LINEAMIENTOS DE SEGURIDAD DE LA INFORMACIÓN PARA PROTEGER LA BASE DE DATOS DEL ASEGURAMIENTO DEL DEPARTAMENTO DE CUNDINAMARCA

DERIAN JESÚS DORADO DAZA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C.
2019

LINEAMIENTOS DE SEGURIDAD DE LA INFORMACIÓN PARA PROTEGER LA BASE DE DATOS DEL ASEGURAMIENTO DEL DEPARTAMENTO DE CUNDINAMARCA

DERIAN JESÚS DORADO DAZA

Trabajo de Grado para optar al título de Especialista en Seguridad Informática

Director: JULIO ALBERTO VARGAS

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C.
2019

Nota de Aceptación

_____

_____

_____

_____
Firma Presidente del Jurado

_____
Firma del Jurado

_____
Firma del Jurado

Bogotá D.C., Noviembre de 2019

DEDICATORIA

A Dios, el héroe en todas mis batallas.

A mis tías y familia, mi soporte vital.

A Aura Daza y Rafael Dorado, quienes me siguen ayudando desde la eternidad.

A mi institución la Gobernación de Cundinamarca, mi gratitud por siempre.

CONTENIDO

pág.

LISTA DE FIGURAS

pág

LISTA DE TABLAS

pág.

LISTA DE ANEXOS

Pág.

GLOSARIO

ADRES: Entidad Administradora de los Recursos del Sistema General de Seguridad Social en Salud [1]

AFILIADO: Corresponde al estado de una persona una vez ha realizado la afiliación y que le confiere el derecho a los servicios de salud que brinda el Sistema General de Seguridad Social en Salud.

BASE DE DATOS: Conjunto estructurado de datos que guardan información sobre un área o contexto particular.

BASE DE DATOS DEL ASEGURAMIENTO: Base de datos relacional implementada en la Dirección de Aseguramiento de la Secretaría de Salud, Gobernación de Cundinamarca. Contiene la información de los afiliados al Sistema General de Seguridad Social en Salud (SGSSS), personas focalizadas en Sisben y Personas Pobres No Afiliadas.

BASE DE DATOS RELACIONAL: Base de datos construida según el modelo relacional que estructura la información en tablas compuestas por filas y columnas.

BDUA: Sigla correspondiente a Base de Datos Única de Afiliados. Elemento que almacena la información a nivel nacional de todos los afiliados y es gestionada por ADRES.

BITÁCORA DE SEGUIMIENTO: Herramienta de registro y seguimiento a las actividades que el administrador realiza en su labor de administración de la Base de Datos del Aseguramiento.

ENTIDAD PROMOTORA DE SALUD (EPS): El término hace referencia a las entidades responsables de la afiliación y gestión de recursos para los afiliados al Régimen Subsidiado, Contributivo y de Excepción. La función principal de las EPSs es administrar los recursos para garantizar la prestación del Plan de Salud Obligatorio a las personas afiliadas.[2]

MAESTRO CONTRIBUTIVO: Archivo de texto con información estructurada de los afiliados al Régimen Contributivo especificado en la Resolución 4622 de 2016.

---

[1] **ADRES:** ¿qué es la ADRES? [En línea], [consultado en noviembre de 2018]. Disponible en internet: https://www.adres.gov.co/La-Entidad/-Qu%C3%A9-es-la-ADRES.

[2] COLOMBIA. MINISTERIO DE SALUD Y PROTECCIÓN SOCIAL. Resolución 4622 de 2016. [En línea], [consultado en noviembre de 2018]. Disponible en internet: https://www.minsalud.gov.co/Normatividad_Nuevo/Resolución%204622%20de%202016.pdf .

MAESTRO SUBSIDIADO: Archivo de texto con información estructurada de los afiliados al Régimen Subsidiado especificado en la Resolución 4622 de 2016.

MAESTRO SISBEN: Archivo de texto con información estructurada de los ciudadanos identificados en el programa Sisben.[3]

MAESTRO PPNA: Archivo de texto con información estructurada de las Personas Pobres No Afiliadas al Sistema General de Seguridad Social en Salud.[4]

SERVIDOR: Un servidor es una plataforma software que atiende y gestiona las peticiones de los usuarios de un sistema de información. El término servidor también se utiliza para referirse al equipo físico en el que funciona dicha plataforma software.

SISTEMA DE GESTIÓN DE BASES DE DATOS: Sistema de información que permite gestionar la información y las consultas sobre una base de datos.

SQL: Esta sigla corresponde a Structured Query Language (en español Lenguaje de Consulta Estructurado). Lenguaje de programación empleado para realizar consultas y gestionar la información de una base de datos relacional.

[3] COLOMBIA. DEPARTAMENTO NACIONAL DE PLANEACIÓN. Diseño del índice SISBEN en su tercera versión –SISBEN [En línea], [consultado en noviembre de 2018]. Disponible en internet: https://www.sisben.gov.co/Documents/Resumen%20ejecutivo/Resumen_ejecutivo_SisbenIII.pdf .

[4] COLOMBIA. MINISTERIO DE SALUD Y PROTECCIÓN SOCIAL. Población Pobre No Asegurada. Metodología para su estimación y resultados obtenidos. [En línea], [consultado en noviembre de 2018]. Disponible en internet: https://www.minsalud.gov.co/sites/rid/Lists/BibliotecaDigital/RIDE/VP/DOA/metodologia-ppna-sisben-junio-oct.pdf

RESUMEN

El presente trabajo aborda el desarrollo de un conjunto de lineamientos metodológicos de seguridad de la información para la Base de Datos del Aseguramiento en el Departamento de Cundinamarca. Este activo de información está establecido en la Dirección de Aseguramiento de la Secretaría de Salud de Cundinamarca, y constituye el contexto principal de este trabajo. En este orden de ideas, los lineamientos metodológicos que plantea este trabajo se desarrollan según los siguientes componentes principales:

Un componente documental que explora las principales bases contextuales, teóricas y conceptuales, que fundamentan este trabajo.

Un componente para la revisión del nivel de cumplimiento de las actividades de administración de la Base de datos del Aseguramiento frente a lo dispuesto en los objetivos y controles de norma ISO 27001.

Un componente para el análisis y gestión de riesgos de la seguridad de la información basado en la metodología MAGERIT que permite identificar de manera rigurosa y sistemática los riesgos que actualmente afronta la Base de Datos del Aseguramiento.

Un componente que a partir de los riesgos identificados plantea un conjunto de lineamientos de seguridad de la información con base en la norma 27001. De modo tal que constituyen un referente para la protección de la base de datos.

INTRODUCCIÓN

El procedimiento de Seguimiento a la Base de Datos del Aseguramiento en Salud en el Departamento de Cundinamarca constituye el contexto del presente trabajo. En este procedimiento el activo principal es la Base de Datos del Aseguramiento sobre la cual se realizan actividades de consolidación, depuración y gestión técnica de la información sobre los afiliados al Sistema General de Seguridad Social en Salud (SGSSS) de modo tal que permita identificar la población asegurada y no asegurada del departamento. La gestión de esta base de datos permite identificar la población asegurada y no asegurada del departamento, y provee elementos para determinar el nivel de cumplimiento de las metas institucionales que la entidad ha asumido en materia de cobertura del aseguramiento en salud.

Puesto que la Base de Datos del Aseguramiento maneja un volumen elevado de información de naturaleza confidencial, se requiere aplicar lineamientos propios de la seguridad de la información que permitan identificar metódicamente los riesgos que afronta y los controles que pueden ser aplicados.

Es por estas razones que este trabajo propone desarrollar un conjunto de lineamientos de seguridad de la información para proteger la Base de Datos del Aseguramiento, con base en la metodología de análisis y gestión de riesgos MAGERIT y en los controles propuestos por la norma ISO 27001.

Por otro lado, dada la naturaleza técnica de la base de datos del aseguramiento, este trabajo aborda también una serie de recomendaciones técnicas para proteger los recursos tecnológicos que soportan la operación de la base de datos. Estas recomendaciones complementadas con los lineamientos de seguridad, constituyen en un referente para el administrador de la base de datos y los procesos organizacionales interrelacionados.

1. PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

La Gobernación de Cundinamarca ha venido realizando esfuerzos de seguimiento y mejora continua sobre los distintos procesos y procedimientos que componen el modelo organizacional de la institución. Estos esfuerzos están documentados en el Sistema Integrado de Gestión y Control articulado directamente con las metas institucionales[5].

Sin embargo, el alcance de este instrumento no llega hasta la definición de las políticas y lineamientos para brindar seguridad de la información a procedimientos específicos y netamente técnicos como el procedimiento de Seguimiento a la Base de Datos del Aseguramiento. En las diferentes actividades que componen este procedimiento es necesario emplear un conjunto de herramientas y sistemas informáticos de mediana complejidad, cuyo componente principal es la Base de Datos del Aseguramiento.

Por tanto, es necesario aplicar para el entorno técnico que soporta la Base de Datos del Aseguramiento, las mejores prácticas de seguridad con el fin de mitigar los riesgos sobre la información que se almacena y maneja en este importante recurso de la institución.

1.2 DESCRIPCIÓN DEL PROBLEMA

La gestión de la Base de Datos del Aseguramiento, no está exenta de riesgos de seguridad de la información provenientes desde variables de distinta naturaleza. Estos riesgos pueden ser clasificados de manera general como de tipo organizacional y técnico. Desde el punto de vista organizacional se han identificado varias debilidades entre las que se pueden citar las siguientes:

- Escaso personal con conocimientos especializados para el manejo de bases de datos, servidores y demás áreas técnicas relacionadas con el procedimiento.

- No se cuenta con documentación detallada sobre el flujo de información que ocurre en el procedimiento: Fuentes de información, diagrama de flujo, actores, entradas y salidas de información.

[5] COLOMBIA. GOBERNACIÓN DE CUNDINAMARCA. Sistema Integrado de Gestión y Control – SIGC - Versión 9. 2018. Bogotá D.C. [En línea], [consultado en noviembre de 2018]. Disponible en internet: http://isolucion.cundinamarca.gov.co/Isolucion .

- Existe una cultura organizacional muy débil frente al tema del manejo seguro de la información.

- Carencia de un marco general para la seguridad de la información en la institución.

- Existen factores administrativos que causan dificultades operativas en los procedimientos.

Desde el punto de vista técnico, entre otras, podemos mencionar las siguientes debilidades:

- No existen lineamientos para identificar rigurosamente los activos de información, y sus respectivas amenazas, vulnerabilidades y nivel de riesgo que corren en el contexto de la seguridad de la información.

- Escasa documentación técnica sobre la infraestructura TI (Tecnologías de la Información) en la que está implementada la Base de Datos del Aseguramiento: Topología de red, especificaciones de los ambientes de servidores, modelo de datos, entre otros.

- No existen lineamientos para la revisión de configuraciones y acciones de seguridad en el SGBD (Sistema de Gestión de Base de Datos).

- No existen lineamientos para la ejecución de pruebas de penetración para identificar posibles vulnerabilidades de seguridad en la infraestructura TI que soporta la Base de Datos del Aseguramiento.

1.3 FORMULACIÓN DEL PROBLEMA

Así pues, se plantea la siguiente cuestión ¿Desarrollar lineamientos metodológicos de seguridad de la información y aplicarlos a la administración de la Base de Datos del Aseguramiento del Departamento de Cundinamarca, contribuye a mejorar los niveles de protección de la información almacenada en este recurso?

1.4 JUSTIFICACIÓN

En el marco de las políticas y metas de salud del departamento de Cundinamarca es de suma importancia el seguimiento constante al comportamiento de los distintos indicadores, cobertura y estado de afiliación en el Régimen Subsidiado y Contributivo de los cundimarqueses y especialmente de aquellas personas más vulnerables. Atendiendo a esta necesidad, el procedimiento de Seguimiento a la

Base de Datos del Aseguramiento desempeña una función central al aportar información puntual que permite evaluar periódicamente el nivel de cumplimiento de la Dirección de Aseguramiento de la Secretaría de Salud frente a las metas institucionales establecidas en el plan de desarrollo departamental.

Adicionalmente es importante anotar que la información que se almacena en la Base de Datos del Aseguramiento contiene información sensible de los usuarios vinculados al Sistema General de Seguridad Social en Salud (SGSSS), al Sisben (Sistema de Identificación de Potenciales Beneficiarios de Programas Sociales), a grupos de Poblaciones especiales, o que hacen parte de la Población Pobre No Afiliada (PPNA); de tal modo que durante el almacenamiento, consulta y reporte de esta información debe observarse un estricto manejo confidencial de esta información de acuerdo con las exigencias legales y los requerimientos en materia de seguridad de la información.

Ante las circunstancias anteriormente mencionadas, es necesario garantizar la protección de esta información, la cual se encuentra alojada en la Base de Datos del Aseguramiento. Dado que el procedimiento actual no contempla medidas de protección, se hace indispensable el desarrollo de lineamientos metodológicos y adherirlos a este procedimiento.

2. OBJETIVOS

2.1 Objetivo General.

Diseñar lineamientos metodológicos para garantizar la seguridad de la Base de Datos del Aseguramiento del Departamento de Cundinamarca.

2.2 Objetivos específicos

- Establecer el estado actual en materia de seguridad de la información para la Base de Datos del Aseguramiento mediante el proceso de análisis y gestión de riesgos empleando la metodología MAGERIT y los controles de la norma ISO 27001.

- Desarrollar los lineamientos para brindar seguridad a la Base de Datos del Aseguramiento.

- Entregar una guía con recomendaciones de seguridad para proteger la Base de Datos del Aseguramiento.

3. MARCO DE REFERENCIA

3.1 MARCO CONTEXTUAL

3.1.1 Contexto organizacional.

En el contexto nacional, la Gobernación de Cundinamarca es una entidad territorial del orden departamental que de acuerdo con la Constitución Política, tiene autonomía para la administración de los asuntos territoriales así como la planificación y promoción del desarrollo económico y social [6]. La entidad en su permanente gestión de gobierno y a través de las secretarías internas, fijan distintas metas y propósitos institucionales de largo alcance para mejorar la calidad de vida de la población cundinamarquesa, integrar a las comunidades y potencializar el territorio.
Al interior de la Gobernación de Cundinamarca, la dirección del sector salud corresponde a la Secretaría de Salud, dependencia que propende por la consecución de las metas institucionales en esta área consignadas en el Plan de Desarrollo Departamental y en el Plan Territorial de Salud[7].

En este orden de ideas, dentro de la organización interna de la Secretaría de Salud, la Dirección de Aseguramiento es la dependencia encargada de ejecutar directamente las metas relacionadas con el aseguramiento en salud de la población cundinamarquesa. Las funciones principales de esta dependencia pueden encontrarse directamente en el portal web institucional de la Gobernación[8].

Por otro lado, es importante anotar que la Gobernación de Cundinamarca cuenta con el Sistema Integrado de Gestión y Control[9], que constituye un instrumento a través del cual la institución se propone mejorar la calidad de los servicios, procesos internos y el desempeño institucional.

---

[6] COLOMBIA. CORTE CONSTITUCIONAL. Constitución Política de Colombia, 1991. [En línea], [consultado en noviembre de 2018]. Disponible en internet: http://www.corteconstitucional.gov.co/inicio/Constitucion%20politica%20de%20Colombia.pdf.

[7] COLOMBIA. GOBERNACIÓN DE CUNDINAMARCA. Plan de Desarrollo Departamental 2016 -2019, Gobernación de Cundinamarca. [En línea], [consultado en noviembre de 2018]. Disponible en internet: http://www.cundinamarca.gov.co/wcm/connect/2a9dd7d1-d693-414a-94cd-37fe5f901e7d/PLAN+DE+DESARROLLO+VERSION+FINAL.pdf?MOD=AJPERES&CVID=IDlW39U .

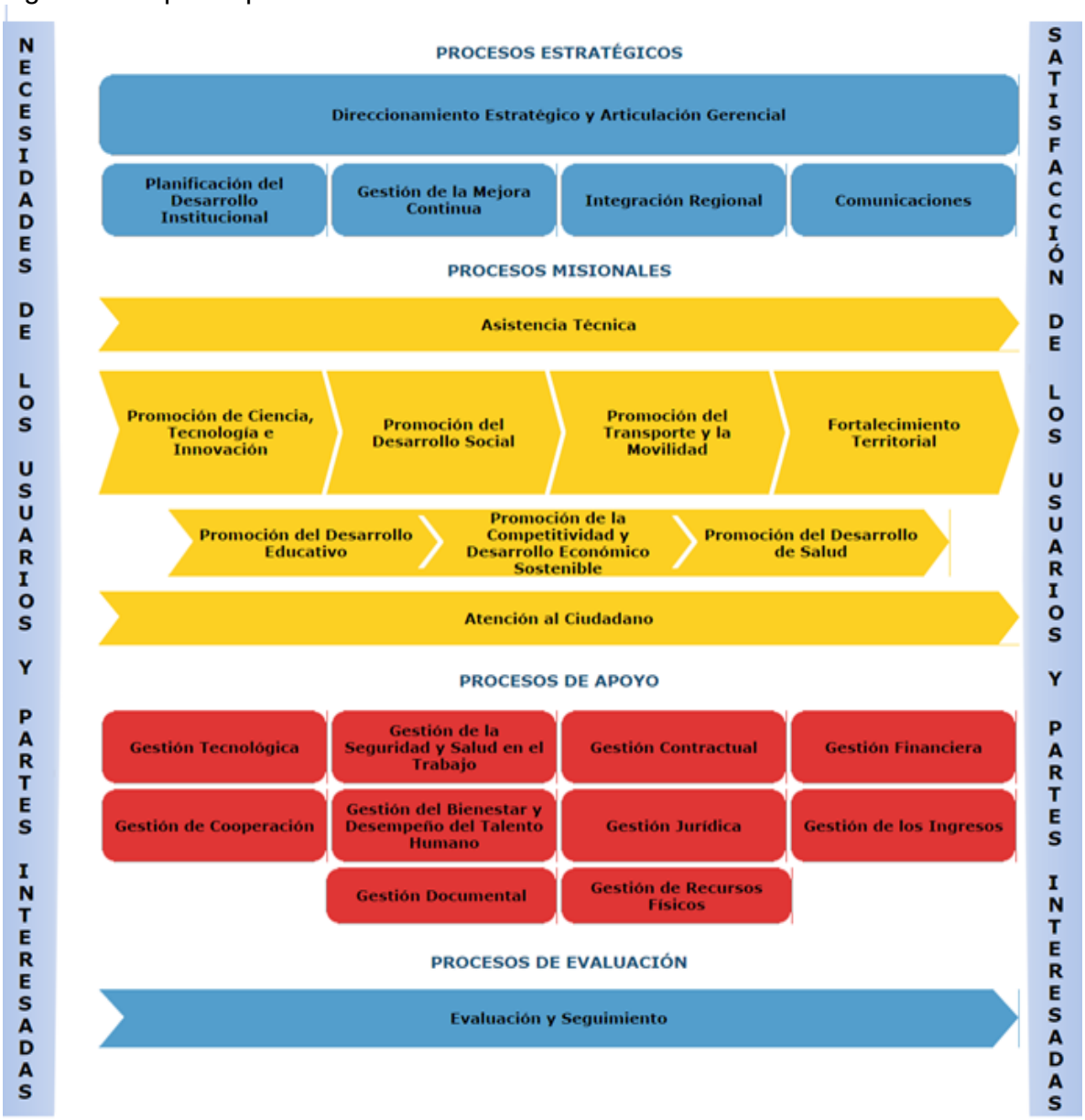
[8] COLOMBIA. GOBERNACIÓN DE CUNDINAMARCA. Dirección de Aseguramiento. Funciones de la Dirección de Aseguramiento. [En línea], [consultado en noviembre de 2018]. Disponible en internet: http://www.cundinamarca.gov.co/Home/SecretariasEntidades.gc/Secretariadesalud/SecretariadesaludDespliegue/ascontenido/asquienes_somos/assecresalud_quienesestrucorgydirec/csecresalud_quienesestrucorgydirec_diraseg .

[9] CUNDINAMARCA. Sistema Integrado de Gestión y Control – SIGC. Manual del Sistema Integral de Gestión y Control. Función Pública, Gobernación de Cundinamarca. [En línea],[consultado en noviembre de 2018]. Disponible en internet: http://isolucion.cundinamarca.gov.co/Isolucion

La figura 1 muestra el mapa de procesos de la Institución que están clasificados de manera general en Procesos Estratégicos, Procesos Misionales, Procesos de Apoyo y Procesos de Evaluación.

Cada proceso a su vez está compuesto por diversos subprocesos y procedimientos que coadyuvan a la consecución de las metas institucionales trazadas.

Figura 1. Mapa de procesos de la Gobernación de Cundinamarca.



Fuente: Gobernación de Cundinamarca.

El proceso correspondiente a la Secretaría de Salud es el denominado Promoción del Desarrollo de Salud dentro del cual se encuentra el Subproceso de Aseguramiento en Salud.

En este contexto organizacional se encuentra enmarcado el procedimiento de Seguimiento a la Base de Datos del Aseguramiento en el Departamento de Cundinamarca, formalmente identificado y establecido en el Sistema Integrado de Gestión y Control – SIGC. Este procedimiento tiene como objetivo principal consolidar, depurar y promover la actualización de la Base de Datos del Aseguramiento en salud del Departamento de Cundinamarca (Afiliados al Régimen Subsidiado y Contributivo, Sisben, listados censales y personas no afiliadas), para establecer registros de población asegurada y no asegurada, establecer la cobertura del aseguramiento a nivel departamental y por municipio, y apoyar la gestión a través de la medición de distintos indicadores.

Las actividades formalmente establecidas en el procedimiento son las siguientes:

- Conocer y socializar la normatividad vigente, para el seguimiento a la Base de Datos del Aseguramiento.

- Realizar Asistencia Técnica sobre los diferentes temas relacionados con el manejo técnico de información del aseguramiento en salud.

- Realizar seguimiento al proceso de actualización de la BDUA (Base de Datos Única de Afiliados).

- Notificar a los Municipios los resultados del cargue de novedades a la BDUA.

- Identificar los Municipios que no cumplen con el reporte al flujo de Información de la BDUA.

- Realizar cargue de la Base de Datos en medios locales y procesar la información

- Generar estadísticas mensuales del comportamiento del Aseguramiento, por Municipios, EPS y Grupos Etarios.

- Apoyar la generación de los informes sobre Poblaciones Especiales.

- Realizar acciones de seguridad sobre la información.

- Determinar el comportamiento del aseguramiento por Municipio.

- Reportar Población Pobre No Asegurada a Entes Territoriales.

- Realizar seguimiento a la información sobre la población PPNA en los Municipios.

- Evaluar los Indicadores del Aseguramiento.

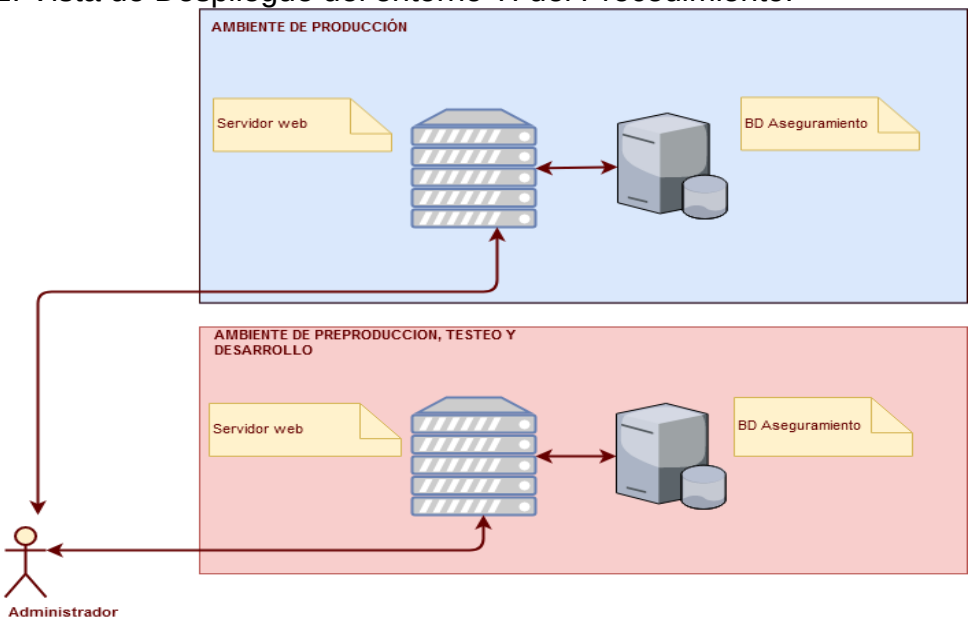
3.1.2 Contexto TI.

Actualmente el uso de Tecnologías de la Información y las Comunicaciones (TIC) es un factor clave en la operación diaria de los procesos en las organizaciones; En el marco de este trabajo, el contexto técnico está definido por el requerimiento de manejo de grandes volúmenes de información mediante bases de datos y sistemas de gestión de bases de datos. Sin embargo, este escenario trae aparejados varios riesgos de seguridad de la información que de no ser identificados y tratados pueden ocasionar serios reveses a la organización y sus procesos.

El procedimiento está soportado tecnológicamente en los recursos computacionales de la Gobernación de Cundinamarca. La institución cuenta con los recursos de TI que han permitido implementar el entorno técnico para gestionar la información que alimenta la Base de Datos del Aseguramiento y ejecutar las distintas actividades técnicas de administración.

La figura 2 muestra una vista básica de despliegue del contexto TI del procedimiento.

Figura 2. Vista de Despliegue del entorno TI del Procedimiento.



Fuente: Autor.

De acuerdo con el diagrama anterior, el elemento central del procedimiento es la Base de Datos del Aseguramiento que está soportada en el Sistema de Gestión de Bases de Datos Relacionales (SGBDR) MySQL.

La gestión de la base de datos se realiza a través de un sistema de información basado en tecnología web al cual se accede a través de un servidor web Apache.
El procedimiento cuenta con tres ambientes de trabajo que permiten realizar por etapas las tareas técnicas de cargue de información y consultas de información a la base de datos.

Ambiente de Producción: Este ambiente está ubicado en el centro de datos de la Gobernación, y se ejecuta en dos máquinas virtuales. En una de ellas corre el servidor web Apache que aloja la plataforma principal de administración de MySQL y una aplicación web de apoyo para tareas específicas de administración.
Sobre la segunda máquina virtual corre el servidor de base de datos de MySQL.
El servidor MySQL contiene la Base de Datos del Aseguramiento y respectivas tablas con los archivos maestros actuales e históricos del Régimen Subsidiado, Régimen Contributivo, PPNA y Sisben. Así como tablas de apoyo que facilitan las consultas cruzadas que se realizan constantemente (Municipios del departamento, EPSs y poblaciones especiales).

En el servidor MySQL no se cuenta con usuario root para administración total del servidor MySQL, sino que están configurados dos usuarios para gestión exclusiva sobre la Base de Datos del Aseguramiento.

- Un usuario administrador con permisos de Lectura y Escritura. Este usuario está asignado al administrador de la Base de Datos del Aseguramiento que actualmente corresponde al autor de este trabajo.

- Un usuario con permisos de solo lectura. Es importante anotar que en este ambiente no se carga o actualiza información, o se ejecutan consultas, si antes no se han probado en los ambientes previos de Pre-producción y Desarrollo.

Ambiente de Pre-producción: Este ambiente está implementado en una máquina independiente del Ambiente de Producción.
En este ambiente fue implementado el Sistema de Gestión de Base de Datos MySQL que contiene una copia exacta de la base de datos en producción.
Desde este ambiente el administrador carga o actualiza información al Ambiente de Producción.

Ambiente de Desarrollo: Este ambiente está implementado en la misma máquina del Ambiente de Pre-producción.

Sobre este ambiente fue implementada una base de datos de prueba (independiente de la base de datos de pre-producción) que permite realizar distintas

pruebas sobre la estructura actual pero también permite incorporar nuevos elementos según sea requerido ingresar al modelo de datos y que deben ser debidamente ajustados.

Estructura básica de la Base de Datos. A la fecha de escritura de este trabajo la Base de Datos del Aseguramiento posee alrededor de 170 millones de registros organizados en un modelo compuesto por 7 tipos de tablas:

Tablas Principales

- Maestros del Régimen Subsidiado
- Maestros del Régimen Contributivo
- Maestros Sisben
- Maestros PPNA

Tablas Auxiliares

- Tabla de EPSs
- Tabla de Poblaciones Especiales
- Tabla de Municipios

3.2 MARCO CONCEPTUAL

El presente trabajo está enmarcado en dos grandes áreas conceptuales: Por un lado, el tema de la Seguridad de la Información y por otro lado el manejo de información en el área del aseguramiento en salud. Sobre estos dos componentes se abordan los principales conceptos que fundamentan este trabajo.

3.2.1 Seguridad de la Información

3.2.1.1 Definición.

De acuerdo con la norma ISO 27000 [10] , la seguridad de la información en su definición más fundamental trata sobre la preservación de la Confidencialidad, Integridad y Disponibilidad de la Información.

[10]NORMA TÉCNICA COLOMBIANA NTC-ISO-IEC 27000. Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información. Visión General y Vocabulario. Bogotá: Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC) Apartado 14237.2017, p.13

Hay que tener en cuenta que la información puede estar almacenada en diferentes medios, desde documentos físicos hasta información digital estructurada en bases de datos. Por tanto, el alcance de la definición es amplio en cuanto a lo que debe ser protegido; y muy puntual frente a los principios que deben cumplirse.

Por otro lado, existe una amplia gama de factores que pueden afectar el cumplimiento de dichos principios de seguridad de la información: Desde la degradación o pérdida de los medios físicos que contienen la información hasta los complejos ataques informáticos sobre los sistemas de información.

Por estas razones la Seguridad de la Información aborda las políticas organizacionales y los procedimientos técnicos necesarios para salvaguardar la información.

3.2.1.2 Principios de Seguridad de la Información.

Los principios de Confidencialidad, Integridad y Disponibilidad constituyen la base sobre la cual deben orientarse toda acción o proyecto tendiente a garantizar la seguridad de la información en la organización. Estos principios se conocen también como la triada CID (Confidencialidad, Integridad y Disponibilidad). (Ver figura 3)

Figura 3. Principios de Confidencialidad, Integridad y Disponibilidad de la Información

Fuente: Autor.

Confidencialidad: Hace referencia a la protección de la información contra el acceso o publicación no autorizada. Implica el acceso solo a personas autorizadas a diferentes tipos o niveles información. En otras palabras, la correcta gestión de los niveles de permiso para acceder a la información de la organización.

Integridad: Hace referencia a la necesidad de mantener la información libre de alteraciones o modificaciones no autorizadas. La información debe mantenerse tal cual fue generada para de este modo asegurar su confiabilidad y validez.

Disponibilidad: Hace referencia al requerimiento de garantizar el acceso a la información de la organización a aquellas personas que están autorizadas para ello.

3.2.1.3 Riesgos en la Seguridad de la Información.

Un riesgo puede ser comprendido a nivel fundamental como una medida del grado al que una organización está expuesta a amenazas provenientes de circunstancias o eventos internos o externos [11]. El riesgo se expresa en función de:

- Los impactos adversos que podrían surgir si ocurre la circunstancia o evento.
- La probabilidad de ocurrencia.

En el tema de los riesgos en seguridad de la información surgen varios conceptos que es necesario precisar para darle mayor enfoque a este asunto y aplicabilidad al objeto del presente trabajo. Las definiciones consignadas a continuación están basadas principalmente en la norma ISO 27000.

Aceptación del riesgo: Decisión comunicada o expresada formalmente sobre el conocimiento y acto de asumir un determinado riesgo.

Análisis de riesgos*:* Proceso cuyo propósito es la comprensión de la naturaleza del riesgo de tal modo que permita determinar el nivel de riesgo, esto es la probabilidad de ocurrencia, el impacto causado y las salvaguardas adicionales que permitan su mitigación.

Comunicación y consulta de riesgos: Proceso o estrategia continua mediante la cual la organización provee, comparte u obtiene información con todas las partes interesadas o implicadas en la gestión del riesgo.

Criterios de riesgo: Son aquellos parámetros de referencia contra los cuales se evalúa el riesgo.

