ANÁLISIS DE LOS PRINCIPALES RIESGOS DE SEGURIDAD ASOCIADOS A LA BASE DE DATOS TERRIDATA (DNP)

LITO ALEXANDER GUEVARA PARRA

UNIVERSIDAD SANTO TOMÁS

FACULTAD DE INGENIERÍA

INGENIERÍA DE TELECOMUNICACIONES

BOGOTÁ D.C

2021

ANÁLISIS DE LOS PRINCIPALES RIESGOS DE SEGURIDAD ASOCIADOS A LA BASE DE DATOS TERRIDATA (DNP)

Presentado por:

LITO ALEXANDER GUEVARA PARRA

CÓDIGO: 2209792

Trabajo opción de grado Pasantías en el Departamento Nacional de Planeación.

Director: MSc. JULIANA ALEJANDRA ARÉVALO HERRERA

UNIVERSIDAD SANTO TOMÁS

FACULTAD DE INGENIERÍA

INGENIERÍA DE TELECOMUNICACIONES

BOGOTÁ D.C

2021

RECTOR GENERAL
Padre José Gabriel Mesa Angulo, O.P.

VICERRECTOR ADMINISTRATIVO Y FINANCIERO GENERAL
Padre, Wilson Mendoza Rivera, O.P.

VICERRECTOR ACADÉMICO GENERAL
P. Eduardo Gonzáles Gil, O.P.

SECRETARIA GENERAL
Abog. Ingrid Lorena Campos Vargas

SECRETARIA DE DIVISIÓN
E. C. Luz Patricia Rocha Caicedo

DECANO FACULTAD DE INGENIERÍA DE TELECOMUNICACIONES
Ingeniero Germán Macías Muñoz

Nota de Aceptación.

_____
_____
_____
_____

_____
Firma Ingeniero. JULIANA ALEJANDRA ARÉVALO HERRERA
Tutor Asignado

_____
Firma del Jurado

_____
Firma del Jurado

_____
Fecha

AGRADECIMIENTOS

En primer lugar, quiero realizar un especial agradecimiento a mi tutora Juliana Alejandra Arévalo Herrera, quien me ha guiado a lo largo de la creación de esta monografía y quien constituyó una parte fundamental de mi carrera y gusto por la misma gracias a su gran manera de enseñar. Así mismo al profesor Julio Cesar Pulido Mora, que, sin duda, me enseñó a darle la importancia que merece cada detalle de un trabajo y lo que hacer las cosas correctamente puede significar para la vida. También quiero agradecer a mi familia, quienes son mi más grande apoyo y motivación para estudiar y terminar este proceso. Finalmente, quiero agradecer a las personas que siempre creyeron en mí, me motivaron, ayudaron y apoyaron para llegar a este punto.

Tabla de contenido

Lista de figuras

Lista de tablas

Lista de anexos

Resumen ejecutivo

Con el objetivo de determinar los posibles riesgos de seguridad asociados a la Base de datos Terridata del Departamento Nacional de Planeación (DNP) y teniendo en cuenta su implementación, se realiza un estudio de la misma con sus principales características. Así mismo, se maneja una metodología que contribuye en la detección y el entendimiento de estos riesgos. Para lograr este fin, se identifican las características principales para el entendimiento de las Base de datos. De la misma manera, que se realiza una revisión de las metodologías de auditoría de seguridad de Base de datos, y se generan recomendaciones para dar solución y prevenir los riesgos encontrados.

Marco referencial

Introducción

A través de este trabajo de grado se pretende realizar un análisis de los riesgos de seguridad asociados a la Base de datos Terridata del Departamento Nacional de Planeación (DNP), así como una revisión a la página web desde la cual se tiene acceso a la Base de datos, dado que es donde se realiza la implementación y puede configurarse como un gran riesgo de seguridad.

Hoy en día la seguridad de la información es considerada una de las principales prioridades para cualquier empresa, dado que esta constituye la principal ventaja competitiva que pueda otorgarles en el mercado. Así mismo, la información representa el recurso fundamental para cualquier entidad del estado al almacenar diferente información necesaria para el correcto planteamiento de planes o distribución de recursos.

En este sentido, Terridata se constituye como una Base de datos referencial desde la cual se puede acceder a la información relacionada con cada aspecto relacionado a cualquier región del País, por lo cual adquiere gran importancia el mantenimiento de la seguridad e integridad de la misma. De esta forma, en el presente trabajo se plantean los riesgos asociados a su diseño, mantenimiento e implementación, para finalmente realizar recomendaciones que permitan generar una mejoría en la seguridad de la información que esta contiene al mitigar las posibles eventualidades a través de diferentes planes de acción.

Planteamiento del problema

La información se ha convertido en el recurso más importante de cualquier compañía, dado que esta contiene todas las características y ventajas competitivas de las mismas. Con el tiempo y la evolución de las tecnologías tanto para obtenerla como para almacenarla, dicha información ha venido creciendo de manera exponencial haciendo necesaria una gestión de la información más eficiente y sobre todo segura.

El Departamento Nacional de Planeación establece sus políticas de seguridad teniendo en cuenta el estándar ISO27000, por lo cual la información debe seguir lineamientos claros para su mantenimiento, seguridad y control, por lo cual se hace necesario identificar y establecer controles de riesgos y seguridad de la información para Terridata.

En el caso del DNP se usa como Gestor de Base de datos para su información Microsoft SQL server, herramienta en la cual se centrará este trabajo, y dada la importancia de la información que maneja, se hace especialmente provechoso realizar una auditoría al funcionamiento de la Base de datos donde se encuentra gran parte de la información que posee la entidad para realizar y compartir los datos que posee.

Este trabajo responde a la necesidad de mantener segura y confiable la información alojada en Terridata, teniendo en cuenta los potenciales riesgos de seguridad, integridad y confidencialidad de la Base de datos con el fin de mitigar el posible impacto de los mismos, teniendo en cuenta el estándar ISO27002 y las buenas prácticas presentadas por el Gestor de Base de datos. Por otra parte, la seguridad de la Base de datos debe complementarse con la página web de Terridata, desde la cual se accede a los datos alojados en ella.

Justificación

Dada la importancia de las Base de datos, es de fundamental importancia mantener segura la información para mantenerla dentro de los estándares de seguridad del DNP (ISO27002:2013). Para cumplir este propósito se dispone de algunas herramientas provistas por los mismos gestores de Base de datos que permiten mediante distintos niveles asegurar los datos almacenados y gestionados a través de estos, Lo anterior se justifica teniendo en cuenta los riesgos que implican un fallo de seguridad para la Base de datos en diferentes aspectos para el DNP, derivando en un coste elevado en el mantenimiento de la Base de datos, pérdida de confianza en la institución y los incumplimientos de los estándares y normas de seguridad de la información.

El Departamento Nacional de Planeación es la entidad del gobierno encargada de gestionar el Plan Nacional de Desarrollo, su integración y cumplimiento a lo largo del periodo presidencial, del mismo modo, se encarga de verificar el cumplimiento de los planes municipales y de las distintas ciudades haciendo estudios sobre el impacto que tienen las políticas de desarrollo en cada uno.

Por otra parte, la plataforma Terridata posee indicadores de desarrollo propios de cada entidad territorial en el país, por lo cual es consultado desde cada una de las gobernaciones correspondientes para cargar la información relacionada al cumplimiento de dichos indicadores.

Alcance

Se analizará la Base de datos Terridata del DNP y se realizará una revisión de la página web desde donde se tiene acceso a los datos para establecer los riesgos de seguridad relacionados tanto con la Base de datos como con la página web.

Limitaciones

Se realiza el análisis sobre un Backup de la Base de datos generado en marzo de 2021, por lo cual no se tienen en cuenta cambios desde esa fecha.

Dada la confidencialidad de la información del DNP, la información sobre la implementación de la Base de datos y su mantenimiento se encuentra incompleta.

No existe una documentación definida donde se establezca la gestión de la Base de datos.

