social		
ESTADO:	Producción		
USUARIOS:	Administrador – Contratistas – Siso – Usuario		
PLATAFORMA TECNOLÓGICA			
SERVIDORES:			
	PROCESADOR	**MEMORIA**	**DISCO**
HW:	Core i3	8GB	500GB
SW:	OS Ubuntu 16.04	Docker	PHP – Laravel – MySQL
PC'S:			
	PROCESADOR	**MEMORIA**	**DISCO**
HW:	Intel® Core ™ i3-5005U	Ram 2.00 GB	1.70 GHz 2.00 GHz
SW:	Sistema operativo de 32 bits		
REDES:	**Internet dedicado empresarial UNE 20MB**		
FW:			
PX:			
MÓDULOS			
Administrador: Administración general del sistema y usuarios. Contratistas: Modulo para que los contratistas realicen el ingreso de sus trabajadores. Siso: Modulo en el cual se registran los datos necesarios para el pago de la seguridad social como lo son los días trabajados, reconocimiento de Jornales, Obras, datos personales, planillas de pago. Usuario: Usuario es el perfil que permite el control de la información personal de los trabajadores, es decir este usuario se encarga de ingresar y actualizar los datos personales de los trabajadores sin modificar información de pagos en las planillas.			
MANUALES			
No hay manuales			
PROCEDIMIENTOS DE BACKUP			

Se realizan backups cada 12 Horas del código fuente y la base de datos. Adicionalmente se trabaja con un sistema de control de versiones GIT, que nos permite tener el histórico de cambios que ha tenido el proyecto.

9.2 Entrevista de familiarización

9.2.1 Introducción de la entrevista.

Anexo 2 Introducción a la entrevista

CARACTERÍSTICAS DE LA ENTREVISTA	
Fecha de aplicación	15/04/2019
Tipo de entrevista	Estructurada
Enfoque	Sujeto-Objeto
Objetivos	Identificar algunas características importantes del estado actual de la base de datos de Seguridad Social y la aplicación que la aloja.
Quién realiza la entrevista	Ing. Adriana Bautista
Nombre Entrevistado	Cesar Camilo Cruz Cáceres
Edad	28 años
Ocupación	Desarrollador
Nivel de educación	Tecnólogo
Relación con el proyecto	Desarrollador del sistema de Seguridad Social, diseñador de la BD y administrador de la misma.

Formulario Preparado

A. Introducción
Como proyecto investigativo se planea realizar una auditoría a una base de datos de la empresa Inversiones Alcabama S.A., la Base de Datos seleccionada es la de Seguridad Social que se encuentra enfocada a Contratistas y a la cual se le evaluará el nivel de seguridad a fin de detectar posibles vulnerabilidades que pongan en riesgo la información de los colaboradores de la compañía.
B. Identificar entrevistados y participantes

A continuación, se describe la información recolectada a través de los cuestionarios por componente:

9.2.2 Seguridad lógica y pistas de auditoría.

Se evidencia que se cuenta con una política de control de acceso a la BD de seguridad social de la empresa Alcabama, no se encuentra documentada, pero en el proceso cuentan con un lineamiento que el equipo de TI práctica, aunque no existe una política documentada existe un proceso formal para la creación de usuarios nuevos. Para la creación de usuarios existe una Matriz de Roles y Perfiles para la asignación de los permisos. Existe un usuario diferente al DBA que tiene acceso a la BD los usuarios súper administradores en TI. Se cuenta con procedimientos para la inactivación, modificación y creación de usuarios, pero no está documentada, se evidencia que no existen políticas de bloqueo de sesión de usuarios en la aplicación, existe estándar para cambio de contraseñas y estas se guardan encriptadas, aunque no está documentado el estándar. No se cuenta con un convenio externo para custodia de claves. Se evidencia que no tienen pistas de auditoria activas, se realiza revisión periódica de los logs, no se limitan campos de almacenamiento en la creación de tablas y campos. Se evidencia Ver Cuestionario – Anexo 1

Anexo 3 Cuestionario Seguridad lógica y pistas de auditoría

SEGURIDAD LÓGICA Y PISTAS DE AUDITORÍA

FECHA: 14-04-19

Nº	PREGUNTA	SI	NO	N/A	OBSERVACIONES
1	¿Se cuenta con una politica o estandar que haya sido definida por el área de TI para el control de acceso a las BDs?	X			solo usuarios de el directorio activo con permisos del grupo de TI
2	¿Se cuenta con una lista de usuarios de la BD?	X			
3	¿El dueño de la base de datos realiza certificación de usuarios?	X			se realiza directamente en el directorio activo
4	¿Existe un proceso formal para la solicitud de creación de nuevos usuarios?	X			
5	¿El proceso de solicitud de usuarios nuevos se encuentra documentado?		X		→ Sin documentación que soporte el proceso.
6	¿Existen diferentes estados de usuario como Activo, Inactivo, bloqueado?	X			
7	¿Se realizan validaciones para que no existan campos nulos?	X			
8	¿Existe una Matriz de Roles y Perfiles de la base de datos?	X			
9	¿Se cuenta con un estandar definido que permita aplicar controles que garanticen la adecuada asignación de privilegios y roles?	X			
10	¿Existen usuarios que tengan acceso directo a la BD, diferentes a los DBA?	X			5 usuarios super-admin en TI
11	¿La creación, Modificación y eliminación de cuentas de usuario se encuentra a cargo del DBA?		X		se realiza el administrador del sistema, no se necesario solo se inactivan
12	¿Se eliminan las cuentas de usuario inactivas?	X			luego de un periodo de 3 meses
13	¿Se cuenta con una asignación de permisos para creación, modificación, y consulta a las tablas de a cuerdo a los roles y perfiles existentes?	X			
14	¿Existe un límite de caracteres para la longitud máxima en la creación del usuario?	X			50 caracteres
15	¿Existe bloqueo de sesión por inactividad de usuarios en el sistema?	X	(X)		→ La sesión permanece activa
16	¿Existe un límite de caracteres para la longitud máxima en la creación de contraseñas?	X			12 caracteres
17	¿La contraseña puede ser igual a la identificación del usuario?		X		Debe contener caracteres alfanumé
18	¿Cuando un usuario ingresa por primera vez se solicita realizar el cambio de su contraseña?	X			
19	¿Se tiene establecido el numero de intentos fallidos de la conexión por parte del usuario antes de que la cuenta sea bloqueada?	(X)			→ Validar 6 intentos
20	¿Se tienen tiempos definidos para vencimiento de contraseña?		X		
21	¿Cuando la contraseña se guarda es encriptada?	X			
22	¿La contraseña es guardada en un area de la base de datos accesible para los usuarios?		X		
23	¿Al crear roles y perfiles de usuario se cuenta con una longitud máxima de caracteres?	X			20 caracteres
24	¿El perfil del DBA es acorde a la persona que ejerce el rol junto con todas sus responsabilidades asignadas?	X			
25	¿Se realizan validaciones de los permisos asociados a los perfiles sensibles y que hayan sido asignados correctamente únicamente a los perfiles autorizados?	X			
26	¿Se tiene un proceso formal de custodia de claves para los usuarios propios de la BD?	X			
27	¿Se tiene algún convenio externo para el almacenamiento o custodia de las claves?		X		
28	¿Existen procesos definidos para monitorear la seguridad de la BD?	X			
29	¿La BD puede generar Logs?	X			
30	¿La BD tiene activa las pistas de auditoria?		X		
31	¿Se tiene definida una revisión periodica de los losgs de la BD?		X		
32	¿Se realiza una revisión y gestión periodica al log de transacciones dejando evidencia de las gestiones realizadas?	X			
33	¿Existen Triggers para el monitoreo de las bases de datos?	X			
34	¿Existen registros de los intentos de accesos satisfactorios o denegados a estructuras, tablas fisicas y logicas del repositorio?	X			
35	¿Se limitan las estructuras de almacenamiento (tamaño) para creación de objetos?		X		
36	¿Se limita el tamaño en la BD para la creación de tablas y campos?	X			
Totales					

Datos de quien atiende la entrevista

Nombre: Cesar Cruz **Documento:**

Cargo: Desarrollador PHP **Firma:**

9.2.3 Integridad.

El cuestionario deja ver que el sistema cuenta con un Modelo E/R, DD y BD, la BD se actualiza cada vez que se realiza una transacción y el DD se actualiza con cada cambio a la BD. Se evidencia que cuando se realizan cambios o actualizaciones a la BD no queda un registro que lo respalde. En cuanto al manejo de las claves se evidencia que no solo el DBA tiene acceso a las claves de la aplicación, existe procedimiento de recuperación de claves en caso de pérdida, pero estos no se encuentran documentados. Se encuentra según el cuestionario que se lleva un control de usuarios, el motor de BD soporta herramientas de auditoria, existe herramientas de monitoreo de la BD, se cuenta con proceso de recuperación en caso de caída, se tienen definidos proceso de Rollback para recuperar instancias, se indica que el DBMS no cuenta con procesos de recuperación, se indica que el DBMS no permite procesos de recuperación, existen medidas de contingencia en caso de pérdida de datos pero no se encuentran documentadas.

Anexo 4 Cuestionario de Integridad

CUESTIONARIO INTEGRIDAD

FECHA: 14-04-19

Nº	PREGUNTA	SI	NO	N/A	OBSERVACIONES
1	¿El sistema cuenta con un MER?	(V)			→ Suministrado por DBA
2	¿Hay un responsable de mantener el MER?	X			
3	¿Existe un Diccionario de datos?	X			
4	¿El DD se actualiza con cada modificación en la BD?	X			
5	¿Quién actualiza las BD?				DBA
6	¿Con qué periodicidad se actualiza la BD?				cada vez que hay una actualización
7	¿El DBA puede modificar información de la BD?	X			
8	¿Se cuenta con documentación de la BD?	(X)			→ solo MER
9	¿Todos los cambios o actualizaciones en BD son registrados por escrito?		X		
10	¿Solo el DBA tiene acceso a las claves de la aplicación?		X		
11	¿Si el DBA no se encuentra, alguién mas puede acceder a la aplicación?	X			no con un usuario diferente
12	¿Existe un procedimiento de recuperación en caso de pérdida de claves? Se aplica?	(X)			→ no documentado
13	¿El DBA lleva un control de usuarios?	X			
14	Si es necesario restablecer la BD, ¿se le comunica al DBA?	X			
15	¿El motor de base de datos soporta herramientas de auditoría?	X			
16	¿Existen herramientas de monitoreo de datos?	X			
17	En caso de caida, ¿se cuenta con un proceso de recuperación?	X			
18	¿Hay definidos y activados segmentos de Rollback para recuperar instancias?	X			
19	¿El DBMS permite procesos de recuperación?		X		
20	¿Que herramientas se utilizan para la recuperación de datos?		X		
21	¿Existen medidas de contingencia en caso de pérdida de datos? Cuáles?	X			Detener la operación, analizar el siniestro, restaurar backups.
Totales					

Datos de quien atiende la entrevista

Nombre: Cesar Cruz **Documento:**

Cargo: Desarrollador PHP **Firma:**

9.2.4 Continuidad - backup y restauración.

Se encontró que se realizan copias de seguridad diariamente aunque no existe procedimiento documentado para estas, indica que se lleva un registro de las copias de seguridad que se realizan, indica que se realiza la revisión de las copias de seguridad una vez terminada para verificar la terminación exitosa de esta y se realiza registro de la validación del log, se realiza el almacenamiento de estas copias bajo llave, aunque este almacenamiento lo realizan varias personas de TI, este proceso no se encuentra bajo un solo responsable, se encuentra que realizan copias de seguridad cada vez que se realiza un cambio en la BD. Se indica que no existen contratos con terceros para procesos de contingencia, sin embargo, cuenta con un servidor alterno ubicado en otra ubicación geográfica, no se tiene plan de contingencia, se cuenta con sistema de detección de incendios. No se cuenta con proceso documentado para realizar restauración de copias de seguridad, se realizan pruebas de recuperación periódica en los ambientes de pruebas y desarrollo, no se cuenta con un cronograma de mantenimiento y pruebas de contingencia.