[11] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY - NIST. Glossary of Key Information Security Terms. [En línea], [consultado el 2 de febrero de 2019]. Disponible en internet: https://nvlpubs.nist.gov/nistpubs/ir/2013/nist.ir.7298r2.pdf .

Gestión del riesgo: Hace referencia a las políticas y respectivas actividades encaminadas a dirigir y controlar una organización frente a los riesgos identificados.

Evaluación del riesgo: Es el proceso de comparación de los resultados obtenidos en el análisis del riesgo contra los criterios de riesgo, de modo tal que permita determinar si el nivel de riesgo es aceptable.

Nivel de riesgo*:* Magnitud del riesgo expresada en términos de la combinación del impacto y la probabilidad de ocurrencia.

Riesgo Residual*:* Dado que los riesgos no pueden ser totalmente eliminados, el riesgo residual es aquel que permanece luego de ejercer el tratamiento.

Valoración del riesgo: De acuerdo con la norma ISO 27000, es el proceso global de identificación, análisis y evaluación del riesgo.

Identificación del riesgo: Proceso metódico mediante el cual se encuentran, reconocen y describen los riesgos.

3.2.2 Aseguramiento en salud.

Esta área de la salud constituye el eje central para el cual se ejecuta el procedimiento de seguimiento y administración de la Base de Datos del Aseguramiento.

3.2.2.1 Definición.

Para comprender de manera integral el aseguramiento en salud es necesario primero que todo remitirse a la Constitución Política que en el artículo 49 establece el derecho a la atención en salud, al acceso a los servicios de promoción, protección y recuperación de la salud; y establece que “corresponde al Estado organizar, dirigir y reglamentar la prestación de servicios de salud a los habitantes y de saneamiento ambiental conforme a los principios de eficiencia, universalidad y solidaridad. También, establecer las políticas para la prestación de servicios de salud por entidades privadas, y ejercer su vigilancia y control”.

En coherencia con este mandato constitucional, la ley 100 de 1993[12], articulo 157, “establece la obligatoriedad para todos los colombianos de la afiliación al Sistema

[12]COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 100 de 1993. . [En línea], [consultado el 2 de noviembre de 2018]. Disponible en internet: http://www.secretariasenado.gov.co/senado/basedoc/ley_0100_1993.html .

General de Seguridad Social en Salud" (SGSSS), a través de los siguientes mecanismos:

- Régimen Contributivo: "Los afiliados al Sistema mediante el régimen contributivo son las personas vinculadas a través de contrato de trabajo, los servidores públicos, los pensionados y jubilados y los trabajadores independientes con capacidad de pago".[13]

- Régimen Subsidiado: "Los afiliados al Sistema mediante el régimen subsidiado son las personas sin capacidad de pago para cubrir el monto total de la cotización. Serán subsidiadas en el Sistema General de Seguridad Social en Salud la población más pobre y vulnerable del país en las áreas rural y urbana".[14]

Es importante anotar que uno de los criterios más importantes de afiliación al Régimen subsidiado es la población focalizada en los niveles 1 y 2 del Sisben. Además, al Régimen Subsidiado también podrán ser afiliadas las poblaciones especiales como: Victimas y Desplazados por el conflicto armado, comunidades indígenas, desmovilizados, población infantil abandonada a cargo del ICBF, personas mayores en centros de protección, ciudadanos repatriados, entre otras).

- Personas Vinculadas al sistema: "Los participantes vinculados son aquellas personas que por motivos de incapacidad de pago y mientras logran ser beneficiarios del régimen subsidiado tendrán derecho a los servicios de atención de salud que prestan las instituciones públicas y aquellas privadas que tengan contrato con el Estado"[15].

Así pues, se puede establecer que el Aseguramiento en Salud es la estrategia estatal en cabeza el Ministerio de Salud, que garantiza a través de los mecanismos establecidos en la ley, el acceso a los servicios de salud del Sistema General de Seguridad Social en Salud.

3.2.2.2 Base de Datos Única de Afiliados – BDUA.

Como puede inferirse, la información que debe manejarse en el Aseguramiento en Salud es de gran magnitud en tamaño y complejidad. Por tanto, el uso de

[13] MINISTERIO DE SALUD Y PROTECCIÓN SOCIAL. Régimen contributivo. [En línea], [consultado el 2 de noviembre de 2018]. Disponible en internet: https://www.minsalud.gov.co/proteccionsocial/Regimencontributivo/Paginas/regimen-contributivo.aspx

[14] SALUD CAPITAL. Régimen subsidiado. . [En línea], [consultado el 2 de noviembre de 2018].Disponible en internet http://www.saludcapital.gov.co/DASEG/Paginas/RegimenSubsidiado.aspx

[15] Ibíd., p. 31

tecnologías de la información y las comunicaciones es indispensable para gestionar eficazmente estos volúmenes de datos.

En Colombia la entidad que gestiona los recursos del SGSS y la información de los afiliados es ADRES (Administradora de los Recursos del Sistema General de Seguridad Social en Salud); entidad que fue creada por la ley 1753 de 2015[16]. De acuerdo con el artículo 66 de esta norma entre otras, ADRES tiene la función expresa de administrar la información propia de sus operaciones. Esto implica la responsabilidad de ADRES sobre la administración del recurso técnico conocido como la Base de Datos Única de Afiliados -BDUA-.

La Base de Datos Única de Afiliados – BDUA, contiene la información a nivel nacional de los afiliados a los distintos regímenes establecidos en el Sistema General de Seguridad Social en Salud. (Régimen Contributivo, Régimen Subsidiado, Regímenes de Excepción y Especiales y entidades prestadoras de Planes Voluntarios de Salud). La norma que especifica la administración y actualización de la BDUA es la Resolución 4622 de 2016; la resolución detalla los procesos, responsabilidades, tiempos y estructura de archivos que se manejan en la BDUA.

En el contexto de este trabajo es importante la comprensión de la Resolución 4622 de 2016 por las siguientes razones fundamentales:

- ADRES pone a disposición de los entes territoriales los archivos maestros del Régimen Subsidiado y Contributivo. Además de otros maestros como el correspondiente a la Población Pobre No Afiliada (PPNA) y la Liquidación Mensual de Afiliados (LMA).

- La entrega de estos archivos maestros se realiza bajo las debidas condiciones de confidencialidad de las que trata la Ley 1581 de 2012 (Habeas Data).

- Los archivos maestros contienen la información actualizada según el proceso de cargue mensual de novedades a ADRES cuya responsabilidad por el cargue mismo y la calidad de los datos corresponde a las entidades descritas en la resolución.

[16]COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1753 de 2015. [En línea], [consultado el 2 de noviembre de 2018]. Disponible en internet: http://www.secretariasenado.gov.co/senado/basedoc/ley_1753_2015_pr001.html

3.3 MARCO TEÓRICO

En la sociedad actual, el uso de las Tecnologías de la Información y las Comunicaciones (TIC) al tiempo que trae grandes ventajas y apalanca los diferentes procesos de las organizaciones, también trae aparejados grandes riesgos en materia de seguridad de la información. Riesgos que provienen de una amplia gama de amenazas y vulnerabilidades que de materializarse pueden obstaculizar o detener completamente la operación y el consiguiente incumplimiento de los objetivos de una organización.
La Gobernación de Cundinamarca y específicamente el procedimiento de Seguimiento a la Base de Datos del Aseguramiento, no están exentos de estos riesgos asociados al uso de las TIC. En sus operaciones diarias, la entidad y sus distintos procesos emplean masivamente varios recursos tecnológicos y manejan grandes volúmenes de información que requieren ser asumidos con un enfoque de seguridad de la información.

Una de las primeras acciones para el procedimiento es el análisis de riesgos que requiere de una metodología precisa que guíe la identificación de activos de TI, así como también las amenazas y riesgos a los que están expuestos; de tal modo que las organizaciones puedan enfocar el esfuerzo de tratamiento de los riesgos y activos más críticos. En este escenario surge la metodología MAGERIT, una herramienta para la gestión y análisis de riesgos que propone el Consejo Superior de Administración Electrónica (CSAE) de España dirigida principalmente a entidades gubernamentales pero que aplica para todo tipo de organizaciones. Es importante anotar que MAGERIT está basada a su vez en la norma ISO 31000 para gestión de riesgos en las organizaciones.

Por otro lado, en Colombia un buen referente lo constituye el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), que ha definido políticas generales como el Modelo de Seguridad y Privacidad de la Información[17].Una iniciativa dirigida a las entidades gubernamentales del país que propende por el uso seguro de las tecnologías de la información y las comunicaciones con el ánimo de salvaguardar la información y los activos de TI de nuestras instituciones. Una revisión detallada de este modelo muestra que está basado a su vez en la norma ISO 27001.

Lo anterior indica que las normas internacionales constituyen un verdadero referente para abordar los objetivos trazados en este trabajo. Por tal razón a continuación se estudia con mayor detalle la metodología MAGERIT, la norma ISO 27001 y la norma ISO 27002.

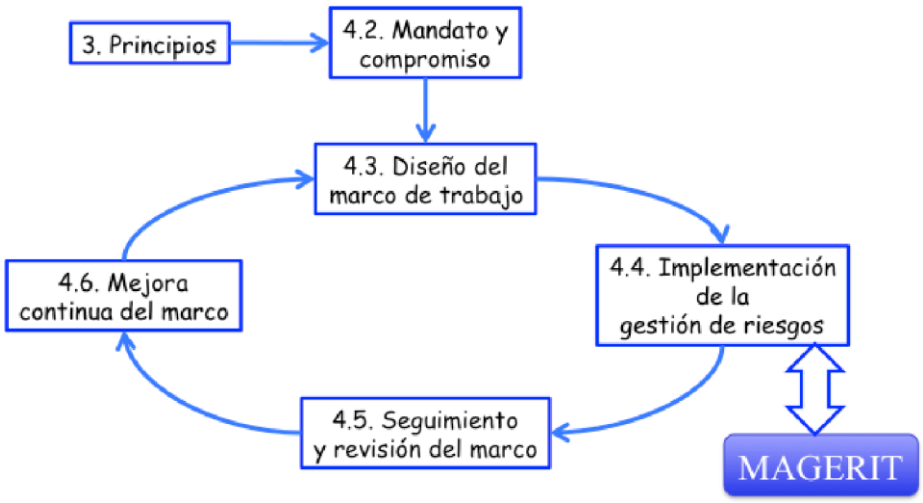
[17]COLOMBIA. MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES – MinTIC, (2016). Modelo de Seguridad y Privacidad de la Información. [En línea], [consultado el 2 de noviembre de 2018]. Disponible en internet: https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

3.3.1 MAGERIT

El análisis y gestión de riesgos de TI es una actividad central para las organizaciones porque permite enfocar las decisiones y esfuerzos en áreas críticas que requieren soluciones efectivas y rápidas en las operaciones. Es por esta razón que el proceso de identificación de los riesgos debe ser riguroso y metódico de tal modo que reduzca los factores subjetivos del analista y propenda por resultados que guíen efectivamente las acciones de tratamiento.
MAGERIT (Metodología para Análisis y Gestión de Riesgos de TI)[18] responde a esta necesidad desde una propuesta de marco de trabajo metodológico bien establecido y probado en diferentes escenarios, que permite la identificación y valoración de los riesgos asociados al uso de las tecnologías de la información y las comunicaciones.

MAGERIT está enmarcado en la normativa ISO 31000[19] (familia de normas ISO para Gestión del Riesgo) e implementa el "Proceso de la gestión de riesgos". La figura 4 ilustra la ubicación de MAGERIT en el proceso de gestión de riesgos de la normatividad ISO 31000.

Figura 4. Campo de acción de MAGERIT



Fuente: MAGERIT.

[18] PORTAL DE ADMINISTRACIÓN ELECTRÓNICA. MAGERIT v.3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Madrid, España. [En línea], [consultado el 2 de noviembre de 2018]. Disponible en internet: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.WsBSPS7wbIU .
[19] NORMA TÉCNICA COLOMBIANA NTC-ISO-IEC 31000. Gestión del Riesgo. Principios y Directrices. Bogotá: Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC) Apartado 14237.

A continuación, se transcriben los objetivos de MAGERIT:

3.3.1.1 Objetivos directos

- Concientizar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos.
- Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC).
- Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control.

3.3.1.2 Objetivos indirectos

- Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.[20]

Actualmente MAGERIT está en su tercera versión y está organizada en tres libros a saber:

Libro 1.- Método: Presenta la descripción de la metodología y las definiciones fundamentales sobre varios conceptos de seguridad de la información.

En este libro, MAGERIT presenta la visión general sobre las tareas que se deben realizar en un proceso de Gestión de Riesgos:

Análisis de Riesgos: En esta actividad se abordan la identificación de los activos, las amenazas y las salvaguardas.

Tratamiento de los Riesgos: En esta actividad se aborda la forma sistemática de organizar la estrategia para reducir los riesgos y la defensa contra las amenazas.

El método general para el análisis de riesgos en el marco de MAGERIT puede resumirse en los siguientes pasos:

- Identificar los activos de TI más importantes de la Organización, su interrelación y su valor, en el sentido de qué perjuicio (coste) supondría su degradación (daño o fallo).

- Identificar a qué amenazas están expuestos los activos identificados.

- Determinar qué salvaguardas hay dispuestas y cuán eficaces son frente al riesgo.

[20] MAGERIT. Proceso de gestión de riesgos. [En línea], [consultado el 2 de noviembre de 2018]. Disponible en: https://administraciónelectrónica.gob.es/pae-home/pae/magerit.html.

- Estimar el impacto, definido como el daño sobre el activo derivado de la materialización de una amenaza.

- Estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia (o probabilidad de materialización) de una amenaza.

Libro 2.- Catálogo de Elementos

En este libro MAGERIT presenta los elementos, tareas y terminología específica, necesarios para abordar el proceso de gestión de riesgos. En otros términos, en este libro se describen los elementos técnicos que permiten implementar los conceptos presentados en el libro 1.

Los objetivos de este libro se presentan textualmente a continuación:

- "Facilitar la labor de las personas que desarrollan el proyecto de análisis y gestión de riesgos, de modo tal que cuente con un referente estándar a los que puedan remitirse rápidamente, centrándose en lo específico del sistema objeto del análisis".

- "Homogeneizar los resultados de los análisis, promoviendo una terminología y unos criterios que permitan comparar e incluso integrar análisis realizados por diferentes equipos".

El catálogo está compuesto por los siguientes elementos abordados en el libro 2:
- Tipo de Activos
- Dimensiones de valoración
- Criterios de valoración
- Amenazas
- Salvaguardas

Libro 3.- Guía de técnicas

En este libro MAGERIT propone algunas técnicas o algoritmos para abordar el manejo de la información que resulta del proceso de análisis y gestión de riesgos. Dado que en un proyecto de mediana complejidad se identifican varios activos, amenazas y riesgos, el cruce de todos los parámetros generados requiere el uso de estas técnicas que incluso pueden ser sistematizadas.

MAGERIT propone las siguientes técnicas:
- Tablas para la obtención sencilla de resultados
- Algoritmos para resultados más complejos
- Arboles de Ataque para complementar el análisis sobre las amenazas sobre un activo.

3.3.2 NORMAS ISO 27001 e ISO 27002.

Las salvaguardas de las que trata la metodología MAGERIT están enmarcadas en los controles propuestos por la norma ISO 27001 y que son ampliadas en la norma ISO 27002. De ahí que sea importante estudiar con detalle estas normas.

3.3.2.1 ISO 27001. Esta norma constituye actualmente el principal estándar internacional en seguridad de la Información. Fue desarrollada por la Organización Internacional para la Estandarización (ISO) en colaboración con la Comisión Electrotécnica Internacional (IEC). La versión actual de la norma es la 2013, de tal modo que en la literatura el nombre técnico es ISO/IEC 27001:2013.

En Colombia la versión de la norma es la NTC-ISO-IEC 27001:2013 que adopta y traduce de manera idéntica la norma original, siendo impresa y distribuida exclusivamente por el Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC)[21].

El alcance declarado de la norma ISO 27001 es la especificación de los requerimientos para el establecimiento, la implementación, el mantenimiento y la mejora continua de un Sistema de Gestión de Seguridad de la Información (SGSI) en la organización. La norma en sí misma no es extensa o de gran complejidad, y los requerimientos están elaborados de modo tal que sean transversales y puedan aplicar a cualquier clase de organización.

La norma está divida en dos partes principales. La primera parte está compuesta por 10 capítulos que componen la parte teórica la norma.

Capítulo 1. Alcance
Capítulo 2. Referencias normativas
Capítulo 3. Términos y definiciones
Capítulo 4. Contexto de la Organización
Capítulo 5. Liderazgo
Capítulo 6. Planificación
Capítulo 7. Soporte
Capítulo 8. Operación
Capítulo 9. Evaluación de desempeño
Capítulo 10. Mejora

Una organización cumple integralmente con la norma cuando cumple a cabalidad con todos los requerimientos establecidos en los capítulos del 4 al 10.

[21]NORMA TÉCNICA COLOMBIANA NTC-ISO-IEC 27001. Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Bogotá: Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC), 2013, p. 4

La segunda parte de la norma corresponde al anexo A y especifica los dominios, objetivos de control y controles, que constituyen un referente técnico y específico para la implementación de la norma en la organización. Existen 14 Dominios, 35 Objetivos de Control y 114 Controles, que son detallados en la norma ISO 27002.

Los dominios de la norma ISO27001 anexo A son los siguientes:

- Política de seguridad
- Organización de la seguridad de la información
- Seguridad de los recursos humanos
- Gestión de Activos
- Control de Acceso.
- Criptografía.
- Seguridad Física y Ambiental.
- Seguridad de las Operaciones.
- Seguridad de las comunicaciones.
- Adquisición, desarrollo y mantenimientos de sistemas.
- Relación con los Proveedores.
- Gestión de incidentes de seguridad de la información.
- Aspectos de seguridad de la información de la gestión de continuidad de negocio.
- Cumplimiento.

3.3.2.2 ISO 27002. La norma ISO 27002 puede considerarse como un complemento de la norma ISO 27001 a través de la ampliación del anexo A. La versión actual de la norma es la 2013, de tal modo que en la literatura el nombre técnico es ISO/IEC 27002:2013. En Colombia esta norma corresponde a NTC-ISO-IEC 27002:2013[22].

El alcance de la norma ISO 27002 es el establecimiento de un catálogo de buenas prácticas que aporta un conjunto de objetivos de control y respectivos controles para que a través de su implementación pueda darse tratamiento a los riesgos que enfrenta la organización en materia de seguridad de la información.

La norma permite a las organizaciones:

- Definir controles en el marco de la implementación de un Sistema de Gestión de Seguridad de la Información.

- Implementar controles estándar para la seguridad de la información

[22]NORMA TÉCNICA COLOMBIANA NTC-ISO-IEC 27002. Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Requisitos. 2013. Bogotá: Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC) Apartado 14237, 2013. p. 120

- Implementar guías de referencia para gestión de la seguridad de la información.

3.3.3 MySQL.

MySQL es la plataforma tecnológica que constituye el componente central del procedimiento de Seguimiento a la Base de Datos del Aseguramiento en el departamento de Cundinamarca. Es por esta razón que en el presente apartado se estudia con cierto nivel de detalle las principales características.

MySQL[23] es un Sistema de Gestión de Bases de Datos Relacionales (SGBDR) bien establecido y utilizado en muchos sistemas de información alrededor del mundo. Es uno de los SGBDR más estables que existen actualmente, principalmente empleado en aplicaciones web e implementado por defecto en la mayoría de los servicios de hosting.

MySQL hace parte de Oracle Corporation, está desarrollado y distribuido bajo Licencia Publica General GNU (GPL GNU) y también bajo licencia comercial. Es importante notar que la versión GPL es distribuida con la versión MySQL Community con código fuente abierto. A la fecha de redacción de este documento, la última versión estable es la 8.0.13. Existe también una rama de desarrollo de MySQL (fork) llamada María DB que esencialmente se diferencia en el tipo de licenciamiento bajo el cual es distribuida; siendo netamente GPL GNU.

3.3.3.1 Principales características. De acuerdo con la documentación oficial de MYSQL, entre las principales características podemos mencionar las siguientes:

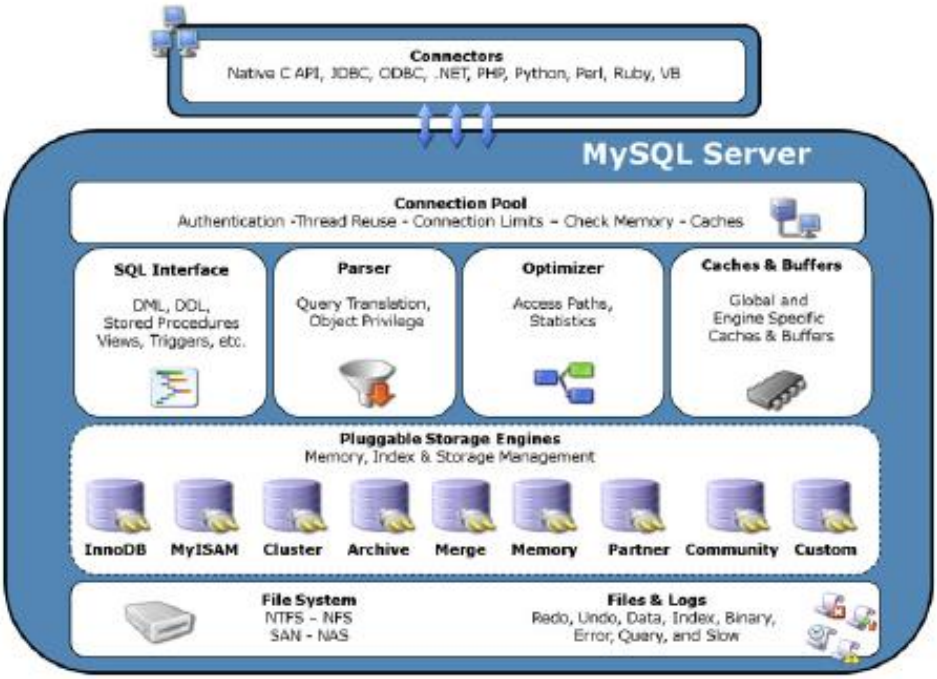
- Desarrollado en lenguajes C y C++.
- Probado con diferentes compiladores.
- Funciona en diferentes plataformas.
- Usa un diseño de servidor multi-capa con módulos independientes.
- Está diseñado para operar en modo completamente multi-hilo usando el kernel del sistema operativo y facilitando el uso de los múltiples procesadores de la máquina.

[23]MYSQL. MySQL 5.6 Reference Manual. [En línea], [consultado el 2 de noviembre de 2018]. Disponible en https://dev.mysql.com/doc/refman/5.6/en/ .

- Provee motores de almacenamiento transaccionales y no transaccionales.
- Usa tablas B-Tree (MyISAM) muy rápidas con compresión de índice.
- Diseñado para que sea relativamente simple añadir otros motores de almacenamiento. Esta característica es útil si se requiere proveer una interface SQL para una base de datos propia de la organización.
- Usa un sistema muy rápido para localización de memoria basada en hilos.
- Ejecuta sentencias JOIN muy rápido gracias al algoritmo '*nested-loop join'*.
- Implementa tablas *hash* en memoria, que son usadas como tablas temporales.
- Implementa sentencias SQL usando una librería altamente optimizada y diseñada para operaciones de alto rendimiento.
- Provee el servidor como un programa separado para usar en un entorno cliente/servidor. También está disponible como librería que puede ser embebida en aplicaciones autónomas.

3.3.3.2 Arquitectura de MySQL. La arquitectura de MySQL corresponde principalmente a una disposición cliente –servidor y puede ser estudiada desde el siguiente modelo (figura 5) de componentes de alto nivel que abarcan las distintas funcionalidades.

Figura 5. Arquitectura de MySQL



Fuente: Schumacher, R. 2004.[24] .

Capa de Acceso o Aplicación: Contiene los servicios que gestionan el acceso al Servidor de MySQL. Aquí se ejecutan las funcionalidades de autenticación, gestión de la conexión, y seguridad.

Capa de la lógica del Servidor MySQL: Es la capa más importante porque contiene las funcionalidades propias de la lógica de negocio del modelo de bases de datos relacionales implementadas en MySQL. En esta capa se ejecutan servicios de Interface SQL, Parsers, Optimizadores, utilidades de backup y restauración, gestión de memoria.

Capa de motores de almacenamiento: En esta capa se ejecutan los mecanismos o motores implementados en MySQL para almacenamiento de datos. Los principales motores de almacenamiento en MySQL son MyISAM e InnoDB.

[24] SCHUMACHER, R. MySQL 5.0's Pluggable Storage Engine Architecture, Part 1: An Overview. MySQL AB. 2004. [En línea], [consultado el 2 de noviembre de 2018]. Disponible en: http://download.nust.na/pub6/mysql/tech-resources/articles/mysql_5.0_psea1.html .

3.3.3.3 Tipos de datos. Dado el variado y elevado número de registros que se manejan en el contexto de la Base de Datos del Aseguramiento, es muy importante conocer los tipos de datos que maneja un sistema de gestión de base de datos. En MySQL estos datos son:

- Enteros con signo o sin signo de 1, 2, 3, 4 y 8 bytes de longitud
- FLOAT
- DOUBLE
- CHAR
- VARCHAR
- BINARY
- VARBINARY
- TEXT
- BLOB
- DATETIME
- TIME
- TIMESTAMP
- YEAR
- SET
- ENUM
- Espaciales tipo OpenGIS

3.3.3.4 Tipos de tablas. En el contexto de este trabajo es importante conocer este aspecto de MySQL porque actualmente todas las tablas de la Base de Datos del Aseguramiento son de consulta.

MySQL maneja diferentes tipos de tablas:

- Tablas ISAM (*Index Sequential Access Method*): El Método de Acceso Secuencial Indexado es el primer mecanismo de almacenamiento desarrollado y empleado en las versiones anteriores a la 3.23. En este tipo de tablas solo fue posible manejar archivos de hasta 4 GB de tamaño.

- Tablas MyISAM: Es el mecanismo que reemplaza al tipo ISAM, desarrollado y empleado en versiones posteriores a la 3.23. Es el tipo de almacenamiento recomendado para tablas de solo consulta dado su alto desempeño en la lectura de la tabla y la optimización de los índices empleados.

MyISAM no está orientado a modelos transaccionales, por tal razón tales requerimientos son implementados a nivel de la capa de lógica de negocio de una aplicación. En operaciones transaccionales, MySQL bloquea la tabla hasta que se realiza la inserción o modificación de un registro.

Las tablas MyISAM se almacenan en tres tipos de archivos: Un archivo de datos (con extensión .MYD), un archivo de índices (con la extensión .MYI) y un archivo con la definición de la tabla (con extensión .frm).

El formato manejado en MyISAM es independiente de la plataforma, por lo que constituye una gran ventaja al permitir migrar fácilmente los datos y los índices de una tabla solo copiando los archivos entre servidores en diferentes plataformas.

Las tablas de la Base de Datos del Aseguramiento están configuradas con el tipo de almacenamiento MyISAM.

- Tablas InnoDB: Este tipo de tablas están basadas en el motor de almacenamiento del mismo nombre y están orientadas a un modelo transaccional; es decir, incorporan la capacidad de insertar o modificar registros en tiempo real, bloqueando solo el registro que está siendo accedido y no la tabla completa.

3.3.4 Auditoría de bases de datos.

La auditoría de bases de Datos se define como el procedimiento mediante el cual se realiza seguimiento y registro riguroso de las acciones que los usuarios realizan sobre las bases de datos. Este procedimiento puede estar enfocado en acciones individuales como las sentencias SQL que se ejecutan, accesos de usuarios específicos o el desempeño del motor de base de datos; también puede enfocarse en combinaciones más complejas de factores como desempeño de las sentencias SQL de aplicaciones específicas y los usuarios que las ejecutan.

3.3.4.1 Objetivos de la Auditoría de Bases de Datos. El administrador o encargado de la auditoría busca los siguientes propósitos:

– Establecer responsabilidades sobre las acciones en un esquema, tabla, o fila particular, así como las acciones sobre un contenido específico.

– Disuadir a los usuarios de acciones inapropiadas con base en los privilegios establecidos.

– Identificar acciones sospechosas.

– Identificar usuarios con niveles de permisos no autorizados que le permiten realizar acciones restringidas de modificación, inserción o borrado de datos.

– Obtener reportes estadísticos de uso de las bases de datos y el desempeño del motor de base de datos.

– Determinar fechas y horas de acceso a las bases de datos.

– Determinar el origen de red de la conexión.

– Determinar las sentencias SQL ejecutadas.

– Determinar accesos y tiempos de sesión.

– Determinar el dispositivo y aplicación desde el cual se accede a la base de datos.

Se puede afirmar que como propósito general de largo alcance[25], la auditoría de bases de datos busca:

- La disminución de los riesgos de seguridad, con miras a garantizar los principios básicos de la seguridad de la información.

– El cumplimiento de estándares de gestión de la seguridad de información como la norma ISO 27001.

– El cumplimiento de marcos normativos existentes como es el caso de la ley 1273 de 2009[26] y 1581 de 2012[27].

- La mejora continua de las vulnerabilidades y riesgos identificados.

3.3.4.2. Metodología general. Toda auditoría de sistemas informáticos en términos generales debe agotar las siguientes etapas[28]:

- Definición de alcance y objetivos de la auditoría.
- Exploración y reconocimiento inicial del entorno que se va a auditar.
- Determinación de recursos necesarios para el desarrollo de la auditoría.
- Elaboración del plan de trabajo.
- Ejecución de las actividades puntuales de la auditoría.
- Elaboración del informe final.

[25] UNIVERSIDAD AUTÓNOMA DEL ESTADO DE HIDALGO. Auditoría de Bases de Datos. [En línea], [consultado el 2 de noviembre de 2018]. Disponible en: http://cidecame.uaeh.edu.mx/lcc/mapa/PROYECTO/libro21/322_auditoria_de_bases_de_datos.html .
[26] COLOMBIA, SENADO DE LA REPÚBLICA. 2018. Ley 1273 De 2009. [En línea], [consultado el 2 de noviembre de 2018]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html . .
[27] COLOMBIA, SENADO DE LA REPÚBLICA. 2018. Ley 1581 de 2012. [En línea], [consultado el 2 de noviembre de 2018]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html .
[28] UNITED NATIONS DEVELOPMENT PROGRAMME. IT Audit Manual. [En línea], [consultado el 2 de noviembre de 2018]. Disponible en: http://www.al.undp.org/content/dam/albania/docs/STAR/IT%20AUDIT%20MANUAL.pdf .

Por otro lado, en el marco específico de un proceso de auditoría de bases de datos se deben tener en cuenta los siguientes frentes de trabajo[29] :

- Auditoría de Autenticación y Acceso
- Auditoría de Usuarios y Administradores.
- Monitoreo a actividades de seguridad.
- Auditoría de Amenazas y vulnerabilidades en SGBD y BD.
- Auditoría del cambio.

3.3.4.3 Identificación de vulnerabilidades. Las vulnerabilidades de distinta naturaleza en las bases de datos y los SGBD son precisamente lo que impulsa la realización periódica de las auditorías de bases de datos.

Esto es así porque de ser explotadas estas vulnerabilidades se genera el indeseado escenario de la materialización de los riesgos de seguridad sobre la información con las consecuencias de distinto nivel de gravedad para la base de datos.

El siguiente listado muestra las principales vulnerabilidades identificadas en los sistemas de gestión de bases de datos, en la estructura y modelo de datos, a nivel de administración, y a nivel organizacional.

[29]BARNES, ROB. Database Auditing: Best Practices. [En línea], [consultado el 2 de noviembre de 2018]. Disponible en: http://www.sfisaca.org/images/May09_Slides.pdf?1Q,M3,521fd9a2-f86d-4991-8428-8e8324b89ecd .