Objetivo general

Analizar los riesgos asociados a la Base de datos Terridata, del DNP, para generar recomendaciones que disminuyan su posible impacto, ya sea de disponibilidad, integridad y confidencialidad de la información.

Objetivos específicos

- Identificar las características y conceptos principales para el funcionamiento y entendimiento de las Base de datos.
- Realizar una revisión de las metodologías de auditoría de seguridad de Base de datos y su aplicación con el objetivo de aplicarla a Terridata.
- Realizar un levantamiento de información técnica y de uso de la Base de datos Terridata con el fin de entender su funcionamiento.
- Establecer los riesgos relacionados a la Base de datos Terridata del DNP e identificar los elementos susceptibles de mejora.
- Establecer los riesgos relacionados a la página web donde se encuentra implementada la Base de datos e identificar los elementos susceptibles de mejora.
- Generar recomendaciones de seguridad sobre Terridata con el fin de prevenir y mitigar posibles riesgos relacionados con la seguridad de la información.

Metodología

Para la elaboración y desarrollo del presente trabajo, se tiene en cuenta una metodología de investigación cuantitativa, desde la cual se recopila información relevante que permita determinar una serie de recomendaciones sobre seguridad e integridad de la Base de datos. La recolección de la información técnica se realizó mediante el gestor de Base de datos usado para Terridata (Microsoft SQL Server) y la herramienta Lighthouse del navegador Opera GX. Por otra parte, la información recopilada en este trabajo es obtenida desde el Grupo de Estudios Territoriales (GET) para su utilización en este trabajo, además de una revisión bibliográfica sobre los temas propuestos.

Teniendo esto presente, el objetivo de esta investigación es contribuir en la detección y el entendimiento de los diferentes riesgos que puede tener una Base de datos, específicamente Terridata.

Para empezar, se identifican las características principales para el entendimiento de las Base de datos y específicamente de Microsoft SQL Server, se realiza una revisión de las metodologías de auditoría de seguridad de Base de datos y se generan recomendaciones para dar solución y prevenir los riesgos encontrados.

Cronograma

A continuación (figura 1), se presenta el cronograma de actividades realizado para el desarrollo del proyecto mediante un diagrama de Gantt elaborado en Microsoft Project con las fechas correspondientes.

Tabla 1
Cronograma

Nombre de tarea	Duración	Comienzo	Fin	Predecesoras
Cronograma	2 días	lun 15/02/21	mar 16/02/21	
Marco referencial	15 días	mié 17/02/21	mar 9/03/21	1
Estado actual del tema	20 días	mié 10/03/21	mar 6/04/21	2
Revisión metodologías para auditoria en BD	15 días	mié 7/04/21	mar 27/04/21	3
Levantamiento de informacion	60 días	mié 17/02/21	mar 11/05/21	1
Análisis BD Terridata	30 días	mié 12/05/21	mar 22/06/21	5
Análisis de riesgos	11 días	mié 23/06/21	mié 7/07/21	6
Resultados y recomendaciones	6 días	jue 8/07/21	jue 15/07/21	7
Conclusiones	3 días	vie 16/07/21	mar 20/07/21	8
Correcciones Preentrega	20 días	mié 21/07/21	mar 17/08/21	9
Correcciones Pos-entrega	25 días	mié 18/08/21	mar 21/09/21	10

Figura 1
Diagrama de Gantt

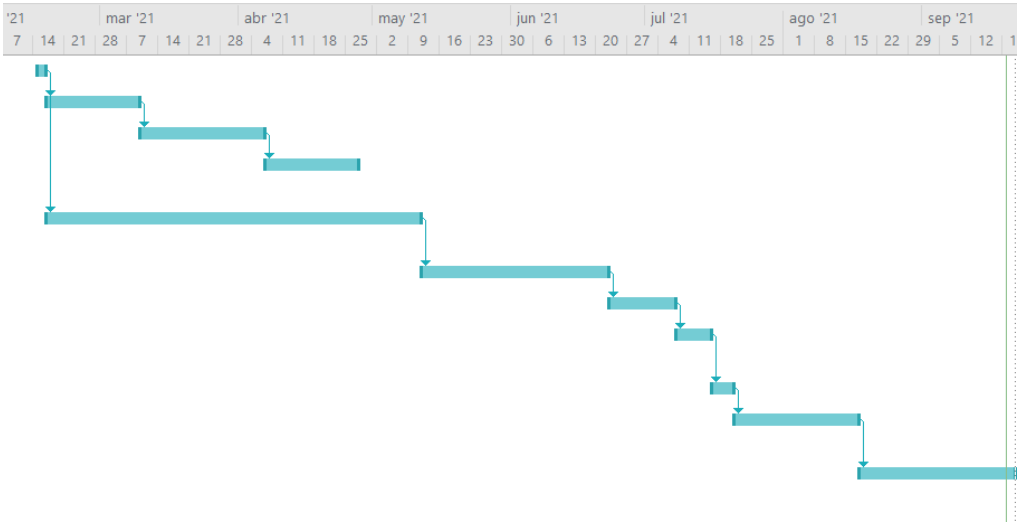
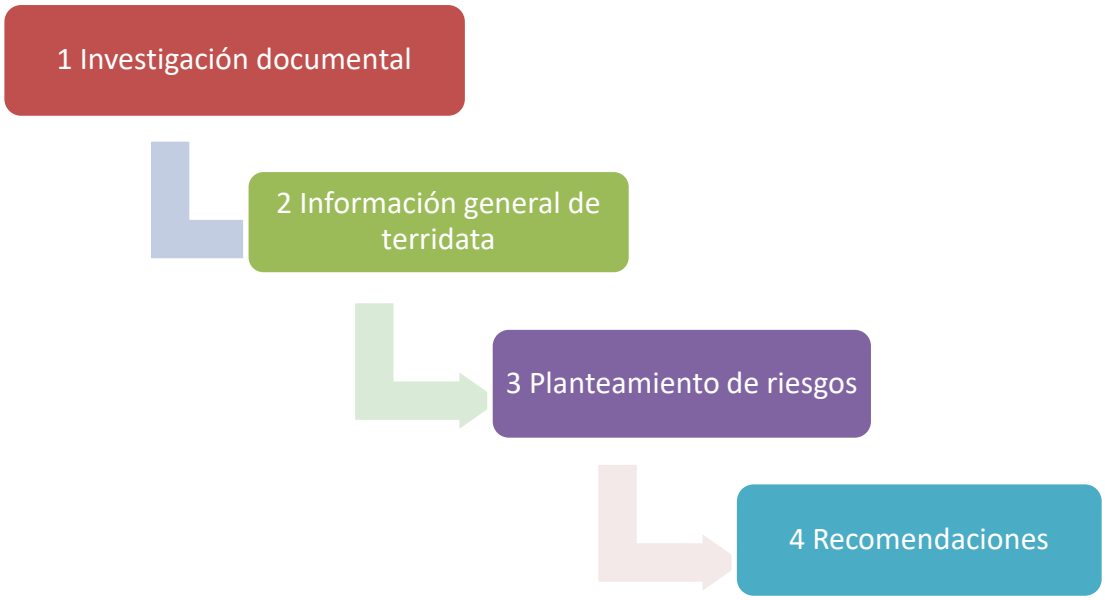


Figura 2
Metodología



La metodología se plantea en cuatro fases que abarcan todo el proceso de la elaboración del trabajo, estas fases se plantean en la figura 2 y corresponden al siguiente orden:

1. Investigación documental.
2. Información general Terridata
3. Planteamiento de riesgos
4. Recomendaciones

Estado Actual del tema

Con el objetivo de entender el funcionamiento de las Base de datos, se deben tener en cuenta algunos conceptos clave que permiten conocer cómo trabajan y se estructuran las Base de datos. A continuación, se presentan dichos conceptos tomando como referencia el libro *Consulta de SQL, Volumen 1* de IBM e información recopilada desde la web de Oracle e IBM.