Anexo 5 Cuestionario Continuidad - Backup y Restauración

CUESTIONARIO CONTINUIDAD

FECHA:

Nº	PREGUNTA	SI	NO	N/A	OBSERVACIONES
1	¿Realiza copias de seguridad de la BD?	X			
2	¿Existe un procedimiento documentado para realizar las copias de seguridad?		(X)		no hay soporte escrito
3	¿Realiza copias de seguridad a diario?	X			
4	¿Existe un responsable del procedimiento para realizar copias de seguridad?	X			
5	¿Lleva un control / planilla para registro de las copias de seguridad?	X			
6	¿Revisa las copias de seguridad? Que hayan sido efectivas, que contengan la información respaldada	X			
7	¿Revisa el log de la copia de seguridad?	X			
8	¿Deja evidencia (informe/registro novedades/bitácora) de la revisión de este log? Cuál?	(X)			no informa cuál
9	¿Guarda bajo llave las copias de seguridad?	X			
10	¿Ud es la única persona encargada de salvaguardar las copias de seguridad en la organización?		X		
11	¿Realiza copia de seguridad cada vez que se hacen cambios a la BD?	X			
12	¿Realiza manualmente la copia de seguridad?		X		
13	¿Tiene automatizado el precedimiento de realización de copias de seguridad?	X			
14	¿Rotula adecuadamente las copias de seguridad?		X		
15	¿Realiza copia de seguridad completa?	X			
16	¿Realiza copia de seguridad diferencial?		X		
17	¿Realiza copia de seguridad en cintas?	X			
18	¿Realiza copia de seguridad en discos?	X			
19	¿Realiza copia de seguridad en en la nube?		X		
20	¿Guarda copia de seguridad fuera de la organización?		X		
21	¿Tiene contrato de alquiler de servidor con terceros en caso de una contingencia?		X		
22	¿Tiene algún servidor alterno, localizado en otra ubicación geográfica?	X			
23	¿Se tienen alternativas de funcionamiento de la BD en caso de un evento no deseado?		X		
24	¿Bajo qué condiciones realiza copias de seguridad?				cada 6 horas se realiza
25	¿Qué pasa si ocurre un incendio?				El sistema antiincendios se dispara las máquinas se apagan automáticame ya ha sucedido y se deben restable cer los backups
26	¿Qué pasa si se daña el servidor?				
27	¿Existe un procedimiento documentado para realizar restauración de copias de seguridad?		(X)		sin soporte escrito
28	¿Existe un responsable del procedimiento para realizar restauración de copias de seguridad?	X			
29	¿Realiza pruebas de recuperación de información periódicas en el ambiente de producción-pruebas o desarrollo?	X			
30	¿Cuenta con un documento Plan de Recuperación del Negocio?		(X)		

31	¿Ha realizado pruebas de recuperación de información, con el fin de verificar la veracidad de la información almacenada en las copias de seguridad?	X		
32	¿Ha realizado procedimientos de recuperación de información en los últimos 6 meses?	X		
33	¿La BD se encuentra incluida dentro del Plan de Recuperación del Negocio?	X		
34	¿La BD está clasificada como crítica en el Plan de Recuperación del Negocio?	X		
35	¿Se tiene estipulado un cronograma de mantenimiento y pruebas de contingencia?		X	
36	¿Se valida el cumplimiento del cronograma de mantenimiento y pruebas de contingencia?		X	
37	¿Se registra el seguimiento al cronograma de mantenimiento y pruebas de contingencia?		X	
Totales				

Datos de quien atiende la entrevista

Nombre: Cesar Cruz Documento:

Cargo: Desarrollador PHP Firma:

9.2.5 Seguridad en el ambiente.

Se indica en el cuestionario que no se cuenta con un control de acceso biométrico al centro de cómputo, el acceso a este es por medio de llave, no se lleva un registro del personal que ingresa al Centro de Computo, tiene sistema de vigilancia atreves de cámaras, UPS para proteger los equipos de descargas de voltaje, se realiza monitoreo de la temperatura, no cuenta con pisos falsos, se cuenta con un plan alterno en caso de fallas de energía, los servidores se encuentran en RAC, cuenta con firewall, proxy, planta telefónica, se indica que se realiza mantenimiento de los servidores, se realiza actualización de antivirus en los servidores y pc, se cuenta con Directorio activo, existe política para cambio periódico de contraseñas, y se cuenta con procedimientos para la actualización de software pero no se encuentran documentados.

Anexo 6 Seguridad en el Ambiente

CUESTIONARIO AMBIENTE

FECHA: 14-04-19

Nº	PREGUNTA	SI	NO	N/A	OBSERVACIONES
1	¿Controlan el acceso al centro de cómputo a través de guarda de seguridad?		X		
2	¿Controlan el acceso al centro de cómputo a través de identificación dactilar?		X		
3	¿Controlan el acceso al centro de cómputo a través de tarjeta electrónica?		X		→ Riesgo de acceso no autorizado
4	¿Controlan el acceso al centro de cómputo a través de clave?		X		
5	¿Controlan el acceso al centro de cómputo a través de identificación biométrica?		X		
6	¿Se lleva registro del ingreso al centro de cómputo?		X		
7	¿El centro de cómputo es vigilado a través de cámaras?	(X)			→ solo registro de cámaras.
8	¿Se cuenta con UPS en el centro de cómputo?	X			
9	¿Se realiza monitoreo a la UPS?	X			
10	¿Se monitorea la temperatura del centro de cómputo?	X			
11	¿Se registra medición de temperaturas del centro de cómputo?	X			
12	¿El centro de Computo Cuenta con piso falso?		(X)		→ Riesgo
13	¿Se cuenta Con un plan alterno en caso de falta de energía?	X			
14	¿Se cuenta con sistema de detección de incendios?	X			
15	¿Los servidores se encuentran en un RAC?	X			
16	¿Se cuenta con Firewall?	X			
17	¿Se cuenta con proxy?	X			
18	¿Se cuenta con planta telefónica en el centro de cómputo?	X			
19	¿Se hace mantenimiento a los servidores?	X			
20	¿Se registra el mantenimiento a los servidores?	X			
21	¿Se cuenta con antivirus actualizado en los servidores y pc?	(X)			→ Validar en un PC
22	¿Se controla la instalación de software no permitido?	(X)			→ Validar
23	¿Se cuenta con Directorio activo?	X			
24	¿Se tiene restringida la configuración de los PC para los usuarios?	X			
25	¿Se solicita periodicamente cambiar contraseñas para ingreso al SO/Aplicativos?	X			
26	¿Se cuenta con procedimientos para la actualización de software?	X			
Totales					

Datos de quien atiende la entrevista

Nombre: Cesar Cruz **Documento:**

Cargo: Desarrollador PHP **Firma:**

9.3 Matriz de riesgos

Una vez recolectada y entendida la información de los componentes, se definió la matriz de riesgos y controles:

Anexo 7 Matriz de Riesgos

Empresa: Inversiones Alcabama S.A.									
Análisis de Riesgos									
Identificación y valoración de Riesgos									
Escenario	**Actividad**	**Código**	**Nombre**	**Descripción**	**Impacto**		**Probabilidad**		**Control**
					Categoría	**Peso**	**Categoría**	**Peso**	
SEGURIDAD LÓGICA	AC01 - Creación de nuevos usuarios	RSA1-01	Pérdida de integridad por permitir acceso a usuarios no autorizados a la BD	Pérdida de integridad por permitir acceso a usuarios no autorizados a la BD, causando información errada en los procesos de liquidación	Mayor	4	Posible	3	Configuración de permisos de usuarios de acuerdo a roles y perfiles establecidos
		RSA1-02	Divulgación de información	Divulgación de información por permitir ingreso a usuarios no autorizados a la BD causando multas o sanciones por divulgación de información sensible	Catastrófico	5	Posible	4	Configuración de permisos de usuarios de acuerdo a roles y perfiles establecidos
	AC02 - Bloqueo de sesión de usuario por inactividad	RSA2-01	Pérdida de información por ingreso de usuario no permitido	Pérdida de información por ingreso de usuario no permitido al sistema, lo cual puede generar multas por el retraso en el pago de Seguridad social	Mayor	5	Probable	3	Implementar políticas de bloqueo de usuario automático después de 5 minutos de inactividad
		RSA2-02	Fuga de información por ingreso de usuario no autorizado	Fuga de información por ingreso de usuario no autorizado al sistema lo cual puede ocasionar multas por divulgar información sensible.	Mayor	5	Casi Seguro	5	Implementar políticas de bloqueo de usuario automático después de 5 minutos de inactividad

AC03 - Monitoreo de Logs	RSA3-01	Pérdida de Información por no detección de error	Pérdida de información por no detección de errores en la BD omitiendo liquidación de seguridad social de algunos empleados.	Menor	2	Improbable	2	Realizar monitoreo continuo de logs a la BD y verificación de logs de transacciones
AC04 - Almacenamiento en la BD	RSA4-01	Indisponibilidad de la BD y la aplicación	Indisponibilidad de la aplicación por saturación de procesos lo cual puede ocasionar demoras en generación de reportes de Seguridad Social	Mayor	5	Improbable	1	Realizar mantenimiento periódico al servidor de BD para evitar saturación de información no necesaria
AC05- Asignación de roles y perfiles de acceso a BD y aplicaciones	RSA5-01	Pérdida de confidencialidad por información sensible expuesta	Pérdida de confidencialidad por información sensible expuesta debido a ingreso de usuarios a la BD sin autorización.	Mayor	5	Probable	2	Realizar configuración de permisos de usuarios de acuerdo a roles y perfiles establecidos
	RSA5-02	Indisponibilidad de la BD por borrado de información	Indisponibilidad de la BD por borrado de información debido a ingreso de usuarios con permiso de administrador	Mayor	5	Improbable	1	Realizar configuración de permisos de usuarios de acuerdo a roles y perfiles establecidos
	RSA5-03	Perdida de información por permitir acceso como administrador	Perdida de información por permitir ingreso del grupo de Active Directory “Administradores de dominio” y el grupo “Administradores” administrador local de acceso, como un administrador de la base, al SQL Server.	Catastrófico	5	Posible	3	Grupos de usuarios de Windows “Administradores de dominio” o “Administradores” no deben tener acceso a SQL Server.