Tabla 1. Principales vulnerabilidades de una base de datos

Origen	Vulnerabilidad
Sistema de Gestión de Base de Datos (SGBD)	Contraseñas y cuentas por defecto Configuración débil de seguridad Limitaciones en desempeño y gestión de recursos. Acceso no autorizado
Base de datos	Modelo relacional inexistente Formularios y lógica de aplicaciones sin validaciones de seguridad Sentencias mal construidas indexación y normalización inexistentes No existe política de backups
Procedimientos y herramientas software de Administración	Privilegios de usuarios mal asignados o excesivos Contraseñas débiles No se realizan actualizaciones al SGBD No se han configurado las opciones de seguridad del SGBD.
Organizacionales	Escaso personal con conocimientos especializados. Ausencia de políticas y lineamientos básicos de seguridad de la información. Ausencia de documentación básica de administración de bases de datos

Fuente: Autor

4. MARCO METODOLÓGICO

4.1 METODOLOGÍA

Para el desarrollo del proyecto se emplearán los principios de la Metodología Cuantitativa. Este enfoque metodológico es acorde con la modalidad de proyecto aplicado; Así pues, se ejecuta la medición y diagnóstico de distintos aspectos técnicos, documentales y procedimentales a través de formatos, plantillas y herramientas software que permitirán obtener los insumos necesarios para la consecución de los objetivos propuestos.

4.1.1 Universo. En términos organizacionales, el universo del proyecto lo constituye la Dirección de Aseguramiento de la Secretaría de Salud de la Gobernación de Cundinamarca. En este escenario se encuentran los distintos actores que de manera directa o indirecta interactúan con las actividades de administración de la Base de Datos del Aseguramiento.

En términos técnicos, el alcance lo determinan los entornos de Producción, Preproducción y Desarrollo que soportan la Base de Datos del Aseguramiento y las herramientas de administración.

4.1.2 Instrumentos. El trabajo recurre a los instrumentos de captura de información como formularios y plantillas, enmarcados en la metodología de identificación y análisis de riesgos MAGERIT y en las buenas prácticas de auditoría de sistemas de Información que tienen como referentes las normas ISO 27001 e ISO 27002.

En este punto es conveniente resaltar que la adaptación de estos estándares y buenas prácticas a través de los instrumentos diseñados constituye un aporte concreto de este trabajo a los lineamientos metodológicos de seguridad de la información para la administración de la Base de Datos del Aseguramiento.

Se puede identificar los siguientes instrumentos fundamentales:

- Matriz para la Identificación y valoración de Activos de Información
- Matriz Identificación y valoración de Riesgos sobre los Activos de Información
- Matriz de aplicabilidad para la identificación y auditoría de controles de la norma ISO 27001 que aplican para la Base de Datos del Aseguramiento

4.1.3 Fases metodológicas. La metodología a emplear está en plena correspondencia con los objetivos específicos propuestos y comprende cuatro (4) fases de trabajo.

Fase 1.- Marco de Referencia: esta fase aborda las actividades de exploración y estructuración documental frente al marco contextual, teórico y conceptual para el presente trabajo.

Comprende las siguientes actividades generales:

Actividad 1.1.- Se estructura el marco contextual del proyecto. Se consignan los aspectos institucionales y organizacionales que enmarcan las actividades de administración de la Base de Datos del Aseguramiento.

Actividad 1.2.- Se explora y documenta el marco teórico y conceptual que soporta el trabajo, recurriendo a las disposiciones y orientaciones de las principales normativas de seguridad de la información.

Fase 2.- Diagnóstico: Esta fase está en coherencia con el primer objetivo específico y aborda las actividades necesarias para identificar el estado actual de la Base de Datos del Aseguramiento frente a lineamientos de seguridad de la información.

Comprende las siguientes actividades generales:

Actividad 2.1.- Se elabora el diagnóstico sobre el estado actual de la seguridad de la información de la Base de Datos del Aseguramiento en el Departamento de Cundinamarca.

Actividad 2.2.- Identificación y valoración de los riesgos de seguridad que enfrenta el procedimiento.

Fase 3.- Elaboración de los lineamientos de seguridad: Esta fase está en coherencia con el segundo objetivo específico; aborda las actividades para cumplir con el aporte principal de este trabajo cuál es el diseño de lineamientos metodológicos de seguridad de la información.

Comprende las siguientes actividades generales:

Actividad 3.1.- Se identifican y definen los lineamientos de seguridad de la información que aplican para la Base de Datos del Aseguramiento.

Fase 4.- Elaboración de la guía técnica de seguridad para la Base de Datos del Aseguramiento: Esta fase está en coherencia con el tercer objetivo específico; aborda la elaboración de una guía técnica a partir de los lineamientos de seguridad de la información propuestos.

Comprende las siguientes actividades generales:

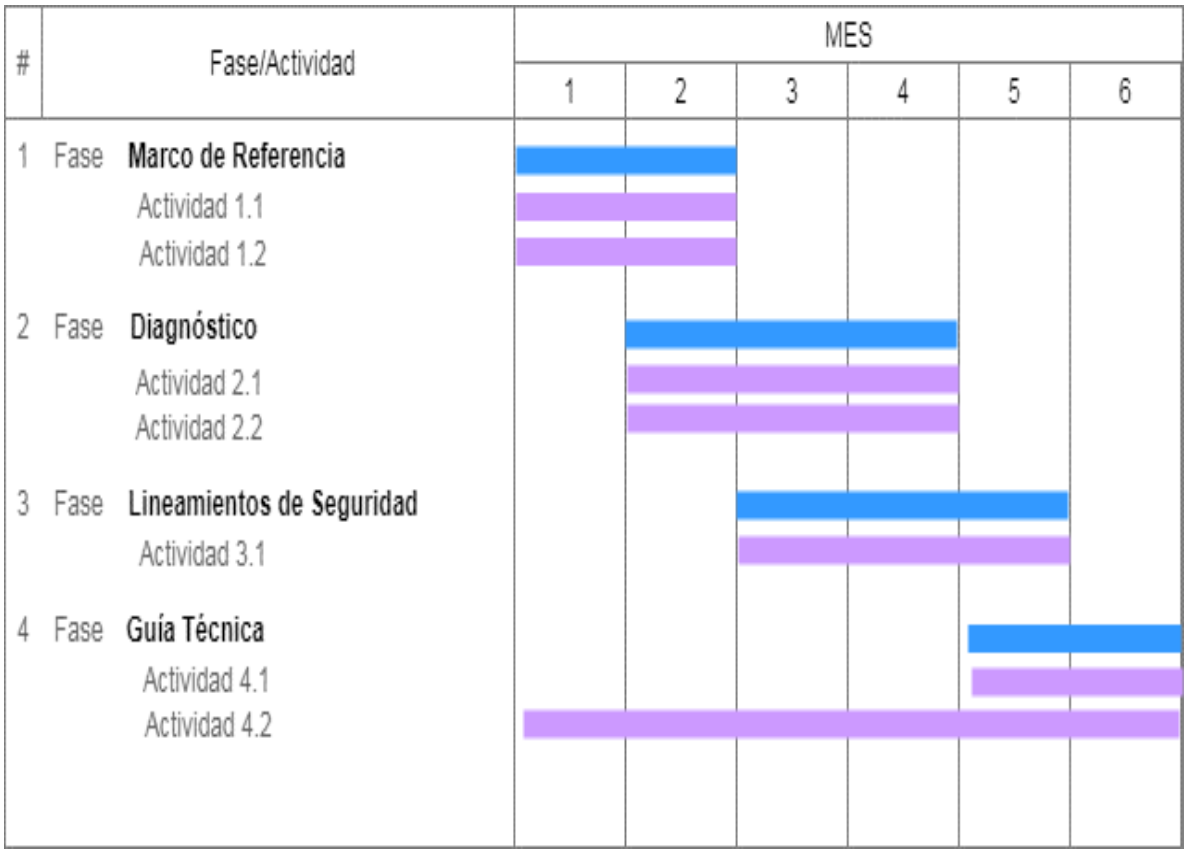
Actividad 4.1.- Elaboración de la guía técnica.

Actividad 4.2.- Revisión y Cierre del Proyecto.

4.2 CRONOGRAMA

A continuación, se presenta el cronograma general del proyecto que distribuye la ejecución de las cuatro fases en un periodo de seis meses.

Figura 6. Cronograma



Fuente: Autor

4.3 PRESUPUESTO

Tabla 2. Presupuesto

RECURSO	DESCRIPCIÓN	PRESUPUESTO
Equipo Humano	1.- Un profesional en ingeniería de sistemas o afines en el rol de Director de trabajo de grado 2.- Un (1) profesional en ingeniería electrónica o afines en el rol de estudiante	1.- Dedicación director: 10 horas/mes Valor estimado de la hora: $150.000 Costo x 6 meses: $ 9.000.000 2.- Dedicación estudiante: 30 horas/ mes Valor estimado/hora: $100.000 Costo x 6meses: $18.000.000 **Subtotal (x 6 meses):** **$ 27.000.000**
Equipos y Software	1.- Un (1) equipo Servidor para la base de datos de producción 2.- Un (1) equipo Servidor para las bases de datos de Pre-producción y Desarrollo. 3.- Un (1) equipo de trabajo. 4.- Un Sistema de Gestión de Base de Datos de licencia libre 5.- Paquete de ofimática	1.- Costo Mes/Servidor dedicado: $300.000. Costo x 6 meses: $1.800.000 2.- Costo Mes/Servidor dedicado: $300.000. Costo x 6 meses: $1.800.000 3.- Costo mes/PC: $50.000 Costo x 6 meses: $300.000 4.- Licencia GNU GPL de MySQL. 5.- Licencia Office 2016: $280.000 **Subtotal: $4.180.000**
Materiales y suministros	Papelería e implementos de oficina	**Subtotal: $600.00**
Bibliografía	1.- Bibliografía especializada de libre consulta en Internet. 1.- Repositorios académicos por suscripción.	1.- No tiene costo 2.- Costo estimado suscripción x 6 meses**: $200.000** **Subtotal: $200.000**
		TOTAL: $31.980.000

Fuente: Autor

5. DESARROLLO DE LA AUDITORIA Y ANÁLISIS DE RIESGO

En este apartado se desarrolla un paralelo entre las prácticas empleadas en la administración de la Base de Datos del Aseguramiento del Departamento de Cundinamarca, frente a los controles que propone la norma ISO 27001 - anexo A. El propósito de esta actividad es la identificación de las debilidades y falencias que actualmente presenta el manejo de los activos de información involucrados en estas actividades de administración, con el fin de mejorar el enfoque de las opciones de mejora a proponer[30].

Es importante anotar que la norma no obliga la implementación de todos los controles. Así pues, dentro del alcance de este trabajo de grado se identificarán aquellos controles que aplican al procedimiento.

A continuación, se desarrolla la Declaración de Aplicabilidad (SOA – Statement Of Applicability) que permite la valoración de los controles o prácticas actuales que se ejecutan en la administración de la Base de Datos del Aseguramiento y su nivel de cumplimento frente a los controles de la norma ISO 27001 anexo A.

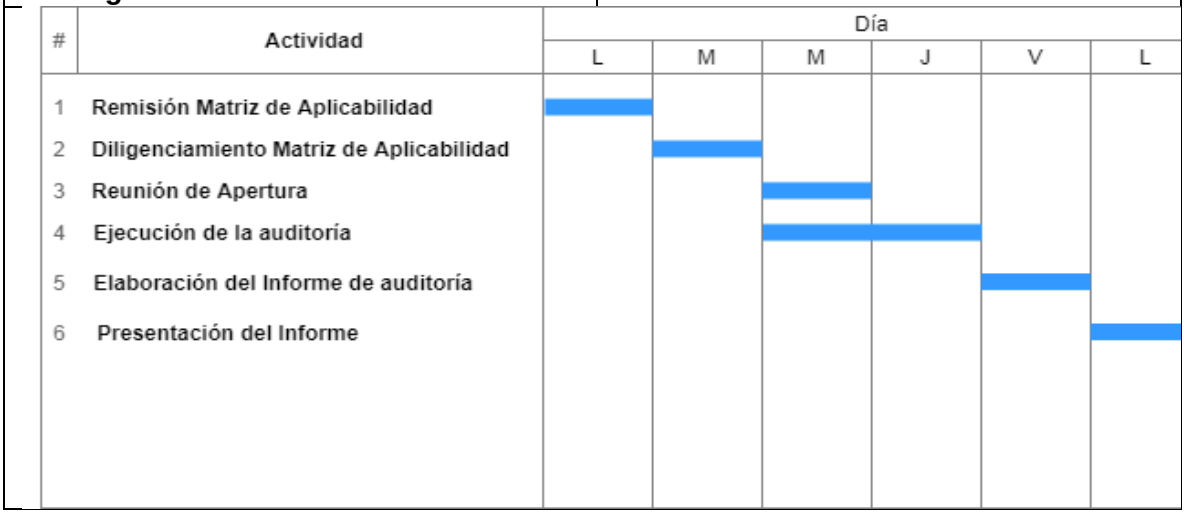
5.1 PLAN DE AUDITORIA

A continuación, se consigna el Plan de Auditoría que formaliza la programación de las actividades para la revisión del cumplimiento de los procedimientos y recursos empleados en la administración de la Base de Datos del Aseguramiento frente a los controles de la norma ISO 27001.

[30]GIRALDO CEPEDA, Luis Enrique. Análisis para la implementación de un sistema de gestión de la seguridad de la información según la norma ISO 27001 en la empresa Servidoc S.A. Cali: Universidad Nacional Abierta y a Distancia. 2016, Especialización en Seguridad Informática. Colombia. [En línea], [consultado el 2 de noviembre de 2018]. Disponible en: https://repository.unad.edu.co/handle/10596/6341?mode=full .

Tabla 3. Plan de Auditoría

PLAN DE AUDITORIA	
Fecha: 15/12/2018	**No. Auditoría:** 1
Procedimiento auditado:	Seguimiento a la Base de Datos del Aseguramiento en Salud en el Departamento de Cundinamarca
Objetivo de la auditoría:	Determinar el estado actual de la seguridad de la información en las actividades de administración de la Base de Datos del Aseguramiento en el marco de la norma ISO 27001 – Anexo A.
Alcance de la auditoría:	Evaluación de la seguridad de la información en las actividades de administración de la Base de Datos del Aseguramiento
Documentos de referencia:	Norma ISO 27001 : 2013
Personal auditado:	Derian Jesús Dorado Daza (Administrador de la Base de Datos del Aseguramiento)
Programa de Auditoría:	
1.- Remisión de la matriz de aplicabilidad 2.- Diligenciamiento de la Matriz de aplicabilidad 3.- Reunión de apertura 4.- Ejecución de la auditoría 5.- Elaboración del informe de auditoría 6.- Presentación del informe	
Cronograma de Auditoría:	



Fuente: Autor

5.2 MATRIZ DE APLICABILIDAD

En el presente apartado se presenta el resultado de la Matriz de Aplicabilidad; la cual fue aceptada como instrumento de valoración y declaración de los controles de seguridad de la información que aplican a las actividades de administración de la Base de Datos del Aseguramiento.

La Declaración de Aplicabilidad fue evaluada a partir de dos criterios discretos: Aplica y No aplica. El criterio No aplica fue utilizado en aquellos controles cuyo alcance no está relacionado con las actividades de administración de la base de datos.

Tabla 4. Matriz de Aplicabilidad.

Dominio/Objetivo de Control/Control		**Valoración**	**Justificación**
A.5 Políticas de seguridad de la información			
A.5.1 Directrices establecidas por la dirección para la seguridad de la información			
A.5.1.1	Políticas para la seguridad de la información	Aplica	
A.5.1.2	Revisión de las políticas para seguridad de la información	Aplica	
A.6. Organización de la seguridad de la información			
A.6.1 Organización interna			
A.6.1.1	Roles y responsabilidades para la seguridad de información	Aplica	
A.6.1.2	Separación de deberes	Aplica	
A.6.1.3	Contacto con las autoridades	Aplica	
A.6.1.4	Contacto con grupos de interés especial	Aplica	
A.6.1.5	Seguridad de la información en la gestión de proyectos	No Aplica	No se aplica metodología de proyectos a la administración de la base de datos.
A.6.2 Dispositivos móviles y teletrabajo			
A.6.2.1	Política para dispositivos móviles	Aplica	
A.6.2.2	Teletrabajo	Aplica	
A.7. Seguridad de los recursos humanos			
A.7.1 Antes de asumir el empleo			

Tabla 4. (Continuación)

Dominio/Objetivo de Control/Control		Valoración	Justificación
A.7.1.1	Selección	Aplica	
A.7.1.2	Términos y condiciones del empleo	Aplica	
A.7.2 Durante la ejecución del empleo			
A.7.2.1	Responsabilidades de la dirección	Aplica	
A.7.2.2	Toma de conciencia, educación y formación en la seguridad de la información	Aplica	
A.7.2.3	Proceso disciplinario	Aplica	
A.7.3 Terminación o cambio de empleo			
A.7.3.1	Terminación o cambio de responsabilidades de empleo	Aplica	
A.8 Gestión de activos			
A.8.1 Responsabilidad por los activos			
A.8.1.1	Inventario de activos	Aplica	
A.8.1.2	Propiedad de los activos	Aplica	
A.8.1.3	Uso aceptable de los activos	Aplica	
A.8.1.4	Devolución de activos	Aplica	
A.8.2 Clasificación de la información			
A.8.2.1	Clasificación de la información	Aplica	
A.8.2.2	Etiquetado de la información	Aplica	
A.8.2.3	Manejo de activos	Aplica	
A.8.3 Manipulación de medios			
A.8.3.1	Gestión de medios removibles	Aplica	
A.8.3.2	Disposición de los medios	Aplica	
A.8.3.3	Transferencia de medios físicos	No aplica	Lo medios físicos no son transportados fuera de las instalaciones de la Gobernación.
A.9. Control de acceso			
A.9.1 Requisitos del negocio para control de acceso			
A.9.1.1	Política de control de acceso	Aplica	

Tabla 4. (Continuación)

Dominio/Objetivo de Control/Control		**Valoración**	**Justificación**
A.9.1.2	Política sobre el uso de los servicios de red	Aplica	
A.9.2 Gestión de acceso de usuarios			
A.9.2.1	Registro y cancelación del registro de usuarios	Aplica	
A.9.2.2	Suministro de acceso de usuarios	Aplica	
A.9.2.3	Gestión de derechos de acceso privilegiado	Aplica	
A.9.2.4	Gestión de información de autenticación secreta de usuarios	Aplica	
A.9.2.5	Revisión de los derechos de acceso de usuarios	Aplica	
A.9.2.6	Retiro o ajuste de los derechos de acceso	Aplica	
A.9.3 Responsabilidades de los usuarios			
A.9.3.1	Uso de la información de autenticación secreta	Aplica	
A.9.4 Control de acceso a sistemas y aplicaciones			
A.9.4.1	Restricción de acceso Información	Aplica	
A.9.4.2	Procedimiento de ingreso seguro	Aplica	
A.9.4.3	Sistema de gestión de contraseñas	Aplica	
A.9.4.4	Uso de programas utilitarios privilegiados	Aplica	
A.9.4.5	Control de acceso a códigos fuente de programas	Aplica	
A.10 Criptografía			
A.10.1 Controles criptográficos			
A.10.1.1	Política sobre el uso de controles criptográficos	Aplica	
A.10.1.2	Gestión de llaves	Aplica	
A.11 Seguridad física y del entorno			
A.11.1 Áreas seguras			
A.11.1.1	Perímetro de seguridad física	Aplica	
A.11.1.2	Controles físicos de entrada	Aplica	
A.11.1.3	Seguridad de oficinas, recintos e instalaciones	Aplica	

Tabla 4. (Continuación)

Dominio/Objetivo de Control/Control		Valoración	Justificación
A.11.1.4	Protección contra amenazas externas y ambientales	Aplica	
A.11.1.5	Trabajo en áreas seguras	Aplica	
A.11.1.6	Áreas de despacho y carga	Aplica	
A.11.2 Equipos			
A.11.2.1	Ubicación y protección de los equipos	Aplica	
A.11.2.2	Servicios de suministro	Aplica	
A.11.2.3	Seguridad del cableado	Aplica	
A.11.2.4	Mantenimiento de equipos	Aplica	
A.11.2.5	Retiro de activos	Aplica	
A.11.2.6	Seguridad de equipos y activos fuera de las instalaciones	No aplica	Los equipos no cambian de ubicación. Permanecen en las instalaciones.
A.11.2.7	Disposición segura o reutilización de equipos	Aplica	
A.11.2.8	Equipos de usuario desatendidos	Aplica	
A.11.2.9	Política de escritorio limpio y pantalla limpia	Aplica	
A.12. Seguridad de las operaciones			
A.12.1. Procedimientos operacionales y responsabilidades			
A.12.1.1	Procedimientos de operación documentados	Aplica	
A.12.1.2	Gestión de cambios	Aplica	
A.12.1.3	Gestión de capacidad	Aplica	
A.12.1.4	Separación de los ambientes de desarrollo, pruebas y operación	Aplica	
A.12.2 Protección contra códigos maliciosos			
A.12.2.1	Controles contra códigos maliciosos	Aplica	
A.12.3 Copias de respaldo			
A.12.3.1	Respaldo de información	Aplica	
A.12.4 Registro y seguimiento			
A.12.4.1	Registro de eventos	Aplica	

Tabla 4. (Continuación)

Dominio/Objetivo de Control/Control		Valoración	Justificación
A.12.4.2	Protección de la información de registro	Aplica	
A.12.4.3	Registros del administrador y del operador	Aplica	
A.12.4.4	Sincronización de relojes	Aplica	
A.12.5 Control de software operacional			
A.12.5.1	Instalación de software en sistemas operativos	Aplica	
A.12.6 Gestión de la vulnerabilidad técnica			
A.12.6.1	Gestión de las vulnerabilidades técnicas	Aplica	
A.12.6.2	Restricciones sobre la instalación de software	Aplica	
A.12.7 Consideraciones sobre auditorías de sistemas de información			
A.12.7.1	Información controles de auditoría de sistemas	Aplica	
A.13 Seguridad de las comunicaciones			
A.13.1 Gestión de la seguridad de las redes			
A.13.1.1	Controles de redes	Aplica	
A.13.1.2	Seguridad de los servicios de red	Aplica	
A.13.1.3	Separación en las redes	Aplica	
A.13.2 Transferencia de información			
A.13.2.1	Políticas y procedimientos de transferencia de información	Aplica	
A.13.2.2	Acuerdos sobre transferencia de información	Aplica	
A.13.2.3	Mensajería electrónica	Aplica	
A.13.2.4	Acuerdos de confidencialidad o de no divulgación	Aplica	
A.14 Adquisición, desarrollo y mantenimientos de sistemas			
A.14.1 Requisitos de seguridad de los sistemas de información			
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	Aplica	
A.14.1.2	Seguridad de servicios de las aplicaciones en redes públicas	Aplica	

Tabla 4. (Continuación)

Dominio/Objetivo de Control/Control		Valoración	Justificación
A.14.1.3	Protección de transacciones de los servicios de las aplicaciones	Aplica	
A.14.2 Seguridad en los procesos de desarrollo y soporte			
A.14.2.1	Política de desarrollo seguro	Aplica	
A.14.2.2	Procedimientos de control de cambios en sistemas	Aplica	
A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	Aplica	
A.14.2.4	Restricciones en los cambios a los paquetes de software	Aplica	
A.14.2.5	Principios de construcción de sistemas seguros	Aplica	
A.14.2.6	Ambiente de desarrollo seguro	Aplica	
A.14.2.7	Desarrollo contratado externamente	Aplica	
A.14.2.8	Pruebas de seguridad de sistemas	Aplica	
A.14.2.9	Prueba de aceptación de sistemas	Aplica	
A.14.3 Datos de prueba			
A.14.3.1	Protección de datos de prueba	Aplica	
A.15 Relación con los proveedores			
A.15.1 Seguridad de la información en las relaciones con los proveedores			
A.15.1.1	Política de seguridad de la información para las relaciones con proveedores	No Aplica	No intervienen proveedores en las actividades de administración de la Base de Datos del Aseguramiento.
A.15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores	No aplica	Dado que no intervienen proveedores, no se establecen acuerdos.
A.15.1.3	Cadena de suministro de tecnología de información y comunicación	No Aplica	Los servidores son aprovisionados al interior de la Gobernación.
A.15.2 Gestión de la prestación de servicios con los proveedores			
A.15.2.1	Seguimiento y revisión de los servicios de los proveedores	No Aplica	Dado que no intervienen proveedores, no se realizan actividades de seguimiento.

Tabla 4. (Continuación)

Dominio/Objetivo de Control/Control		Valoración	Justificación
A.15.2.2	Gestión de cambios en los servicios de proveedores	No aplica	Dado que no intervienen proveedores, no se realizan actividades de gestión de cambios.
A.16 Gestión de incidentes de seguridad de la información			
A.16.1 Gestión de incidentes y mejoras en la seguridad de la información			
A.16.1.1	Responsabilidad y procedimientos	Aplica	
A.16.1.2	Reporte de eventos de seguridad de la información	Aplica	
A.16.1.3	Reporte de debilidades de seguridad de la información	Aplica	
A.16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	Aplica	
A.16.1.5	Respuesta a incidentes de seguridad de la información	Aplica	
A.16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	Aplica	
A.16.1.7	Recolección de evidencia	Aplica	
A.17 Aspectos de seguridad de la información de la gestión de continuidad de negocio			
A.17.1 Continuidad de seguridad de la información			
A.17.1.1	Planificación de la continuidad de la seguridad de la información	Aplica	
A.17.1.2	Implementación de la continuidad de la seguridad de la información	Aplica	
A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	Aplica	
A.17.2 Redundancias			
A.17.2.1	Disponibilidad de instalaciones de procesamiento de información.	Aplica	
A.18 Cumplimiento			
A.18.1 Cumplimiento de requisitos legales y contractuales			
A.18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	Aplica	
A.18.1.2	Derechos de propiedad intelectual	Aplica	

Tabla 4. (Continuación)

Dominio/Objetivo de Control/Control		Valoración	Justificación
A.18.1.3	Protección de registros	Aplica	
A.18.1.4	Privacidad y protección de datos personales	Aplica	
A.18.1.5	Reglamentación de controles criptográficos	Aplica	
A.18.2 Revisiones de seguridad de la información			
A.18.2.1	Revisión independiente de la seguridad de la información	Aplica	
A.18.2.2	Cumplimiento con las políticas y normas de seguridad	Aplica	
A.18.2.3	Revisión del cumplimiento técnico	Aplica	

Fuente: Autor.

5.3 MATRIZ DE HALLAZGOS

El presente apartado presenta la Matriz de Hallazgos que consolida los resultados encontrados durante las actividades de auditoría sobre los procedimientos y recursos empleados actualmente en la administración de la Base de Datos del Aseguramiento.

Tabla 5. Matriz de hallazgos.

Dominio/Objetivo de Control/Control		Valoración	Hallazgo
A.5 Políticas de seguridad de la información			
A.5.1 Directrices establecidas por la dirección para la seguridad de la información			
A.5.1.1	Políticas para la seguridad de la información	No cumple	No se evidencia la existencia de políticas para la seguridad de la información.
A.5.1.2	Revisión de las políticas para seguridad de la información	No cumple	No se evidencia planificación para la revisión periódica de políticas de seguridad de la información.
A.6. Organización de la seguridad de la información			
A.6.1 Organización interna			
A.6.1.1	Roles y responsabilidades para la seguridad de información	No cumple	No se evidencia la existencia del personal necesario para seguir conductos regulares a la hora de

Tabla 5. (Continuación)

Dominio/Objetivo de Control/Control		Valoración	Hallazgo
			garantizar la seguridad de la información.
A.6.1.2	Separación de deberes	Cumple	Se evidenció la existencia de normatividad y cumplimiento de la misma, que asigna responsabilidades en el manejo y actualización de la información que alimenta la Base de Datos del Aseguramiento.
A.6.1.3	Contacto con las autoridades	Cumple	Se evidenció el contacto con las entidades que se constituyen la autoridad en el manejo de la información de la Base de Datos del Aseguramiento.
A.6.1.4	Contacto con grupos de interés especial	Cumple	Se evidenció el contacto con las entidades que prestan asesoría y ayuda frente a actividades del manejo de la información de la Base de Datos del Aseguramiento.
A.6.1.5	Seguridad de la información en la gestión de proyectos	No Aplica	No se aplica metodología de proyectos a la administración de la base de datos.
A.6.2 Dispositivos móviles y teletrabajo			
A.6.2.1	Política para dispositivos móviles	No cumple	No se evidencia la existencia de una política específica para garantizar la seguridad de la información cuando se emplean dispositivos móviles.
A.6.2.2	Teletrabajo	Cumple	Se evidencia la existencia de procedimientos claros que promueven la seguridad de la información para los funcionarios que acceden de manera remota a recursos computacionales.
A.7. Seguridad de los recursos humanos			
A.7.1 Antes de asumir el empleo			

Tabla 5. (Continuación)

Dominio/Objetivo de Control/Control		Valoración	Hallazgo
A.7.1.1	Selección	Cumple	Los candidatos son seleccionados de acuerdo a la normatividad vigente para contratación de personal experto y que cumple con los requisitos profesionales y legales.
A.7.1.2	Términos y condiciones del empleo	No cumple	No se evidencia la inclusión de cláusulas o compromisos específicos en el contrato o manual de funciones frente al tema de la seguridad de la información.
A.7.2 Durante la ejecución del empleo			
A.7.2.1	Responsabilidades de la dirección	No cumple	No hay evidencia de que la Dirección tome medidas frente al manejo seguro de la información.
A.7.2.2	Toma de conciencia, educación y formación en la seguridad de la información	No cumple	No se evidencia la realización de jornadas educativas frente al manejo seguro de la información.
A.7.2.3	Proceso disciplinario	No cumple	No se evidencia la existencia de procedimientos sobre sanciones disciplinarias para los casos en los que un funcionario ha incurrido en faltas deliberadas en el manejo de la información.
A.7.3 Terminación o cambio de empleo			
A.7.3.1	Terminación o cambio de responsabilidades de empleo	No cumple	No se evidencia lineamientos que apliquen cuando un funcionario deja el cargo y se requiere mantener la seguridad de la información sobre los activos.
A.8 Gestión de activos			
A.8.1 Responsabilidad por los activos			
A.8.1.1	Inventario de activos	No cumple	No se evidencia la existencia de un inventario de los activos de información involucrados en las actividades de administración de la Base de Datos del Aseguramiento.
A.8.1.2	Propiedad de los activos	No cumple	No se evidencia asignación de responsabilidad o propiedad sobre los activos de información.
A.8.1.3	Uso aceptable de los activos	No cumple	No se evidencia la existencia de lineamientos que traten sobre el

Tabla 5. (Continuación)

Dominio/Objetivo de Control/Control		Valoración	Hallazgo
			uso apropiado de los activos de información.
A.8.1.4	Devolución de activos	No cumple	No se evidencia la existencia de lineamientos que indiquen el modo en que serán retornados los activos de información una vez el funcionario deja el cargo.
A.8.2 Clasificación de la información			
A.8.2.1	Clasificación de la información	No cumple	No se evidencia la clasificación de la información en cuanto a requisitos legales, valor, criticidad y sensibilidad.
A.8.2.2	Etiquetado de la información	No cumple	No se evidencia un lineamiento para el etiquetado de la información acorde con el esquema de clasificación adoptado.
A.8.2.3	Manejo de activos	No cumple	No se evidencia un lineamiento para el manejo apropiado de los activos de información.
A.8.3 Manipulación de medios			
A.8.3.1	Gestión de medios removibles	No cumple	No se evidencia la existencia de un lineamiento para la gestión de medios removibles que esté en concordancia con el esquema de clasificación de la información manejada en la administración de la Base de Datos del Aseguramiento.
A.8.3.2	Disposición de los medios	No cumple	No se evidencia un lineamiento para la disposición de los medios que almacenan la información cuando sean reemplazados, transferidos o dados de baja.
A.8.3.3	Transferencia de medios físicos	No aplica	Lo medios físicos no son transportados fuera de las instalaciones de la Gobernación.
A.9. Control de acceso			
A.9.1 Requisitos del negocio para control de acceso			
A.9.1.1	Política de control de acceso	No cumple	No se evidencia la existencia de una política de control de acceso a los activos de información y a las herramientas para la

Tabla 5. (Continuación)