Base de datos relacionales

Este tipo de Base de datos tienen como característica principal la relación entre los accesos a puntos, esto quiere decir que, en estas Base de datos, cada fila posee un registro único denominado clave; los datos almacenados también poseen atributos registrados en las columnas, por lo tanto, existe también un valor para cada uno de estos atributos. Esta manera de organizar la información permite generar las relaciones entre los datos.

Estructura

Las Base de datos relacionales poseen estructuras lógicas de datos, de tal manera que estas se separan de las estructuras físicas necesarias para el almacenamiento. De tal manera, se les permite a los gestores administrar el aspecto físico de la Base de datos sin afectar el uso de la Base de datos como una estructura lógica.

Mediante dicha separación, se permite realizar operaciones en la Base de datos, haciendo énfasis en el aspecto a tener en cuenta para modificar sin afectar el otro, ya sea físico o lógico, las Base de datos relacionales permiten a las aplicaciones modificar los datos de manera lógica. Por otro lado, en el aspecto físico se determina la manera de acceder a los mismos.

Otro punto importante a tener en cuenta es la integridad de la información en las Base de datos, esto significa que las Base de datos relacionales deben seguir reglas que garanticen dicha integridad.

Base de datos relacional distribuida

En este tipo de Base de datos cada conjunto de tablas están distribuidos en diferentes sistemas que están conectados entre sí. De tal manera que, cada uno de ellos tiene un gestor propio para manejar sus tablas asociadas, dichos gestores permiten realizar comandos entre ellos y así mismo, entre los diferentes sistemas.

Base de datos relacional particionada

Estas Base de datos se gestionan separando los datos en distintas particiones, de tal manera que su gestión se basa en el manejo de dichas particiones, lo que significa que para el usuario el manejo entre sentencias SQL entre las diferentes particiones se efectúa de una forma transparente, permitiendo, sin embargo, hacer una distinción en algunas ocasiones entre los grupos de particiones a través de comandos específicos.

Tablas

En una Base de datos relacional, las tablas corresponden a estructuras de carácter lógico conformadas por filas y columnas, donde a la unión de las mismas se le denomina valor. Teniendo esto en cuenta, tanto filas como columnas poseen ciertas características en común. Por ejemplo, en el caso de las columnas, estas comparten valores de un mismo tipo; mientras que la fila corresponde a la secuencia de valores de manera ordenada en relación a la columna relacionada.

Claves

En las Base de datos relacionales puede existir relación entre distintas tablas, para generar dicha relación se presenta el concepto de claves (keys). Existen 2 tipos de claves conocidas como primarias y foráneas. Dichas claves corresponden a la unión de tablas para realizar consultas y obtener información de relaciones entre las mismas.

Claves primarias

Corresponden a una columna cuyo valor es único en la tabla e identifica a una sola fila dentro de esta. Dentro de las Base de datos relacionales, la regla impone dicha característica con el objetivo de mantener de mejor manera la integridad de las tablas permitiendo solo una fila a una clave primaria.

Claves foráneas

Estas claves corresponden al valor de las claves primarias obtenidas de otras tablas, de esta manera se permite añadir a una tabla los valores de dichas tablas manteniendo siempre el orden de los datos.

Modelo relacional

Este modelo es usado para representar la manera en la que se relacionan distintos datos entre sí, a través de distintos componentes. Este modelo posee varios elementos que lo conforman, estos son: Entidades, atributos, relaciones, cardinalidad, tupla y claves.

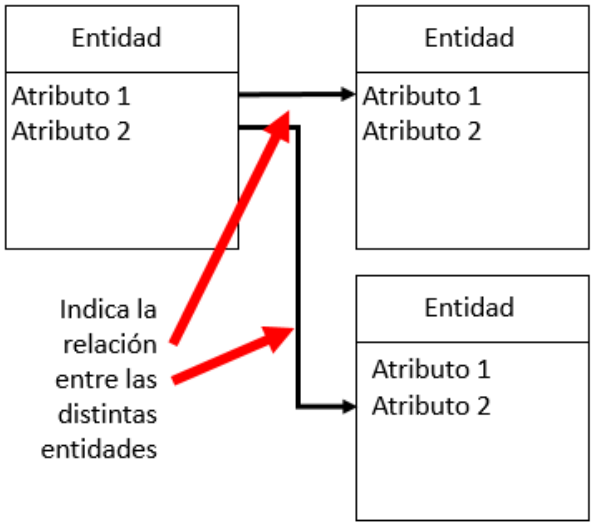
- Entidades: corresponden a cada componente en si, por ejemplo, en una Base de datos podría corresponder a los datos de un cliente.

- Atributos: Los atributos en el modelo entidad relación, describen las propiedades de las entidades, por ejemplo, en el caso anterior, corresponderían al nombre, apellidos, dirección, etc.

- Relaciones: Las relaciones determinan la manera en la que se unen las distintas entidades, por ejemplo, determinarían que cada cliente debe tener asociada otra entidad como puede serlo una factura o un servicio.
- Cardinalidad: Corresponde al número de columnas y campos de la tabla.
- Tupla: Es un registro donde se representan las filas y columnas de la Base de datos como un campo.
- Claves: Corresponden al identificador único de cada tabla.

Existe una manera gráfica de representar el modelo relacional. A través de él es posible identificar de manera gráfica y sencilla tanto las entidades, como sus atributos y los tipos de relaciones entre las diferentes entidades. A continuación, se muestra un ejemplo de este diagrama.

Figura 3
Diagrama relacional



Cabe resaltar que existen varias relaciones entre diferentes entidades como lo son: la relación uno a uno, donde un dato de una entidad solo puede estar relacionado con otro de una entidad distinta; la relación uno a varios, donde un dato de una entidad puede estar relacionado a varios de otra entidad y finalmente la relación varios a varios, donde varios datos de una entidad pueden estar relacionados con varios de otra.

Gestores de Base de datos

Un sistema Gestor de Base de datos permite la creación y administración de Base de datos, permitiendo realizar distintos tipos de operaciones controladas por los usuarios a través de un lenguaje de definición de datos, manipulación y consulta.

Microsoft SQL Server

Es un sistema que permite la administración de Base de datos relacionales, Microsoft SQL Server tiene como característica principal que cada componente del mismo posee seguridad individual y separada del resto de componentes. Del mismo modo, este sistema está pensado para proveer servicio a distintas aplicaciones que pueden comunicarse con el mismo a nivel local o remoto a través de internet. Sumado a esto, es un servidor que provee una alta disponibilidad, además de eficiencia al gestionar adecuadamente los recursos de memoria.

MySQL

MySQL es un Gestor de Base de datos relacional de código abierto desarrollado en conjunto por Oracle. Este gestor tiene como características el uso de un lenguaje de SQL extendido, un amplio soporte en diferentes sistemas y plataformas, conectividad segura y replicación, entre otras. Además, posee características únicas para este gestor como la

posible elección entre distintos motores de almacenamiento o agrupación de transacciones, permitiendo incrementar el número de transacciones por segundo.

Oracle

Oracle es el Gestor de Base de datos de tipo objeto-relacional más robusto del mercado, posee como principales características el soporte de transacciones, la estabilidad y la escalabilidad, además de ofrecer gran soporte y compatibilidad con cualquier posible implementación para las Base de datos. Además de estar relacionado con MySQL al colaborar en la creación del mismo.

Seguridad en las Base de datos

Dentro de las Base de datos la gestión de la seguridad cumple un rol primordial para mantener la integridad de los datos, es por ello que existe una gran cantidad de métodos que intentan asegurar dicha información, pasando desde la encriptación de los datos, hasta la misma seguridad física del lugar donde se encuentren los servidores.

Teniendo esto en cuenta, SQL server posee varias capas que permiten proteger las comunicaciones y los datos propios de la Base de datos. En una primera capa, a través del protocolo TLS o SSL se cifra la información con el fin de mantenerla a salvo hasta llegar a la API de Windows

Mediante la API de protección de datos de Windows (DPAPI – Data Protección API) se cifran y descifran los datos, siendo este algoritmo de cifrado diferente en cada servidor. Por otra parte, se encuentran las instancias de seguridad como el usuario, la contraseña y los certificados. Sumado a la API de Windows, SQL server posee una clave de cifrado creada en el primer inicio de la aplicación, cabe resaltar que el usuario no puede crear dicha

clave, solo puede realizar una copia de seguridad de la misma para su posterior restauración en caso de ser necesario.