INTEGRIDAD	AC01-Control de cambios	RSA5-04	Perdida de información por asignar roles de DBA a un usuario por error	Perdida de información por la asignación de la función DBA a personas no autorizadas aumenta el riesgo de que los comandos del sistema no autorizados lo cual puede ocasionar acceso no autorizado a los objetos (es decir, tablas de datos) y puede ocasionar una pérdida de información	Catastrófico	5	Improbable	2	La función de DBA debe configurarse solo a los usuarios que requieren dicho acceso, ya que este papel es un papel DBA administración creada durante la instalación inicial de la base de datos. Este papel es privilegiado. Cualquier persona asignada a esta función tendrá acceso prácticamente ilimitado a los recursos del sistema y de objetos.
		RSA5-05	Perdida de integridad en la información por tener activo usuarios genéricos con privilegios	Perdida de integridad en la información de las BD porque el usuario invitado tiene acceso a la función pública, que a menudo tiene los derechos sobre privilegiados y puede ocasionar daños en la BD.	Catastrófico	5	improbable	1	Las cuentas en las BD que estén como usuario invitado deben encontrarse desactivadas
		RIA1-01	Falta de disponibilidad debido a cambio instalado en producción	Falta de disponibilidad por cambio instalado en producción el cual genera retrasos en la liquidación de seguridad social que pueden acarrear pérdidas económicas por multas.	Mayor	5	Probable	4	Realizar procedimientos de solicitud y pruebas de control de cambios

		RIA1-02	Perdida de información por permitir actualizaciones al sistema de Catalogo	Perdida de información por permitir actualizaciones al sistema de Catalogo lo cual permite realizar actualizaciones, eliminaciones o inserciones en la base de datos, lo cual puede generar multas y sanciones por error en los pagos de seguridad social	Mayor	4	Improbable	1	La opción de configuración del servidor debe configurarse para no permitir actualizaciones directas en las tablas del sistema.
	AC02-Custodia de claves de la aplicación	RIA2-01	Pérdida de confidencialidad por ingreso de usuario no permitido	Pérdida de confidencialidad por ingreso de usuario no permitido con perfil de administrador, lo cual causa fuga de información sensible.	Mayor	5	Raro	1	Realizar configuración de permisos de usuarios de acuerdo a roles y perfiles establecidos
CONTINUIDAD - BACKUP Y RESTAURACIÓN	AC01 - Realización de backups	RCA1-01	Indisponibilidad de la información por error en backup	Pérdida de disponibilidad de la información de proveedores de la empresa, ocasionado por procedimiento errado en la toma de backups por el personal de TI, ocasionando pérdidas económicas y de reputación	Mayor	4	Improbable	2	Revisión de logs de la herramienta de backup verificando que haya terminado de manera exitosa
		RCA1-02	Pérdida de información por omisión de backup diario	Pérdida de información de los planes de pago de los clientes debido a que el encargado de realizar los backups omitió la creación del backup diario del servidor de archivos ocasionando una posible pérdida reputacional	Insignificante	2	Raro	1	Revisión de logs de la herramienta de backup verificando que se ejecute diariamente de manera exitosa
	AC02 - Almacenamiento y restablecimiento de Backups	RCA2-01	Pérdida de información por backup mal restablecido	Se afecta la integridad de la información de la empresa debido a procedimiento mal efectuado en el restablecimiento de backups ocasionando posible pérdida de información.	Moderado	2	Improbable	2	Verificar y documentar procedimiento de restablecimiento de backups

AC03 - Gestión de plan de Continuidad	RCA2-02	Información no disponible por fallo en la BD	Se afecta la disponibilidad de la BD de Seguridad social de la empresa debido a la falta de previsión de eventos no deseados en el funcionamiento de la BD con posible afectación a los usuarios de esta.	Moderado	4	Probable	4	Verificar procedimientos para restablecimiento de la BD posterior a una caída del sistema
	RCA2-03	Pérdida de información por caída del sistema	Se afecta la integridad de la información de las BD de la empresa por caída del sistema al no poder restaurarlo rápidamente por no contar con un plan alterno ocasionando una posible pérdida económica	Menor	2	Improbable	2	Contar con un procedimiento documentado para aplicar el plan de contingencia
	RCA2-04	Indisponibilidad de la BD y la Aplicación, porque se restauró backup que se encontraba incompleto	Indisponibilidad de la aplicación y las BD por restauración de backup que se encontraba incompleto lo cual ocasiona Pérdidas económicas por multa en el pago de seguridad social de los empleados.	Mayor	4	Improbable	1	Revisión de logs de la herramienta de backup verificando que haya terminado de manera exitosa
	RCA2-05	Pérdida de Credibilidad de la información	Pérdida de credibilidad de la información de los pagos de seguridad social por errores en el backup lo que genera problemas en la prestación del servicio a los trabajadores afiliados	Mayor	5	Improbable	2	Contar con un ambiente de pruebas para verificar que el restablecimiento de backups es correcto
	RCA3-01	Pérdida de información por personal no informado sobre medidas de emergencia	Se afecta la integridad de la información de la BD de Seguridad Social debido a falta de información sobre plan alterno en caso de emergencia con posibles errores de procedimiento en caso de presentarse una contingencia.	Mayor	3	raro	1	Documentar y divulgar el plan de continuidad del negocio al personal de TI

SEGURIDAD EN EL AMBIENTE	AC01- Control de acceso físico al centro de computo	RCA3-02	Pérdidas económicas por falta de información	Pérdida financiera de la empresa por caída del sistema que explotó la falta de información de colaboradores al presentarse un evento inesperado	Mayor	5	Improbable	2	Documentar y divulgar el plan de continuidad del negocio al personal de TI
		RAA1-01	Acceso no permitido a centro de cómputo	Se afecta la integridad y disponibilidad de la información de todas las BD de la empresa debido a que personal ajeno al área de TI explotó la falta de mecanismos de control de acceso al centro de cómputo con posible pérdida económica.	Catastrófico	5	Probable	4	Llevar registro de control de acceso al centro de cómputo
		RAA1-02	Daño en equipo del centro de cómputo por intrusión de personal no autorizado	Daño en los equipos del centro de cómputo debido a que personal externo a la empresa explotó la falta de control de acceso al centro de cómputo con posible afectación financiera	Mayor	4	Posible	2	El personal ajeno a TI debe estar acompañado de una persona de TI para el ingreso al centro de cómputo
	AC02- Seguridad de centro de computo	RAA2-01	Ausencia de pisos falsos en centro de cómputo	Se afecta la integridad de los equipos del centro de cómputo de la compañía debido a inundación de las instalaciones que explotó la falta de medidas de seguridad para centros de datos	Mayor	3	Posible	3	Contar con pisos falsos para evitar daños en los equipos
		RAA2-02	Pérdida de equipos por descarga eléctrica	Pérdida de equipos del centro de cómputo por descarga eléctrica que explotó la falta de pisos falsos del centro de cómputo	Catastrófico	4	Improbable	2	Contar con UPS para regular las sobrecargas de voltaje

	RAA2-03	Pérdida de información por infección en servidores	Pérdida de información personal de los clientes debido a que un ataque informático explotó la falta de actualización del antivirus de los equipos ocasionando pérdidas económicas y de reputación	Catastrófico	5	Improbable	1	Realizar la actualización periódica de los antivirus e instalar las actualizaciones de los parches de seguridad

9.4 Evaluación de impacto

Anexo 8 Evaluación de Impacto

IMPACTO	
Catastrófico	5
Mayor	4
Moderado	3
Menor	2
Insignificante	1

9.5 Evaluación de probabilidad

Anexo 9 Evaluación de Probabilidad

		PROBABILIDAD
Casi Seguro	5	Más de 2 veces al año
Probable	4	1 vez cada año
Posible	3	1 vez cada 2 años
Improbable	2	1 vez cada 5 años
Raro	1	1 vez cada 10 años

9.6 Diccionario de Datos

Anexo 10 Creación tabla actividad contratista

```
DROP TABLE IF EXISTS `actividad_contratista`;

CREATE TABLE `actividad_contratista` (
  `id` bigint(19) unsigned NOT NULL AUTO_INCREMENT,
  `nombre` varchar(200) CHARACTER SET latin1 DEFAULT NULL,
  PRIMARY KEY (`id`)
) ENGINE=InnoDB DEFAULT CHARSET=utf8 ROW_FORMAT=COMPACT;
```

Anexo 11 Creación tabla activity log

```
DROP TABLE IF EXISTS `activity_log`;

CREATE TABLE `activity_log` (
  `id` int(10) unsigned NOT NULL AUTO_INCREMENT,
  `log_name` varchar(255) DEFAULT NULL,
  `description` varchar(255) NOT NULL,
  `subject_id` int(11) DEFAULT NULL,
  `subject_type` varchar(255) DEFAULT NULL,
  `causer_id` int(11) DEFAULT NULL,
  `causer_type` varchar(255) DEFAULT NULL,
  `properties` text,
  `created_at` timestamp NULL DEFAULT NULL,
  `updated_at` timestamp NULL DEFAULT NULL,
  PRIMARY KEY (`id`)
) ENGINE=InnoDB DEFAULT CHARSET=utf8 ROW_FORMAT=COMPACT;
```

Anexo 12 Creación tabla afp

```
DROP TABLE IF EXISTS `afp`;

CREATE TABLE `afp` (
  `id` bigint(19) unsigned NOT NULL AUTO_INCREMENT,
  `nombre` varchar(200) DEFAULT NULL,
  PRIMARY KEY (`id`)
) ENGINE=InnoDB DEFAULT CHARSET=utf8 ROW_FORMAT=COMPACT;
```