Dominio/Objetivo de Control/Control		Valoración	Hallazgo
			administración de la Base de Datos del Aseguramiento
A.9.1.2	Política sobre el uso de los servicios de red	Cumple	Se evidenciaron los procedimientos para controlar el acceso a las facilidades de red de acuerdo con los perfiles de los usuarios y específicamente con el perfil que necesita el administrador de la Base de Datos del Aseguramiento.
A.9.2 Gestión de acceso de usuarios			
A.9.2.1	Registro y cancelación del registro de usuarios	No cumple	No se evidencia la existencia de un procedimiento específico para el registro de los usuarios que requieran acceso a la administración o consulta de la Base de Datos del Aseguramiento
A.9.2.2	Suministro de acceso de usuarios	No cumple	No se evidencia la existencia de un procedimiento específico para la asignación de acceso a los usuarios registrados
A.9.2.3	Gestión de derechos de acceso privilegiado	No cumple	No se evidencia un procedimiento específico para la gestión de los permisos y privilegios de acceso a los usuarios registrados
A.9.2.4	Gestión de información de autenticación secreta de usuarios	No cumple	No se evidencia la existencia de un lineamiento específico para la gestión de la información de autenticación de los usuarios registrados.
A.9.2.5	Revisión de los derechos de acceso de usuarios	No cumple	No se evidencia la existencia de un procedimiento puntual para la revisión periódica de los derechos de acceso de los usuarios registrados.
A.9.2.6	Retiro o ajuste de los derechos de acceso	No cumple	No se evidencia la existencia de un lineamiento específico para la deshabilitación o eliminación de los derechos de acceso a la Base de Datos del Aseguramiento y a las herramientas software de administración, cuando el usuario termina su contrato o las funciones del cargo.
A.9.3 Responsabilidades de los usuarios			

Tabla 5. (Continuación)

Dominio/Objetivo de Control/Control		Valoración	Hallazgo
A.9.3.1	Uso de la información de autenticación secreta	No cumple	No se evidencia la existencia de un lineamiento específico que reglamente el uso apropiado de la información secreta por parte de los usuarios registrados.
A.9.4 Control de acceso a sistemas y aplicaciones			
A.9.4.1	Restricción de acceso Información	Cumple	Se evidencia la existencia de controles para restringir el acceso a la información de la Base de Datos del Aseguramiento de acuerdo con el nivel de acceso y privilegios asignado
A.9.4.2	Procedimiento de ingreso seguro	Cumple	Se evidencia la existencia de controles de inicio de sesión seguro.
A.9.4.3	Sistema de gestión de contraseñas	No cumple	No se evidencia la existencia de un sistema de gestión de contraseñas.
A.9.4.4	Uso de programas utilitarios privilegiados	Cumple	Se evidencia la existencia de controles para restringir el uso de herramientas de software que puedan acceder a la Base de Datos del Aseguramiento.
A.9.4.5	Control de acceso a códigos fuente de programas	Cumple	Se evidencia la existencia de controles para el acceso a código fuente empleado en herramientas de administración y consulta a la base de datos
A.10 Criptografía			
A.10.1 Controles criptográficos			
A.10.1.1	Política sobre el uso de controles criptográficos	No cumple	No se evidencia la existencia de un lineamiento específico para el uso de controles criptográficos sobre información Confidencial.
A.10.1.2	Gestión de llaves	No cumple	No se evidencia la existencia de un lineamiento para la gestión del ciclo de vida de claves criptográficas.
A.11 Seguridad física y del entorno			
A.11.1 Áreas seguras			
A.11.1.1	Perímetro de seguridad física	Cumple	Se evidencia la existencia y funcionamiento de un recinto con perímetro de seguridad física para la infraestructura TI que

Tabla 5. (Continuación)

Dominio/Objetivo de Control/Control		Valoración	Hallazgo
			soporta la Base de Datos del Aseguramiento.
A.11.1.2	Controles físicos de entrada	Cumple	Se evidencia la existencia y funcionamiento de controles electrónicos (autenticación mediante huella y tarjeta digital) dispuestos en la entrada a la infraestructura TI que soporta la Base de Datos del Aseguramiento.
A.11.1.3	Seguridad de oficinas, recintos e instalaciones	Cumple	Se evidencia la existencia y funcionamiento de controles electrónicos y físicos para el ingreso a las oficinas de la Entidad.
A.11.1.4	Protección contra amenazas externas y ambientales	Cumple	Se evidencia la existencia de los elementos requeridos para contrarrestar amenazas externas y ambientales.
A.11.1.5	Trabajo en áreas seguras	Cumple	Se evidencia la existencia de políticas de seguridad en el trabajo y un comité de personal dedicado al respectivo seguimiento.
A.11.1.6	Áreas de despacho y carga	Cumple	Se evidencia la existencia de zonas restringidas y específicas para la recepción y despacho de mensajería en la entidad
A.11.2 Equipos			
A.11.2.1	Ubicación y protección de los equipos	Cumple	Se evidencia que la ubicación y los elementos de protección contra amenazas externas y ambientales son los adecuados para la seguridad física de la infraestructura de TI que soporta la Base de Datos del Aseguramiento.
A.11.2.2	Servicios de suministro	Cumple	Se evidencia la existencia y funcionamiento de la red eléctrica regulada, sistema de alimentación ininterrumpida (UPS), banco de baterías y planta generadora diesel.
A.11.2.3	Seguridad del cableado	Cumple	El cableado de la red corporativa cumple con las normas de instalación y protección contra

Tabla 5. (Continuación)

Dominio/Objetivo de Control/Control		Valoración	Hallazgo
			accidentes, interferencia o interceptación.
A.11.2.4	Mantenimiento de equipos	Cumple	La entidad cuenta con un área específica de mesa de ayuda que brinda mantenimiento de los equipos.
A.11.2.5	Retiro de activos	Cumple	Se evidencia la ejecución de las condiciones contractuales y debida autorización para retirar o desinstalar equipos y herramientas software.
A.11.2.6	Seguridad de equipos y activos fuera de las instalaciones	No aplica	Los equipos no cambian de ubicación. Permanecen en las instalaciones de la Gobernación de Cundinamarca.
A.11.2.7	Disposición segura o reutilización de equipos	No Cumple	No se evidenció un lineamiento específico para la revisión y disposición final de información almacenada en equipos que serán reemplazados, reasignados o dados de baja.
A.11.2.8	Equipos de usuario desatendidos	Cumple	Se evidencia la existencia de lineamientos y actividades pedagógicas para evitar que los equipos de trabajo desatendidos queden expuestos a interacción directa por parte de terceras personas.
A.11.2.9	Política de escritorio limpio y pantalla limpia	Cumple	Se evidencia la existencia de lineamientos y promoción para que los funcionarios mantengan el puesto de trabajo libre de documentos y pantalla de inicio limpia.
A.12. Seguridad de las operaciones			
A.12.1. Procedimientos operacionales y responsabilidades			
A.12.1.1	Procedimientos de operación documentados	Cumple	Se evidencia la existencia de la documentación del procedimiento de seguimiento a la Base de Datos del Aseguramiento. Así como guías técnicas para actualización y gestión de la base de datos.
A.12.1.2	Gestión de cambios	No cumple	No se evidencia un lineamiento claro frente a cambios

Tabla 5. (Continuación)

Dominio/Objetivo de Control/Control		Valoración	Hallazgo
			organizacionales, procedimientos, o técnicos que puedan afectar la seguridad de la información en la Base de Datos del Aseguramiento.
A.12.1.3	Gestión de capacidad	No cumple	No se evidencia un lineamiento claro para el seguimiento y acciones a seguir frente a la capacidad de los recursos computacionales asignados para la operación de la Base de Datos del Aseguramiento.
A.12.1.4	Separación de los ambientes de desarrollo, pruebas y operación	Cumple	Se evidencia la existencia de los ambientes de Operación, Pruebas y Desarrollo.
A.12.2 Protección contra códigos maliciosos			
A.12.2.1	Controles contra códigos maliciosos	No cumple	No se evidencia un lineamiento frente a eventos de seguridad ocasionados por código malicioso.
A.12.3 Copias de respaldo			
A.12.3.1	Respaldo de información	No Cumple	No es claro el lineamiento para la actividad de realización de respaldo de información en el marco de las actividades de la Administración de la base de Datos del aseguramiento
A.12.4 Registro y seguimiento			
A.12.4.1	Registro de eventos	No cumple	No se evidencia la existencia de un lineamiento para el registro de eventos que puedan afectar la seguridad de la información.
A.12.4.2	Protección de la información de registro	No cumple	No se evidencia la existencia de controles para la protección de la información de registro de eventos
A.12.4.3	Registros del administrador y del operador	No cumple	No se evidencia de controles para la protección de los eventos de inicio y actividades de sesión de los usuarios registrados en la Base de Datos del Aseguramiento.
A.12.4.4	Sincronización de relojes	No cumple	No se evidencia la sincronización de los servidores que soportan la

Tabla 5. (Continuación)

Dominio/Objetivo de Control/Control		Valoración	Hallazgo
			Base de Datos del Aseguramiento contra servicios externos de medición del tiempo.
A.12.5 Control de software operacional			
A.12.5.1	Instalación de software en sistemas operativos	Cumple	Se evidencia la existencia de los procedimientos y controles requeridos para la instalación de software en equipos de trabajo y servidores
A.12.6 Gestión de la vulnerabilidad técnica			
A.12.6.1	Gestión de las vulnerabilidades técnicas	No cumple	No se evidencia la existencia de un lineamiento para la identificación y gestión de las vulnerabilidades técnicas que pueden afectar las herramientas software que soportan la operación de la Base de Datos del Aseguramiento.
A.12.6.2	Restricciones sobre la instalación de software	Cumple	Se evidencia la existencia de lineamientos y controles para la instalación de software.
A.12.7 Consideraciones sobre auditorías de sistemas de información			
A.12.7.1	Información controles de auditoría de sistemas	No cumple	No se evidencia lineamientos ni actividades de auditoría planificadas para la verificación del estado de los sistemas de información y herramientas software que soportan la operación de la base de Datos del Aseguramiento
A.13 Seguridad de las comunicaciones			
A.13.1 Gestión de la seguridad de las redes			
A.13.1.1	Controles de redes	Cumple	Se evidencia la existencia de procedimientos, controles y herramientas especializadas para la administración segura de la red corporativa.
A.13.1.2	Seguridad de los servicios de red	Cumple	Se evidencia la existencia delineamientos, herramientas y cláusulas contractuales para garantizar la seguridad en los servicios de red de la entidad.

Tabla 5. (Continuación)

Dominio/Objetivo de Control/Control		Valoración	Hallazgo
A.13.1.3	Separación en las redes	Cumple	Se evidencia la existencia de la división apropiada de la red corporativa en segmentos y secciones de acuerdo con los requerimientos de seguridad y administración.
A.13.2 Transferencia de información			
A.13.2.1	Políticas y procedimientos de transferencia de información	No cumple	No se evidencia la existencia de un lineamiento específico para la transferencia de información en el marco de las actividades de administración de la Base de Datos del Aseguramiento.
A.13.2.2	Acuerdos sobre transferencia de información	No cumple	No se evidencia la existencia de un lineamiento específico para la transferencia de información entre la Dirección de Aseguramiento y entidades externas.
A.13.2.3	Mensajería electrónica	No cumple	No se evidencia la existencia de lineamiento y mecanismos para garantizar que información con carácter Confidencial sea apropiadamente protegida en una comunicación vía el servicio de correo electrónico.
A.13.2.4	Acuerdos de confidencialidad o de no divulgación	No cumple	No se evidencia la existencia de un lineamiento y un documento de Acuerdo de confidencialidad que garantice la protección de la información manejada en las actividades de administración de la base de Datos del Aseguramiento.
A.14 Adquisición, desarrollo y mantenimientos de sistemas			
A.14.1 Requisitos de seguridad de los sistemas de información			
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	No cumple	No se evidencia un lineamiento que oriente la inclusión de requerimientos de seguridad de la información en el desarrollo de sistemas de información o en los que existen actualmente y apoyan las actividades de administración

Tabla 5. (Continuación)

Dominio/Objetivo de Control/Control		Valoración	Hallazgo
			de la Base de Datos del Aseguramiento
A.14.1.2	Seguridad de servicios de las aplicaciones en redes publicas	No cumple	No se evidencian mecanismos para proteger la información que se transfiere a través de redes públicas al utilizar aplicaciones que apoyan las actividades administración de la Base de Datos del Aseguramiento
A.14.1.3	Protección de transacciones de los servicios de las aplicaciones	No cumple	No se evidencian mecanismos para proteger las operaciones transaccionales que se aplican a la base de datos.
A.14.2 Seguridad en los procesos de desarrollo y soporte			
A.14.2.1	Política de desarrollo seguro	No cumple	No se evidencia un lineamiento que reglamente los procedimientos de seguridad de la información que deben observarse durante el desarrollo de software para consulta y actualización de la Base de Datos del Aseguramiento
A.14.2.2	Procedimientos de control de cambios en sistemas	No cumple	No se evidencia un lineamiento que reglamente el control de cambios durante el desarrollo de software para la base de datos.
A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	No cumple	No se evidencia un lineamiento que direccione el procedimiento después de cambios en la plataforma de operación (Servidor de base de datos y servidor web).
A.14.2.4	Restricciones en los cambios a los paquetes de software	No cumple	No se evidencia un lineamiento para restringir cambios innecesarios en las herramientas software.
A.14.2.5	Principios de construcción de sistemas seguros	No cumple	No se evidencia la existencia de un lineamiento que oriente los principios de construcción de sistemas seguros para el apoyo a la administración y operación de la base de datos.
A.14.2.6	Ambiente de desarrollo seguro	No cumple	No se evidencia la existencia de un lineamiento que direccione el establecimiento de un ambiente seguro de desarrollo.

Tabla 5. (Continuación)

Dominio/Objetivo de Control/Control		Valoración	Hallazgo
A.14.2.7	Desarrollo contratado externamente	No cumple	No se evidencia la existencia de un lineamiento que contenga las actividades supervisión de la seguridad de la información en los casos donde se requiera contratar externamente proyectos desarrollo para apoyar la administración de la base de datos.
A.14.2.8	Pruebas de seguridad de sistemas	No cumple	No se evidencia un lineamiento que reglamente la realización de pruebas de seguridad de la información sobre proyectos de desarrollo de software
A.14.2.9	Prueba de aceptación de sistemas	No cumple	No se evidencia un lineamiento que reglamente la realización de pruebas de aceptación de desarrollos de software en el marco de la seguridad de la información.
A.14.3 Datos de prueba			
A.14.3.1	Protección de datos de prueba	No cumple	No se evidencia un lineamiento para la protección de los datos de prueba empleados en los proyectos de desarrollo de software.
A.15 Relación con los proveedores			
A.15.1 Seguridad de la información en las relaciones con los proveedores			
A.15.1.1	Política de seguridad de la información para las relaciones con proveedores	No Aplica	No intervienen proveedores en las actividades de administración de la Base de Datos del Aseguramiento.
A.15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores	No aplica	Dado que no intervienen proveedores, no se establecen acuerdos.
A.15.1.3	Cadena de suministro de tecnología de información y comunicación	No Aplica	Los servidores son aprovisionados al interior de la Gobernación.
A.15.2 Gestión de la prestación de servicios con los proveedores			
A.15.2.1	Seguimiento y revisión de los servicios de los proveedores	No Aplica	Dado que no intervienen proveedores, no se realizan actividades de seguimiento.
A.15.2.2	Gestión de cambios en los servicios de proveedores	No aplica	Dado que no intervienen proveedores, no se realizan

Tabla 5. (Continuación)

Dominio/Objetivo de Control/Control		Valoración	Hallazgo
			actividades de gestión de cambios.
A.16 Gestión de incidentes de seguridad de la información			
A.16.1 Gestión de incidentes y mejoras en la seguridad de la información			
A.16.1.1	Responsabilidad y procedimientos	No cumple	No se evidencia la existencia de un lineamiento específico que oriente la organización de responsabilidades y procedimiento frente a los incidentes de seguridad que puedan afectar la Base de Datos del Aseguramiento.
A.16.1.2	Reporte de eventos de seguridad de la información	No cumple	No se evidencia un procedimiento para reportar oportunamente posibles eventos de seguridad de la información.
A.16.1.3	Reporte de debilidades de seguridad de la información	No cumple	No se evidencia un procedimiento para reportar oportunamente debilidades de seguridad que puedan ser halladas en las herramientas software que soportan la operación y administración de la base de datos.
A.16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	No cumple	No se evidencia la existencia de un lineamiento para la evaluación y toma de decisiones sobre posibles eventos de seguridad de la información.
A.16.1.5	Respuesta a incidentes de seguridad de la información	No cumple	No se evidencia la existencia de un lineamiento que oriente el procedimiento a seguir en caso de presentarse un evento de seguridad de la información.
A.16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	No cumple	No se evidencia un lineamiento específico que trate sobre la gestión del conocimiento obtenido al enfrentar y dar respuesta a eventos de seguridad de la información.
A.16.1.7	Recolección de evidencia	No cumple	No se evidencia un lineamiento para la identificación, recolección y preservación de la información que puede servir como evidencia

Tabla 5. (Continuación)

Dominio/Objetivo de Control/Control		Valoración	Hallazgo
			en caso de presentarse un evento de seguridad de la información.
A.17 Aspectos de seguridad de la información de la gestión de continuidad de negocio			
A.17.1 Continuidad de seguridad de la información			
A.17.1.1	Planificación de la continuidad de la seguridad de la información	No cumple	No se evidencia un lineamiento que oriente el procedimiento a seguir para garantizar la continuidad de la seguridad de la información en caso de materialización de un evento adverso.
A.17.1.2	Implementación de la continuidad de la seguridad de la información	No cumple	No evidencia la implementación de procedimientos y controles para garantizar la seguridad de la información en situaciones adversas.
A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	No cumple	No se evidencia la existencia de un lineamiento que trate sobre la revisión periódica de los procedimientos y controles de la seguridad de la información. De tal manera que estén actualizados y puedan responder eficazmente ante situaciones adversas
A.17.2 Redundancias			
A.17.2.1	Disponibilidad de instalaciones de procesamiento de información.	No cumple	No se evidencia la existencia de instalaciones e infraestructura adicional de procesamiento de información.
A.18 Cumplimiento			
A.18.1 Cumplimiento de requisitos legales y contractuales			
A.18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	No cumple	Aunque se identifica el marco normativo de la base de datos del Aseguramiento, no se evidencia actualización periódica y articulación con otras normas de protección de datos personales
A.18.1.2	Derechos de propiedad intelectual	No cumple	No se evidencia un lineamiento para verificar el cumplimiento de la normatividad relacionada con la propiedad intelectual o

Tabla 5. (Continuación)

Dominio/Objetivo de Control/Control		Valoración	Hallazgo
			licenciamiento de las herramientas software empleadas en la administración y operación de la Base de Datos del Aseguramiento.
A.18.1.3	Protección de registros	No cumple	No se evidencia la existencia de un lineamiento para la protección de los registros de la base de datos en articulación con el marco normativo aplicable y los requerimientos de la Dirección de Aseguramiento.
A.18.1.4	Privacidad y protección de datos personales	No cumple	No se evidencia un lineamiento específico, que en el marco de la legislación vigente, oriente el tratamiento que debe recibir la información que contiene datos personales.
A.18.1.5	Reglamentación de controles criptográficos	No cumple	No se evidencia un lineamiento específico, que en el marco de la legislación vigente, oriente la aplicación de mecanismos criptográficos a la información Confidencial.
A.18.2 Revisiones de seguridad de la información			
A.18.2.1	Revisión independiente de la seguridad de la información	No cumple	No se evidencia un lineamiento que garantice la revisión independiente de la seguridad de la información para la base de Datos del Aseguramiento.
A.18.2.2	Cumplimiento con las políticas y normas de seguridad	No cumple	No se evidencia un lineamiento para la revisión periódica del nivel de cumplimiento con las normas de seguridad de la información de los procedimientos Base de Datos del Aseguramiento.
A.18.2.3	Revisión del cumplimiento técnico	No cumple	No se evidencia un lineamiento para la revisión periódica del nivel de cumplimiento de las herramientas software que apoyan la administración y operación de la base de datos.

Fuente: Autor

A partir de los resultados obtenidos en la etapa de auditoría, a continuación, se presenta la tabla 6 y respectivo diagrama que consolidan los resultados obtenidos por cada dominio de la norma ISO 27001 – Anexo A.

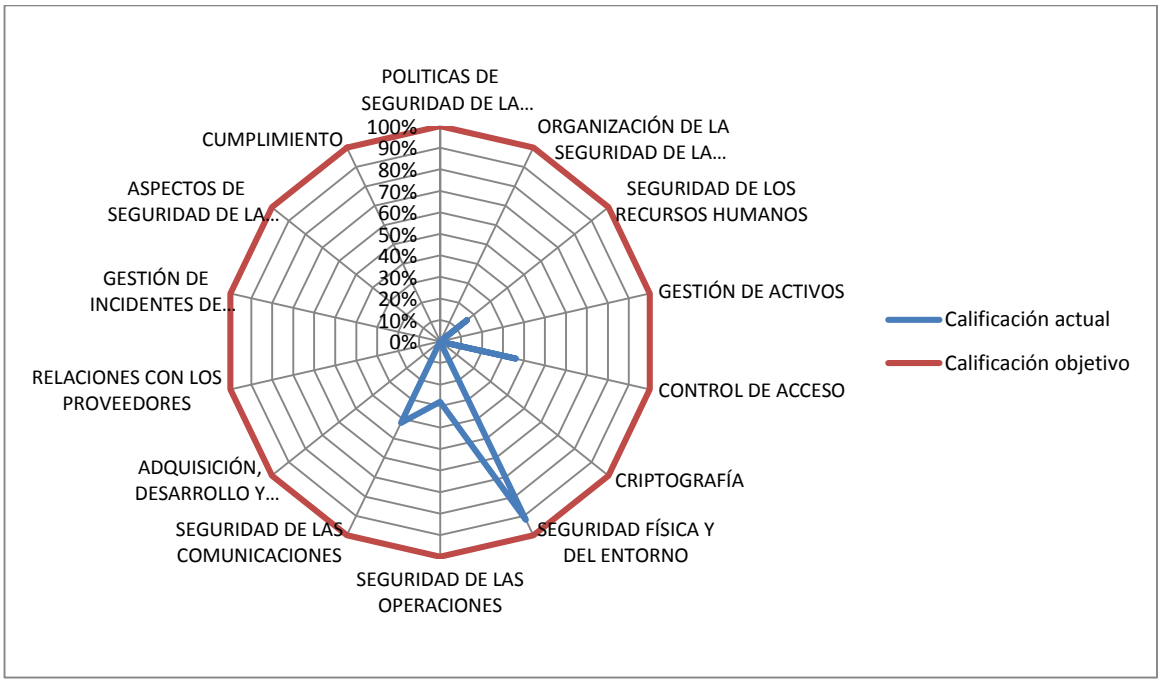
Tabla 6. Nivel de cumplimiento frente a los dominios de la norma ISO 27001.

	DOMINIO	Calificación Actual	Calificación Objetivo
A.5	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	0%	100%
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	0%	100%
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	16%	100%
A.8	GESTIÓN DE ACTIVOS	0%	100%
A.9	CONTROL DE ACCESO	36%	100%
A.10	CRIPTOGRAFÍA	0%	100%
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	92%	100%
A.12	SEGURIDAD DE LAS OPERACIONES	28%	100%
A.13	SEGURIDAD DE LAS COMUNICACIONES	42%	100%
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	0%	100%
A.15	RELACIONES CON LOS PROVEEDORES	No aplica	100%
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	0%	100%
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	0%	100%
A.18	CUMPLIMIENTO	0%	100%
PROMEDIO EVALUACIÓN DE CONTROLES		**16%**	**100%**

Fuente: Autor.

El siguiente diagrama (figura 7) presenta de manera gráfica los resultados obtenidos. Es interesante notar la extensión del área que debe ser mejorada en lo relativo a la seguridad de la información para la administración de la base de Datos del Aseguramiento.

Figura 7. Diagrama de nivel de cumplimiento



Fuente: Autor

Los resultados muestran que actualmente la administración de la Base de Datos del Aseguramiento en el Departamento de Cundinamarca, se ubica en un nivel de cumplimiento estimado en el 16% frente a los controles propuestos por la norma ISO 27001.

5.4 ANÁLISIS DE RIESGOS

En este apartado se desarrollan las actividades que desarrollan el análisis de riesgos para las actividades de administración de la Base de Datos del Aseguramiento en el Departamento de Cundinamarca. Específicamente se desarrollan las actividades fundamentales propuestas por la metodología MAGERIT versión 3.

5.5 IDENTIFICACIÓN DE ACTIVOS

De acuerdo con el Libro II “Catalogo de Elementos” de MAGERIT, podemos identificar los activos dentro de la siguiente clasificación y codificación que aporta la metodología:

[D] Datos.
[K] Claves Criptográficas.
[S] Servicios.
[SW] Software – Aplicaciones informáticas.
[HW] Equipamiento informático (Hardware).
[COM] Redes de Comunicaciones.
[Media] Soportes de Información.
[AUX] Equipamiento Auxiliar.
[L] Instalaciones.
[P] Personal.

Con base en MAGERIT y en el Contexto TI, podemos identificar los siguientes activos involucrados en la administración de la base de datos:

1.- [D] Datos / Información: Constituyen el activo intangible pero esencial de la administración de la Base de Datos del Aseguramiento.

[ARCHIVOS MAESTROS] Archivos maestros con información de aseguramiento

[TABLAS_BD] Tablas e información en la base de datos

[BACKUP] Copia de respaldo de la Base de datos

[DATOS_ACCESO_BD] Datos de acceso de los usuarios configurados en la base de datos

[COD_SQL] Código fuente SQL para consultas y reportes.

2.- [S] Servicios: Se identifican los servicios que se emplean en las actividades de administración de la base de datos y son provistos por la Gobernación de Cundinamarca.

[INTERNET] Servicio de Internet

[DIRECTORIO_ACTIVO] Gestión de identidad de usuario en la red corporativa

3.- [SW] Software – Aplicaciones informáticas. Se identifican las aplicaciones y plataformas software empleadas.

[SGBDR_MySQL] Sistema de Gestión de Base de Datos Relacionales MySQL– Producción

[SERVIDOR_WEB] Servidor web Apache– Producción

[SW_ADMIN_BD] Software para administración de la base de datos-Producción

[SO_PC_TRABAJO] Sistema Operativo del PC de trabajo

[SW_BDWEB_PC_TRABAJO] Plataforma en PC de Trabajo que contiene los entornos de Desarrollo y Preproducción

[SW_OFIMATICA] Suite de Ofimática

4.- [HW] Equipamiento informático (Hardware). Se identifica el equipamiento hardware empleado.

[SERVIDOR FÍSICO] Servidor físico que aloja el Servidor web y de Base de datos

[ALMACENAMIENTO SAN] Almacenamiento tipo SAN

[PC_TRABAJO] Máquina que implementa los ambientes de Pre-producción y Desarrollo

[SWITCH] Equipo Switch de piso

5.- [COM] Redes de comunicaciones. Se identifican los elementos de red empleados.

[LAN] Red LAN

[EQ_INTERNET] Equipamiento para el servicio de Internet.

6.- [P] Personal. Se identifican los funcionarios involucrados en la administración técnica de la base de datos y aquellos que participan en la toma de decisiones frente a asuntos organizacionales relacionados.

[ADMINISTRADOR_ASEG] Administrador de la Base de Datos del Aseguramiento.

[DIRECTOR_ASEG] Director de la Dirección de Aseguramiento en la Gobernación de Cundinamarca.

5.6 VALORACIÓN DE ACTIVOS

En MAGERIT la valoración de los activos se realiza de acuerdo con 5 dimensiones de seguridad asignando un valor que el activo presenta para cada una de ellas. A continuación, se anotan estas dimensiones, su definición y sus respectivos códigos:

1.- [D] Disponibilidad: Propiedad de los activos consistente en su disponibilidad de uso cuando es requerido por parte de los usuarios autorizados para acceder al activo.

2.- [I] Integridad de los datos: Propiedad de los activos que garantiza que los datos no han sido alterados o dañados, sino que están completos y tal cual fueron generados.

3.- [C] Confidencialidad de la Información: Propiedad de los activos de información que garantiza que la información está a disposición solo para los usuarios autorizados.

4.- [A] Autenticidad: Requerimiento que debe observarse rigurosamente a la hora de identificar un usuario o sistema externo que pretende el acceso a los activos. También aplica para el origen verídico de la fuente donde se generó la información.

5.- [T] Trazabilidad: Propiedad que permite garantizar que la responsabilidad sobre el manejo que un usuario da a un activo de información, puede ser asignada exclusivamente a dicho usuario.

MAGERIT también aporta la escala de valores para evaluar los activos en las distintas dimensiones. La tabla 7 consigna los diferentes valores y criterios de valoración que indican la importancia que tiene el activo en la organización mediante el impacto que causaría en caso de que llegue a sufrir la materialización de una amenaza.

Tabla 7. Escala de valores MAGERIT para valorar los activos

VALOR		CRITERIO
10	Extremo **[E]**	Daño extremadamente grave
9	Muy Alto **[MA]**	Daño muy grave
6-8	Alto **[A]**	Daño grave
3-5	Medio **[M]**	Daño importante
1-2	Bajo **[B]**	Daño menor
0	Despreciable **[D]**	Daño despreciable o irrelevante

Fuente: MAGERIT.

A continuación, se presenta la tabla 8 que consolida la valoración de los activos identificados. Se recurre al uso de colores para enfatizar la magnitud del criterio aplicado.

Tabla 8. Valoración de activos.

# Ítem	NOMBRE DEL ACTIVO	DESCRIPCIÓN	DIMENSIONES				
			D	I	C	A	T
DATOS							
1	ARCHIVOS_MAESTROS	Archivos maestros con información de aseguramiento	**MA**	**MA**	**MA**		
2	TABLAS_BD	Tablas e información en la base de datos	**MA**	**MA**	**MA**		

Tabla 8. (Continuación)

# Ítem	NOMBRE DEL ACTIVO	DESCRIPCIÓN	DIMENSIONES				
			D	I	C	A	T
3	BACKUP	Copia de respaldo de la Base de datos	**B**	**B**	**B**		
4	DATOS_ACCESO_BD	Datos de acceso de los usuarios configurados en la base de datos	**MA**	**MA**	**MA**		
5	COD_SQL	Código fuente SQL para consultas y reportes	**M**	**M**	**M**		
SERVICIOS							
6	INTERNET	Servicio de Internet	**A**				
7	DIRECTORIO_ACTIVO	Gestión de identidad de usuario en la red corporativa	**M**	**M**	**M**		
SOFTWARE							
8	SGBD_MYSQL	Sistema de Gestión de Base de Datos Relacionales MySQL – Producción	**MA**	**MA**	**MA**	**A**	**A**
9	SERVIDOR_WEB	Servidor web Apache – Producción	**A**	**A**	**A**		**M**
10	SW_ADMIN_BD	Software para administración de la base de datos – Producción	**A**	**A**	**A**		
11	SO_PC_TRABAJO	Sistema Operativo del PC de trabajo	**M**	**M**	**M**		
12	SW_BDWEB_PC_TRABAJO	Plataforma en PC de Trabajo que contiene los ambientes de Desarrollo y Pre-producción	**M**	**M**	**M**		

Tabla 8. (Continuación)

# Ítem	NOMBRE DEL ACTIVO	DESCRIPCIÓN	DIMENSIONES				
			D	I	C	A	T
13	SW_OFIMATICA	Suite de Ofimática	**M**				
HARDWARE							
14	SERVIDOR_FISICO	Servidor físico que aloja el Servidor web y de Base de datos	**MA**				
15	ALMACENAMIENTO_SAN	Almacenamiento tipo SAN	**A**	**A**			
16	PC_TRABAJO	Software para administración de la base de datos	**M**				
17	SWITCH	Equipo switch de piso	**M**				
REDES DE COMUNICACIONES							
18	LAN	Red LAN	**M**				
19	EQ_INTERNET	Equipamiento para el servicio de Internet	**M**				
PERSONAL							
20	ADMINISTRADOR_ASEG	Administrador del entorno técnico y encargado del procedimiento	**MA**	**A**	**A**		
21	DIRECTOR_ASEG	Director de la Dirección de Aseguramiento en la Gobernación de Cundinamarca			**A**		

Fuente: Autor

5.7 IDENTIFICACIÓN Y VALORACIÓN DE LAS AMENAZAS

MAGERIT define las amenazas como los eventos o cosas que le pueden suceder a los activos y que de ocurrir ocasionan un perjuicio a la organización.