SQL server se ejecuta como un servicio de Windows, de tal manera que este se encuentra ligado a la sesión en el sistema operativo y a la seguridad asociada a ella, por lo cual se requiere una cuenta de servicio para acceder a los privilegios de seguridad.

Algoritmos de cifrado de SQL server

SQL server posee diferentes algoritmos que varían en función de las claves de cifrado, de tal manera que soporta una serie de algoritmos distintos como AES en sus diferentes versiones, DES, MD5, SHA2 y RC4.

Es posible encriptar toda la Base de datos para evitar que la información se vea comprometida en caso de un robo. SQL server posee una función llamada 'Cifrado transparente de la Base de datos' que se ejecuta solo en el momento de leer y escribir los datos en el disco.

SSL en SQL Server

El protocolo SSL (Secure Sockets Layer) es una tecnología que permite asegurar una comunicación protegiendo la información enviada a través de internet. Para lograr esto, el protocolo cifra la información para codificar los datos que son enviados por la Base de datos.

SQL server realiza la transferencia de datos mediante el protocolo TDS (Tabular Data Stream), un protocolo correspondiente a la capa de aplicación usado específicamente para las Base de datos relacionales de Microsoft. Dicho protocolo de comunicación no se encuentra cifrado, de manera que, al realizar la transferencia de información, este es cifrado

mediante SSL para proteger los datos. Por otra parte, el protocolo SSL necesita un certificado autorizado con el objetivo de reforzar aún más su seguridad.

Puertos usados por SQL Server

SQL server usa una serie de puertos para realizar sus comunicaciones, estos puertos deben estar correctamente configurados de manera que sea posible controlar la información que entra y sale de la Base de datos. Así mismo, es necesario realizar un monitoreo de los mismos para garantizar su seguridad. Dichos puertos se muestran en la siguiente tabla.

Tabla 2
Puertos SQL server

TIPO DE PUERTO	PUERTO	DESCRIPCIÓN
TCP	1433	Motor de Base de datos
UDP	1434	Navegador
TCP	2383	Analysis Services
TCP	4022	Service Broker

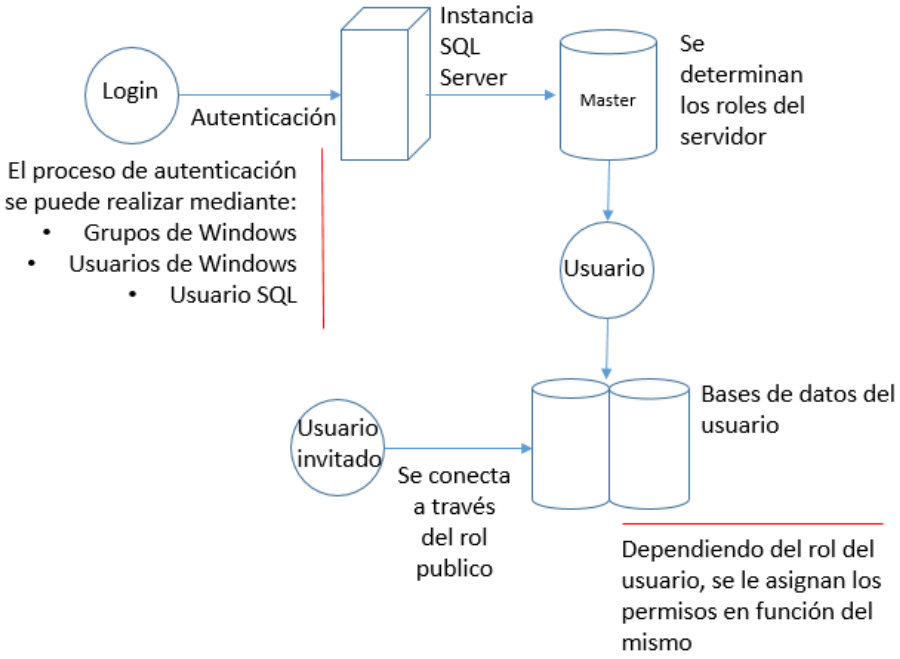
Autenticación

Existen 3 métodos de autenticación en SQL server, estos son mediante el usuario de Windows, a través del grupo de usuarios de Windows o mediante un usuario especifico de SQL Server.

Una vez el usuario es identificado, SQL Server le asigna los correspondientes derechos administrativos a través de los roles del servidor en función del nivel del usuario, esto significa que, dependiendo del rol, puede tener mayor o menor acceso a ciertas características de la Base de datos.

A continuación, se muestra el modelo de seguridad usado en las Base de datos para realizar la autenticación de un usuario y la asignación de permisos provista por SQL Server para cada caso.

Figura 4
Autenticación SQL Server



Metodologías para auditoria en Base de datos

En el presente capitulo se presenta una revisión de distintas metodologías empleadas para la elaboración de auditorías para la seguridad de la información y Base de datos.

Dichas metodologías plantean los lineamientos que deben seguirse para la implementación de la auditoria, desde la planeación, pasando por las pruebas, hasta la generación de recomendaciones y buenas prácticas a emplearas.

ISO 27000

Este trabajo presenta un análisis de riesgos y recomendaciones complementado con los algunos de los lineamientos que correspondan dentro del estándar ISO 27000, el cual conforma el grupo de estándares relacionados a la gestión de la seguridad de la información, controles y buenas prácticas.

El conjunto de estándares de la serie 27000 soporta la implantación de un Sistemas de Gestión de Seguridad de la Información (SGSI) y posee información y controles para los Sistemas de Gestión de Seguridad de la Información, donde se encuentran los distintos pasos para generar y monitorear un SGSI. La serie 27000 se encuentra dividida de esta manera:

- ISO 27001: Corresponde a los requisitos para implementar un SGSI.
- ISO 27002: Proporciona estándares de seguridad de la información, controles y diversas prácticas de gestión tomando como base el riesgo asociado.

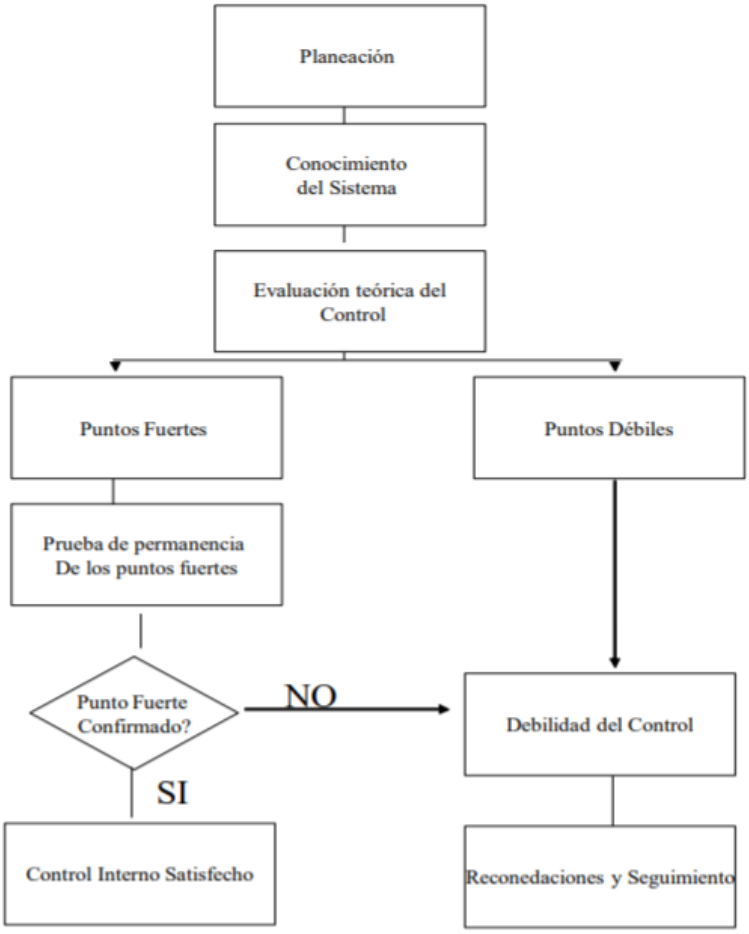
- ISO 27003: Presenta las directivas generales en la implementación de un Sistema de gestión de la seguridad de la información
- ISO 27004: Este estándar relaciona las métricas necesarias para la implementación de un sistema de gestión de la información con un la retroalimentación de los procesos.
- ISO 27005: Guía sobre cómo abordar la gestión de riesgos.
- ISO 27006: Conjunto de requisitos de acreditación.
- ISO 27007: guía para organismos de certificación acreditados en relación con la norma.