Anexo 13 Creación tabla archivo planilla

```
DROP TABLE IF EXISTS `archivo_planilla`;

CREATE TABLE `archivo_planilla` (
  `id` int(10) unsigned NOT NULL AUTO_INCREMENT,
  `nombre` varchar(200) DEFAULT NULL,
  `archivo` varchar(50) DEFAULT NULL,
  `created_at` datetime DEFAULT NULL,
  `updated_at` datetime DEFAULT NULL,
  `entry_by` int(11) DEFAULT NULL,
  PRIMARY KEY (`id`)
) ENGINE=InnoDB DEFAULT CHARSET=utf8;
```

Anexo 14 Creación tabla arl

```
DROP TABLE IF EXISTS `arl`;

CREATE TABLE `arl` (
  `id` bigint(19) unsigned NOT NULL AUTO_INCREMENT,
  `nombre` varchar(200) DEFAULT NULL,
  PRIMARY KEY (`id`)
) ENGINE=InnoDB DEFAULT CHARSET=utf8 ROW_FORMAT=COMPACT;
```

Anexo 15 Creación tabla audits

```
DROP TABLE IF EXISTS `audits`;

CREATE TABLE `audits` (
  `id` char(36) NOT NULL,
  `type` varchar(255) NOT NULL,
  `auditable_id` int(10) unsigned NOT NULL,
  `auditable_type` varchar(255) NOT NULL,
  `old` text,
  `new` text,
  `user_id` varchar(255) DEFAULT NULL,
  `route` varchar(255) DEFAULT NULL,
  `ip_address` varchar(45) DEFAULT NULL,
  `created_at` timestamp NOT NULL DEFAULT CURRENT_TIMESTAMP ON UPDATE CURRENT_TIMESTAMP,
  PRIMARY KEY (`id`),
  KEY `audits_auditable_id_auditable_type_index` (`auditable_id`,`auditable_type`)
) ENGINE=InnoDB DEFAULT CHARSET=utf8 ROW_FORMAT=COMPACT;
```

Anexo 16 Creación tabla bdc actividad cargo

```
DROP TABLE IF EXISTS `bdc_actividad_cargo`;

CREATE TABLE `bdc_actividad_cargo` (
  `id` bigint(19) unsigned NOT NULL AUTO_INCREMENT,
  `nombre` varchar(200) DEFAULT NULL,
  `bdc_tipo_cargo_id` bigint(19) unsigned NOT NULL,
  PRIMARY KEY (`id`),
  KEY `fk_bdc_actividad_cargo_bdc_tipo_cargo1_idx` (`bdc_tipo_cargo_id`),
  CONSTRAINT `bdc_actividad_cargo_ibfk_1` FOREIGN KEY (`bdc_tipo_cargo_id`) REFERENCES `bdc_tipo_cargo` (`id`) ON DELETE NO ACTION ON UPDATE NO ACTION
) ENGINE=InnoDB DEFAULT CHARSET=utf8 ROW_FORMAT=COMPACT;
```

Anexo 17 bdc asignación

```sql
DROP TABLE IF EXISTS `bdc_asignacion`;

CREATE TABLE `bdc_asignacion` (
  `id` bigint(19) unsigned NOT NULL AUTO_INCREMENT,
  `bdc_datos_trabajador_id` bigint(19) unsigned NOT NULL,
  `fecha_afiliacion` date DEFAULT NULL,
  `fecha_ingreso` date DEFAULT NULL,
  `contratistas_id` bigint(19) unsigned NOT NULL,
  `obras_id` bigint(20) unsigned NOT NULL,
  `bdc_tipo_cargo_id` bigint(19) unsigned NOT NULL,
  `bdc_actividad_cargo_id` bigint(19) unsigned NOT NULL,
  `estado` tinyint(1) DEFAULT NULL,
  `bdc_frentes_id` bigint(19) unsigned NOT NULL,
  `descripcion_frente` text,
  `created_at` datetime DEFAULT NULL,
  `updated_at` datetime DEFAULT NULL,
  `entry_by` int(11) DEFAULT NULL,
  PRIMARY KEY (`id`),
  KEY `fk_bdc_asignacion_bdc_datos_trabajador1_idx` (`bdc_datos_trabajador_id`),
  KEY `fk_bdc_asignacion_bdc_tipo_cargo1_idx` (`bdc_tipo_cargo_id`),
  KEY `fk_bdc_asignacion_bdc_actividad_cargo1_idx` (`bdc_actividad_cargo_id`),
  KEY `fk_bdc_asignacion_bdc_frentes1_idx` (`bdc_frentes_id`),
  CONSTRAINT `bdc_asignacion_ibfk_1` FOREIGN KEY (`bdc_frentes_id`) REFERENCES `bdc_frentes` (`id`) ON DELETE NO ACTION ON UPDATE NO ACTION,
  CONSTRAINT `bdc_asignacion_ibfk_4` FOREIGN KEY (`bdc_datos_trabajador_id`) REFERENCES `bdc_datos_trabajador` (`id`) ON DELETE NO ACTION ON UPDATE NO ACTION,
  CONSTRAINT `bdc_asignacion_ibfk_5` FOREIGN KEY (`bdc_tipo_cargo_id`) REFERENCES `bdc_tipo_cargo` (`id`) ON DELETE NO ACTION ON UPDATE NO ACTION
) ENGINE=InnoDB DEFAULT CHARSET=utf8 ROW_FORMAT=COMPACT;
```

Anexo 18 bdc carnet

```sql
DROP TABLE IF EXISTS `bdc_carnet`;

CREATE TABLE `bdc_carnet` (
  `id` bigint(19) unsigned NOT NULL AUTO_INCREMENT,
  `bdc_datos_trabajador_id` bigint(19) unsigned NOT NULL,
  `estado` char(1) DEFAULT NULL,
  `fecha_creacion` date DEFAULT NULL,
  `fecha_vencimiento` date DEFAULT NULL,
  PRIMARY KEY (`id`),
  KEY `fk_bdc_carnet_bdc_datos_trabajador1_idx` (`bdc_datos_trabajador_id`),
  CONSTRAINT `bdc_carnet_ibfk_1` FOREIGN KEY (`bdc_datos_trabajador_id`) REFERENCES `bdc_datos_trabajador` (`id`) ON DELETE NO ACTION ON UPDATE NO ACTION
) ENGINE=InnoDB DEFAULT CHARSET=utf8 ROW_FORMAT=COMPACT;
```

Anexo 19 bdc carnet reimpresión

```sql
DROP TABLE IF EXISTS `bdc_carnet_reimpresion`;

CREATE TABLE `bdc_carnet_reimpresion` (
  `id` bigint(19) unsigned NOT NULL AUTO_INCREMENT,
  `fecha` date DEFAULT NULL,
  `motivo` text,
  `bdc_carnet_id` bigint(19) unsigned NOT NULL,
  PRIMARY KEY (`id`),
  KEY `fk_bdc_carnet_reimpresion_bdc_carnet1_idx` (`bdc_carnet_id`),
  CONSTRAINT `bdc_carnet_reimpresion_ibfk_1` FOREIGN KEY (`bdc_carnet_id`) REFERENCES `bdc_carnet` (`id`) ON DELETE NO ACTION ON UPDATE NO ACTION
) ENGINE=InnoDB DEFAULT CHARSET=utf8 ROW_FORMAT=COMPACT;
```

Anexo 20 Creación tabla bdc caso accidentes

```sql
DROP TABLE IF EXISTS `bdc_caso_accidente`;

CREATE TABLE `bdc_caso_accidente` (
  `id` bigint(19) unsigned NOT NULL AUTO_INCREMENT,
  `nombres` varchar(200) DEFAULT NULL,
  `telefono` varchar(10) DEFAULT NULL,
  `celular` varchar(20) DEFAULT NULL,
  `ciudad_id` bigint(20) unsigned NOT NULL,
  `bdc_datos_trabajador_id` bigint(19) unsigned NOT NULL,
  `created_at` datetime DEFAULT NULL,
  `updated_at` datetime DEFAULT NULL,
  `entry_by` int(11) DEFAULT NULL,
  PRIMARY KEY (`id`),
  KEY `fk_bdc_caso_accidente_bdc_datos_trabajador1_idx` (`bdc_datos_trabajador_id`),
  KEY `fk_bdc_caso_accidente_ciudad1_idx` (`ciudad_id`),
  CONSTRAINT `bdc_caso_accidente_ibfk_1` FOREIGN KEY (`bdc_datos_trabajador_id`) REFERENCES `bdc_datos_trabajador` (`id`) ON DELETE NO ACTION ON UPDATE NO ACTION,
  CONSTRAINT `bdc_caso_accidente_ibfk_2` FOREIGN KEY (`ciudad_id`) REFERENCES `ciudad` (`id`) ON DELETE NO ACTION ON UPDATE NO ACTION
) ENGINE=InnoDB DEFAULT CHARSET=utf8 ROW_FORMAT=COMPACT;
```