El Libro 2 Catálogo de Elementos de MAGERIT, describe una serie de amenazas que los activos pueden enfrentar en todo tipo de entornos y circunstancias. Al igual que los activos, las amenazas compiladas por MAGERIT constituyen un importante guía de referencia y describen varios posibles incidentes o accidentes de distinta naturaleza que pueden dañar o degradar un activo.

A continuación, se presenta la tabla 9 que consolida la identificación de las amenazas más relevantes que existen sobre los activos identificados en el apartado anterior.

Tabla 9. Identificación de amenazas

# Ítem	ACTIVO	AMENAZA
DATOS		
1	ARCHIVOS_MAESTROS	[E.2] Errores del administrador
		[A.5] Suplantación de la identidad del usuario
2	TABLAS_BD	[E.2] Errores del administrador
		[A.11] Acceso no autorizado
		[A.5] Suplantación de la identidad del usuario
3	BACKUP	[E.2] Errores del administrador
		[A.5] Suplantación de la identidad del usuario
4	DATOS_ACCESO_BD	[A.5] Suplantación de la identidad del usuario
		[A.11] Acceso no autorizado
5	COD_SQL	[E.2] Errores del administrador
		[A.5] Suplantación de la identidad del usuario
SERVICIOS		
6	INTERNET	[I.8] Fallo de servicios de comunicaciones
7	DIRECTORIO ACTIVO	[A.11] Acceso no autorizado

Tabla 9. (Continuación)

# Ítem	ACTIVO	AMENAZA
SOFTWARE		
8	SGBD_MYSQL	[A.11] Acceso no autorizado
		[E.20] Vulnerabilidades de los programas (software)
9	SERVIDOR_WEB	[E.2] Errores del administrador
		[A.11] Acceso no autorizado
		[A.5] Suplantación de la identidad del usuario
10	SW_ADMIN_BD	[E.2] Errores del administrador
		[A.11] Acceso no autorizado
		[A.5] Suplantación de la identidad del usuario
		[E.20] Vulnerabilidades de los programas (software)
11	SO_PC_TRABAJO	[A.5] Suplantación de la identidad del usuario
12	SW_BDWEB_PC_TRABAJO	[E.2] Errores del administrador
		[A.5] Suplantación de la identidad del usuario
13	SW_OFIMATICA	[E.21] Errores de mantenimiento / actualización de programas (software)
HARDWARE		
14	SERVIDOR FÍSICO	[I.5] Avería de origen físico o lógico
15	ALMACENAMIENTO_SAN	[I.5] Avería de origen físico o lógico
		[E.24] Caída del sistema por agotamiento de recursos
16	PC_TRABAJO	[I.5] Avería de origen físico o lógico
17	SWITCH	[I.5] Avería de origen físico o lógico
REDES DE COMUNICACIONES		
18	LAN	[I.5] Avería de origen físico o lógico
19	EQ_INTERNET	[I.5] Avería de origen físico o lógico

Tabla 9. (Continuación)

# Ítem	ACTIVO	AMENAZA
PERSONAL		
20	ADMINISTRADOR_ASEG	[E.15] Alteración accidental de la información
		[E.14] Escapes de información
		[E.7] Deficiencias en la organización
21	DIRECTOR_ASEG	[E.14] Escapes de información
		[A.30] Ingeniería social

Fuente: Autor.

5.7.1 Valoración de Amenazas. MAGERIT propone valorar las amenazas sobre los activos de acuerdo con la probabilidad de ocurrencia (Probabilidad) y el nivel del daño causado (Degradación).

5.7.1.1 Criterios y estimación de la Degradación. MAGERIT propone los criterios presentados en la tabla 10 para valorar la degradación que puede sufrir un activo en caso de materialización de una amenaza.

Tabla 10. Escala de valoración MAGERIT para la Degradación

MA	Muy alto	Casi seguro	Fácil
A	Alto	Muy Alto	Medio
M	Media	Posible	Difícil
B	Baja	Poco Probable	Muy Difícil
MB	Muy Baja	Muy Raro	Extremadamente Difícil

Fuente: MAGERIT.

Criterios y estimación para la Probabilidad: MAGERIT propone los criterios presentados en la tabla 11 para valorar la probabilidad de ocurrencia de una amenaza.

Tabla 11. Escala de valoración MAGERIT para la probabilidad de ocurrencia

MA	100	Muy Frecuente	A diario
A	10	Frecuente	Mensualmente
M	1	Normal	Una vez al año
B	1/10	Poco Frecuente	Cada varios años
MB	1/100	Muy poco frecuente	Siglos

Fuente: MAGERIT.

A continuación, se presenta la tabla 12 que muestra la valoración de las amenazas identificadas sobre los activos.

Tabla 12. Valoración de las amenazas

# Ítem	NOMBRE DEL ACTIVO	AMENAZA	DEGRADACIÓN					PROBABILIDAD
			D	I	C	A	T	
DATOS								
1	ARCHIVOS MAESTROS	[E.2] Errores del administrador	**M**	**M**	**B**			**B**
		[A.5] Suplantación de la identidad del usuario	**A**	**A**	**A**			**B**
2	TABLAS_BD	[E.2] Errores del administrador	**M**	**M**	**M**			**B**

Tabla 12. (Continuación)

# Ítem	NOMBRE DEL ACTIVO	AMENAZA	DEGRADACIÓN					PROBABILIDAD
			D	I	C	A	T	
		[A.11] Acceso no autorizado	MA	MA	MA			B
		[A.5] Suplantación de la identidad del usuario	MA	MA	MA			B
3	BACKUP	[E.2] Errores del administrador	B	B	B			B
		[A.5] Suplantación de la identidad del usuario	M	M	M			B
4	DATOS_ACCESO_BD	[A.5] Suplantación de la identidad del usuario	A	A	A			B
		[A.11] Acceso no autorizado	A	A	A			B
5	COD_SQL	[E.2] Errores del administrador	B	B	B			B
		[A.5] Suplantación de la identidad del usuario	M	M	M			B
SERVICIOS								
6	INTERNET	[I.8] Fallo de servicios de comunicaciones	M					M
7	DIRECTORIO_ACTIVO	[A.11] Acceso no autorizado	A	A	A			B
SOFTWARE								
8	SGBD_MYSQL	[A.11] Acceso no autorizado	MA	MA	MA			B

Tabla 12. (Continuación)

# Ítem	NOMBRE DEL ACTIVO	AMENAZA	DEGRADACIÓN					PROBABILIDAD
			D	I	C	A	T	
		[E.20] Vulnerabilidades de los programas (software)	M	M	M			B
9	SERVIDOR_WEB	[E.2] Errores del administrador	B	B	B			B
		[A.11] Acceso no autorizado	B	B	B			B
		[A.5] Suplantación de la identidad del usuario	B	B	B			B
10	SW_ADMIN_BD	[E.2] Errores del administrador	B	B	B			B
		[A.11] Acceso no autorizado	A	A	A			B
		[A.5] Suplantación de la identidad del usuario	A	A	A			B
		[E.20] Vulnerabilidades de los programas (software)	M	M	M			B
11	SO_PC_TRABAJO	[A.5] Suplantación de la identidad del usuario	M	M	M			B
12	SW_BDWEB_PC_TRABAJO	[E.2] Errores del administrador	B	B	B			B
		[A.5] Suplantación de la identidad del usuario	B	B	B			B
13	SW_OFIMATICA	[E.21] Errores de mantenimiento / actualización de programas (software)	B	B	B			B

Tabla 12. (Continuación)

# Ítem	NOMBRE DEL ACTIVO	AMENAZA	DEGRADACIÓN					PROBABILIDAD
			D	I	C	A	T	
HARDWARE								
14	SERVIDOR_FISICO	[I.5] Avería de origen físico o lógico	**A**					**M**
15	ALMACENAMIENTO_SAN	[I.5] Avería de origen físico o lógico	**A**					**M**
		[E.24] Caída del sistema por agotamiento de recursos	**MA**					
16	PC_TRABAJO	[I.5] Avería de origen físico o lógico	**A**					**B**
17	SWITCH	[I.5] Avería de origen físico o lógico	**M**					**B**
REDES DE COMUNICACIONES								
18	LAN	[I.5] Avería de origen físico o lógico	**M**					**B**
19	EQ_INTERNET	[I.5] Avería de origen físico o lógico	**A**					**B**
PERSONAL								
20	ADMINISTRADOR_ASEG	[E.15] Alteración accidental de la información		**A**				**B**
		[E.14] Escapes de información			**A**			**B**

Tabla 12. (Continuación)

# Ítem	NOMBRE DEL ACTIVO	AMENAZA	DEGRADACIÓN					PROBABILIDAD
			D	I	C	A	T	
		[E.7] Deficiencias en la organización	M					M
21	DIRECTOR_ASEG	[E.14] Escapes de información			A			B
		[A.30] Ingeniería social			B			B

Fuente: Autor.

5.8 VALORACIÓN DEL IMPACTO Y RIESGO POTENCIAL

Para la valoración del Impacto Potencial y el Riesgo Potencial se recurre a la técnica de análisis mediante tablas que MAGERIT propone en el libro 3, Guía de Técnicas.

5.8.1. Impacto Potencial. Medida del daño causado sobre un activo por la materialización de una amenaza. Este valor resulta del cruce entre la Degradación y el valor del Activo para las dimensiones consideradas ([D][I][C][A][T]).

Los criterios para calificar el impacto potencial son los siguientes:

MB: Muy Bajo

B: Bajo

M: Medio

A: Alto

MA: Muy Alto

A continuación, se presenta la tabla 13 que presenta los criterios para la valoración del impacto potencial.

Tabla 13. Matriz de valoración del Impacto Potencial

Impacto Potencial		Degradación				
		MB	B	M	A	MA
Activo	MA	M	M	A	MA	MA
	A	B	M	A	MA	MA
	M	B	B	M	A	A
	B	MB	B	B	M	A
	MB	MB	MB	MB	B	B

Fuente: García & Ruiz, 2017[31].

La tabla 14 presenta la valoración del impacto potencial sobre los activos del procedimiento de administración de la Base de Datos del Aseguramiento.

Tabla 14. Valoración del Impacto Potencial

# Ítem	NOMBRE DEL ACTIVO	AMENAZA	IMPACTO POTENCIAL				
			D	I	C	A	T
DATOS							
1	ARCHIVOS_MAESTROS	[E.2] Errores del administrador	A	A	M		
		[A.5] Suplantación de la identidad del usuario	MA	MA	MA		
2	TABLAS_BD	[E.2] Errores del administrador	A	A	A		
		[A.11] Acceso no autorizado	MA	MA	MA		

[31]GARCÍA HERNÁNDEZ, D., RUIZ MURILLO, J. Análisis y gestión de riesgos en el marco del SGSI, basado en la metodología MAGERIT y apoyado en un api web para su ejecución. Bogotá, Colombia. Universidad Distrital Francisco José de Caldas, Pregrado en Ingeniería Telemática , 2017.

Tabla 14. Continuación

# Ítem	NOMBRE DEL ACTIVO	AMENAZA	IMPACTO POTENCIAL				
			D	I	C	A	T
		[A.5] Suplantación de la identidad del usuario	MA	MA	MA		
3	BACKUP	[E.2] Errores del administrador	B	B	B		
		[A.5] Suplantación de la identidad del usuario	B	B	B		
4	DATOS_ACCESO_BD	[A.5] Suplantación de la identidad del usuario	MA	MA	MA		
		[A.11] Acceso no autorizado	MA	MA	MA		
5	COD_SQL	[E.2] Errores del administrador	B	B	B		
		[A.5] Suplantación de la identidad del usuario	M	M	M		
SERVICIOS							
6	INTERNET	[I.8] Fallo de servicios de comunicaciones	A				
7	DIRECTORIO_ACTIVO	[A.11] Acceso no autorizado	A	A	A		
SOFTWARE							
8	SGBD_MYSQL	[A.11] Acceso no autorizado	MA	MA	MA		
		[E.20] Vulnerabilidades de los programas (software)	A	A	A		
9	SERVIDOR_WEB	[E.2] Errores del administrador	M	M	M		
		[A.11] Acceso no autorizado	M	M	M		
		[A.5] Suplantación de la identidad del usuario	M	M	M		
10	SW_ADMIN_BD	[E.2] Errores del administrador	M	M	M		
		[A.11] Acceso no autorizado	MA	MA	MA		

Tabla 14. Continuación

# Ítem	NOMBRE DEL ACTIVO	AMENAZA	IMPACTO POTENCIAL				
			D	I	C	A	T
		[A.5] Suplantación de la identidad del usuario	MA	MA	MA		
		[E.20] Vulnerabilidades de los programas (software)	A	A	A		
11	SO_PC_TRABAJO	[A.5] Suplantación de la identidad del usuario	M	M	M		
12	SW_BDWEB_PC_TRABAJO	[E.2] Errores del administrador	B	B	B		
		[A.5] Suplantación de la identidad del usuario	B	B	B		
13	SW_OFIMATICA	[E.21] Errores de mantenimiento / actualización de programas (software)	B				
HARDWARE							
14	SERVIDOR_FISICO	[I.5] Avería de origen físico o lógico	MA				
15	ALMACENAMIENTO_SAN	[I.5] Avería de origen físico o lógico	MA				
		[E.24] Caída del sistema por agotamiento de recursos	MA				
16	PC_TRABAJO	[I.5] Avería de origen físico o lógico	A				
17	SWITCH	[I.5] Avería de origen físico o lógico	M				
REDES DE COMUNICACIONES							
18	LAN	[I.5] Avería de origen físico o lógico	M				
19	EQ_INTERNET	[I.5] Avería de origen físico o lógico	M				
PERSONAL							
20	ADMINISTRADOR_ASEG	[E.15] Alteración accidental de la información		MA			

Tabla 14. Continuación

# Ítem	NOMBRE DEL ACTIVO	AMENAZA	IMPACTO POTENCIAL				
			D	I	C	A	T
		[E.14] Escapes de información			MA		
		[E.7] Deficiencias en la organización	A				
21	DIRECTOR_ASEG	[E.14] Escapes de información			MA		
		[A.30] Ingeniería social			M		

Fuente: Autor.

5.8.2 Riesgo Potencial. Medida del daño probable sobre un activo ante la materialización de una amenaza. Este valor resulta del cruce entre la Probabilidad y el valor del Activo para las dimensiones consideradas ([D][I][C][A][T]).

La escala de criterios para calificar el impacto, la probabilidad y el riesgo potencial se muestran en la tabla 15 y tabla 16 respectivamente.

Tabla 15. Criterios para valoración del impacto, probabilidad y riesgo.

escalas		
impacto	probabilidad	riesgo
MA: muy alto	**MA:** prácticamente seguro	**MA:** crítico
A: alto	**A:** probable	**A:** importante
M: medio	**M:** posible	**M:** apreciable
B: bajo	**B:** poco probable	**B:** bajo
MB: muy bajo	**MB:** muy raro	**MB:** despreciable

Fuente: MAGERIT.

Tabla 16. Herramienta para valoración de Riesgo Potencial

riesgo		*probabilidad*				
		MB	B	M	A	MA
impacto	MA	A	MA	MA	MA	MA
	A	M	A	A	MA	MA
	M	B	M	M	A	A
	B	MB	B	B	M	M
	MB	MB	MB	MB	B	B

Fuente: MAGERIT.

A continuación, se presenta la tabla 17 que consolida la valoración del riesgo potencial sobre los activos del procedimiento de Seguimiento a la Base de Datos del Aseguramiento del Departamento de Cundinamarca.

Tabla 17. Valoración del Riesgo Potencial

# Ítem	**NOMBRE DEL ACTIVO**	**AMENAZA**	**RIESGO POTENCIAL**				
			D	**I**	**C**	**A**	**T**
DATOS							
1	ARCHIVOS_MAESTROS	[E.2] Errores del administrador	**MA**	**MA**	**MA**		
		[A.5] Suplantación de la identidad del usuario	**MA**	**MA**	**MA**		
2	TABLAS_BD	[E.2] Errores del administrador	**MA**	**MA**	**MA**		
		[A.11] Acceso no autorizado	**MA**	**MA**	**MA**		
		[A.5] Suplantación de la identidad del usuario	**MA**	**MA**	**MA**		
3	BACKUP	[E.2] Errores del administrador	**B**	**B**	**B**		

Tabla 17. (Continuación)

# Ítem	NOMBRE DEL ACTIVO	AMENAZA	RIESGO POTENCIAL				
			D	I	C	A	T
		[A.5] Suplantación de la identidad del usuario	B	B	B		
4	DATOS_ACCESO_BD	[A.5] Suplantación de la identidad del usuario	MA	MA	MA		
		[A.11] Acceso no autorizado	MA	MA	MA		
5	COD_SQL	[E.2] Errores del administrador	M	M	M		
		[A.5] Suplantación de la identidad del usuario	M	M	M		
SERVICIOS							
6	INTERNET	[I.8] Fallo de servicios de comunicaciones	A				
7	DIRECTORIO_ACTIVO	[A.11] Acceso no autorizado	M	M	M		
SOFTWARE							
8	SGBD_MYSQL	[A.11] Acceso no autorizado	MA	MA	MA		
		[E.20] Vulnerabilidades de los programas (software)	MA	MA	MA		
9	SERVIDOR_WEB	[E.2] Errores del administrador	A	A	A		
		[A.11] Acceso no autorizado	A	A	A		
		[A.5] Suplantación de la identidad del usuario	A	A	A		
10	SW_ADMIN_BD	[E.2] Errores del administrador	A	A	A		

Tabla 17. (Continuación)

# Ítem	NOMBRE DEL ACTIVO	AMENAZA	RIESGO POTENCIAL				
			D	I	C	A	T
		[A.11] Acceso no autorizado	A	A	A		
		[A.5] Suplantación de la identidad del usuario	A	A	A		
		[E.20] Vulnerabilidades de los programas (software)	A	A	A		
11	SO_PC_TRABAJO	[A.5] Suplantación de la identidad del usuario	M	M	M		
12	SW_BDWEB_PC_TRABAJO	[E.2] Errores del administrador	M	M	M		
		[A.5] Suplantación de la identidad del usuario	M	M	M		
13	SW_OFIMATICA	[E.21] Errores de mantenimiento / actualización de programas (software)	M				
HARDWARE							
14	SERVIDOR_FISICO	[I.5] Avería de origen físico o lógico	MA				
15	ALMACENAMIENTO_SAN	[I.5] Avería de origen físico o lógico	A	A			
		[E.24] Caída del sistema por agotamiento de recursos	MA				
16	PC_TRABAJO	[I.5] Avería de origen físico o lógico	M				
17	SWITCH	[I.5] Avería de origen físico o lógico	M				
REDES DE COMUNICACIONES							

Tabla 17. (Continuación)

# Ítem	NOMBRE DEL ACTIVO	AMENAZA	RIESGO POTENCIAL				
			D	I	C	A	T
18	LAN	[I.5] Avería de origen físico o lógico	**M**				
19	EQ_INTERNET	[I.5] Avería de origen físico o lógico	**M**				
PERSONAL							
20	ADMINISTRADOR_ASEG	[E.15] Alteración accidental de la información	**MA**	**A**	**A**		
		[E.14] Escapes de información	**MA**	**A**	**A**		
		[E.7] Deficiencias en la organización	**MA**	**A**	**A**		
21	DIRECTOR_ASEG	[E.14] Escapes de información			**A**		
		[A.30] Ingeniería social			**A**		

Fuente: Autor.

De acuerdo con los resultados obtenidos en esta actividad de análisis de riesgos, podemos identificar que los activos con mayor impacto y riesgo potencial son los siguientes:

- ARCHIVOS_MAESTROS
- TABLAS_BD
- DATOS_ACCESO_BD
- SGBD_MYSQL
- SW_ADMIN_BD
- SERVIDOR FÍSICO
- ALMACENAMIENTO SAN
- ADMINISTRADOR_ASEG
- DIRECTOR_ASEG

5.9 SALVAGUARDAS

Se define una salvaguarda como la medida de protección que mitiga el riesgo de materialización de una amenaza sobre un activo.

A este respecto MAGERIT provee por un lado los conceptos fundamentales sobre las salvaguardas, la clasificación, y los criterios para su selección y aplicación; por otro lado, provee un conjunto de salvaguardas específicas que están en concordancia con la norma ISO 27001.

Las salvaguardas específicas provistas en el Libro 2, Catálogo de Elementos de MAGERIT se clasifican según las siguientes categorías:

- Protecciones generales u horizontales
- Protección de los datos/información
- Protección de las claves criptográficas
- Protección de los servicios
- Protección de las aplicaciones (software)
- Protección de los equipos (hardware)
- Protección de las comunicaciones
- Protección en los puntos de interconexión con otros sistemas
- Protección de los soportes de información
- Protección de los elementos auxiliares
- Seguridad física – Protección de las instalaciones
- Salvaguardas relativas al personal
- Salvaguardas de tipo organizativo
- Continuidad de operaciones
- Internalización
- Adquisición y desarrollo

De acuerdo con el libro 1 de MAGERIT, el nivel de madurez y eficacia de las salvaguardas pueden ser valoradas según los siguientes criterios indicados en la tabla 18.

Tabla 18. Criterios para valoración de cumplimiento de las salvaguardas

factor	nivel	significado
0%	L0	inexistente
	L1	inicial / ad hoc
	L2	reproducible, pero intuitivo
	L3	proceso definido
	L4	gestionado y medible
100%	L5	optimizado

Fuente: MAGERIT

Con base en estos elementos, a continuación, se consigna la tabla 19 que consolida las salvaguardas que aplican para el procedimiento de Seguimiento a la Base de Datos del Aseguramiento y el nivel de cumplimiento actual frente al nivel óptimo.

Tabla 19. Nivel de cumplimiento de las salvaguardas.

Tipo de Salvaguarda	Salvaguardas	Nivel Actual
Preventivas	Protecciones generales u horizontales	L1
Preventivas	Protección de los datos / información	L2
Preventivas	Protección de los servicios	L2
Preventivas	Protección de las aplicaciones (software)	L2
Preventivas	Protección de los equipos (hardware)	L2
Preventivas	Protección de las comunicaciones	L2
Preventivas	Protección de los soportes de información	L1
Preventivas	Salvaguardas relativas al personal	L1

Fuente: Autor

5.10 VALORACIÓN DEL IMPACTO Y RIESGO RESIDUAL

5.10.1 Impacto Residual. El Impacto Residual se define como la medida de la degradación que persiste sobre un activo luego del despliegue de una serie de salvaguardas y el nivel de madurez con que son gestionadas.

Para la valoración del impacto residual se ha empleado los criterios de la tabla 20 que permiten cruzar el Impacto Potencial frente al nivel de eficacia de las salvaguardas identificadas actualmente en las actividades de administración de la Base de Datos del Aseguramiento.

Tabla 20. Criterios para valoración del Impacto Residual

Impacto Residual		Eficacia de la Salvaguarda				
		MA [L5]	A [L3-L4]	M [L3-L2]	B [L1]	MB [L0]
Impacto Potencial	MA	M	M	A	MA	MA
	A	B	M	A	MA	MA
	M	B	B	M	A	A
	B	MB	B	B	M	A
	MB	MB	MB	MB	B	B

Fuente: Autor

La tabla 21 muestra los resultados de la valoración del Impacto Residual se muestran a continuación.

Tabla 21. Valoración del Impacto Residual.

# Ítem	NOMBRE DEL ACTIVO	AMENAZA	IMPACTO RESIDUAL				
			D	I	C	A	T
DATOS							
1	ARCHIVOS MAESTROS	[E.2] Errores del administrador	A	A	M		
		[A.5] Suplantación de la identidad del usuario	A	A	A		
2	TABLAS_BD	[E.2] Errores del administrador	A	A	A		
		[A.11] Acceso no autorizado	A	A	A		

Tabla 21. (Continuación)

# Ítem	NOMBRE DEL ACTIVO	AMENAZA	IMPACTO RESIDUAL				
			D	I	C	A	T
		[A.5] Suplantación de la identidad del usuario	A	A	A		
3	BACKUP	[E.2] Errores del administrador	M	M	M		
		[A.5] Suplantación de la identidad del usuario	M	M	M		
4	DATOS_ACCESO_BD	[A.5] Suplantación de la identidad del usuario	A	A	A		
		[A.11] Acceso no autorizado	A	A	A		
5	COD_SQL	[E.2] Errores del administrador	M	M	M		
		[A.5] Suplantación de la identidad del usuario	M	M	M		
SERVICIOS							
6	INTERNET	[I.8] Fallo de servicios de comunicaciones	A				
7	DIRECTORIO_ACTIVO	[A.11] Acceso no autorizado	A	A	A		
SOFTWARE							
8	SGBD_MYSQL	[A.11] Acceso no autorizado	A	A	A		
		[E.20] Vulnerabilidades de los programas (software)	A	A	A		
9	SERVIDOR_WEB	[E.2] Errores del administrador	M	M	M		
		[A.11] Acceso no autorizado	M	M	M		
		[A.5] Suplantación de la identidad del usuario	M	M	M		

Tabla 21. (Continuación)

# Ítem	NOMBRE DEL ACTIVO	AMENAZA	IMPACTO RESIDUAL				
			D	I	C	A	T
10	SW_ADMIN_BD	[E.2] Errores del administrador	M	M	M		
		[A.11] Acceso no autorizado	A	A	A		
		[A.5] Suplantación de la identidad del usuario	A	A	A		
		[E.20] Vulnerabilidades de los programas (software)	A	A	A		
11	SO_PC_TRABAJO	[A.5] Suplantación de la identidad del usuario	M	M	M		
12	SW_BDWEB_PC_TRABAJO	[E.2] Errores del administrador	M	M	M		
		[A.5] Suplantación de la identidad del usuario	M	M	M		
13	SW_OFIMATICA	[E.21] Errores de mantenimiento / actualización de programas (software)	M				
HARDWARE							
14	SERVIDOR_FISICO	[I.5] Avería de origen físico o lógico	A				
15	ALMACENAMIENTO_SAN	[I.5] Avería de origen físico o lógico	A				
		[E.24] Caída del sistema por agotamiento de recursos	A				
16	PC_TRABAJO	[I.5] Avería de origen físico o lógico	A				
17	SWITCH	[I.5] Avería de origen físico o lógico	M				

Tabla 21. (Continuación)

# Ítem	NOMBRE DEL ACTIVO	AMENAZA	IMPACTO RESIDUAL				
			D	I	C	A	T
REDES DE COMUNICACIONES							
18	LAN	[I.5] Avería de origen físico o lógico	**M**				
19	EQ_INTERNET	[I.5] Avería de origen físico o lógico	**M**				
PERSONAL							
20	ADMINISTRADOR_ASEG	[E.15] Alteración accidental de la información		**A**			
		[E.14] Escapes de información			**A**		
		[E.7] Deficiencias en la organización	**A**				
21	DIRECTOR_ASEG	[E.14] Escapes de información			**A**		
		[A.30] Ingeniería social			**M**		

Fuente: Autor.

5.10.2 Riesgo Residual: El Riesgo Residual se define como la medida de la probabilidad de ocurrencia de una amenaza que persiste sobre un activo luego del despliegue de una serie de salvaguardas y el nivel de madurez con que son gestionadas. Se habla entonces de una Probabilidad Residual que de acuerdo con MAGERIT tiene la siguiente equivalencia:

Probabilidad residual = Efectividad Perfecta – Efectividad Real.

Así pues, considerando los anteriores conceptos, para la valoración del impacto residual se ha empleado la siguiente tabla que permite cruzar el Riesgo Potencial frente a la Probabilidad residual de ocurrencia de las amenazas.

Tabla 22. Criterios para valoración del Riesgo Residual

Riesgo Residual		Probabilidad Residual				
		MB [L5]	B [L4-L3]	M [L3-L2]	A [L1]	MA [L0]
Riesgo Potencial	MA	M	M	A	MA	MA
	A	B	M	A	MA	MA
	M	B	B	M	A	A
	B	MB	B	B	M	A
	MB	MB	MB	MB	B	B

Fuente: Autor

Los resultados de la valoración del Riesgo Residual se muestran en la tabla 23 que se consigna a continuación:

Tabla 23. Valoración del Riesgo Residual

# Ítem	NOMBRE DEL ACTIVO	AMENAZA	RIESGO RESIDUAL				
			D	I	C	A	T
DATOS							
1	ARCHIVOS_MAESTROS	[E.2] Errores del administrador	**A**	**A**	**A**		
		[A.5] Suplantación de la identidad del usuario	**A**	**A**	**A**		
2	TABLAS_BD	[E.2] Errores del administrador	**A**	**A**	**A**		
		[A.11] Acceso no autorizado	**A**	**A**	**A**		
		[A.5] Suplantación de la identidad del usuario	**A**	**A**	**A**		

Tabla 23. (Continuación)

# Ítem	NOMBRE DEL ACTIVO	AMENAZA	RIESGO RESIDUAL				
			D	I	C	A	T
3	BACKUP	[E.2] Errores del administrador	**B**	**B**	**B**		
		[A.5] Suplantación de la identidad del usuario	**B**	**B**	**B**		
4	DATOS_ACCESO_BD	[A.5] Suplantación de la identidad del usuario	**A**	**A**	**A**		
		[A.11] Acceso no autorizado	**A**	**A**	**A**		
5	COD_SQL	[E.2] Errores del administrador	**M**	**M**	**M**		
		[A.5] Suplantación de la identidad del usuario	**M**	**M**	**M**		
SERVICIOS							
6	INTERNET	[I.8] Fallo de servicios de comunicaciones	**A**				
7	DIRECTORIO_ACTIVO	[A.11] Acceso no autorizado	**M**	**M**	**M**		
SOFTWARE							
8	SGBD_MYSQL	[A.11] Acceso no autorizado	**A**	**A**	**A**		
		[E.20] Vulnerabilidades de los programas (software)	**A**	**A**	**A**		
9	SERVIDOR_WEB	[E.2] Errores del administrador	**A**	**A**	**A**		
		[A.11] Acceso no autorizado	**A**	**A**	**A**		

Tabla 23. (Continuación)

# Ítem	NOMBRE DEL ACTIVO	AMENAZA	RIESGO RESIDUAL				
			D	I	C	A	T
		[A.5] Suplantación de la identidad del usuario	A	A	A		
10	SW_ADMIN_BD	[E.2] Errores del administrador	A	A	A		
		[A.11] Acceso no autorizado	A	A	A		
		[A.5] Suplantación de la identidad del usuario	A	A	A		
		[E.20] Vulnerabilidades de los programas (software)	A	A	A		
11	SO_PC_TRABAJO	[A.5] Suplantación de la identidad del usuario	M	M	M		
12	SW_BDWEB_PC_TRABAJO	[E.2] Errores del administrador	M	M	M		
		[A.5] Suplantación de la identidad del usuario	M	M	M		
13	SW_OFIMATICA	[E.21] Errores de mantenimiento / actualización de programas (software)	M				
HARDWARE							
14	SERVIDOR_FISICO	[I.5] Avería de origen físico o lógico	A				
15	ALMACENAMIENTO_SAN	[I.5] Avería de origen físico o lógico	A	A			
		[E.24] Caída del sistema por	A				

Tabla 23. (Continuación)

# Ítem	NOMBRE DEL ACTIVO	AMENAZA	RIESGO RESIDUAL				
			D	I	C	A	T
		agotamiento de recursos					
16	PC_TRABAJO	[I.5] Avería de origen físico o lógico	**M**				
17	SWITCH	[I.5] Avería de origen físico o lógico	**M**				
REDES DE COMUNICACIONES							
18	LAN	[I.5] Avería de origen físico o lógico	**M**				
19	EQ_INTERNET	[I.5] Avería de origen físico o lógico	**M**				
PERSONAL							
20	ADMINISTRADOR_ASEG	[E.15] Alteración accidental de la información	**A**	**A**	**A**		
		[E.14] Escapes de información	**A**	**A**	**A**		
		[E.7] Deficiencias en la organización	**A**	**A**	**A**		
21	DIRECTOR_ASEG	[E.14] Escapes de información			**A**		
		[A.30] Ingeniería social			**A**		

Fuente: Autor.