Guía de auditoria: seguridad y privacidad de la información MINTIC

Según MinTIC la auditoria debe evaluar la forma de manejo de la información y como esta se protege a través de los diferentes sistemas de información. Del mismo modo, califica la gestión realizada por el área de talento humano encargada de administrar dicho recurso.

Esta metodología tiene como objetivo principal “la verificación del sistema de información, su confiabilidad y el uso del mismo por parte de la entidad” (MinTIC, 2016). De esta manera, plantea un proceso diseñado para la auditoria. A continuación, se muestra dicho proceso.

Figura 5
Metodología para auditoria



Nota: Adaptado de MinTIC

Como se muestra en la figura anterior, el proceso de metodología parte de una planeación e identificación del sistema, con el fin de tener clara la operación que se va a realizar. A continuación, plantea una evaluación teórica donde se determinan los puntos fuertes y débiles del sistema, para finalizar con el seguimiento de los mismos.

Por otra parte, propone el uso de métricas que contribuyan a medir las propiedades del sistema a evaluar. Según IEEE las métricas se definen como “medida cuantitativa del grado en que un sistema, componente o proceso posee un atributo dado” y se dividen en métricas directas e indirectas.

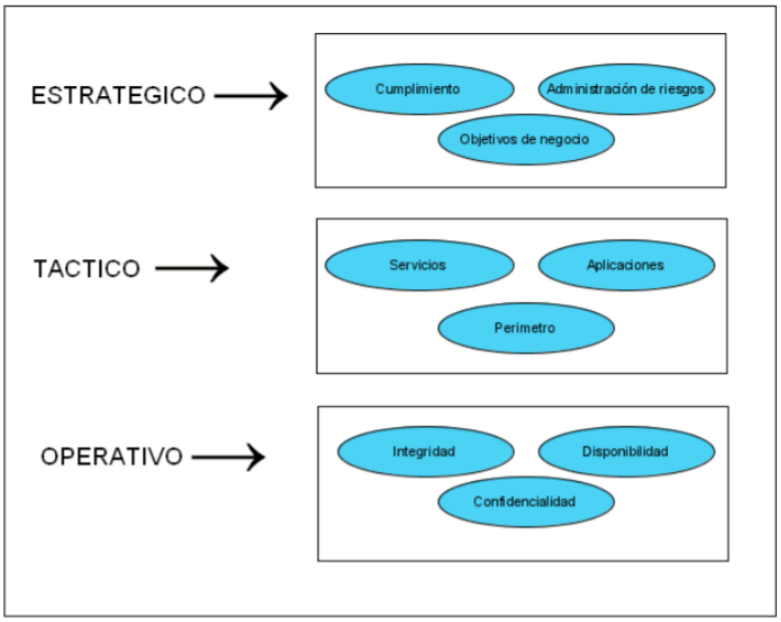
- “Métrica indirecta: en esta se centran en la calidad, complejidad, fiabilidad, eficiencia, funcionalidad, facilidad de mantenimiento, etc.

- Métrica directa: respecto a esta se engloba en velocidad de ejecución, defectos encontrados en una cantidad de tiempo, costo, tamaño de memoria usada, número de líneas de código, etc.” (MinTIC, 2016)

Métricas de seguridad

Estas métricas están diseñadas para auditar los procesos de seguridad, evaluando el grado de riesgo sobre el sistema. Con el objetivo de llevar esto a cabo, se presenta un modelo estratégico de las métricas respecto a la seguridad de la información (MEMSI). Dicho modelo se presenta a continuación.

Figura 6
MEMSI



Nota: Adaptado de MinTIC

En el nivel estratégico se encuentran las métricas encargadas de revisar los estándares, los controles relativos a los riesgos y la responsabilidad ante los posibles

incidentes que den lugar. Por otra parte, el nivel táctico se encarga de gestionar las métricas relativas al control de cambios, respaldos y fallos, así como las pruebas de vulnerabilidad y la efectividad de la seguridad. Finalmente, el nivel operativo, se encarga de la gestión de las medidas que se deben tomar para salvaguardar la información.

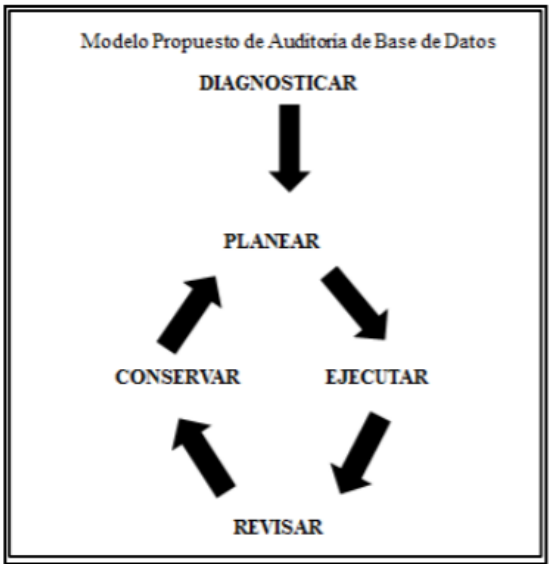
Auditoria de Base de datos fundamentada en Estándares y Buenas Prácticas

Es una metodología basada en algunos estándares del manejo de las tecnologías de la información, de manera que a través de los estándares se puede cumplir con los requisitos que garantizan la calidad de la auditoria.

> “La metodología se fundamenta en un modelo de 5 etapas tomando como referencia el círculo de Deming y adaptado al prototipo de madurez de COBIT considerando 5 niveles y su correspondiente ponderación. Los objetivos de control de ISO/IEC 27001-27002 se alinean a COBIT e ITIL y se utilizan como referente para definir los procesos propios de la auditoría de Base de datos. “ (Saucedo Mejía , Gutierrez Diaz de León, Ayala López, & Lozoya Arandia, 2014).

De esta manera se plantean varias etapas desde las cuales se pretenden lograr tareas específicas que en conjunto garantizan la fiabilidad de la auditoria. Como ser muestra en el siguiente diagrama.

Figura 7
Modelo de auditoria de Base de datos (estándares y buenas practicas)



Nota: Adaptado de Metodología para Auditar Base de datos fundamentada en Estándares y Buenas Prácticas (2014)

- Diagnosticar: Mediante esta etapa se pretende conocer el estado actual de la organización, así como sus políticas y las personas responsables de la gestión de la Base de datos.

- Planear: esta etapa corresponde a la identificación de aspectos de seguridad y controles de la información, de manera que al repetirse el ciclo disminuyan cada vez más las posibles problemáticas encontradas.

- Ejecutar: Teniendo en cuenta la anterior etapa, se generan las tareas relacionadas a los controles que con cada ciclo no se cumplen.

- Revisar: A través de esta etapa se revisa si las tareas generadas y solucionadas cumplen con los controles y estándares que fueron planteados.

- Conservar: Esta etapa permite generar mecanismos que garanticen que dichos resultados se mantengan actualizados, a través de la misma se permite gestionar el estado actual de la Base de datos, así como visualizar sus posibles fallos para generar las acciones necesarias a ser implementadas en el caso de que ocurra algún incidente.