Anexo 21 Creación tabla bdc datos trabajador

```
DROP TABLE IF EXISTS `bdc_datos_trabajador`;

CREATE TABLE `bdc_datos_trabajador` (
  `id` bigint(19) unsigned NOT NULL AUTO_INCREMENT,
  `numero_documento` varchar(20) DEFAULT NULL,
  `tipo_documento_id` bigint(20) unsigned NOT NULL,
  `fecha_expedicion` date DEFAULT NULL,
  `nombres` varchar(200) DEFAULT NULL,
  `apellidos` varchar(200) DEFAULT NULL,
  `alias` varchar(100) DEFAULT NULL,
  `fecha_nacimiento` date DEFAULT NULL,
  `genero_id` bigint(20) unsigned NOT NULL,
  `grupo_sanguineo_id` bigint(19) unsigned NOT NULL,
  `estado_civil_id` bigint(19) unsigned NOT NULL,
  `ciudad_id` bigint(20) unsigned NOT NULL,
  `direccion` varchar(200) DEFAULT NULL,
  `barrio` varchar(200) DEFAULT NULL,
  `telefono` varchar(10) DEFAULT NULL,
  `celular` varchar(15) DEFAULT NULL,
  `correo` varchar(100) DEFAULT NULL,
  `eps_id` bigint(19) unsigned NOT NULL,
  `arl_id` bigint(19) unsigned NOT NULL,
  `afp_id` bigint(19) unsigned NOT NULL,
  `caja_compensacion_id` bigint(19) unsigned NOT NULL,
  `zona_proviene_id` bigint(20) unsigned NOT NULL,
  `tiempo_num_vive_bogota` int(11) DEFAULT NULL,
  `tiempo_dma_vive_bogota` varchar(45) DEFAULT NULL,
  `fiestas_id` bigint(20) unsigned NOT NULL,
  `historia` longtext,
  `estado` tinyint(1) DEFAULT NULL COMMENT 'Activo\nInactivo',
  `created_at` datetime DEFAULT NULL,
  `updated_at` datetime DEFAULT NULL,
  `entry_by` int(11) DEFAULT NULL,
  PRIMARY KEY (`id`),
  KEY `fk_bdc_datos_trabajador_genero1_idx` (`genero_id`),
  KEY `fk_bdc_datos_trabajador_grupo_sanguineo1_idx` (`grupo_sanguineo_id`),
  KEY `fk_bdc_datos_trabajador_eps1_idx` (`eps_id`),
  KEY `fk_bdc_datos_trabajador_arl1_idx` (`arl_id`),
  KEY `fk_bdc_datos_trabajador_afp1_idx` (`afp_id`),
  KEY `fk_bdc_datos_trabajador_caja_compensacion1_idx` (`caja_compensacion_id`),
  KEY `fk_bdc_datos_trabajador_tipo_documento1_idx` (`tipo_documento_id`),
  KEY `fk_bdc_datos_trabajador_ciudad1_idx` (`ciudad_id`),
  KEY `fk_bdc_datos_trabajador_ciudad2_idx` (`zona_proviene_id`),
  KEY `fk_bdc_datos_trabajador_ciudad3_idx` (`fiestas_id`),
  KEY `fk_bdc_datos_trabajador_estado_civil1_idx` (`estado_civil_id`),
  CONSTRAINT `bdc_datos_trabajador_ibfk_1` FOREIGN KEY (`afp_id`) REFERENCES `afp` (`id`) ON DELETE NO ACTION ON UPDATE NO ACTION,
  CONSTRAINT `bdc_datos_trabajador_ibfk_10` FOREIGN KEY (`arl_id`) REFERENCES `arl` (`id`) ON DELETE NO ACTION ON UPDATE NO ACTION,
  CONSTRAINT `bdc_datos_trabajador_ibfk_11` FOREIGN KEY (`caja_compensacion_id`) REFERENCES `caja_compensacion` (`id`) ON DELETE NO ACTION ON UPDATE NO ACTION,
  CONSTRAINT `bdc_datos_trabajador_ibfk_2` FOREIGN KEY (`ciudad_id`) REFERENCES `ciudad` (`id`) ON DELETE NO ACTION ON UPDATE NO ACTION,
  CONSTRAINT `bdc_datos_trabajador_ibfk_3` FOREIGN KEY (`zona_proviene_id`) REFERENCES `ciudad` (`id`) ON DELETE NO ACTION ON UPDATE NO ACTION,
  CONSTRAINT `bdc_datos_trabajador_ibfk_4` FOREIGN KEY (`fiestas_id`) REFERENCES `ciudad` (`id`) ON DELETE NO ACTION ON UPDATE NO ACTION,
  CONSTRAINT `bdc_datos_trabajador_ibfk_5` FOREIGN KEY (`eps_id`) REFERENCES `eps` (`id`) ON DELETE NO ACTION ON UPDATE NO ACTION,
  CONSTRAINT `bdc_datos_trabajador_ibfk_6` FOREIGN KEY (`estado_civil_id`) REFERENCES `estado_civil` (`id`) ON DELETE NO ACTION ON UPDATE NO ACTION,
  CONSTRAINT `bdc_datos_trabajador_ibfk_7` FOREIGN KEY (`genero_id`) REFERENCES `genero` (`id`) ON DELETE NO ACTION ON UPDATE NO ACTION,
  CONSTRAINT `bdc_datos_trabajador_ibfk_8` FOREIGN KEY (`grupo_sanguineo_id`) REFERENCES `grupo_sanguineo` (`id`) ON DELETE NO ACTION ON UPDATE NO ACTION,
  CONSTRAINT `bdc_datos_trabajador_ibfk_9` FOREIGN KEY (`tipo_documento_id`) REFERENCES `tipo_documento` (`id`) ON DELETE NO ACTION ON UPDATE NO ACTION
) ENGINE=InnoDB DEFAULT CHARSET=utf8 ROW_FORMAT=COMPACT;
```

Anexo 22 Creación tabla bdc documentos

```
DROP TABLE IF EXISTS `bdc_documentos`;

CREATE TABLE `bdc_documentos` (
  `id` bigint(19) unsigned NOT NULL AUTO_INCREMENT,
  `documento` varchar(255) DEFAULT NULL,
  `eps` varchar(255) DEFAULT NULL,
  `certificado_fondo_pensiones` varchar(255) DEFAULT NULL,
  `certificado_caja_compensacion` varchar(255) DEFAULT NULL,
  `arl` varchar(255) DEFAULT NULL,
  `certificado_alturas` varchar(255) DEFAULT NULL,
  `hoja_vida` varchar(255) DEFAULT NULL,
  `foto` varchar(255) DEFAULT NULL,
  `bdc_datos_trabajador_id` bigint(19) unsigned NOT NULL,
  `estado` enum('Activo','Inactivo') DEFAULT 'Activo',
  `created_at` datetime DEFAULT NULL,
  `updated_at` datetime DEFAULT NULL,
  `entry_by` int(11) DEFAULT NULL,
  PRIMARY KEY (`id`),
  KEY `fk_bdc_documentos_bdc_datos_trabajador1_idx` (`bdc_datos_trabajador_id`),
  CONSTRAINT `bdc_documentos_ibfk_1` FOREIGN KEY (`bdc_datos_trabajador_id`) REFERENCES `bdc_datos_trabajador` (`id`) ON DELETE NO ACTION ON UPDATE NO ACTION
) ENGINE=InnoDB DEFAULT CHARSET=utf8 ROW_FORMAT=COMPACT;
```

Anexo 23 Creación tabla bdc frentes

```
CREATE TABLE `bdc_frentes` (
  `id` bigint(19) unsigned NOT NULL AUTO_INCREMENT,
  `nombre` varchar(100) DEFAULT NULL,
  `estado` enum('Activo','Inactivo') DEFAULT 'Activo',
  `created_at` datetime DEFAULT NULL,
  `updated_at` datetime DEFAULT NULL,
  `entry_by` int(11) DEFAULT NULL,
  PRIMARY KEY (`id`)
) ENGINE=InnoDB DEFAULT CHARSET=utf8 ROW_FORMAT=COMPACT;
```

Anexo 24 Creación tabla bdc info hijos

```
DROP TABLE IF EXISTS `bdc_info_hijos`;

CREATE TABLE `bdc_info_hijos` (
  `id` bigint(19) unsigned NOT NULL AUTO_INCREMENT,
  `nombres` varchar(200) DEFAULT NULL,
  `apellidos` varchar(200) DEFAULT NULL,
  `edad` int(11) DEFAULT NULL,
  `genero_id` bigint(20) unsigned NOT NULL,
  `bdc_datos_trabajador_id` bigint(19) unsigned NOT NULL,
  `created_at` datetime DEFAULT NULL,
  `updated_at` datetime DEFAULT NULL,
  `entry_by` int(11) DEFAULT NULL,
  PRIMARY KEY (`id`),
  KEY `fk_bdc_info_hijos_genero1_idx` (`genero_id`),
  KEY `fk_bdc_info_hijos_bdc_datos_trabajador1_idx` (`bdc_datos_trabajador_id`),
  CONSTRAINT `bdc_info_hijos_ibfk_1` FOREIGN KEY (`bdc_datos_trabajador_id`) REFERENCES `bdc_datos_trabajador` (`id`) ON DELETE NO ACTION ON UPDATE NO ACTION,
  CONSTRAINT `bdc_info_hijos_ibfk_2` FOREIGN KEY (`genero_id`) REFERENCES `genero` (`id`) ON DELETE NO ACTION ON UPDATE NO ACTION
) ENGINE=InnoDB DEFAULT CHARSET=utf8 ROW_FORMAT=COMPACT;
```

Anexo 25 Creación tabla bdc info padres

```
CREATE TABLE `bdc_info_padres` (
  `id` bigint(19) unsigned NOT NULL AUTO_INCREMENT,
  `nombres` varchar(200) DEFAULT NULL,
  `apellidos` varchar(200) DEFAULT NULL,
  `telefono` varchar(10) DEFAULT NULL,
  `celular` varchar(20) DEFAULT NULL,
  `estado` text,
  `tipo` smallint(6) DEFAULT NULL COMMENT '1: Papá\n2: Mamá',
  `bdc_datos_trabajador_id` bigint(19) unsigned NOT NULL,
  `created_at` datetime DEFAULT NULL,
  `updated_at` datetime DEFAULT NULL,
  `entry_by` int(11) DEFAULT NULL,
  PRIMARY KEY (`id`),
  KEY `fk_bdc_info_padres_bdc_datos_trabajador1_idx` (`bdc_datos_trabajador_id`),
  CONSTRAINT `bdc_info_padres_ibfk_1` FOREIGN KEY (`bdc_datos_trabajador_id`) REFERENCES `bdc_datos_trabajador` (`id`) ON DELETE NO ACTION ON UPDATE NO ACTION
) ENGINE=InnoDB DEFAULT CHARSET=utf8 ROW_FORMAT=COMPACT;
```

Anexo 26 Creación tabla bdc paz y salvo

```
DROP TABLE IF EXISTS `bdc_paz_y_salvo`;

CREATE TABLE `bdc_paz_y_salvo` (
  `id` bigint(19) unsigned NOT NULL AUTO_INCREMENT,
  `bdc_retiros_id` bigint(19) unsigned NOT NULL,
  PRIMARY KEY (`id`),
  KEY `fk_bdc_paz_y_salvo_bdc_retiros1_idx` (`bdc_retiros_id`),
  CONSTRAINT `bdc_paz_y_salvo_ibfk_1` FOREIGN KEY (`bdc_retiros_id`) REFERENCES `bdc_retiros` (`id`) ON DELETE NO ACTION ON UPDATE NO ACTION
) ENGINE=InnoDB DEFAULT CHARSET=utf8 ROW_FORMAT=COMPACT;
```