5.11 ANÁLISIS DE RIESGOS

MAGERIT permitió identificar metódicamente los activos de información presentes en el procedimiento. Así como también las amenazas, el Impacto Potencial y el Riesgo Potencial que los afecta. A partir de las salvaguardas implementadas actualmente y el nivel de madurez que presentan, se pudo identificar el Impacto Residual y el Riesgo Residual sobre los activos de información.

A continuación, se presenta la tabla 24 que consolida el número de activos identificados en cada nivel de Riesgo Residual.

Tabla 24. Resultado Riesgo Residual por activos

Nivel de Riesgo Residual	Número de Activos
Muy Alto	0
Alto	11
Medio	9
Bajo	1
Muy Bajo	0
Total	**21**

Fuente: Autor

Por otro lado, se identificó que los activos de información con Riesgo Residual Alto y por consiguiente donde deben enfocarse los proyectos de tratamiento del riesgo, son los que se presentan en la tabla 25.

Tabla 25. Activos críticos.

DATOS
ARCHIVOS_MAESTROS
TABLAS_BD
DATOS_ACCESO_BD
SERVICIOS
INTERNET
SOFTWARE
SGBD_MYSQL
SERVIDOR_WEB
SW_ADMIN_BD
HARDWARE
SERVIDOR_FISICO
ALMACENAMIENTO_SAN
PERSONAL
ADMINISTRADOR_ASEG
DIRECTOR_ASEG

Fuente: Autor

6. INFORME DE RESULTADOS DEL ANÁLISIS DE SEGURIDAD DE LA BASE DE DATOS DEL ASEGURAMIENTO

A continuación, se listan los activos críticos identificados en la etapa de análisis de riesgos:

- ARCHIVOS_MAESTROS
- TABLAS_BD
- DATOS_ACCESO_BD
- INTERNET
- SGBD_MYSQL
- SERVIDOR WEB
- SW_ADMIN_BD
- SERVIDOR_FISICO
- ALMACENAMIENTO_SAN
- ADMINISTRADOR_ASEG
- DIRECTOR_ASEG

En este orden de ideas, de acuerdo con la Declaración de Aplicabilidad, los dominios de la norma ISO 27001 – Anexo A sobre los cuales deben enfocarse los lineamientos para la protección de estos activos críticos son los siguientes:

- SEGURIDAD DE LOS RECURSOS HUMANOS
- CONTROL DE ACCESO
- CRIPTOGRAFÍA
- SEGURIDAD DE LAS OPERACIONES

A continuación, se presenta un informe de resultados producto de haber realizado una revisión de seguridad basada en la norma ISO 27001 y la metodología MAGERIT a la Base de Datos del Aseguramiento:

1.- Se evidencia debilidad en los procesos de contratación de la institución; no se realiza un estudio de seguridad al personal que va a ingresar.

- Recomendación: Realizar estudio de seguridad previo al ingreso de personal.

2.- Tras la revisión de los contratos de personal especializado no se evidencia que existen acuerdos de cumplimiento de lineamientos de seguridad de la información de la institución.

- Recomendación: Incluir en el proceso de contratación acuerdos de cumplimiento de los lineamientos de seguridad de la información.

3.- No se evidencian mecanismos que impidan el acceso a la base de datos del aseguramiento por parte de funcionarios o contratistas que han terminado sus funciones o contrato con la institución.

- Recomendación: Establecer los lineamientos para garantizar que los funcionarios o contratistas no cuenten con los privilegios de acceso a la base de datos una vez se retiren de la institución.

4.- No se evidencia la existencia de procedimientos de seguridad de la información para la creación y gestión de los perfiles y permisos de usuarios con acceso a la Base de Datos del Aseguramiento.

- Recomendación: Establecer un lineamiento para la creación y gestión de usuarios con distintos niveles de permisos sobre la base de datos.

5.- No se evidencia la existencia de procedimientos de seguridad de la información para la creación y gestión de usuarios con acceso a las herramientas de administración de la Base de Datos del Aseguramiento.

- Recomendación: Establecer un lineamiento para la creación y gestión de usuarios con acceso a las herramientas de administración de la base de datos.

6.-No se evidencia la existencia de controles criptográficos para la información confidencial.

- Recomendación: Establecer un lineamiento y procedimientos para la aplicación de controles criptográficos a la información clasificada como confidencial.

7.- No se evidencia la existencia de procedimientos para evitar la introducción y ejecución de software malicioso en los recursos técnicos empleados en la administración de la Base de Datos del Aseguramiento.

- Recomendación: Definir un lineamiento para la protección de los activos de información contra software malicioso.

8.- No se evidencia la existencia de procedimientos de seguridad de la información para el monitoreo de los recursos software y hardware que soportan la operación de la Base de Datos del Aseguramiento.

- Recomendación: Establecer un lineamiento y procedimientos para realizar seguimiento a los recursos técnicos que soportan la base de datos del Aseguramiento.

9.- No se evidencian procedimientos de seguridad de la información para la ejecución de backups de la información de la Base de Datos del Aseguramiento.

- Recomendación: Establecer un lineamiento que defina la periodicidad y la información que debe tener copias de seguridad.

10.- No se evidencian procedimientos de seguridad de la información para la identificación de vulnerabilidades en los recursos técnicos que soportan la operación de la Base de Datos del Aseguramiento.

- Recomendación: Establecer un lineamiento que defina la ejecución de pruebas técnicas para la identificación de vulnerabilidades técnicas.

6.1 RECOMENDACIONES GENERALES

A partir de los resultados obtenidos en las distintas etapas de este trabajo, a continuación, se realizan las siguientes recomendaciones generales:

- Dado que los resultados obtenidos en este trabajo muestran un nivel de cumplimiento inicial frente a los controles de la norma ISO 27001, es necesario la formulación de una hoja de ruta o plan de acción para la puesta en marcha inmediata de los lineamientos de seguridad formulados para la Base de Datos del Aseguramiento y su articulación con el Sistema Integral de Gestión y Control de la institución.

Por otro lado, es necesario que los lineamientos se extiendan a los controles y activos de información con menor criticidad, pero igualmente importantes en aras de garantizar la seguridad integral para la Base de Datos del Aseguramiento.

- Es recomendable la planeación y ejecución de una actividad de socialización al interior de la Dirección de Aseguramiento en la que sean presentados los resultados obtenidos en este trabajo con el propósito de concientizar sobre la necesidad de abordar los lineamientos propuestos para proteger la información de la Base de Datos del Aseguramiento.

- Atendiendo al resultado sobre identificación de los activos más críticos en el marco de las actividades de administración de la Base de Datos del Aseguramiento, es altamente recomendable migrar la base de datos de producción a un servidor dedicado. En este sentido también es altamente recomendable la asignación como mínimo de un (1) terabyte del almacenamiento SAN corporativo exclusivo para

atender las necesidades de espacio que requiere el crecimiento actual de la base de datos y futuros requerimientos.

- Es recomendable la ejecución periódica de la auditoría sobre los ambientes de Producción, Pre-producción y Desarrollo. Adicionalmente se hace necesario la creación de un plan de acción para la corrección efectiva de las vulnerabilidades técnicas que sean encontradas en los servidores y herramientas de administración que soportan la operación de la Base de Datos del Aseguramiento.

- Es recomendable considerar la extensión de los lineamientos de seguridad a fuentes de información provenientes de otros procesos de la Dirección de Aseguramiento interrelacionados y que en un futuro podrían requerir almacenar información en la base de datos del aseguramiento.

Lo anterior con miras a garantizar la seguridad de la información para la base de datos en un marco organizacional más amplio.

7. LINEAMIENTOS DE SEGURIDAD DE LA INFORMACIÓN

En este apartado se proponen los lineamientos de seguridad para gestionar y mitigar los riesgos identificados sobre la Base de Datos del Aseguramiento del Departamento de Cundinamarca.

7.1 LINEAMIENTOS PROPUESTOS PARA LA BASE DE DATOS DEL ASEGURAMIENTO

A continuación, se propone un conjunto de lineamientos de seguridad para la Base de Datos del Aseguramiento con base en la articulación de resultados que permitieron identificar los activos críticos y su estrecha relación con los dominios de la norma ISO 27001:

7.1.1 Lineamientos de seguridad de los recursos humanos

7.1.1.1 Antes de asumir el empleo.

Objetivo: Definir la inclusión de los Lineamientos de Seguridad de la Información y el Acuerdo de Confidencialidad en las cláusulas del contrato o funciones del cargo (cualquiera sea el tipo de vinculación laboral) para la administración de la Base de Datos del Aseguramiento.

Alcance: Este lineamiento aplica sobre el proceso de contratación (contratista) o las funciones (personal de planta) del funcionario que asumirá las actividades de administración de la Base de Datos del Aseguramiento.

Es importante anotar que el Acuerdo de Confidencialidad no pierde validez al dejar el cargo o terminación de contrato.

Responsables: Director y el área de contratación de la Dirección de Aseguramiento.

Directrices:

- El Director da instrucciones al área de contratación para que realice un estudio de seguridad sobre los aspirantes al cargo. Este estudio incluye mínimo los siguientes requisitos: Revisión de los antecedentes judiciales, revisión de la historia laboral y referencias, verificación de estudios y experiencia.

- El Director socializa e imparte instrucciones al área de contratación para la inclusión de los Lineamientos de Seguridad de la Información y el Acuerdo de Confidencialidad.
- El área de contratación de la Dirección de Aseguramiento debe incluir el respectivo compromiso o cláusula de cumplimiento relacionada con los Lineamientos de Seguridad de la Información y el Acuerdo de Confidencialidad (ver Anexo 3).

7.1.1.2 Durante la ejecución del empleo.

Objetivo: Establecer las acciones de seguimiento frente al cumplimiento de los Lineamientos de Seguridad de la Información y el Acuerdo de Confidencialidad para las actividades de administración de la Base de Datos del Aseguramiento.

Alcance: Este lineamiento aplica sobre el ejercicio de las funciones o proceso contractual durante el cual se ejercen las actividades de administración de la Base de Datos del Aseguramiento.

Responsables*:* Director, Supervisor y el Administrador de la base de datos.

Directrices*:*

- En el caso de un funcionario de planta que asume la administración de la Base de Datos del Aseguramiento, el Director socializa e imparte instrucciones para el cumplimiento de los Lineamientos de Seguridad de la Información y el Acuerdo de Confidencialidad.

- En el caso de un contratista que asume la administración de la Base de Datos del Aseguramiento, para el inicio formal del contrato el Supervisor debe socializar los Lineamientos de Seguridad de la Información y el Acuerdo de Confidencialidad, e incluir este compromiso específico en el Acta de Inicio. Posteriormente solicita al área de informática de la Gobernación de Cundinamarca (Secretaría de TIC) la configuración del acceso a la base de datos y a las herramientas de administración.

- Durante las actividades periódicas de seguimiento al contrato, el supervisor además del avance en el cumplimento global del contrato, verifica el cumplimiento de las clausulas específicas relacionadas con el Acuerdo de Confidencialidad y Lineamientos de Seguridad de la Información.

7.1.1.3 Terminación y cambio de empleo

Objetivo: Garantizar que los recursos técnicos y activos de información empleados en las actividades de administración de la Base de Datos del Aseguramiento sean

adecuadamente protegidos de acceso no autorizado por parte del funcionario que ha dejado el cargo o terminado el contrato.

Alcance: Este lineamiento aplica sobre la información y las herramientas software que soportan la operación de la Base de Datos del Aseguramiento.

Responsables: Director, Supervisor y el Administrador de la base de datos.

Directrices*:*

- El supervisor dentro del cumplimiento global del contrato, debe verificar el cumplimiento de las clausulas específicas relacionadas con el Acuerdo de Confidencialidad y los Lineamientos de Seguridad de la Información.

- El supervisor debe incluir en el acta de cierre del contrato la observación sobre el hecho de que el Acuerdo de Confidencialidad no pierde vigencia con el evento de cese contractual.

- El Supervisor debe solicitar al área de informática de la Gobernación (Secretaría de TIC) la desactivación de los datos de acceso a la base de datos y a las herramientas software de administración para el contratista que termina su contrato.

- En el caso de un funcionario de planta que termina sus funciones de administración de la Base de Datos del Aseguramiento, el Director debe verificar el cumplimiento del Acuerdo de confidencialidad y el compromiso de mantener este acuerdo. Adicionalmente debe solicitar al área de informática de la Gobernación (Secretaría de TIC) la desactivación de los datos de acceso a la base de datos y a las herramientas software de administración para el funcionario que termina su cargo.

7.1.2 Lineamientos de control de acceso

7.1.2.1 Responsabilidades de acceso de los usuarios

Objetivo*:* Establecer los mecanismos necesarios para que los funcionarios con acceso a las herramientas que soportan la operación de la Base de Datos del Aseguramiento, asuman la responsabilidad sobre el correcto uso de los datos de acceso (usuario y contraseña) asignados.
Alcance*:* Este lineamiento aplica para los datos de acceso (usuario, contraseña, direcciones IP, URL, etc.) asignados al funcionario de planta o contratista que asume la administración de la Base de Datos del Aseguramiento.

Responsables*:* Administrador y usuarios de consulta a quienes se ha asignado datos de acceso a las herramientas que soportan la operación de la Base de Datos del Aseguramiento.

Directrices*:*

- El administrador de la base de datos y los usuarios de consulta deben manejar con estricta confidencialidad los datos de acceso asignados.

- El administrador de la base de datos y los usuarios de consulta no deben compartir con terceras partes los datos de acceso asignados. Estos datos son intransferibles.

- El Director y Supervisor deben promover la importancia de manejar con estricta confidencialidad los datos de acceso.

7.1.2.2 Gestión de acceso a herramientas de administración

Objetivo*:* Establecer los mecanismos necesarios para la creación y asignación de perfiles de usuarios con los respectivos permisos sobre la Base de Datos del Aseguramiento y herramientas de administración.

Alcance*:* Este lineamiento aplica para la configuración de privilegios de administración en el Servidor de base de datos y herramientas de administración en los ambientes de Producción, Pre-producción y Desarrollo.

Responsables: Administrador de la Base de Datos del Aseguramiento.

Directrices*:*

- El administrador de la Base de Datos del Aseguramiento debe definir la política de control y asignación de acceso a la base de datos y las herramientas de administración según los siguientes criterios:

- Debe existir un solo usuario administrador.

- Podrán existir usuarios adicionales de solo consulta.

- Para la creación de un usuario de consulta, debe mediar una solicitud formal, deben ser registrados todos los datos de la persona responsable a quien ha sido asignado y estos datos deben ser entregados formalmente.

- La contraseña del usuario administrador y los usuarios de consulta debe ser creada con al menos 8 caracteres alfanuméricos, almacenada y transferida de manera encriptada, y actualizada periódicamente.

- El administrador de la Base de Datos del Aseguramiento debe gestionar periódicamente los usuarios y perfiles creados con el fin de eliminarlos, actualizarlos o limitar los privilegios (ver Anexo C).

- El administrador de la Base de Datos del Aseguramiento (Dirección de Aseguramiento) debe enviar solicitud formal al administrador del servidor de MySQL (Secretaría de TIC) con los perfiles y permisos requeridos para la administración de la Base de Datos del Aseguramiento que corre en el ambiente de Producción. Entre estos perfiles se encuentra el de administrador (en un momento dado solo podrá existir un único usuario administrador) y los usuarios con algunos permisos de actualización y/o consulta según se requiera.

- En la citada solicitud, el administrador también debe indicar el tipo de acceso remoto para los usuarios autorizados y posibles aplicaciones que requieran conexión con la base de datos.

- En caso de requerimientos provenientes de proyectos de desarrollo de software que requieran conexión con la base de datos, el administrador de la base de datos (Dirección de Aseguramiento) debe tomar las medidas de seguridad pertinentes para atender este requerimiento de interoperabilidad.

- El administrador de la base de datos, debe configurar los perfiles y permisos requeridos para la administración de la respectiva versión de la Base de Aseguramiento que corre en los ambientes de Pre-producción y Desarrollo.

- El administrador debe consignar en la Bitácora de Seguimiento las actividades relacionadas con este lineamiento.

7.1.2.3 Control de acceso a sistemas y aplicaciones

Objetivo*:* Establecer los mecanismos necesarios para controlar el acceso a la Base de Datos del Aseguramiento y las herramientas de administración.

Alcance*:* Este lineamiento aplica a las actividades de seguimiento y gestión que el administrador debe realizar sobre el acceso que ha sido autorizado a los usuarios con diferentes privilegios sobre la Base de Datos del Aseguramiento y herramientas de administración en los ambientes de Producción, Pre-producción y Desarrollo.

Responsables: Administrador de la Base de Datos del Aseguramiento

Directrices*:*

- El administrador de la Base de Datos del Aseguramiento debe gestionar los mecanismos y procedimientos para garantizar el acceso seguro a las herramientas de administración. Esto incluye principalmente el estricto control de puertos y servicios, encriptación de la comunicación, gestión del mecanismo de autenticación y sesión de usuario.

- El administrador debe controlar el acceso al código fuente de las herramientas de administración, al código SQL de consultas a la base de datos, a los diagramas detallados del modelo de datos y vista de despliegue.

- El administrador de la Base de Datos del Aseguramiento debe monitorear periódicamente el historial y logs de acceso a los ambientes de Producción, Pre-producción y Desarrollo.

- El administrador debe consignar en la Bitácora de Seguimiento las actividades relacionadas con este lineamiento.

7.1.3 Lineamiento de criptografía

7.1.3.1 Controles criptográficos

Objetivo*:* Aplicar técnicas criptográficas a la información clasificada como Confidencial de tal modo que pueda ser almacenada y transferida de manera segura.

Alcance*:* Este lineamiento aplica para la información con carácter Confidencial que se maneja en las actividades de administración de la Base de Datos del Aseguramiento.

Responsables: La aplicación de este lineamiento corresponde al administrador de la base de datos.

Directrices*:*

– El administrador de la base de datos aplicará las técnicas de cifrado requeridas sobre la información clasificada como Confidencial, de tal modo que se garanticen los principios de confidencialidad e integridad a la hora de almacenarla, o transferirla a otras aplicaciones o partes autorizadas. La información con carácter confidencial es la siguiente:

- Contraseña de acceso de los usuarios
- Copias de seguridad de los maestros y de la base de datos
- Estructura de la base de datos
- Diagramas del modelo de datos y vista de despliegue
- Código fuente de aplicaciones y de consultas SQL

– El administrador debe consignar en la Bitácora de Seguimiento las actividades relacionadas con este lineamiento.

7.1.4 Lineamientos de seguridad de las operaciones

7.1.4.1. Protección contra códigos maliciosos

Objetivo*:* Garantizar que la Base de Datos del Aseguramiento y las herramientas de administración cuenten con las debidas protecciones contra códigos maliciosos.

Alcance*:* Este lineamiento aplica sobre los siguientes activos:

- Sistemas operativos de las máquinas que soportan los ambientes de Producción, Pre-producción y Desarrollo.

- Sistema de gestión de base de datos MySQL en los ambientes de Producción, Pre-producción y Desarrollo.

- Herramientas de administración de la base de datos.

- Herramientas de ofimática que apoyan las actividades de administración de la base de datos.

Responsables*:* Administrador de la Base de Datos del Aseguramiento.

Directrices:

- El administrador de la base de datos debe solicitar y coordinar con el área de informática (Secretaría de TIC) de la Gobernación de Cundinamarca la instalación, gestión y actualización del sistema de antivirus corporativo para los servidores de los ambientes de Producción, Desarrollo y Pre-producción.

- El administrador de la base de datos debe coordinar con el área de informática de la Gobernación, las reglas que deben aplicarse y gestionarse sobre el firewall corporativo tendientes a la protección de la Base de Datos del Aseguramiento.

- El administrador de la base de datos debe verificar que los archivos adjuntos y enlaces externos asociados al correo electrónico, provienen de fuentes seguras.

- El administrador de la base de datos debe verificar que los archivos maestros provienen directamente de las fuentes oficiales.

- El administrador de la base de datos debe verificar periódicamente que las herramientas de administración están debidamente protegidas contra la ejecución remota de códigos maliciosos.

- El administrador debe consignar en la Bitácora de Seguimiento las actividades relacionadas con este lineamiento.

7.1.4.2 Copias de respaldo de la información

Objetivo: Establecer las actividades requeridas para el respaldo de la información almacenada en la Base de Datos del Aseguramiento, los archivos maestros, los reportes generados, la documentación y demás información relacionada.

Alcance: Este lineamiento aplica para los siguientes activos:

- La estructura de las tablas y datos que componen la base de datos.

- Los archivos maestros del Régimen Subsidiado y Contributivo, Sisben, Población Pobre No Afiliada.

- Reportes e informes generados a partir de las distintas consultas a la base de datos.

- Documentación técnica y procedimental.

- Código fuente de funcionalidades específicas para administración de la base de datos.

- Código fuente SQL empleado en las consultas a la base de datos.

- Demás información relacionada con las actividades de administración de la base de datos.

Responsables: Administrador de la Base de Datos del Aseguramiento.

Directrices:

- El administrador de la base de datos debe consolidar con periodicidad mensual la información que será respaldada.

- El administrador debe cargar la información que será respaldada al respectivo servidor de backups de la gobernación.

- El administrador realiza con una periodicidad trimestral, pruebas de integridad y funcionalidad de las copias de la base de datos y de las funcionalidades de administración que han sido respaldadas.

- El administrador debe consignar en la Bitácora de Seguimiento las actividades relacionadas con este lineamiento.

7.1.4.3 Registro y seguimiento de los recursos tecnológicos y los sistemas de información

Objetivo*:* Permitir el registro y seguimiento de los eventos y actividades realizadas en el marco de administración de la Base de Datos del Aseguramiento.

Alcance: Este lineamiento aplica para:

- La información de actividades ejecutadas sobre la base de datos que deben consignarse en la herramienta Bitácora de Seguimiento: Cargue de archivos maestros, actualización de tablas secundarias o auxiliares, generación de reportes, actividad de respaldo de información, revisión de logs, mejoras y cambios sobre el modelo de datos, actualización de la estructura y configuración de las tablas, gestión de usuarios.

- Actualización, corrección de errores, optimización y desarrollo de código fuente de consultas y funcionalidades de administración.

- La información registrada en los logs de los servidores de los ambientes de Producción, Pre-producción y Desarrollo.

Responsables: Administrador de la Base de Datos del Aseguramiento.

Directrices:

- El administrador de la base de datos debe registrar en la Bitácora de Seguimiento las actividades de administración que realiza sobre la Base de Datos del Aseguramiento (ver Anexo A).

- La Bitácora de Seguimiento debe ser accesible y debe facilitar la generación de reportes que muestren el comportamiento de los principales incidentes, fallos, actividades de mantenimiento, actividades de gestión.

- El administrador de la base de datos debe revisar periódicamente los logs de los servidores de los ambientes de Producción, Pre-producción y Desarrollo.

- El administrador de la Base de Datos del Aseguramiento debe coordinar con el área de informática de la gobernación (Secretaría de TIC) las acciones de mejora a realizar ante eventos registrados en el ambiente de Producción y que pueden afectar la seguridad de la información en la Base de Datos del Aseguramiento.

- El administrador de la base de datos debe realizar seguimiento a los siguientes eventos:

  (i) Alertas o notificaciones relacionadas con el espacio disponible.

  (ii) Alertas o notificaciones relacionadas con el rendimiento de los servidores.

7.1.4.4 Control de software operacional

Objetivo*:* Garantizar el óptimo funcionamiento del software operacional que soporta la Base de Datos del Aseguramiento.

Alcance*:* Este lineamiento aplica para las plataformas software que soportan la operación de la Base de Datos del Aseguramiento.

- Aplicaciones web para administración de la base de datos

- Herramientas de ofimática que apoyan las actividades de administración de la base de datos.

- Servidor web y servidor de base de datos.

- Sistema operativo de las máquinas que soportan los ambientes de Producción, Pre-producción y Desarrollo.

Responsables: Administrador de la Base de Datos del Aseguramiento.

Directrices:

- El administrador de la base de datos debe brindar soporte a los servidores de los ambientes de Pre-Producción y Desarrollo. Esto incluye la Instalación o

actualización de paquetes, actualizaciones de seguridad, o módulos funcionales de software, etc.

- El administrador de la base de Datos (Dirección de Aseguramiento) debe coordinar con el área de informática (Secretaría de TIC) de la Gobernación de Cundinamarca, la instalación o actualización de paquetes, actualizaciones de seguridad, o módulos funcionales de software, etc. en el Ambiente de Producción.

- El administrador de la Base de Datos del Aseguramiento debe brindar soporte a las herramientas que permiten la gestión de la base de datos: Aplicaciones web y clientes de administración de la base de datos.

7.1.4.5 Gestión de la vulnerabilidad técnica

Objetivo*:* Establecer los mecanismos específicos para identificar y mitigar las vulnerabilidades técnicas de las principales herramientas software que soportan la operación de la Base de Datos del Aseguramiento.

Alcance*:* Este lineamiento aplica para las siguientes herramientas software:

- Servidor MySQL, servidor Web y Sistema Operativo de los ambientes de Producción, Pre-producción y Desarrollo.

- Herramientas de administración de la Base de Datos.

Responsables: Administrador de la Base de Datos del Aseguramiento.

Directrices*:*

- El administrador de la Base de Datos del Aseguramiento debe realizar periódicamente en los ambientes de Pre-producción y Desarrollo, las pruebas necesarias para detectar posibles vulnerabilidades técnicas en los principales componentes de software que soportan la operación de la base de datos: Servidor MySQL, servidor web y sistema operativo.

- El administrador de la Base de Datos del Aseguramiento debe coordinar con el área de informática (Secretaría de TIC) de la Gobernación de Cundinamarca, la ejecución periódica en el ambiente de Producción, de las pruebas necesarias para detectar posibles vulnerabilidades técnicas en los principales componentes software que soportan la operación de la base de datos: Servidor MySQL, servidor web y sistema operativo.

- El administrador de la Base de Datos del Aseguramiento debe realizar periódicamente las pruebas necesarias para detectar posibles vulnerabilidades

técnicas en las herramientas software empleadas en la administración de la base de datos (ver Anexo D).

- El administrador de la Base de Datos del Aseguramiento debe consultar periódicamente en fuentes seguras el reporte o aparición de nuevas vulnerabilidades técnicas para los principales componentes y herramientas software que soportan la operación de la base de datos.

- A partir de los resultados obtenidos, el administrador debe coordinar y ejecutar las acciones necesarias para mitigar los riesgos y amenazas que surgen producto de las vulnerabilidades técnicas identificadas.

8. GUÍA CON RECOMENDACIONES DE SEGURIDAD

El presente apartado desarrolla una guía que propone una serie de recomendaciones concretas de seguridad para la Base de Datos del Aseguramiento a partir de los lineamientos de seguridad definidos en el capítulo anterior.

Esta guía se aborda desde los siguientes componentes generales:

- Componente de Auditoría: En este componente se recurre al área de la auditoría de bases de datos para elaborar una herramienta especifica tipo lista de chequeo para verificar el estado de la seguridad en la base de datos y gestionar las medidas necesarias para contrarrestar las vulnerabilidades identificadas.

- Componente Técnico: En este componente se recurre a los principales procedimientos técnicos empleados en la administración de bases de datos para ajustarlos a las características puntuales de la Base de Datos del Aseguramiento (ver Anexo B).

8.1 INSTRUMENTO DE AUDITORÍA PARA LA BASE DE DATOS DEL ASEGURAMIENTO

En línea con los aspectos compilados en la tabla 1 sobre las principales vulnerabilidades identificadas en la administración de bases de datos, en este componente se propone un instrumento tipo cuestionario que permite relacionar y evaluar distintos aspectos en el proceso de auditoría sobre la Base de Datos del Aseguramiento. Se propone también las respectivas recomendaciones que el administrador de la base de datos debe considerar a la hora minimizar los riesgos y amenazas de seguridad.

SECCIÓN # 1: SISTEMA DE GESTIÓN DE BASE DE DATOS

1.- ¿Se han configurado las opciones de seguridad de MySQL?

SI___ NO___

Si la respuesta es NO, entonces considere la siguiente recomendación: MySQL incluye la funcionalidad ‘mysql_secure_installation’ para mejorar la seguridad del sistema de gestión de base de datos. Esta funcionalidad permite cambiar el password de la cuenta root, eliminar las cuentas de usuarios anónimos, deshabilitar el acceso remoto, eliminar la base de datos de prueba (test).

2.- ¿Existe una cuenta que reemplaza la cuenta 'root' de MySQL por defecto?

SI___ NO___

Si la respuesta es NO, entonces siga la siguiente recomendación: Con el propósito de prevenir ataques de fuerza bruta empleando diccionarios, es altamente recomendable eliminar la cuenta 'root' por defecto y sustituirla por otra cuenta de administrador.

3.- ¿Se han desactivado las demás cuentas MySQL por defecto?

SI___ NO___

Si la respuesta es NO, entonces considere la siguiente recomendación: Similar a la cuestión anterior, este ítem tiene el propósito de prevenir ataques de fuerza bruta mediante el empleo de diccionarios. Es altamente recomendable eliminar las cuentas por defecto que MySQL tiene configuradas por defecto.

4.- De acuerdo con el esquema de red corporativa, ¿el servidor MySQL está expuesto a redes públicas como internet?

SI___ NO___

Si la respuesta es NO, entonces considere la siguiente recomendación: Si el servidor de MySQL está expuesto en una zona desmilitarizada (DMZ), debe reubicarse al interior debidamente protegido de la red corporativa.

5.- ¿La base de datos está en un servidor compartido?

SI___ NO___

Si la respuesta es NO, entonces considere la siguiente recomendación: Si el servidor de MySQL es un recurso compartido donde conviven otras bases de datos, dada la sensibilidad y tamaño de la Base de Datos del Aseguramiento, es recomendable la migración a una máquina exclusiva. Esta medida garantiza por un lado la seguridad de la información y, por otro lado, el rendimiento para las distintas consultas a la base de datos.

6.- ¿Está configurado el reporte de logs de MySQL?

SI___ NO___

Si la respuesta es NO, entonces considere la siguiente recomendación: Se debe configurar el reporte de logs del servidor MySQL. Una correcta configuración del reporte de logs permitirá al administrador verificar el tipo de evento, la fecha de

ejecución, las consultas, los usuarios y demás parámetros importantes para la seguridad de la información.

.

7.- ¿Se revisan periódicamente los logs del servidor y los accesos a la base de datos?

SI___ NO___

Si la respuesta es NO, entonces considere la siguiente recomendación: Es necesario que la revisión de los logs del servidor MySQL se realice de manera periódica y metódica por parte del administrador. Esto implica la programación de la revisión y la consignación por escrito de los resultados encontrados.
Esta información debe ser clasificada como Confidencial y el administrador debe tomar las medidas de protección pertinentes para garantizar su confidencialidad.

8.- ¿Se lleva un registro de los intentos de acceso fallidos o denegados a la base de datos?

SI___ NO___

Si la respuesta es NO, entonces considere la siguiente recomendación: Uno de los parámetros más importantes durante la revisión periódica de logs del servidor de MySQL es la observación de los intentos fallidos o denegados. Un análisis de dichos eventos brindará al administrador las señales de advertencia sobre el intento fraudulento de acceso a la base de datos.

Esta información debe ser clasificada como Confidencial y el administrador debe tomar las medidas de protección pertinentes para garantizar su confidencialidad.

SECCIÓN # 2: BASE DE DATOS

9.- ¿La base de datos posee un modelo relacional de datos?

SI___ NO___

Si la respuesta es NO, entonces considere la siguiente recomendación: El modelo de datos constituye la abstracción de los elementos del contexto real que son instanciados en la base de datos. Esto le confiere un carácter arquitectónico a partir del cual operan las distintas relaciones y operaciones que se realizan sobre la base de datos. La correcta comprensión y diseño del modelo de datos garantiza la integridad de la información, la escalabilidad de la base de datos, la comprensión de alto nivel por parte de otros actores relacionados con la base de datos.

En caso de no contar con el modelo de datos o estar desactualizado, es necesario que el administrador proceda a su elaboración o actualización.