Base de datos Terridata

La Base de datos Terridata almacena información relacionada a la caracterización y tableros de control a partir de datos estadísticos de cada entidad territorial (departamentos, municipios y regiones) en el país, mediante diferentes dimensiones que permiten evaluar el cumplimiento de diferentes indicadores.

A través de la información consultada en Terridata se pretende brindar la información suficiente a cada entidad territorial para realizar el diseño de programas y proyectos para su respectiva región. Del mismo modo, permite evaluar la gestión, a través de los indicadores y por consiguiente efectuar un control de la gestión. Por otra parte, cabe resaltar que esta información se encuentra disponible para cualquier persona, dado que la misma es de carácter público.

Usuarios BD

Para la Base de datos Terridata existen varios roles designados desde el diseño de la Base de datos, asignados al área técnica del GET (Grupo de Estudios Territoriales) quienes son los encargados de realizar la gestión de la Base de datos. Además de estos roles, se encuentran los roles predeterminados. A continuación, se evidencia a través de un query en SQL los roles de usuarios de Terridata.

Figura 8
Usuarios Base de datos Terridata

DBName	Name	GroupName	LoginName	default_database_name	default_schema_name	Principal_id
TDT	dbo	db_owner	sa	master	dbo	1
TDT	DNP\[redacted] Ingeniero1	db_owner	NULL	NULL	dbo	6
TDT	DNP\[redacted] Ingeniero2	db_owner	NULL	NULL	dbo	5
TDT	DNP\s-terridatadb	db_owner	NULL	NULL	dbo	9
TDT	DNP\s-terridatard	db_datareader	NULL	NULL	dbo	8
TDT	guest	public	NULL	NULL	guest	2
TDT	INFORMATION_SCHEMA	public	NULL	NULL	NULL	3
TDT	sys	public	NULL	NULL	NULL	4
TDT	webddts	db_datareader	NULL	NULL	dbo	7
TDT	webddts	db_datawriter	NULL	NULL	dbo	7
TDT	webkat	db_datareader	NULL	NULL	dbo	10

Nota: Adaptado de SQL Server Management Terridata

Como se muestra en la figura anterior, además de los roles básicos, se encuentran los correspondientes a los ingenieros del GET (DNP\ingeniero1 y DNP\ingeniero2), roles a los cuales se les cambia el nombre debido a restricciones de seguridad para la protección de la Base de datos. Además de dos roles generales para la plataforma (DNP\s-terridatadb y DNP\s-terridatard).

Los roles DNP\ingeniero1, DNP\ingeniero2 y DNP\s-terridatadb corresponden al rol fijo db_owner, por lo cual poseen la facultad de realizar cualquier actividad de configuración y mantenimiento en la Base de datos. Mientras que DNP\s-terridatard posee permisos de solo lectura.

Diagrama relacional Base de datos

En el siguiente diagrama se muestran las relaciones entre todas las tablas de la Base de datos con sus respectivas claves tanto primarias como foráneas.

Figura 9
Diagrama Relacional Base de datos Terridata

Nota: Adaptado de SQL Server Management Terridata

Análisis de riesgos

Con el objetivo de determinar la seguridad presentada por la Base de datos de Terridata, se presenta el análisis de algunos aspectos que permiten determinar las vulnerabilidades que puede tener dicha Base de datos, tanto en el acceso por parte de la página web, como por políticas o lineamientos propios del diseño de la Base de datos.

Para lograr este objetivo, toma como base la metodología presentada en la sección *Auditoria en Base de datos basada en MinTIC.* Más específicamente a través del modelo MEMSI se plantean varios aspectos a tener en cuenta relacionados a la seguridad en la Base de datos y de la información en sí. El presente análisis de riesgos se determina en un proceso de tres fases que permite caracterizar la vulnerabilidad de la Base de datos y la página web desde la cual se accede a los datos alojados en Terridata.

De esta manera, es necesario presentar las políticas existentes relevantes para la Base de datos, en la gestión de la seguridad de la información para luego enfocar las fases del modelo MEMSI.

Por otra parte, es necesario presentar las políticas existentes relevantes para la Base de datos, en la gestión de la seguridad de la información. Es por esto que desde el DNP se manejan una clasificación de la información basada en la Ley de Transparencia, Ley de protección de datos personales y la corte constitucional, como se muestra a continuación.

Tabla 3
Clasificación de la información DNP

Clasificación Ley de Transparencia	Relación otras clasificaciones
Información pública	Requerimientos de Confidencialidad • Público Clasificación Datos personales • Dato público • Datos personales laborales (puesto, domicilio, correo electrónico y teléfono del trabajo); • Datos personales académicos (trayectoria educativa, título, número de cédula, certificados, etc.) Clasificación según Habeas Data • Pública o de dominio público
Información pública clasificada: Información exceptuada por daño de derechos a personas naturales o jurídicas	Clasificación según Ley de Transparencia • Los secretos comerciales, industriales y profesionales • El derecho de toda persona a la intimidad • El derecho de toda persona a la vida, la salud o la seguridad Requerimientos de Confidencialidad • Uso interno • Uso privado Clasificación según Habeas Data • Semi-privada • Privada • Reservada o secreta Clasificación Datos personales (Datos sensibles)
	• Ideológicos: creencias religiosas, afiliación política y/o sindical, pertenencia a organizaciones de la sociedad civil y/o asociaciones religiosas. • Sobre la vida y hábitos sexuales, origen (étnico y racial.) • Características físicas: color de piel, iris y cabellos, señales particulares, etc. • Características como tipo de sangre, ADN, huella digital, etc. • Salud: estado de salud, historial clínico, enfermedades, información relacionada con cuestiones de carácter psicológico y/o psiquiátrico, etc. • Patrimoniales: información fiscal, historial crediticio, cuentas bancarias, ingresos y egresos, etc. • Identificación: nombre, domicilio, teléfono, correo electrónico, firma, RFC, CURP, fecha de nacimiento, edad. • Datos personales de menores
Información pública reservada: Información exceptuada por daño a los intereses público	Requerimientos de Confidencialidad • Confidencial Clasificación según Ley de Transparencia • La defensa y seguridad nacional • La seguridad pública • Las relaciones internacionales • La prevención, investigación y persecución de los delitos y las faltas disciplinarias • El debido proceso y la igualdad de las partes en los procesos judiciales • La administración efectiva de la justicia • Los derechos de la infancia y la adolescencia • La estabilidad macroeconómica y financiera del país • La salud pública

Nota: Adaptado de Manual y políticas de seguridad de la información del Departamento Nacional de Planeación, Bogotá, Abril de 2019

Nivel estratégico

Terridata es gestionada por los ingenieros del Grupo de Estudios Territoriales del DNP, quienes controlan todos los elementos relacionados con la misma, de tal manera que tanto el ingreso como las políticas de seguridad empleadas dependen de ellos.

Como activos de información, Terridata contiene toda la información correspondiente a los servicios ofrecidos por la página web. Terridata maneja distintos tipos de indicadores de cada región y municipio de Colombia, donde se determina el cumplimiento de objetivos regionales y distintas dimensiones que permiten conocer el estado actual en cada aspecto relacionado con el desarrollo de las regiones, como lo pueden ser: indicadores sociales, seguridad, conflicto armado, educación, ecosistemas. Etc.

De esta manera, es posible a través de la página web realizar búsquedas que permitan conocer dicha información a través de gráficas y distintas herramientas, conectadas a través de APIs a la Base de datos.