Anexo 27 Creación tabla bdc referencias

```
DROP TABLE IF EXISTS `bdc_referencias`;

CREATE TABLE `bdc_referencias` (
  `id` bigint(19) unsigned NOT NULL AUTO_INCREMENT,
  `bdc_datos_trabajador_id` bigint(19) unsigned NOT NULL,
  `nombres` varchar(200) DEFAULT NULL,
  `telefono` varchar(10) DEFAULT NULL,
  `celular` varchar(20) DEFAULT NULL,
  `ciudad_id` bigint(20) unsigned NOT NULL,
  `anio` int(11) DEFAULT NULL,
  `tipo_referencia` smallint(6) DEFAULT NULL COMMENT '1: Laboral\n2: Personal',
  `created_at` datetime DEFAULT NULL,
  `updated_at` datetime DEFAULT NULL,
  `entry_by` int(11) DEFAULT NULL,
  PRIMARY KEY (`id`),
  KEY `fk_bdc_referencias_laborales_bdc_datos_trabajador1_idx` (`bdc_datos_trabajador_id`),
  KEY `fk_bdc_referencias_ciudad1_idx` (`ciudad_id`),
  CONSTRAINT `bdc_referencias_ibfk_1` FOREIGN KEY (`ciudad_id`) REFERENCES `ciudad` (`id`) ON DELETE NO ACTION ON UPDATE NO ACTION,
  CONSTRAINT `bdc_referencias_ibfk_2` FOREIGN KEY (`bdc_datos_trabajador_id`) REFERENCES `bdc_datos_trabajador` (`id`) ON DELETE NO ACTION ON UPDATE NO ACTION
) ENGINE=InnoDB DEFAULT CHARSET=utf8 ROW_FORMAT=COMPACT;
```

Anexo 28 Creación tabla bdc registros

```
CREATE TABLE `bdc_retiros` (
  `id` bigint(19) unsigned NOT NULL AUTO_INCREMENT,
  `bdc_datos_trabajador_id` bigint(19) unsigned NOT NULL,
  `periodo_retiro` varchar(10) DEFAULT NULL,
  `numero_planilla` varchar(15) DEFAULT NULL,
  `bdc_asignacion_id` bigint(19) unsigned NOT NULL,
  `created_at` datetime DEFAULT NULL,
  `updated_at` datetime DEFAULT NULL,
  `entry_by` int(11) DEFAULT NULL,
  PRIMARY KEY (`id`),
  KEY `fk_bdc_retiros_bdc_datos_trabajador1_idx` (`bdc_datos_trabajador_id`),
  KEY `fk_bdc_retiros_bdc_asignacion1_idx` (`bdc_asignacion_id`),
  CONSTRAINT `bdc_retiros_ibfk_1` FOREIGN KEY (`bdc_asignacion_id`) REFERENCES `bdc_asignacion` (`id`) ON DELETE NO ACTION ON UPDATE NO ACTION,
  CONSTRAINT `bdc_retiros_ibfk_2` FOREIGN KEY (`bdc_datos_trabajador_id`) REFERENCES `bdc_datos_trabajador` (`id`) ON DELETE NO ACTION ON UPDATE NO ACTION
) ENGINE=InnoDB DEFAULT CHARSET=utf8 ROW_FORMAT=COMPACT;
```

Anexo 29 Creación tabla bdc soportes

```
DROP TABLE IF EXISTS `bdc_soportes`;

CREATE TABLE `bdc_soportes` (
  `id` int(10) unsigned NOT NULL AUTO_INCREMENT,
  `planilla` varchar(100) DEFAULT NULL,
  `contratistas_id` bigint(19) unsigned NOT NULL,
  `archivo_planilla` varchar(200) DEFAULT NULL,
  `reporte_accidentalidad` text,
  `listado_trabajadores` varchar(100) DEFAULT NULL,
  `fecha_pago` date DEFAULT NULL,
  `periodo` date DEFAULT NULL,
  `operadores_id` int(10) unsigned NOT NULL,
  `fecha` datetime DEFAULT NULL,
  `usuario` varchar(200) DEFAULT NULL,
  `entry_by` int(11) DEFAULT NULL,
  `created_at` datetime DEFAULT NULL,
  `updated_at` datetime DEFAULT NULL,
  PRIMARY KEY (`id`),
  KEY `fk_bdc_soportes_operadores1_idx` (`operadores_id`),
  CONSTRAINT `fk_bdc_soportes_operadores1` FOREIGN KEY (`operadores_id`) REFERENCES `operadores` (`id`) ON DELETE NO ACTION ON UPDATE NO ACTION
) ENGINE=InnoDB DEFAULT CHARSET=utf8 ROW_FORMAT=COMPACT;
```

Anexo 30 Creación tabla bdc traslados

```
DROP TABLE IF EXISTS `bdc_traslados`;

CREATE TABLE `bdc_traslados` (
  `id` bigint(19) unsigned NOT NULL AUTO_INCREMENT,
  `bdc_datos_trabajador_id` bigint(19) unsigned NOT NULL,
  `fecha_traslado` date DEFAULT NULL,
  `tipo` enum('contractor','project') DEFAULT NULL,
  `id_desde` int(10) unsigned NOT NULL,
  `id_hasta` int(10) unsigned NOT NULL,
  `bdc_asignacion_id` bigint(19) unsigned NOT NULL,
  `created_at` datetime DEFAULT NULL,
  `updated_at` datetime DEFAULT NULL,
  `entry_by` int(11) DEFAULT NULL,
  PRIMARY KEY (`id`),
  KEY `fk_bdc_traslados_bdc_datos_trabajador1_idx` (`bdc_datos_trabajador_id`),
  KEY `fk_bdc_traslados_bdc_asignacion1_idx` (`bdc_asignacion_id`),
  CONSTRAINT `bdc_traslados_ibfk_1` FOREIGN KEY (`bdc_asignacion_id`) REFERENCES `bdc_asignacion` (`id`) ON DELETE NO ACTION ON UPDATE NO ACTION,
  CONSTRAINT `bdc_traslados_ibfk_2` FOREIGN KEY (`bdc_datos_trabajador_id`) REFERENCES `bdc_datos_trabajador` (`id`) ON DELETE NO ACTION ON UPDATE NO ACTION
) ENGINE=InnoDB DEFAULT CHARSET=utf8 ROW_FORMAT=COMPACT;
```

Anexo 31 Creación tabla beneficios

```
DROP TABLE IF EXISTS `beneficios`;

CREATE TABLE `beneficios` (
  `id` int(10) unsigned NOT NULL AUTO_INCREMENT,
  `nombre` varchar(100) DEFAULT NULL,
  `porcentaje` varchar(5) DEFAULT NULL COMMENT 'Campo para porcentajes con 2 decimales.',
  `tipo` enum('Eps','Afp','Arl','Caja de compensación') DEFAULT NULL,
  `estado` enum('Activo','Inactivo') DEFAULT 'Activo',
  `entry_by` int(11) DEFAULT NULL,
  `created_at` datetime DEFAULT NULL,
  `updated_at` datetime DEFAULT NULL,
  PRIMARY KEY (`id`)
) ENGINE=InnoDB DEFAULT CHARSET=utf8 ROW_FORMAT=COMPACT;
```

Anexo 32 Creación tabla beneficios contratistas

```
DROP TABLE IF EXISTS `beneficios_contratistas`;

CREATE TABLE `beneficios_contratistas` (
  `id` int(10) unsigned NOT NULL AUTO_INCREMENT,
  `contratista_id` int(10) unsigned DEFAULT NULL,
  `beneficios_id` int(10) unsigned NOT NULL,
  `entry_by` int(11) DEFAULT NULL,
  `created_at` datetime DEFAULT NULL,
  `updated_at` datetime DEFAULT NULL,
  `deleted_at` datetime DEFAULT NULL,
  PRIMARY KEY (`id`),
  KEY `fk_beneficios_contratistas_beneficios1_idx` (`beneficios_id`),
  CONSTRAINT `fk_beneficios_contratistas_beneficios1` FOREIGN KEY (`beneficios_id`) REFERENCES `beneficios` (`id`) ON DELETE NO ACTION ON UPDATE NO ACTION
) ENGINE=InnoDB DEFAULT CHARSET=utf8 ROW_FORMAT=COMPACT;
```

Anexo 33 Creación tabla caja compensación

```
DROP TABLE IF EXISTS `caja_compensacion`;

CREATE TABLE `caja_compensacion` (
  `id` bigint(19) unsigned NOT NULL AUTO_INCREMENT,
  `nombre` varchar(200) DEFAULT NULL,
  PRIMARY KEY (`id`)
) ENGINE=InnoDB DEFAULT CHARSET=utf8 ROW_FORMAT=COMPACT;
```

Anexo 34 Creación tabla ciudad

```
DROP TABLE IF EXISTS `ciudad`;

CREATE TABLE `ciudad` (
  `id` bigint(20) unsigned NOT NULL AUTO_INCREMENT,
  `nombre` varchar(200) DEFAULT NULL,
  `departamento_id` bigint(20) unsigned NOT NULL,
  PRIMARY KEY (`id`),
  KEY `fk_ciudad_departamento1_idx` (`departamento_id`),
  CONSTRAINT `ciudad_ibfk_1` FOREIGN KEY (`departamento_id`) REFERENCES `departamento` (`id`) ON DELETE NO ACTION ON UPDATE NO ACTION
) ENGINE=InnoDB DEFAULT CHARSET=utf8 ROW_FORMAT=COMPACT;
```

Anexo 35 Creación tabla contratistas

```
DROP TABLE IF EXISTS `contratistas`;

CREATE TABLE `contratistas` (
  `id` int(11) NOT NULL,
  `nombre` varchar(255) DEFAULT NULL,
  `nit` varchar(255) DEFAULT NULL,
  `email` varchar(200) DEFAULT NULL,
  `password` varchar(255) DEFAULT NULL,
  `status` varchar(255) DEFAULT NULL,
  `dv` int(1) DEFAULT NULL,
  `profiles` varchar(255) DEFAULT NULL,
  `created_at` datetime DEFAULT NULL,
  `updated_at` datetime DEFAULT NULL,
  `entry_by` int(11) DEFAULT NULL,
  PRIMARY KEY (`id`)
) ENGINE=InnoDB DEFAULT CHARSET=utf8;
```

Anexo 36 Creación tabla datos archivo planilla

```
DROP TABLE IF EXISTS `datos_archivo_planilla`;

CREATE TABLE `datos_archivo_planilla` (
  `id` int(10) unsigned NOT NULL AUTO_INCREMENT,
  `archivo_planilla_id` int(10) unsigned NOT NULL,
  `periodo` date DEFAULT NULL,
  `documento` varchar(20) DEFAULT NULL,
  `dias_planilla` tinyint(2) DEFAULT NULL,
  `dias_director_obra` tinyint(2) DEFAULT NULL,
  `dias_asistencia` tinyint(2) DEFAULT NULL,
  `dias_trabajados` tinyint(2) DEFAULT NULL,
  `created_at` datetime DEFAULT NULL,
  `updated_at` datetime DEFAULT NULL,
  `entry_by` int(11) DEFAULT NULL,
  PRIMARY KEY (`id`),
  KEY `fk_datos_archivo_planilla_archivo_planilla1_idx` (`archivo_planilla_id`),
  CONSTRAINT `fk_datos_archivo_planilla_archivo_planilla1` FOREIGN KEY (`archivo_planilla_id`) REFERENCES `archivo_planilla` (`id`) ON DELETE NO ACTION ON UPDATE NO ACTION
) ENGINE=InnoDB DEFAULT CHARSET=utf8;
```