Esta información debe ser clasificada como Confidencial y el administrador debe tomar las medidas de protección pertinentes para garantizar su confidencialidad.

10.- ¿Se cuenta con un diagrama o vista de despliegue de la base de datos en la estructura de red y recursos computacionales de la entidad?

SI___ NO___

Si la respuesta es NO, entonces considere la siguiente recomendación: La vista de despliegue permite identificar la ubicación e interacción de la base de datos con los demás elementos computacionales de la red corporativa. A partir de esta visión general, el administrador podrá tomar decisiones sobre medidas para mejorar la seguridad de la información a nivel de red.

Si este diagrama no existe, es necesario que el administrador proceda al diseño y respectiva documentación.

La versión con mayor nivel de detalle de este diagrama debe ser clasificada como Confidencial.

11.- ¿La base de datos cuenta con un diccionario de datos?

SI___ NO___

Si la respuesta es NO, entonces considere la siguiente recomendación: Un diccionario de datos es una herramienta documental que consolida de manera formal el listado de los datos que componen el sistema. Así pues, en el marco de la administración de una base de datos, esta herramienta dará cuenta del nombre del campo, tipo de campo, tamaño, descripción. Esta información debe ser clasificada como Confidencial.

Si este documento no existe, el administrador debe proceder a su elaboración.
Esta información debe ser clasificada como Confidencial.

12.- ¿Se realizan pruebas de rendimiento y optimización de código fuente SQL?

SI___ NO___

Si la respuesta es NO, entonces considere la siguiente recomendación: El código fuente SQL (Structured Query Language) es como su nombre lo indica el lenguaje de interacción con la base de datos relacional. Puesto que dentro de las principales funcionalidades que la base de datos brinda al administrador es la generación de reportes esenciales para la toma de decisiones, las sentencias SQL deben ser

correctamente estructuradas y optimizadas para evitar la saturación o incluso caída del servidor.

El administrador debe optimizar el código para garantizar la disponibilidad e integridad de la información de la base de datos.

Por otro lado, el código fuente SQL empleado en los reportes debe ser clasificado como información Confidencial y el administrador debe tomar las medidas de protección pertinentes para garantizar su confidencialidad.

13.- ¿Se aplican índices adecuados a las tablas?

SI___ NO___

Si la respuesta es NO, entonces considere la siguiente recomendación: La correcta indexación de las tablas permitirá agilizar las consultas sobre la base de datos de tal modo que se garantiza el uso óptimo de los recursos de servidor. Entre otras ventajas, la aplicación de índices a las tablas redundará en la disponibilidad de la información al optimizar los tiempos de procesamiento del servidor.

El administrador debe aplicar correctamente los índices a las tablas de la base de datos, especialmente a aquellas que son objetos de continua consulta. Por otro lado, es recomendable elegir aquellos campos que permitan identificar sin ambigüedad cada registro entre los millones que pueden constituir la información almacenada, como es el caso de la Base de Datos del Aseguramiento.

SECCIÓN # 3: PROCEDIMIENTOS Y HERRAMIENTAS DE ADMINISTRACIÓN

14.- ¿Se lleva control de los usuarios, datos de acceso y perfiles configurados?

SI___ NO___

Si la respuesta es NO, entonces considere la siguiente recomendación: Es necesario la gestión de un registro formal y estructurado de los usuarios creados para acceder a la base de datos. Este procedimiento permitirá el control y gestión en todo momento de los usuarios registrados y los niveles de permisos asignados.

Este control puede realizarse directamente mediante la consola de comandos de MySQL o lo más recomendable será emplear herramientas de administración de la base de datos. En todo caso dicho control debe dar cuenta como mínimo de los siguientes parámetros: Nombre completo, usuario, contraseña (encriptada), privilegios, grupo, fecha de creación, fecha de expiración del acceso.

15.- ¿Se asignan contraseñas fuertes a los usuarios?

SI___ NO___

Si la respuesta es NO, entonces considere la siguiente recomendación: Las contraseñas fuertes deben ser alfanuméricas e incluir adicionalmente un carácter especial. Una contraseña fuerte dificultará la ejecución ataques informáticos que traten de vulnerar el proceso de autenticación de un usuario legítimo.

El administrador debe asignar contraseñas de mínimo 8 caracteres de longitud que incluyan uno o más caracteres especiales. La contraseña debe ser almacenada bajo un mecanismo de encriptación.

Esta información debe ser clasificada como Confidencial y el administrador debe tomar las medidas de protección pertinentes para garantizar su confidencialidad.

16.- ¿Se renuevan periódicamente las contraseñas?

SI___ NO___

Si la respuesta es NO, entonces considere la siguiente recomendación: Es necesario que el administrador aplique un procedimiento automático o manual para cambiar con una periodicidad, no superior a tres meses, las contraseñas de los usuarios activos con acceso a la base de datos. Esta acción incrementa el nivel de seguridad del acceso a la base de datos y dificulta la ejecución de ataques informáticos tendientes a vulnerar el proceso de autenticación.

17.- ¿Se obliga el cambio de la primera contraseña asignada?

SI___ NO___

Si la respuesta es NO, entonces considere la siguiente recomendación: Es recomendable que de manera automática el sistema de autenticación para acceso a la base de datos, solicite el cambio de la primera contraseña asignada. Esta acción tiene como propósito la creación de una contraseña significativa para el usuario, así como incrementar el nivel de privacidad de este parámetro.

18.- ¿Se realizan periódicamente backups de la base de datos?

SI___ NO___

Si la respuesta es NO, entonces considere la siguiente recomendación: Es de obligatorio cumplimiento la realización de backups periódicos de la base de datos. Esta medida salvaguarda la información en caso de presentarse un evento de seguridad de la información como un ataque informático, un error accidental de

administrador, un desastre ambiental, indisponibilidad temporal o definitiva del ambiente de Producción, etc.

En MySQL el administrador puede recurrir a la funcionalidad 'dump' y sus diferentes opciones a través de la consola de comandos o puede también realizar el backup mediante una determinada herramienta de administración.

De acuerdo con el lineamiento establecido este backup debe realizarse con una periodicidad mensual.

19.- ¿Se realiza monitoreo constante al espacio disponible en los ambientes de Producción, Preproducción y Desarrollo?

SI___ NO___

Si la respuesta es NO, entonces considere la siguiente recomendación: Los recursos computacionales son limitados. Uno de los recursos más críticos es el espacio de almacenamiento. Si el espacio disponible en el sistema de almacenamiento se agota, colapsa la operación de la base de datos afectando completamente la disponibilidad de la información. Es por esta razón que el administrador debe efectuar seguimiento periódico al espacio disponible.

En el caso de la Base de datos del Aseguramiento el administrador debe realizar el seguimiento con periodicidad mensual y medir la tasa de crecimiento de la base de datos con el propósito de determinar la necesidad de almacenamiento a futuro.

19.- ¿Las copias de respaldo están encriptadas?

SI___ NO___

Si la respuesta es NO, entonces considere la siguiente recomendación: Dado que las copias de seguridad no cuentan con un mecanismo propio de autenticación para su acceso, es recomendable su encriptación. Esta medida evitará el acceso no autorizado a la información.

El administrador debe encriptar las copias de seguridad antes de disponerlas en el servidor de backups de la entidad.

20.- ¿Se realizan periódicamente pruebas de restauración de las copias de respaldo?

SI___ NO___

Si la respuesta es NO, entonces considere la siguiente recomendación: Es necesario comprobar periódicamente el correcto despliegue y funcionamiento de las

copias de seguridad realizadas. Esta acción permitirá un nivel concreto de certidumbre frente a posibles eventos indeseables durante los cuales sea necesario emplear las copias de seguridad.

El administrador debe elaborar una guía de pruebas y con base en este instrumento proceder a su ejecución en el ambiente de Desarrollo.

21.- ¿Se cuenta con Ambiente de Desarrollo, Pre-producción y Pruebas?

SI___ NO___

Si la respuesta es NO, entonces considere la siguiente recomendación: Los ambientes constituyen una buena práctica a la hora de administrar sistemas de información, desarrollar nuevos sistemas o módulos funcionales.

El administrador de la Base de Datos del Aseguramiento debe mantener los ambientes de Desarrollo, Pruebas y Pre-producción como pasos preliminares antes de actualizar el ambiente de Producción. Esta medida contribuirá a garantizar la Disponibilidad e Integridad de la información al permitir que los cambios sean bien probados antes de ejecutarlos sobre el ambiente de Producción.

22.- ¿Se controla el acceso a los ambientes de Desarrollo, Pruebas y Pre-producción?

SI___ NO___

Si la respuesta es NO, entonces considere la siguiente recomendación: Aunque los ambientes de Desarrollo, Pruebas y Pre-producción constituyen pasos preliminares, el acceso y niveles de permisos de los usuarios a estos entornos debe ser igualmente gestionado con rigurosidad.

El administrador de la Base de Datos del Aseguramiento debe aplicar para estos ambientes el mismo control y seguimiento a usuarios que para el ambiente de Producción.

22.- ¿Se realizan periódicamente backups de los ambientes de Desarrollo, Pruebas y Pre-producción?

SI___ NO___

Si la respuesta es NO, entonces considere la siguiente recomendación: El lineamiento de respaldo de la información también debe aplicar para los ambientes de Desarrollo, Pruebas y Pre-producción. Como quiera que en estos ambientes se encuentran información valiosa sobre nuevos desarrollos a aplicar, y la trazabilidad a los cambios que se han aplicado.

23.- ¿Se atienden las advertencias de fallos de seguridad en la versión disponible de MySQL?

SI___ NO___

Si la respuesta es NO, entonces considere la siguiente recomendación: El administrador debe consultar periódicamente los reportes de vulnerabilidades de MySQL publicados en fuentes oficiales y confiables como el Boletín y Alertas de Seguridad de Oracle[32]y los reportes CVE[33](Common Vulnerabilities and Exposures – Exposiciones y Vulnerabilidades Comunes). A partir de esta información, el administrador debe trazar un plan de acción para corregir los fallos de seguridad que pueden afectar la versión de MySQL que se tiene instalada en los distintos ambientes. El orden de aplicación de estas actualizaciones debe ser el siguiente: Entorno de Desarrollo, Entorno de Pruebas, Entorno de Pre-producción y Entorno de Producción.

24.- ¿Se realizan periódicamente pruebas de identificación de vulnerabilidades sobre aplicaciones?

SI___ NO___

Si la respuesta es NO, entonces considere la siguiente recomendación: El administrador debe realizar periódicamente pruebas de seguridad sobre las aplicaciones o herramientas de administración de la base de datos. Específicamente debe consultar por las vulnerabilidades específicas de las aplicaciones en las páginas oficiales de los fabricantes y si son desarrollos propios debe realizar verificaciones de seguridad tales como validación de formularios web, fallos de autenticación, inyección de código, etc.

SECCIÓN #4: ASPECTOS ORGANIZACIONALES

25.- ¿La organización cuenta con personal de respaldo especializado en administración de bases de datos y servidores?

SI___ NO___

Si la respuesta es NO, entonces considere la siguiente recomendación: Dado que la administración de bases de datos requiere conocimientos especializados, es altamente recomendable que la organización (en este caso la Dirección de

[32] ORACLE. Critical Patch Updates, Security Alerts and Bulletins. [En línea], [consultado el 23 de marzo de 2019]. Disponible en Internet: https://www.oracle.com/technetwork/topics/security/alerts-086861.html .

[33] MITRE Corporation. Common Vulnerabilities and Exposures -CVE. . [En línea], [consultado el 23 de marzo de 2019]. Disponible en Internet: http://cve.mitre.org/index.html .

Aseguramiento) cuente con personal de respaldo cualificado para reemplazar al administrador en situaciones de vacancia temporal o definitiva.

26.- ¿La organización ha establecido lineamientos de seguridad de la información para la administración de la base de datos?

SI___ NO___

Si la respuesta es NO, entonces considere la siguiente recomendación: Es necesario que la organización (en este caso la Dirección de Aseguramiento), aplique y actualice periódicamente los lineamientos de seguridad de la información para la administración de la Base de Datos del Aseguramiento.

27.- ¿En la dependencia existe cultura sobre la importancia de la seguridad de la información?

SI___ NO___

Si la respuesta es NO, entonces considere la siguiente recomendación: Es necesario que la organización (en este caso la Dirección de Aseguramiento) diseñe y ejecute estrategias educativas para promover la importancia de la seguridad de la información en todos los procesos y actividades.

9. CONCLUSIONES

El desarrollo de las etapas y actividades propuestas en el presente trabajo, permite obtener las conclusiones que se presentan a continuación:

- Los controles de la norma ISO 27001 - anexo A constituyeron un referente en materia de seguridad de la información durante el desarrollo de este trabajo. Permitieron la identificación metódica del estado actual de las actividades de administración de la Base de Datos del Aseguramiento frente a los dominios, objetivos y controles de la norma que les aplican. Este estado actual se corresponde con un nivel inicial de cumplimiento.

Los resultados obtenidos constituyeron el primer componente para la formulación de los lineamientos de seguridad para la Base de Datos del Aseguramiento.

- La metodología MAGERIT puso a disposición para este trabajo las herramientas procedimentales necesarias para la identificación rigurosa de los activos y el análisis de riesgos presentes en las actividades de administración de la Base de Datos del Aseguramiento.

Los resultados obtenidos aplicando esta metodología, por un lado, aportaron la posibilidad de enfocarse en aquellos activos y riesgos más críticos que deben ser atendidos en el corto plazo; por otro lado, constituyeron el segundo componente para la formulación de los lineamientos de seguridad para la Base de Datos del Aseguramiento.

- Los lineamientos de seguridad de la información formulados en este trabajo, responden a necesidades puntuales y activos críticos en relación con la de seguridad de la información para la Base de Datos del Aseguramiento. Sin embargo, constituyen una primera versión que debe ser revisada, actualizada y ampliada periódicamente de tal modo que alcance un estado de madurez aceptable y pueda servir como referente para otros procesos interrelacionados en la Dirección de Aseguramiento.

- Los instrumentos de seguimiento ajustados o desarrollados en este trabajo de grado permitieron incorporar, registrar y reportar claramente distintos aspectos relacionados con la seguridad de la información en el marco de las actividades de administración de la Base de Datos del Aseguramiento. Las herramientas colaborativas actuales disponibles en la nube permiten implementar rápidamente este tipo de instrumentos y prueban ser eficientes en escenarios de pequeña y mediana complejidad.

- Este trabajo permitió estudiar y aplicar opciones de seguridad al Sistema de Gestión de Bases de Datos Relacionales (SGBDR) MySQL en el marco de las actividades de administración de la Base de Datos del Aseguramiento.

MySQL cuenta con las funcionalidades básicas para cumplir con los distintos requerimientos de seguridad para la información almacenada; sin embargo, es necesario consultar las fuentes oficiales de vulnerabilidades identificadas en este trabajo.

BIBLIOGRAFÍA

ADRES. ¿qué es la ADRES? [En línea], [consultado en noviembre de 2018]. Disponible en internet: https://www.adres.gov.co/La-Entidad/-Qu%C3%A9-es-la-ADRES

BARNES, ROB. Database Auditing: Best Practices. [En línea], [consultado el 2 de noviembre de 2018]. Disponible en: http://www.sfisaca.org/images/May09_Slides.pdf?1Q,M3,521fd9a2-f86d-4991-8428-8e8324b89ecd

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 100 de 1993. . [En línea], [consultado el 2 de noviembre de 2018]. Disponible en internet http://www.secretariasenado.gov.co/senado/basedoc/ley_0100_1993.html

_____,_____. Ley 1753 de 2015. [En línea], [consultado el 2 de noviembre de 2018]. Disponible en internet: http://www.secretariasenado.gov.co/senado/basedoc/ley_1753_2015_pr001.html

COLOMBIA. CORTE CONSTITUCIONAL. Constitución Política de Colombia, 1991. [En línea], [consultado en noviembre de 2018]. Disponible en internet: http://www.corteconstitucional.gov.co/inicio/Constitucion%20politica%20de%20Colombia.pdf

COLOMBIA. DEPARTAMENTO NACIONAL DE PLANEACIÓN. Diseño del índice SISBEN en su tercera versión –SISBEN [En línea], [consultado en noviembre de 2018]. Disponible en internet: https://www.sisben.gov.co/Documents/Resumen%20ejecutivo/Resumen_ejecutivo_SisbenIII.pdf.

COLOMBIA. GOBERNACIÓN DE CUNDINAMARCA. Sistema Integrado de Gestión y Control – SIGC - Versión 9. 2018. Bogotá D.C. [En línea], [consultado en noviembre de 2018]. Disponible en internet: http://isolucion.cundinamarca.gov.co/Isolucion .

_____. _____. Plan de Desarrollo Departamental 2016 -2019, Gobernación de Cundinamarca. [En línea], [consultado en noviembre de 2018]. Disponible en internet http://www.cundinamarca.gov.co/wcm/connect/2a9dd7d1-d693-414a-94cd-37fe5f901e7d/PLAN+DE+DESARROLLO+VERSION+FINAL.pdf?MOD=AJPERES&CVID=lDlW39U

_____. _____. Dirección de Aseguramiento. Funciones de la Dirección de Aseguramiento. [En línea], [consultado en noviembre de 2018]. Disponible en

internet: http://www.cundinamarca.gov.co/Home/SecretariasEntidades.gc/Secretariadesalud/SecretariadesaludDespliegue/ascontenido/asquienes_somos/assecresalud_quienesestrucorgydirec/csecresalud_quienesestrucorgydirec_diraseg .

_____. _____. Sistema Integrado de Gestión y Control – SIGC. Manual del Sistema Integral de Gestión y Control. Función Pública, [En línea], [consultado en noviembre de 2018]. Disponible en internet http://www.cundinamarca.gov.co/wcm/connect/2a9dd7d1-d693-414a-94cd-37fe5f901e7d/PLAN+DE+DESARROLLO+VERSION+FINAL.pdf?MOD=AJPERES&CVID=lDlW39U

COLOMBIA. MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES – MinTIC, (2016). Modelo de Seguridad y Privacidad de la Información. [En línea], [consultado el 2 de noviembre de 2018]. Disponible en internet: https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

COLOMBIA. MINISTERIO DE SALUD Y PROTECCIÓN SOCIAL. Resolución 4622 de 2016. [En línea], [consultado en noviembre de 2018]. Disponible en internet: https://www.minsalud.gov.co/Normatividad_Nuevo/Resolución%204622%20de%202016.pdf

_____. _____. Población Pobre No Asegurada. Metodología para su estimación y resultados obtenidos. [En línea], [consultado en noviembre de 2018]. Disponible en internet: https://www.minsalud.gov.co/sites/rid/Lists/BibliotecaDigital/RIDE/VP/DOA/metodologia-ppna-sisben-junio-oct.pdf

_____, _____, Régimen Contributivo. [En línea], [consultado el 2 de noviembre de 2018]. Disponible en internet : https://www.minsalud.gov.co/proteccionsocial/Regimencontributivo/Paginas/regimen-contributivo.aspx

COLOMBIA, SENADO DE LA REPÚBLICA. 2018. Ley 1273 de 2009. [En línea], [consultado el 2 de noviembre de 2018]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html .

_____. _____. Ley 1581 de 2012. [En línea], [consultado el 2 de noviembre de 2018]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

DAMELE, B. & STAMPAR, M. Sqlmap Features. [en línea]. [consultado el 19 de abril de 2019]. https://github.com/sqlmapproject/sqlmap/wiki/Features

GARCÍA HERNÁNDEZ, D., RUIZ MURILLO, J. Análisis y gestión de riesgos en el marco del SGSI, basado en la metodología MAGERIT y apoyado en un api web para su ejecución. Bogotá, Colombia. Universidad Distrital Francisco José de Caldas, Pregrado en Ingeniería Telemática, 2017. p. 150

GIRALDO CEPEDA, Luis Enrique. Análisis para la implementación de un sistema de gestión de la seguridad de la información según la norma ISO 27001 en la empresa Servidoc S.A. Cali: Universidad Nacional Abierta y a Distancia. 2016, Especialización en Seguridad Informática. Colombia. [En línea], [consultado el 2 de noviembre de 2018]. Disponible en: https://repository.unad.edu.co/handle/10596/6341?mode=full

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS – ICONTEC - Norma Técnica Colombiana NTC-ISO-IEC 27000. Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información. Visión General y Vocabulario. Bogotá: Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC) Apartado 14237.2017, p.13

_____. Norma Técnica Colombiana NTC-ISO-IEC 31000. Gestión del Riesgo. Principios y Directrices. Bogotá: Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC) Apartado 14237.

_____, Norma Técnica Colombiana NTC-ISO-IEC 27001. Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Bogotá: Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC), 2013, p. 4

KALI Linux. Official Kali Linux Documentation. [en línea]. [consultado el 19 de abril de 2019]. Disponible en: https://www.kali.org/kali-linux-documentation/

LYON, Gordon. Guía de referencia de Nmap. [en línea]. California. [consultado el 19 de abril de 2019]. Disponible en: https://nmap.org/man/es

MYSQL. MySQL 5.6 Reference Manual. [En línea], [consultado el 2 de noviembre de 2018]. Disponible en https://dev.mysql.com/doc/refman/5.6/en/ .

MITRE Corporation. Common Vulnerabilities and Exposures -CVE. . [En línea], [consultado el 23 de marzo de 2019]. Disponible en Internet: http://cve.mitre.org/index.html .

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY - NIST. Glossary of Key Information Security Terms. [En línea], [consultado el 2 de febrero de 2019]. Disponible en internet: https://nvlpubs.nist.gov/nistpubs/ir/2013/nist.ir.7298r2.pdf .

ORACLE. Critical Patch Updates, Security Alerts and Bulletins. [En línea], [consultado el 23 de marzo de 2019]. Disponible en Internet: https://www.oracle.com/technetwork/topics/security/alerts-086861.html .

OWASP. OWASP ZAP 2.6 Getting Started Guide. [en línea]. [consultado el 19 de abril de 2019]. Disponible en: https://github.com/zaproxy/zaproxy/releases/download/2.6.0/ZAPGettingStartedGuide-2.6.pdf

PORTAL DE ADMINISTRACIÓN ELECTRÓNICA. MAGERIT v.3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Madrid, España. [En línea], [consultado el 2 de noviembre de 2018]. Disponible en internet: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.WsBSPS7wbIU

SALUD CAPITAL. Régimen subsidiado. [En línea], [consultado el 2 de noviembre de 2018].Disponible en internet http://www.saludcapital.gov.co/DASEG/Paginas/RegimenSubsidiado.aspx .

SCHUMACHER, R. MySQL 5.0's Pluggable Storage Engine Architecture, Part 1: An Overview. MySQL AB. 2004. [En línea], [consultado el 2 de noviembre de 2018]. Disponible en: http://download.nust.na/pub6/mysql/tech-resources/articles/mysql_5.0_psea1.html .

UNITED NATIONS DEVELOPMENT PROGRAMME. IT Audit Manual. [En línea], [consultado el 2 de noviembre de 2018]. Disponible en: http://www.al.undp.org/content/dam/albania/docs/STAR/IT%20AUDIT%20MANUAL.pdf

UNIVERSIDAD AUTÓNOMA DEL ESTADO DE HIDALGO. Auditoría de Bases de Datos. [En línea], [consultado el 2 de noviembre de 2018]. Disponible en: http://cidecame.uaeh.edu.mx/lcc/mapa/PROYECTO/libro21/322_auditoria_de_bases_de_datos.html .

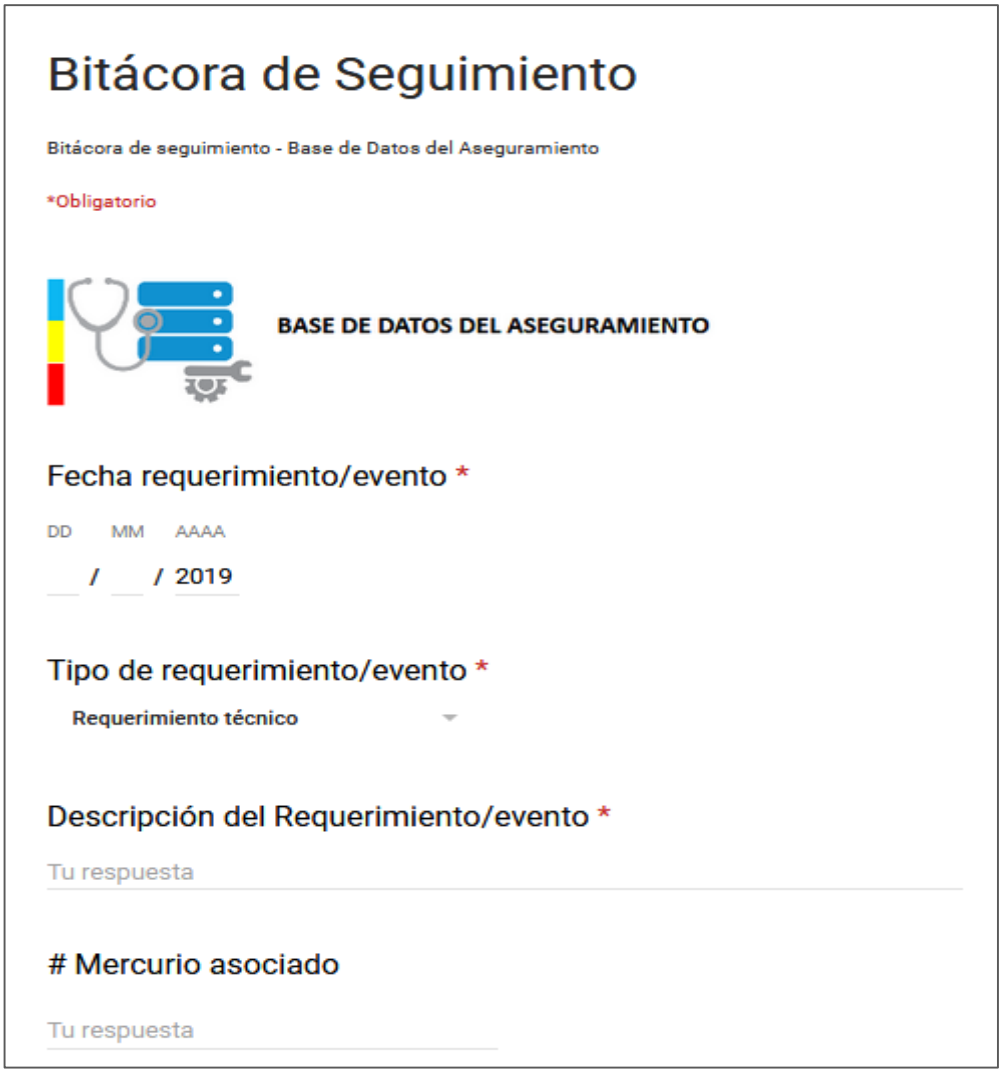
.

ANEXOS

ANEXO A. HERRAMIENTA BITÁCORA DE SEGUIMIENTO

A continuación, se describe la herramienta llamada Bitácora de Seguimiento que es empleada en el marco de las actividades de administración de la Base de Datos. Esta herramienta permite registrar distintos eventos y requerimientos técnicos, entre los cuales se han identificado varios relacionados con seguridad de la información.

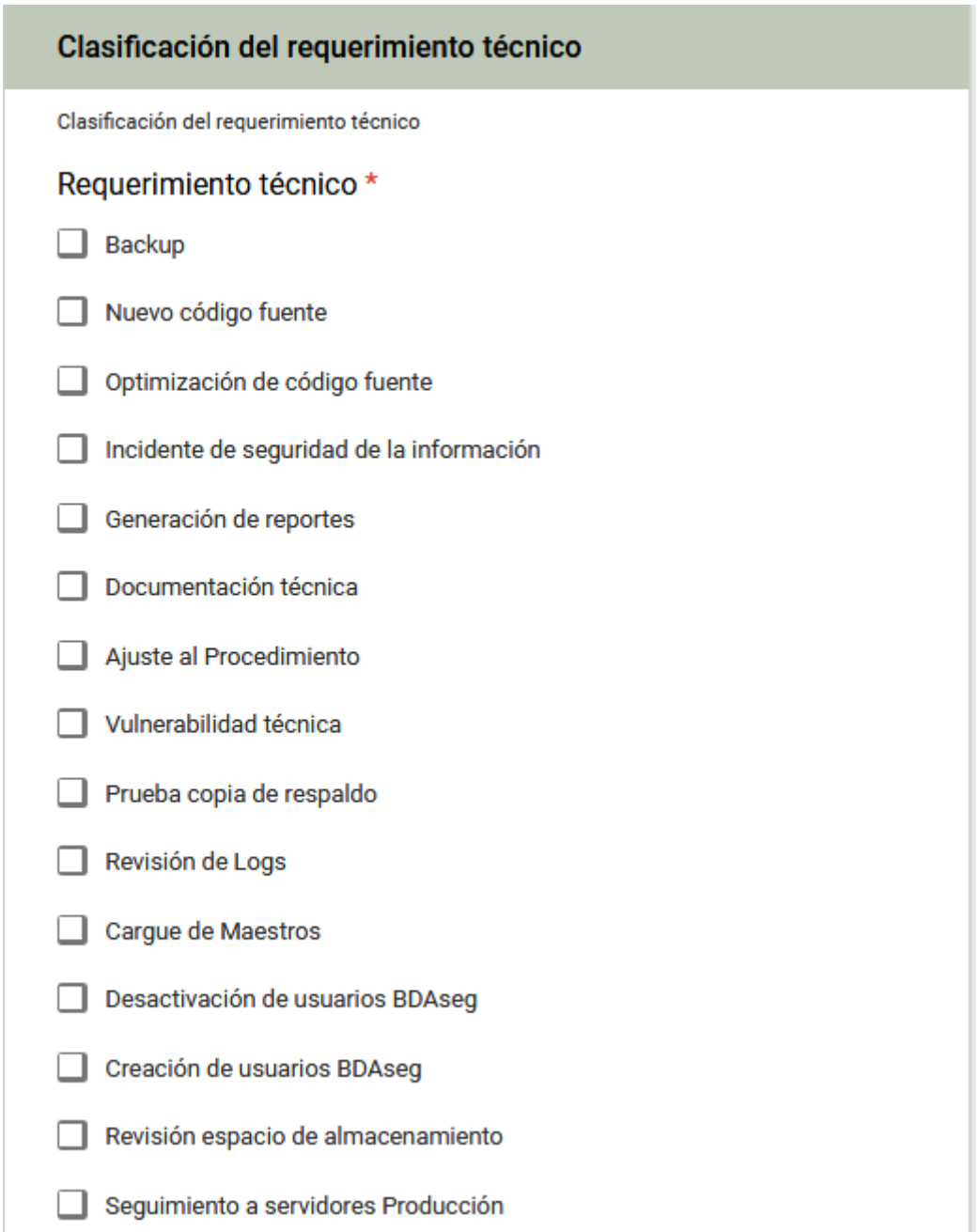
Figura 8. Interfaz inicial



Fuente: Autor.

A los requerimientos de tipo técnico fueron agregadas varias etiquetas relacionadas con seguridad de la información con el propósito de dar seguimiento a los lineamientos de seguridad propuestos en el presente trabajo de grado.

Figura 9. Etiquetas para requerimientos técnicos



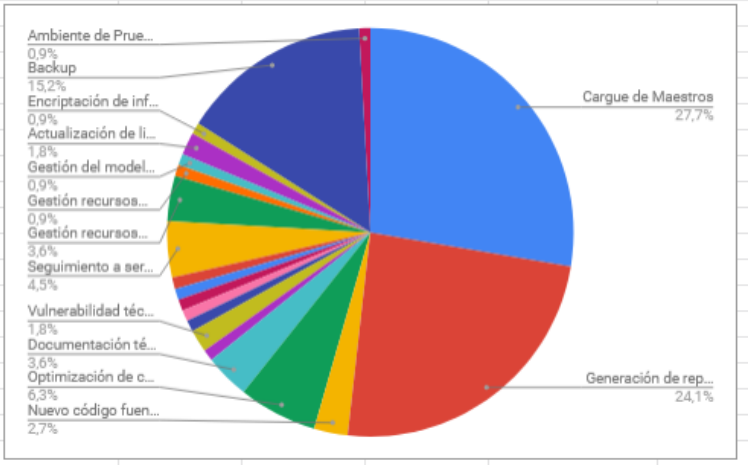
- [ ] Seguimiento a servidores Pre-producción y Desarrollo
- [ ] Gestión recursos ADRES
- [ ] Gestión recursos MinSalud
- [ ] Gestión del modelo de datos
- [ ] Actualización de lineamientos de seguridad
- [ ] Encriptación de información

Fuente: Autor.