Nivel táctico

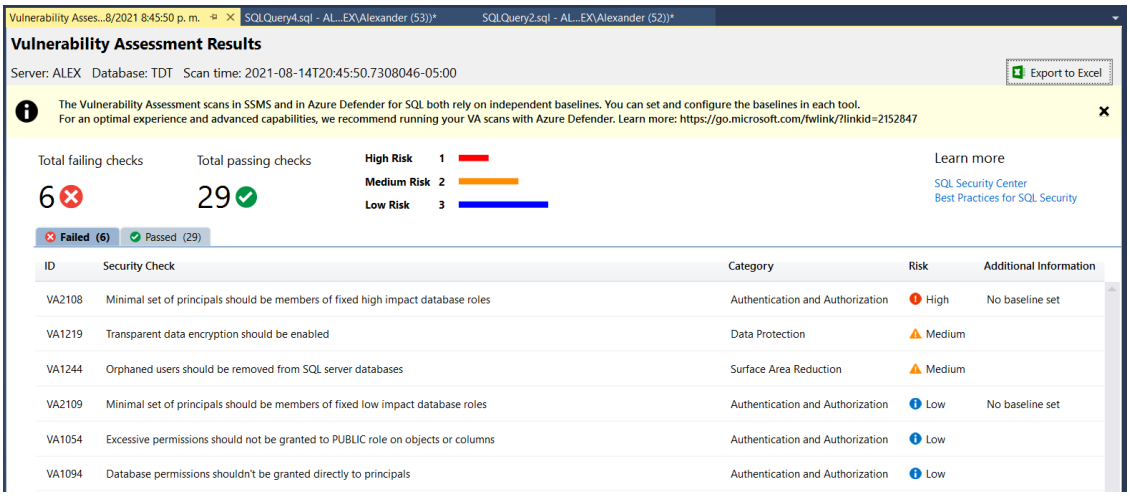
En este nivel se presentan las diferentes pruebas realizadas con el fin de detectar las vulnerabilidades que pueda presentar la Base de datos Terridata y su implementación en la página web. A continuación, se presentan dichas pruebas realizadas mediante el gestor Microsoft SQL server, desde el cual se administra la Base de datos.

Evaluación de vulnerabilidades de SQL (VA)

Para realizar este primer análisis se realiza una evaluación de vulnerabilidades se SQL, a través de un servicio provisto por el gestor, donde se visibiliza el estado de la

seguridad en la Base de datos. Dicho servicio escanea la Base de datos, y evalúa su rendimiento, integridad y seguridad a través de una base de conocimientos propia de Microsoft. Mediante este servicio se evidencian configuraciones incorrectas, permisos mal gestionados y datos desprotegidos. A continuación, se presenta dicha evaluación.

Figura 10
Evaluación de vulnerabilidades

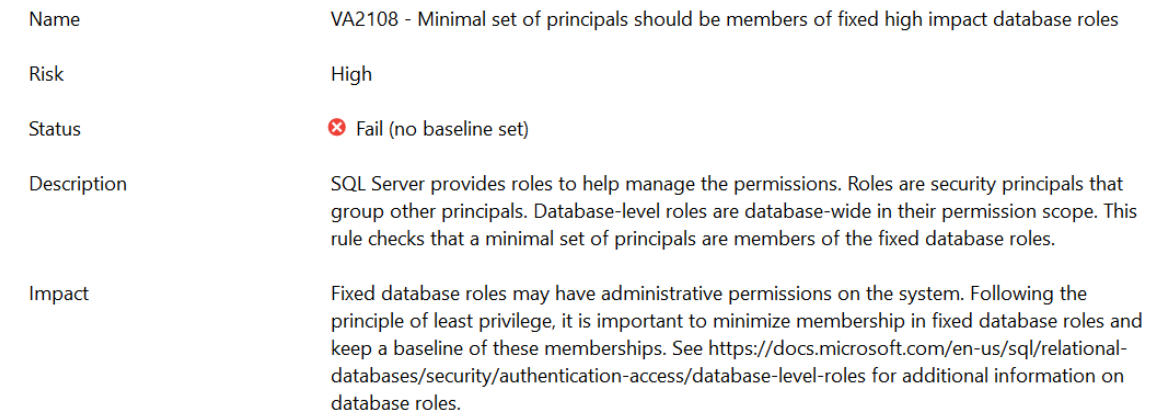


Nota: Adaptado de SQL Server Management Terridata

Mediante la evaluación de vulnerabilidades se detectaron 6 problemas con la Base de datos. A continuación, se presenta cada uno de ellos de manera más detallada.

El primer y más crítico riesgo corresponde a la asignación de usuarios, esto ocurre dado que no existen políticas definidas para la definición de roles en la Base de datos. Por lo que se dificulta la gestión de permisos para el acceso a la Base de datos, poniendo en peligro su seguridad e integridad.

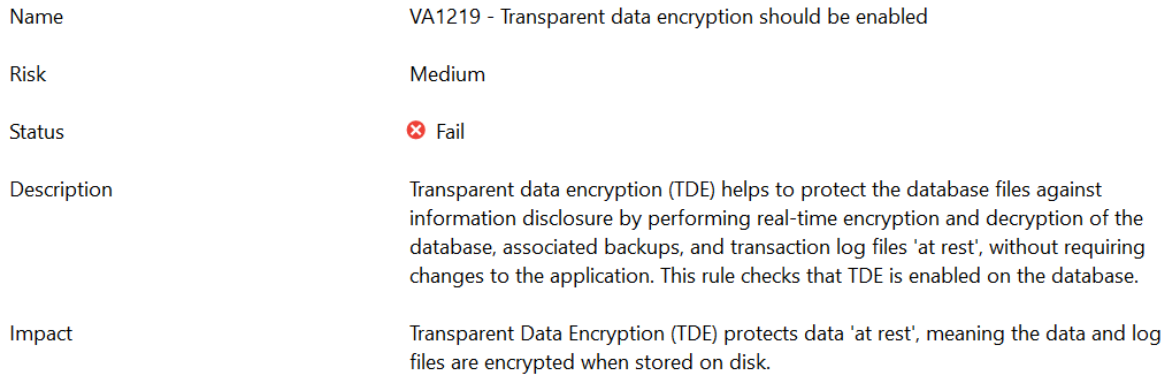
Figura 11
Roles en la Base de datos



Nota: Adaptado de SQL Server Management Terridata

Por otra parte, la Base de datos no posee implementado TDA (Transparent Data Encryption), encargado de proteger los datos ante posibles fugas de información, realizando un encriptado y desencriptado de la información en el momento de almacenar la misma en el disco.

Figura 12
Encriptación

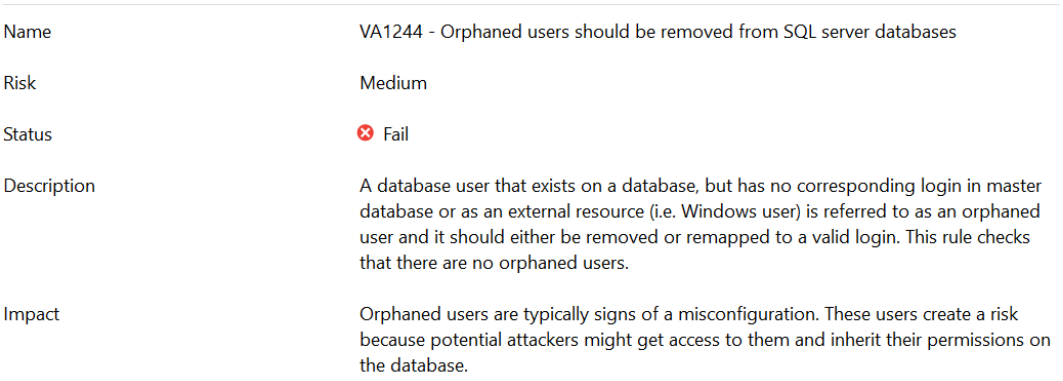


Nota: Adaptado de SQL Server Management Terridata

Los usuarios que no corresponden a roles configurados correctamente pueden ser usados para conceder permisos heredados a posibles atacantes, comprometiendo la

seguridad de la Base de datos, dicha configuración no corresponde a las buenas practicas establecidas por Microsoft.

Figura 13
Usuarios huérfanos general

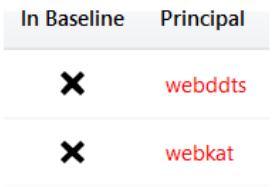


Name	VA1244 - Orphaned users should be removed from SQL server databases
Risk	Medium
Status	Fail
Description	A database user that exists on a database, but has no corresponding login in master database or as an external resource (i.e. Windows user) is referred to as an orphaned user and it should either be removed or remapped to a valid login. This rule checks that there are no orphaned users.
Impact	Orphaned users are typically signs of a misconfiguration. These users create a risk because potential attackers might get access to them and inherit their permissions on the database.