Anexo 37 Creación tabla datos archivo planilla historial

```
DROP TABLE IF EXISTS `datos_archivo_planilla_historial`;

CREATE TABLE `datos_archivo_planilla_historial` (
  `id` int(10) unsigned NOT NULL AUTO_INCREMENT,
  `archivo_planilla_id` int(10) unsigned NOT NULL,
  `periodo` date DEFAULT NULL,
  `documento` varchar(20) DEFAULT NULL,
  `dias_planilla` tinyint(2) DEFAULT NULL,
  `dias_director_obra` tinyint(2) DEFAULT NULL,
  `dias_asistencia` tinyint(2) DEFAULT NULL,
  `dias_trabajados` tinyint(2) DEFAULT NULL,
  `created_at` datetime DEFAULT NULL,
  `updated_at` datetime DEFAULT NULL,
  `entry_by` int(11) DEFAULT NULL,
  PRIMARY KEY (`id`),
  KEY `fk_datos_archivo_planilla_historial_archivo_planilla1_idx` (`archivo_planilla_id`),
  CONSTRAINT `fk_datos_archivo_planilla_historial_archivo_planilla1` FOREIGN KEY (`archivo_planilla_id`) REFERENCES `archivo_planilla` (`id`) ON DELETE NO ACTION ON UPDATE NO ACT
) ENGINE=InnoDB DEFAULT CHARSET=utf8;
```

Anexo 38 Creación tabla departamento

```
DROP TABLE IF EXISTS `departamento`;

CREATE TABLE `departamento` (
  `id` bigint(20) unsigned NOT NULL AUTO_INCREMENT,
  `nombre` varchar(200) DEFAULT NULL,
  `pais_id` bigint(20) unsigned NOT NULL,
  PRIMARY KEY (`id`),
  KEY `fk_departamento_pais1_idx` (`pais_id`),
  CONSTRAINT `departamento_ibfk_1` FOREIGN KEY (`pais_id`) REFERENCES `pais` (`id`) ON DELETE NO ACTION ON UPDATE NO ACTION
) ENGINE=InnoDB DEFAULT CHARSET=utf8 ROW_FORMAT=COMPACT;
```

Anexo 39 Creación tabla eps

```
DROP TABLE IF EXISTS `eps`;

CREATE TABLE `eps` (
  `id` bigint(19) unsigned NOT NULL AUTO_INCREMENT,
  `nombre` varchar(200) DEFAULT NULL,
  PRIMARY KEY (`id`)
) ENGINE=InnoDB DEFAULT CHARSET=utf8 ROW_FORMAT=COMPACT;
```

Anexo 40 Creación tabla estado civil

```
DROP TABLE IF EXISTS `estado_civil`;

CREATE TABLE `estado_civil` (
  `id` bigint(19) unsigned NOT NULL AUTO_INCREMENT,
  `nombre` varchar(100) DEFAULT NULL,
  PRIMARY KEY (`id`)
) ENGINE=InnoDB DEFAULT CHARSET=utf8 ROW_FORMAT=COMPACT;
```

Anexo 41 Creación tabla género

```
DROP TABLE IF EXISTS `genero`;

CREATE TABLE `genero` (
  `id` bigint(20) unsigned NOT NULL AUTO_INCREMENT,
  `nombre` varchar(10) DEFAULT NULL,
  PRIMARY KEY (`id`)
) ENGINE=InnoDB DEFAULT CHARSET=utf8 ROW_FORMAT=COMPACT;
```

Anexo 42 Creación tabla grupo sanguíneo

```
DROP TABLE IF EXISTS `grupo_sanguineo`;

CREATE TABLE `grupo_sanguineo` (
  `id` bigint(19) unsigned NOT NULL AUTO_INCREMENT,
  `nombre` varchar(100) DEFAULT NULL,
  PRIMARY KEY (`id`)
) ENGINE=InnoDB DEFAULT CHARSET=utf8 ROW_FORMAT=COMPACT;
```

Anexo 43 Creación tabla jornales director obra

```
DROP TABLE IF EXISTS `jornales_director_obra`;

CREATE TABLE `jornales_director_obra` (
  `id` int(10) unsigned NOT NULL AUTO_INCREMENT,
  `obra_id` int(11) NOT NULL,
  `catorcena_inicio` date NOT NULL,
  `catorcena_fin` date NOT NULL,
  `contratista_id` int(11) NOT NULL,
  `bdc_asignacion_id` bigint(19) unsigned NOT NULL,
  `bdc_tipo_cargo_id` bigint(19) unsigned NOT NULL,
  `bdc_actividad_cargo_id` bigint(19) unsigned NOT NULL,
  `descripcion_actividad` varchar(45) NOT NULL,
  `valor_jornal` int(11) NOT NULL,
  `dias_laborados` int(2) NOT NULL,
  `horas_extra` int(2) NOT NULL,
  `valor_hora_extra` int(11) NOT NULL,
  `valor_total_jornal` int(11) DEFAULT NULL,
  `estado` enum('Guardado','Confirmado') NOT NULL,
  `created_at` datetime NOT NULL,
  `updated_at` datetime NOT NULL,
  `entry_by` int(11) NOT NULL,
  PRIMARY KEY (`id`),
  KEY `fk_jornales_director_obra_bdc_asignacion1_idx` (`bdc_asignacion_id`),
  KEY `fk_jornales_director_obra_bdc_tipo_cargo1_idx` (`bdc_tipo_cargo_id`),
  KEY `fk_jornales_director_obra_bdc_actividad_cargo1_idx` (`bdc_actividad_cargo_id`),
  CONSTRAINT `fk_jornales_director_obra_bdc_actividad_cargo1` FOREIGN KEY (`bdc_actividad_cargo_id`) REFERENCES `bdc_actividad_cargo` (`id`) ON DELETE NO ACTION ON UPDATE NO ACTI
  CONSTRAINT `fk_jornales_director_obra_bdc_asignacion1` FOREIGN KEY (`bdc_asignacion_id`) REFERENCES `bdc_asignacion` (`id`) ON DELETE NO ACTION ON UPDATE NO ACTION,
  CONSTRAINT `fk_jornales_director_obra_bdc_tipo_cargo1` FOREIGN KEY (`bdc_tipo_cargo_id`) REFERENCES `bdc_tipo_cargo` (`id`) ON DELETE NO ACTION ON UPDATE NO ACTION
) ENGINE=InnoDB DEFAULT CHARSET=utf8 ROW_FORMAT=COMPACT;
```

Anexo 44 Creación tabla liquidación descuentos

```
DROP TABLE IF EXISTS `liquidacion_descuentos`;

CREATE TABLE `liquidacion_descuentos` (
  `id` int(10) unsigned NOT NULL AUTO_INCREMENT,
  `bdc_soportes_id` int(10) unsigned NOT NULL,
  `obra` int(11) DEFAULT NULL,
  `fecha_control` datetime DEFAULT NULL,
  `descuentos_planilla` int(11) DEFAULT NULL,
  `multas` int(11) DEFAULT NULL,
  `otros_descuentos` int(11) DEFAULT NULL,
  `total` int(11) DEFAULT NULL,
  `observaciones` text,
  `jornal` int(11) DEFAULT NULL,
  `created_at` datetime DEFAULT NULL,
  `updated_at` datetime DEFAULT NULL,
  `entry_by` int(11) DEFAULT NULL,
  PRIMARY KEY (`id`),
  KEY `fk_liquidacion_descuentos_bdc_soportes1_idx` (`bdc_soportes_id`),
  CONSTRAINT `fk_liquidacion_descuentos_bdc_soportes1` FOREIGN KEY (`bdc_soportes_id`) REFERENCES `bdc_soportes` (`id`) ON DELETE NO ACTION ON UPDATE NO ACTION
) ENGINE=InnoDB DEFAULT CHARSET=utf8 ROW_FORMAT=COMPACT;
```

Anexo 45 Creación tabla liquidación pago planillas

```
CREATE TABLE `liquidacion_pago_planillas` (
  `id` int(10) unsigned NOT NULL AUTO_INCREMENT,
  `ordenTrabajador` int(11) DEFAULT NULL,
  `bdc_asignacion_id` bigint(19) unsigned NOT NULL,
  `obra_id` int(11) DEFAULT NULL,
  `dias_trabajados` int(11) DEFAULT NULL,
  `sueldo` int(11) DEFAULT NULL,
  `sueldo_dias_trabajados` int(11) DEFAULT NULL,
  `arl` double DEFAULT NULL,
  `eps` double unsigned DEFAULT NULL COMMENT '  ',
  `afp` double DEFAULT NULL,
  `caja_compensacion` double DEFAULT NULL,
  `total_pagar` double DEFAULT NULL,
  `dias_jornal` int(11) DEFAULT NULL,
  `dias_jornal_confirm` int(11) DEFAULT NULL,
  `multa` double DEFAULT NULL,
  `descuento` double DEFAULT NULL,
  `retiro` int(11) DEFAULT '0',
  `paz_salvo` varchar(100) DEFAULT NULL,
  `reconocimiento` int(11) DEFAULT '0',
  `jornal` int(11) DEFAULT '0',
  `bdc_soportes_id` int(10) unsigned NOT NULL,
  `estado` enum('Guardado','Confirmado','Pre Liquidado','Liquidado') DEFAULT NULL,
  `fecha_control` datetime DEFAULT NULL,
  `created_at` datetime DEFAULT NULL,
  `updated_at` datetime DEFAULT NULL,
  `entry_by` int(11) DEFAULT NULL COMMENT ' ',
  PRIMARY KEY (`id`),
  KEY `fk_liquidacion_pago_planillas_bdc_asignacion1_idx` (`bdc_asignacion_id`),
  KEY `fk_liquidacion_pago_planillas_bdc_soportes1_idx` (`bdc_soportes_id`),
  CONSTRAINT `fk_liquidacion_pago_planillas_bdc_asignacion1` FOREIGN KEY (`bdc_asignacion_id`) REFERENCES `bdc_asignacion` (`id`) ON DELETE NO ACTION ON UPDATE NO ACTION,
  CONSTRAINT `fk_liquidacion_pago_planillas_bdc_soportes1` FOREIGN KEY (`bdc_soportes_id`) REFERENCES `bdc_soportes` (`id`) ON DELETE NO ACTION ON UPDATE NO ACTION
) ENGINE=InnoDB DEFAULT CHARSET=utf8 ROW_FORMAT=COMPACT;
```