A continuación, se presenta un reporte básico que muestra la distribución de los requerimientos técnicos para el administrador de la Base de Datos del Aseguramiento:

Figura 10. Número de Requerimientos técnicos

REPORTE GENERAL - REQUERIMIENTOS TECNICOS	
Tipo de Requerimiento	Cantidad
Cargue de Maestros	31
Generación de reportes	27
Nuevo código fuente	3
Optimización de código fuente	7
Incidente de seguridad de la información	0
Documentación técnica	4
Ajuste al procedimiento	1
Vulnerabilidad técnica	2
Prueba copia de respaldo	1
Revisión de logs	1
Desactivacion de Usuarios BDAseg	0
Creación de usuarios BDAseg	1
Revisión espacio de almacenamiento	1
Seguimiento a servidores Producción	1
Seguimiento a servidores Pre-producción y	5
Gestión recursos ADRES	4
Gestión recursos Minsalud	1
Gestión del modelo de datos	1
Actualización de lineamientos de segurida	2
Encriptación de información	1
Backup	17
Ambiente de Producción	0
Ambiente de Pre-Producción	0
Ambiente de Pruebas	1
Ambiente de Desarrollo	0
Total	112



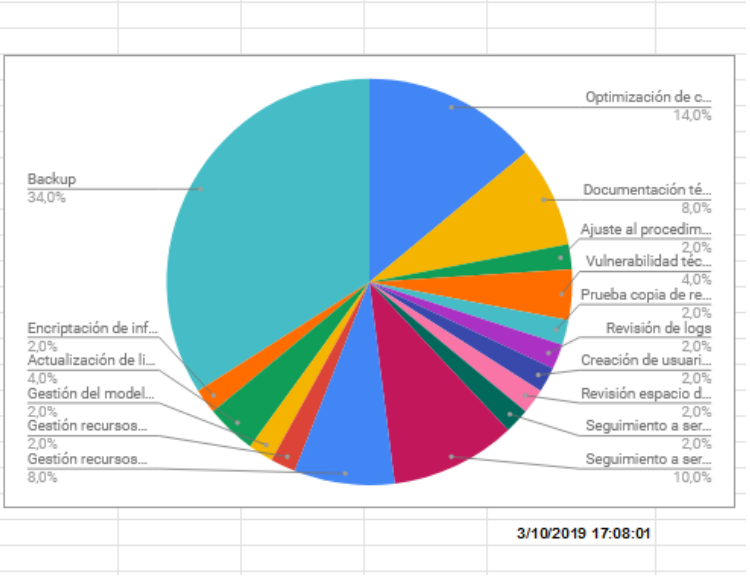
Fuente: Autor.

Este reporte muestra que las principales actividades están relacionadas con actividades operativas como el Cargue de Maestros, Generación de Reportes y ejecución de Backup.

Sin embargo, el siguiente reporte filtra los requerimientos relacionados con la seguridad de la información y muestra que algunos tipos han surgido con motivo de su identificación en el marco del presente trabajo (aquellos cuya cantidad equivale a 1) y se atenderán periódicamente en el futuro. Por otro lado, el reporte permite identificar que hasta la fecha todos los requerimientos son de tipo preventivo; el requerimiento de Incidente de seguridad de la información hasta el momento no se ha presentado.

Figura 11. Requerimientos de Seguridad de la Información

REPORTE - SEGURIDAD DE LA INFORMACION	
Tipo de Requerimiento	Cantidad
Optimización de código fuente	7
Incidente de seguridad de la información	0
Documentación técnica	4
Ajuste al procedimiento	1
Vulnerabilidad técnica	2
Prueba copia de respaldo	1
Revisión de logs	1
Desactivacion de Usuarios BDAseg	0
Creación de usuarios BDAseg	1
Revisión espacio de almacenamiento	1
Seguimiento a servidores Producción	1
Seguimiento a servidores Pre-producción y	5
Gestión recursos ADRES	4
Gestión recursos Minsalud	1
Gestión del modelo de datos	1
Actualización de lineamientos de seguridad	2
Encriptación de información	1
Backup	17
Total	50



Fuente: Autor.

ANEXO B. PROCEDIMIENTOS TÉCNICOS PARA SEGURIDAD DE LA BASE DE DATOS

En este anexo se consolidan algunos comandos y códigos fuente SQL que el administrador de bases de datos puede considerar para llevar a cabo actividades preventivas relacionadas con la seguridad de la información en el Sistema de Gestión de Bases de Datos MySQL:

1.- Configuración de opciones de Seguridad de MySQL

A continuación, se presenta el resultado de la ejecución del comando **mysql_secure_installation** en la terminal de comandos de Linux. Una funcionalidad de MySQL que permite establecer medidas básicas de seguridad como fortalecimiento de las contraseñas de usuario, remoción de usuarios anónimos, restricción de conexiones remotas para el usuario root y remoción de la base de datos de prueba.

```
root@djdorado:/# mysql_secure_installation
Securing the MySQL server deployment.
Connecting to MySQL using a blank password.
VALIDATE PASSWORD PLUGIN can be used to test passwords
and improve security. It checks the strength of password
and allows the users to set only those passwords which are
secure enough. Would you like to setup VALIDATE PASSWORD plugin?

Press y|Y for Yes, any other key for No: y

There are three levels of password validation policy:
LOW    Length >= 8
MEDIUM Length >= 8, numeric, mixed case, and special characters
STRONG Length >= 8, numeric, mixed case, special characters and
dictionary                file

Please enter 0 = LOW, 1 = MEDIUM and 2 = STRONG: 2
Please set the password for root here.

New password:
Re-enter new password:

Estimated strength of the password: 50
Do you wish to continue with the password provided?(Press y|Y for Yes, any
other key for No) : Y
By default, a MySQL installation has an anonymous user,
allowing anyone to log into MySQL without having to have
a user account created for them. This is intended only for
```

```
testing, and to make the installation go a bit smoother.
You should remove them before moving into a production
environment.

Remove anonymous users? (Press y|Y for Yes, any other key for No) : Y
Success.

Normally, root should only be allowed to connect from
'localhost'. This ensures that someone cannot guess at
the root password from the network.

Disallow root login remotely? (Press y|Y for Yes, any other key for No) : Y
Success.

By default, MySQL comes with a database named 'test' that
anyone can access. This is also intended only for testing,
and should be removed before moving into a production
environment.

Remove test database and access to it? (Press y|Y for Yes, any other key for
No) : Y
 - Dropping test database...
Success.

 - Removing privileges on test database...
Success.

Reloading the privilege tables will ensure that all changes
made so far will take effect immediately.

Reload privilege tables now? (Press y|Y for Yes, any other key for No): Y
Success.

All done!
```

2.- Desactivación de la cuenta root

El siguiente código para ejecutar en la terminal de comandos de Linux permite la sustitución de la cuenta root por defecto de MySQL, por una cuenta de administrador con un nombre no común, más ajustado al contexto y que brinda mayor seguridad.

```
root@djdorado:/#  mysql -uroot –p********
mysql> create user bdasegadmin@localhost identified by '********';
mysql> grant all on *.* to bdasegadmin@localhost with grant option;
mysql> exit
root@djdorado:/# mysql -u bdasegadmin -p
mysql>drop user root@localhost;
mysql> exit
```

3.- Programación de Backup con periodicidad mensual

El siguiente código para ejecutar en la terminal de comandos de Linux permite la programación en la funcionalidad **crontab** de un backup con periodicidad mensual aplicado a una base de datos especifica (en el ejemplo **bd**).

La operación se ejecuta el primer día del mes a las 530 h y es guardado en el directorio **/root/backup** con el **nombre bd_fecha.sql.gz**

```
root@djdorado:/# nano /etc/crontab

# backup de bd con periocidad mensual
30 05 1 * * * mysqldump -ubdasegadmin –p********. bd> /root/backup/bd_`date
+%m-%d-%Y`.sql.gz
```

ANEXO C. FORMATOS

A continuación, se propone un conjunto de formatos que apoyan las actividades de administración de una base de datos, específicamente la Base de Datos del Aseguramiento.

1.- Control de Usuarios

Formato general para la gestión de usuarios con acceso a la base de datos. Este formato contiene los campos mínimos que deben tenerse en cuenta en cada registro de un usuario independientemente de la herramienta de administración empleada por el administrador.

Formato para registro de usuarios.

CONTROL DE USUARIOS DE LA BASE DE DATOS								**Versión:**	
# item	**Nombre completo**	**Usuario**	**Contraseña (encriptada)**	**Permisos (Select, Insert, Update, Delete, Create, Drop)**	**Fecha de creación**	**Fecha de expiración**	**Acceso (Local, remoto, IP especifica)**	**Estado actual (Activo, Inactivo)**	**Ambiente: Prod, Pre-prod. Desarr.**
1									
2									
3									

Fuente: Autor.

2.- Diccionario de Datos

A continuación, se presenta el formato para la creación del diccionario de datos para la Base de Datos del Aseguramiento.

Formato para diccionario de datos

DICCIONARIO DE DATOS					**Versión:**
Nombre del documento:					
Descripción:					
Claves y relaciones:					
# ítem	**Nombre de Campo**	**Tipo de dato**	**Tamaño**	**Índice**	**Descripción**
1					
2					
3					

Fuente: Autor.

3.- Acuerdo de Confidencialidad

ACUERDO DE CONFIDENCIALIDAD

Mediante el presente ACUERDO DE CONFIDENCIALIDAD, el funcionario o contratista que suscribe este documento, asume la responsabilidad de NO revelar, divulgar, reproducir, publicar, o comunicar la INFORMACIÓN CONFIDENCIAL que en el cumplimiento de sus funciones reciba, gestione o tenga acceso a ella. En consecuencia, se obliga a mantener esta característica de CONFIDENCIALIDAD protegiendo la información de cualquier forma de acceso no autorizado.

Específicamente el suscrito asume las siguientes obligaciones:

1.- No utilizar la información en beneficio propio o de terceras partes.
2.- Restringir el acceso a la información a terceras partes que no están autorizadas a conocerla.
3.- No publicar, difundir o divulgar la información total o parcialmente.
4.- No realizar copias de la información cuyo destino sea la disposición o entrega a terceras partes no autorizadas.

5.- La información debe ser dispuesta y gestionada en condiciones seguras y deben atenderse todos los lineamientos y políticas de seguridad de la información con el propósito de garantizar la confidencialidad, disponibilidad e integridad.
6.- Realizar seguimiento y reportar los eventos maliciosos o accidentales que afecten la seguridad de la información.
7.- Cumplir con los lineamientos y políticas de seguridad de la información establecida en los procesos de la Institución.
8.- Los datos de acceso a las diferentes aplicaciones, bases de datos y plataformas de la institución deben manejarse con estricta confidencialidad. Estos datos de acceso son intransferibles.
9.- Al finalizar el contrato o funciones del cargo, el suscrito debe entregar los recursos y activos de información.

Observaciones y especificaciones:

El presente **Acuerdo de Confidencialidad** aplica y se suscribe para la administración de la **Base de Datos del Aseguramiento** y la **Información Confidencial que** incluye **toda la información almacenada en la base de datos, código fuente, los datos de acceso asignados y listados de contactos.**

Firma: _____

Nombre Completo:
Tipo y número de Documento:
Fecha de Firma:

ANEXO D. IDENTIFICACIÓN DE VULNERABILIDADES Y PRUEBAS DE PENETRACIÓN

Este anexo presenta los resultados del escaneo de vulnerabilidades y pruebas de penetración ejecutadas sobre el servidor de base de datos, el servidor web y las herramientas web de administración de la base de datos. Se ejecutó un plan de pruebas de penetración que desarrolla las siguientes fases:

- Planeación: Se define el objetivo, alcance, recursos y responsable de la actividad.
- Descubrimiento: Escaneo de vulnerabilidades en los servidores web, de base de datos y herramientas web de administración.
- Pruebas de penetración: Realización de pruebas básicas de penetración con nivel de riesgo bajo.
- Reporte y recomendaciones.

1.- PLANEACIÓN

1.1.- Objetivo: Efectuar un escaneo de vulnerabilidades y pruebas de penetración con nivel de riesgo bajo a los recursos tecnológicos que soportan la operación de la Base de Datos del Aseguramiento en el Ambiente de Producción.

1.2.- Alcance: Esta actividad explora las vulnerabilidades de los siguientes recursos en el Ambiente de Producción:

- Servidor web
- Servidor de base de datos
- Herramientas web de administración de la base de datos

1.3.- Recursos: se emplean activamente las siguientes herramientas de seguridad informática incluidas en la distribución Kali Linux[34].

- Nmap[35]

[34] KALI Linux. Official Kali Linux Documentation. [en línea]. 2019. Disponible en: https://www.kali.org/kali-linux-documentation/
[35] LYON, Gordon. Guía de referencia de Nmap. [en línea]. 2019. Disponible en: https://nmap.org/man/es

- OWASP ZAP[36]
- SQLmap [37]

1.4.- Fechas de ejecución: 25 y 26 de abril de 2019.

1.5.- Responsable: Derian Jesús Dorado Daza

1.6.- Observaciones: En las capturas de pantalla presentadas se han ocultado deliberadamente direcciones IP y dominios por razones de seguridad.

2.- DESCUBRIMIENTO

Descripción: Esta actividad consiste en el escaneo de puertos en los servidores web y de base de datos empleando distintas opciones de la herramienta Nmap, con el propósito de Identificar los puertos abiertos y debilidades de seguridad en los servidores. Por otro lado, también se realiza un escaneo sobre las aplicaciones web que apoyan la administración de la Base de Datos del Aseguramiento.

Ejecución:

Objetivo # 1: Servidor Web

Herramienta: Nmap

Comando: **nmap -sV -T4 -O -F -Pn --version-light "IP del servidor"**

- sV: Esta opción permite realizar un escaneo básico sobre los puertos estándar y respectivos servicios asociados con información sobre las versiones.

- T4: Este comando permite un escaneo con una duración de nivel 4; en la escala de 0 a 5, el nivel T5 es el más rápido.

- Pm: Impide que Nmap ejecute ping al servidor que está siendo examinado. Esto permite evadir posibles cortafuegos o Sistemas de Detección de Intrusos (IDS) que impidan el escaneo con ping inicial al servidor.

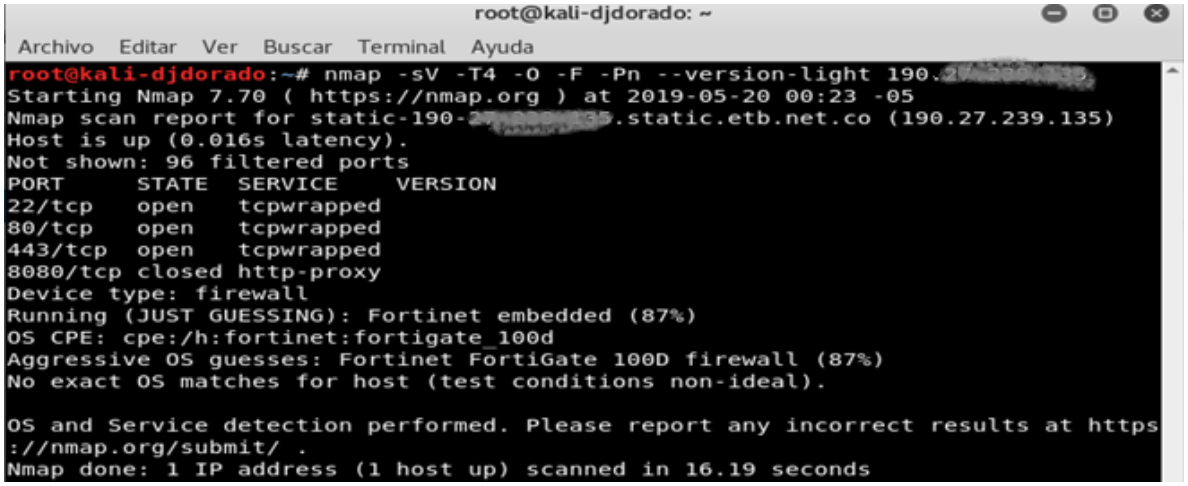
- f: Esta opción permite la fragmentación de los paquetes enviados al servidor. Esto permite camuflar los paquetes de escaneo en componentes más pequeños que posiblemente no sean sospechosos ante un cortafuegos o IDS.

[36] OWASP. OWASP ZAP 2.6 Getting Started Guide. [en línea]. 2019. Disponible en: https://github.com/zaproxy/zaproxy/releases/download/2.6.0/ZAPGettingStartedGuide-2.6.pdf .
[37] DAMELE, B. & STAMPAR, M. Sqlmap Features. [en línea]. 2019. https://github.com/sqlmapproject/sqlmap/wiki/Features .

-- versión-light: Script incluido en las funcionalidades de Nmap que permite un escaneo con nivel de intensidad 2 para la detección de información detallada sobre las versiones de los servicios encontrados.

Resultado:

Figura 12. Puertos abiertos en el servidor web



Fuente: Autor.

Puertos y servicios identificados:

- SFTP - puerto 22
- HTTP - puerto 80
- HTTPS - puerto 443
- HTTP - puerto 8080
- Se identifica un cortafuegos Fortinet

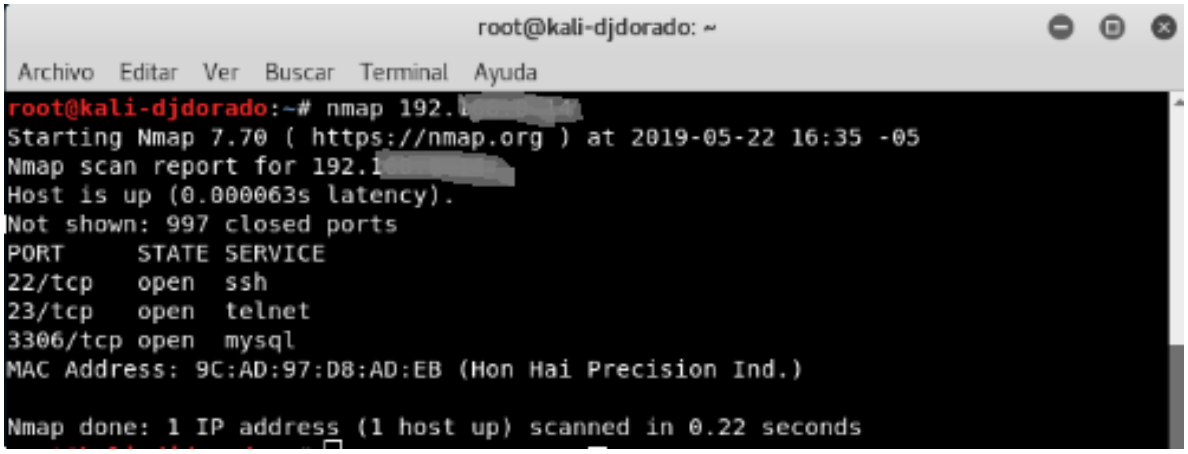
Objetivo # 2: Servidor de base de datos

Herramienta: Nmap

Comando: **nmap “IP del servidor”**

Resultado:

Figura 13. Puertos abiertos en el servidor de base de datos



Fuente: Autor.

Puertos y servicios identificados:

- SFTP - puerto 22
- Telnet - puerto 23
- MySQL - puerto 3306

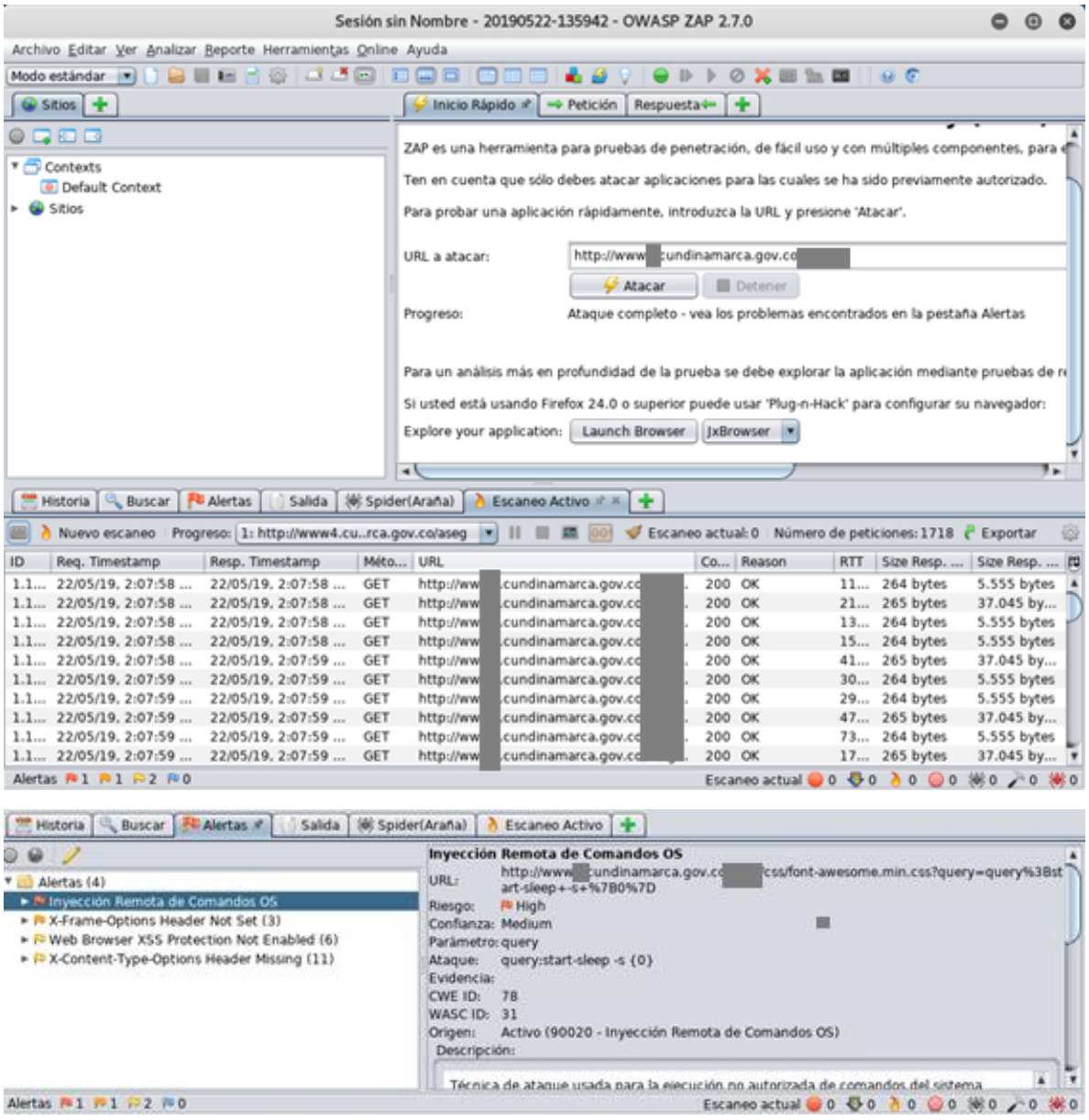
Objetivo # 3: Herramientas web de administración

Herramienta: OWASP ZAP

URL: Sitio web con aplicaciones web de administración

Resultado:

Figura 14. Resultado de vulnerabilidades en herramientas web



Fuente: Autor.

Se identifican las siguientes vulnerabilidades y respectivo nivel de riesgo:

- 1 Vulnerabilidad de riego Alto relacionada con la posibilidad de inyección de comandos de Sistema Operativo.

- 3 Vulnerabilidades de riesgo Medio relacionadas con la configuración de las Opciones del encabezado X-frame para que la página web no pueda ser embebida en marcos desde otro sitio web.

- 6 Vulnerabilidades de riesgo Bajo relacionadas con la protección para que no pueda realizarse ataques de sitio cruzado XSS.

- 11 vulnerabilidades de riesgo Bajo relacionadas con la configuración de las opciones del encabezado X-content-Type para que los datos bajo las etiquetas Content-Type no puedan ser cambiados ni capturados.

3.- Pruebas de penetración

Descripción: A partir de la información sobre puertos y servicios abiertos en los servidores, en esta actividad se realizan pruebas básicas de penetración con base en la herramienta SQLMap.

Ejecución:

Objetivo #1: Base de datos a través de la aplicación web de administración

Herramienta: SQLMap

Comando: **sqlmap -u 'URL'?id=1 --random-agent --tamper=space2comment --tables**

-u: especifica la URL de la aplicación web.

id=1: Parámetro a inyectar para obtener información de la base de datos.

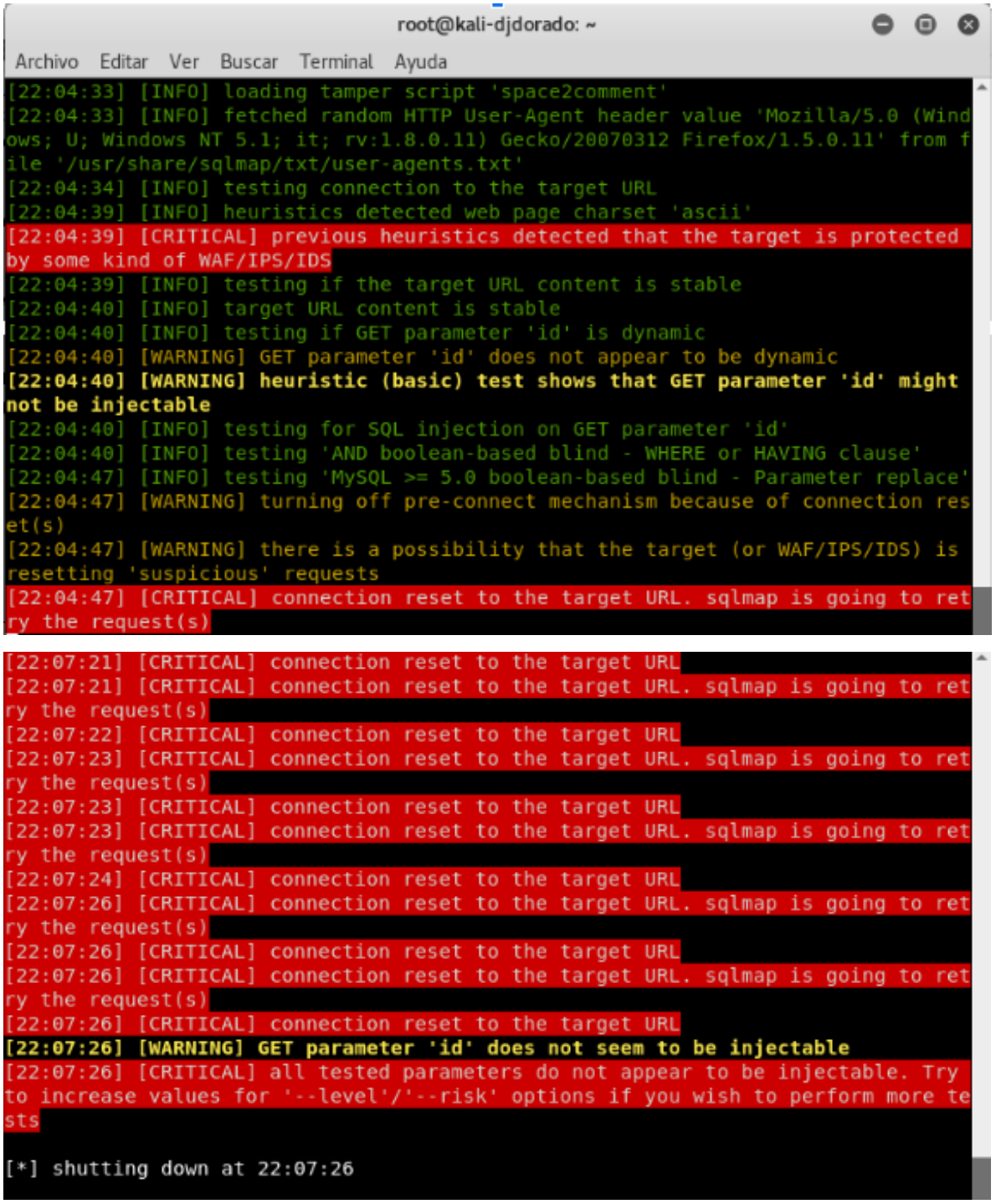
-- random-agent: opción que permite sustituir de manera aleatoria los encabezados de las peticiones http al servidor (generalmente SQLMap se identifica como sqlmap/1.0-dev-xxxxxxx (http://sqlmap.org). Esto brinda la posibilidad de evadir algunas reglas del cortafuegos identificado.

tamper=space2comment: A modo de prueba se experimenta con este script que permite sustituir caracteres de espacio en las consultas para tratar de evadir las reglas del cortafuegos identificado.

--tables: De resultar inyectable el parámetro, esta opción permitirá obtener la información de las tablas presentes en la base de datos.

Resultado:

Figura 15. Resultado de prueba con SQLmap



Fuente: Autor.

Se observa la acción constante del cortafuegos que dificulta la acción de SQLMap. Luego de varios intentos de establecimiento de la conexión y ejecución de la prueba, la herramienta informa que no es posible la inyección del parámetro.

4.- REPORTE Y RECOMENDACIONES

A continuación, se mencionan a modo ejecutivo los principales resultados:

- Las pruebas básicas ejecutadas indican que los recursos tecnológicos que soportan la Base de Datos del Aseguramiento en el Ambiente de Producción no presentan vulnerabilidades críticas que puedan ser explotadas con facilidad.

- Se observa la importancia y acción efectiva del cortafuegos instalado en la red corporativa de la Gobernación de Cundinamarca.

- Las herramientas de escaneo y penetración empleadas, así como las demás disponibles en la distribución Kali Linux, constituyen un verdadero arsenal para la evaluación constante de la seguridad informática sobre los recursos tecnológicos que soportan la operación de la Base de Datos del Aseguramiento.

A continuación, algunas recomendaciones:

- Es necesario realizar pruebas de escaneo con NMAP sobre el Ambiente de Desarrollo empleando opciones de mayor complejidad. Se recomienda el uso de los siguientes scripts disponibles en Nmap: **`Auth, Discovery, Intrusive, Malware, Vuln, All`**. Esta actividad posiblemente brinde resultados que apliquen sobre los Ambientes de Pre-producción y Producción.

- Se recomienda establecer los encabezados X-frame al siguiente valor: **`X-Frame-Options: DENY`**

- Se recomienda establecer los encabezados X-content-Type al siguiente valor: **`X-Content-Type-Options: nosniff`**

- Se recomienda sanear los formularios web mediante validaciones estrictas que impidan el uso de caracteres y palabras especiales. Las validaciones pueden realizarse mediante la elaboración de una lista prohibida contra la cual pueda verificarse la seguridad de la petición.

También es recomendable sanear la conformación de la URL y parámetros posteriores mediante la inclusión de reglas estrictas en el archivo **htaccess** del sitio web que aloja las aplicaciones de administración de la Base de Datos del Aseguramiento.

Los caracteres especiales prohibidos pueden ser los siguientes:

| ; & $ >< ' / \ ! >> # ( ) * = ? ; [ ] ^ ~ ! . ” % @ /
: + , ` { } –

Estas medidas de seguridad contribuyen a disminuir el riesgo de inyección de comandos de sistema operativo y código SQL.

- Se recomienda realizar pruebas de penetración con SQLmap sobre el Ambiente de Desarrollo empleando opciones de mayor nivel de complejidad (**level=5**) y riesgo (**risk=3**). Adicionalmente se recomienda el uso de diferentes **tampers** disponibles para evasión del cortafuegos y aplicación de lógica más compleja en las sentencias SQL de ataque. Esta actividad posiblemente brinde resultados que apliquen sobre los Ambientes de Pre-producción y Producción.

- Se recomienda el establecimiento de una regla en el cortafuegos que impida el escaneo y ataque desde el interior de la red corporativa.