Anexo 46 Creación tabla liquidación préstamos

```sql
DROP TABLE IF EXISTS `liquidacion_prestamos`;

CREATE TABLE `liquidacion_prestamos` (
  `id` int(10) unsigned NOT NULL AUTO_INCREMENT,
  `bdc_soportes_id` int(10) unsigned NOT NULL,
  `obra` int(11) DEFAULT NULL,
  `fecha_control` datetime DEFAULT NULL,
  `numero_trabajadores` int(11) DEFAULT NULL,
  `valor_trabajador` int(11) DEFAULT NULL,
  `total` int(11) DEFAULT NULL,
  `descuento_prestamo` int(11) DEFAULT NULL,
  `observaciones` text,
  `jornal` int(11) DEFAULT NULL,
  `created_at` datetime DEFAULT NULL,
  `updated_at` datetime DEFAULT NULL,
  `entry_by` int(11) DEFAULT NULL,
  PRIMARY KEY (`id`),
  KEY `fk_liquidacion_prestamos_bdc_soportes1_idx` (`bdc_soportes_id`),
  CONSTRAINT `fk_liquidacion_prestamos_bdc_soportes1` FOREIGN KEY (`bdc_soportes_id`) REFERENCES `bdc_soportes` (`id`) ON DELETE NO ACTION ON UPDATE NO ACTION
) ENGINE=InnoDB DEFAULT CHARSET=utf8 ROW_FORMAT=COMPACT;
```

Anexo 47 Creación tabla migrations

```sql
DROP TABLE IF EXISTS `migrations`;

CREATE TABLE `migrations` (
  `migration` varchar(255) NOT NULL,
  `batch` int(11) NOT NULL
) ENGINE=InnoDB DEFAULT CHARSET=utf8 ROW_FORMAT=COMPACT;
```

Anexo 48 Creación tabla módulos

```sql
DROP TABLE IF EXISTS `modulos`;

CREATE TABLE `modulos` (
  `id` int(10) unsigned NOT NULL AUTO_INCREMENT,
  `nombre` varchar(100) DEFAULT NULL,
  `descripcion` text,
  `created_at` datetime DEFAULT NULL,
  `updated_at` datetime DEFAULT NULL,
  `entry_by` int(11) DEFAULT NULL,
  PRIMARY KEY (`id`)
) ENGINE=InnoDB DEFAULT CHARSET=utf8 ROW_FORMAT=COMPACT;
```

Anexo 49 Creación tabla obligaciones

```sql
DROP TABLE IF EXISTS `obligaciones`;

CREATE TABLE `obligaciones` (
  `id` int(10) unsigned NOT NULL AUTO_INCREMENT,
  `nombre` varchar(50) DEFAULT NULL,
  `valor` varchar(5) DEFAULT NULL,
  `created_at` datetime DEFAULT NULL,
  `updated_at` datetime DEFAULT NULL,
  PRIMARY KEY (`id`)
) ENGINE=InnoDB DEFAULT CHARSET=utf8 ROW_FORMAT=COMPACT;
```

Anexo 50 Creación tabla operadores

```
DROP TABLE IF EXISTS `operadores`;

CREATE TABLE `operadores` (
  `id` int(10) unsigned NOT NULL AUTO_INCREMENT,
  `nombre` varchar(200) DEFAULT NULL,
  `entry_by` int(11) DEFAULT NULL,
  `created_at` datetime DEFAULT NULL,
  `updated_at` datetime DEFAULT NULL,
  PRIMARY KEY (`id`)
) ENGINE=InnoDB DEFAULT CHARSET=utf8 ROW_FORMAT=COMPACT;
```

Anexo 51 Creación tabla país

```
DROP TABLE IF EXISTS `pais`;

CREATE TABLE `pais` (
  `id` bigint(20) unsigned NOT NULL AUTO_INCREMENT,
  `nombre` varchar(200) DEFAULT NULL,
  PRIMARY KEY (`id`)
) ENGINE=InnoDB DEFAULT CHARSET=utf8 ROW_FORMAT=COMPACT;
```

Anexo 52 Creación tabla password resets

```
DROP TABLE IF EXISTS `password_resets`;

CREATE TABLE `password_resets` (
  `email` varchar(255) NOT NULL,
  `token` varchar(255) NOT NULL,
  `created_at` timestamp NOT NULL DEFAULT CURRENT_TIMESTAMP ON UPDATE CURRENT_TIMESTAMP,
  KEY `password_resets_email_index` (`email`),
  KEY `password_resets_token_index` (`token`)
) ENGINE=InnoDB DEFAULT CHARSET=utf8 ROW_FORMAT=COMPACT;
```

Anexo 53 Creación tabla perfiles

```
DROP TABLE IF EXISTS `perfiles`;

CREATE TABLE `perfiles` (
  `id` int(10) unsigned NOT NULL AUTO_INCREMENT,
  `nombre` varchar(100) DEFAULT NULL,
  `descripcion` text,
  `modulos` varchar(50) DEFAULT NULL,
  `created_at` datetime DEFAULT NULL COMMENT '
  `updated_at` datetime DEFAULT NULL,
  `entry_by` int(11) DEFAULT NULL,
  PRIMARY KEY (`id`)
) ENGINE=InnoDB DEFAULT CHARSET=utf8 ROW_FORMAT=COMPACT;
```

Anexo 54 Creación tabla rel actividad contratista

```
DROP TABLE IF EXISTS `rel_actividad_contratista`;

CREATE TABLE `rel_actividad_contratista` (
  `id` bigint(19) unsigned NOT NULL AUTO_INCREMENT,
  `contratistas_id` bigint(19) unsigned NOT NULL,
  `actividad_contratista_id` bigint(19) unsigned NOT NULL,
  `estado` enum('Activo','Inactivo') DEFAULT 'Activo',
  `created_at` datetime DEFAULT NULL,
  `updated_at` datetime DEFAULT NULL,
  `entry_by` int(11) DEFAULT NULL,
  PRIMARY KEY (`id`),
  KEY `fk_rel_actividad_contratista_contratistas1_idx` (`contratistas_id`),
  KEY `fk_rel_actividad_contratista_actividad_contratista1_idx` (`actividad_contratista_id`),
  CONSTRAINT `rel_actividad_contratista_ibfk_1` FOREIGN KEY (`actividad_contratista_id`) REFERENCES `actividad_contratista` (`id`) ON DELETE NO ACTION ON UPDATE NO ACTION
) ENGINE=InnoDB DEFAULT CHARSET=utf8 ROW_FORMAT=COMPACT;
```

Anexo 55 Creación tabla revisions

```
DROP TABLE IF EXISTS `revisions`;

CREATE TABLE `revisions` (
  `id` int(10) unsigned NOT NULL AUTO_INCREMENT,
  `revisionable_type` varchar(255) NOT NULL,
  `revisionable_id` int(11) NOT NULL,
  `user_id` int(11) DEFAULT NULL,
  `key` varchar(255) NOT NULL,
  `old_value` text,
  `new_value` text,
  `created_at` timestamp NULL DEFAULT NULL,
  `updated_at` timestamp NULL DEFAULT NULL,
  PRIMARY KEY (`id`),
  KEY `revisions_revisionable_id_revisionable_type_index` (`revisionable_id`,`revisionable_type`)
) ENGINE=InnoDB DEFAULT CHARSET=utf8 ROW_FORMAT=COMPACT;
```

Anexo 56 Creación tabla sistema constructivo

```
DROP TABLE IF EXISTS `sistema_constructivo`;

CREATE TABLE `sistema_constructivo` (
  `id` bigint(20) unsigned NOT NULL AUTO_INCREMENT,
  `nombre` varchar(200) DEFAULT NULL,
  PRIMARY KEY (`id`)
) ENGINE=InnoDB DEFAULT CHARSET=utf8 ROW_FORMAT=COMPACT;
```

Anexo 57 Creación tabla sueldo

```
DROP TABLE IF EXISTS `sueldo`;

CREATE TABLE `sueldo` (
  `id` int(10) unsigned NOT NULL AUTO_INCREMENT,
  `valor` double DEFAULT NULL,
  `estado` smallint(1) DEFAULT '0',
  `created_at` datetime DEFAULT NULL,
  `updatet_at` datetime DEFAULT NULL,
  `entry_by` int(11) DEFAULT NULL,
  PRIMARY KEY (`id`)
) ENGINE=InnoDB DEFAULT CHARSET=utf8 ROW_FORMAT=COMPACT;
```

Anexo 58 Creación tabla tipo documento

```
DROP TABLE IF EXISTS `tipo_documento`;

CREATE TABLE `tipo_documento` (
  `id` bigint(20) unsigned NOT NULL AUTO_INCREMENT,
  `abreviatura` varchar(20) DEFAULT NULL,
  `descripcion` varchar(40) DEFAULT NULL,
  PRIMARY KEY (`id`)
) ENGINE=InnoDB DEFAULT CHARSET=utf8 ROW_FORMAT=COMPACT;
```

Anexo 59 Creación tabla tipo novedad

```sql
DROP TABLE IF EXISTS `tipo_novedad`;

CREATE TABLE `tipo_novedad` (
  `id` bigint(19) unsigned NOT NULL AUTO_INCREMENT,
  `nombre` varchar(200) DEFAULT NULL,
  PRIMARY KEY (`id`)
) ENGINE=InnoDB DEFAULT CHARSET=utf8 ROW_FORMAT=COMPACT;
```

Anexo 60 Creación tabla tipología obra

```sql
DROP TABLE IF EXISTS `tipologia_obra`;

CREATE TABLE `tipologia_obra` (
  `id` bigint(20) unsigned NOT NULL AUTO_INCREMENT,
  `nombre` varchar(200) DEFAULT NULL,
  PRIMARY KEY (`id`)
) ENGINE=InnoDB DEFAULT CHARSET=utf8 ROW_FORMAT=COMPACT;
```

Anexo 61 Creación tabla users

```sql
DROP TABLE IF EXISTS `users`;

CREATE TABLE `users` (
  `id` int(10) unsigned NOT NULL AUTO_INCREMENT,
  `name` varchar(255) NOT NULL,
  `email` varchar(255) NOT NULL,
  `password` varchar(60) NOT NULL,
  `remember_token` varchar(100) DEFAULT NULL,
  `status` smallint(1) DEFAULT NULL,
  `projects` text,
  `profiles` varchar(50) DEFAULT NULL,
  `user_type` enum('Global','Local') DEFAULT NULL,
  `created_at` timestamp NULL DEFAULT NULL,
  `updated_at` timestamp NULL DEFAULT NULL,
  `entry_by` int(11) DEFAULT NULL,
  PRIMARY KEY (`id`),
  UNIQUE KEY `users_email_unique` (`email`)
) ENGINE=InnoDB DEFAULT CHARSET=utf8 ROW_FORMAT=COMPACT;
```

9.7 Modelo entidad relación

Anexo 62 Modelo entidad relación