Nota: Adaptado de SQL Server Management Terridata

Estos usuarios son presentados por la evaluación y corresponden a webddts con permisos de lectura y escritura y webkat con permisos de solo lectura. Estos usuarios no pertenecen a ningún grupo ni directiva administrativa de seguridad en la Base de datos.

Figura 14
Usuarios huérfanos



In Baseline	Principal
✖	webddts
✖	webkat

Nota: Adaptado de SQL Server Management Terridata

SQL Server proporciona unas directivas para la asignación de permisos que agrupan los distintos roles que deben encargarse de determinadas tareas de administración específicas de la Base de datos. En este caso, para la Base de datos Terridata se generaron

diferentes roles que no siguen ninguna directriz ni lineamiento de seguridad para una gestión correcta de la Base de datos.

Figura 15
Roles

Name	VA2109 - Minimal set of principals should be members of fixed low impact database roles
Risk	Low
Status	Fail (no baseline set)
Description	SQL Server provides roles to help manage the permissions. Roles are security principals that group other principals. Database-level roles are database-wide in their permission scope. This rule checks that a minimal set of principals are members of the fixed database roles.
Impact	Fixed database roles may have administrative permissions on the system. Following the principle of least privilege, it is important to minimize membership in fixed database roles and keep a baseline of these memberships. See https://docs.microsoft.com/en-us/sql/relational-databases/security/authentication-access/database-level-roles for additional information on database roles.

Nota: Adaptado de SQL Server Management Terridata

De esta manera, se presentan los usuarios de la Base de datos que no corresponden a las buenas prácticas de seguridad recomendadas por Microsoft.

Figura 16
Asignación de usuarios

In Baseline	Principal	Role	Principal Type
✗	DNP\s-terridatard	db_datareader	WINDOWS_USER
✗	webddts	db_datareader	SQL_USER
✗	webddts	db_datawriter	SQL_USER
✗	webkat	db_datareader	SQL_USER

Nota: Adaptado de SQL Server Management Terridata

El rol PUBLIC dentro de la Base de datos posee demasiados permisos por defecto, es necesario que se revisen los permisos correspondientes a este rol para que estos no puedan influir en la integridad de los datos de la Base de datos, por lo cual es recomendable

revocar algunos permisos a este rol que no son necesarios para el correcto funcionamiento del mismo.

Figura 17
Permisos rol PUBLIC

Name	VA1054 - Excessive permissions should not be granted to PUBLIC role on objects or columns
Risk	Low
Status	Fail
Description	Every SQL Server login belongs to the public server role. When a server principal has not been granted or denied specific permissions on a securable object, the user inherits the permissions granted to public on that object. This rule displays a list of all securable objects or columns that are accessible to all users through the PUBLIC role.
Impact	Database Roles are the basic building block at the heart of separation of duties and the principle of least permission. Granting permissions to principals through the default PUBLIC role defeats this purpose.

Nota: Adaptado de SQL Server Management Terridata

A continuación, se muestran los permisos innecesarios para el rol PUBLIC dentro de la configuración de Terridata, y el objeto asociado a estos roles.

Figura 18
Permisos innecesarios rol PUBLIC

In Baseline	Permission	Schema	Object
✗	EXECUTE	dbo	fn_diagramobjects
✗	EXECUTE	dbo	sp_alterdiagram
✗	EXECUTE	dbo	sp_creatediagram
✗	EXECUTE	dbo	sp_dropdiagram
✗	EXECUTE	dbo	sp_helpdiagramdefinition
✗	EXECUTE	dbo	sp_helpdiagrams
✗	EXECUTE	dbo	sp_renamediagram

Nota: Adaptado de SQL Server Management Terridata

Finalmente, como política de seguridad se debería establecer que los permisos en la Base de datos no deben ser otorgados directamente a los mismos usuarios, sin pasar a través de un mecanismo de control, como lo es el grupo AD que permite centralizar la gestión de control de acceso.

Figura 19
Permisos

Name	VA1094 - Database permissions shouldn't be granted directly to principals
Risk	Low
Status	Fail
Description	Permissions are rules associated with a securable object to regulate which users can gain access to the object. This rule checks that there are no DB permissions granted directly to users.
Impact	Individuals change organizations & job descriptions over time. It is highly recommended to use a centralized access control management through AD group membership.

Nota: Adaptado de SQL Server Management Terridata

Como se muestra en la siguiente figura, se le otorga permisos directamente al usuario webddts, sin estar este regulado desde políticas administrativas de miembros de seguridad debidamente organizados pro roles.

Figura 20
Permisos otorgados directamente

In Baseline	Permission	Permission Class	Class Separator	Object	Principal
✗	EXECUTE	DATABASE	::	TDT	webddts

Nota: Adaptado de SQL Server Management Terridata

Análisis página web

Para completar el análisis de seguridad para Terridata es necesario comprobar los riesgos asociados a la implementación de la página web que le otorga acceso al público a la Base de datos, para realizar consultas de los indicadores almacenados allí.

Teniendo este objetivo en mente, se realizó un análisis de la Base de datos a través de la extensión “Lighthouse” del navegador opera, la cual permite realizar una auditoría a una página web, presentando un informe de rendimiento a través de diferentes indicadores evidenciando posibles fallas en la misma.

Al ejecutar el análisis se encontraron un total de 32 vulnerabilidades correspondientes a la inclusión de librerías desactualizadas, permitiendo a cualquier atacante ejecutar cierto tipo de ataque a la página, en función de la vulnerabilidad que quiera explotar. A continuación, se muestra el resultado del análisis.

Figura 21
Análisis vulnerabilidades página web.

Nota: Adaptado de Opera GX

- Bootstrap 3.3.6: Esta versión de la librería es vulnerable a ataques tipo Cross-site Scripting (XSS), que suceden cuando un atacante engaña a un sitio web para que el navegador ejecute secuencias de comando maliciosas que de otra manera estarían bloqueadas por políticas de los mismos navegadores.

- JQuery 2.2.4: Además de ser vulnerable a ataques tipo Cross-site Scripting (XSS), esta librería posee una vulnerabilidad conocida como Prototype Pollution. A través de esta, un atacante puede modificar un objeto para replicar permisos obtenidos a través del mismo en los demás objetos, esto puede derivar en ataques de DoS a través de scripts.

- Lo-Dash 3.10.1: Esta versión de la librería es vulnerable a ataques de tipo Prototype Pollution, además de ser susceptibles a inyección de comandos y un ataque conocido como ReDOS (Regular Expression Denial of Service).

- AngularJS 1.4.14: En este caso, para esta versión se encuentran diferentes vulnerabilidades para ataques de tipo Cross-site Scripting (XSS), así como varios tipos de ataques Prototype Pollution y DoS. Por otra parte, es vulnerable a ataques del tipo Clickjacking, donde al habilitar la configuración de SVG se expone el sitio a ataques click-hijacking. Derivando en incidentes de phishing. Finalmente, la última vulnerabilidad de esta librería corresponde a JSONP Callback Attack, el cual permite solicitar datos a un servidor de un dominio diferente al del cliente.

Nivel operativo

En este nivel se presentan los lineamientos que se deben seguir para corregir las problemáticas encontradas desde el nivel táctico de la auditoria para Terridata.

Con el objetivo de solucionar las distintas problemáticas que se presentan tanto para la Base de datos como para la página web, es necesario realizar un monitoreo constante de las políticas de gestión de la seguridad para los usuarios de la Base de datos. Así como un monitoreo de la página web, desde el cual se evidencie el estado de las librerías usadas en la programación de la página, para asegurar que estas se encuentren al día en seguridad.

Para complementar los lineamientos de seguridad, se brinda a través de la matriz de riesgos un plan de acción para cada una de estas vulnerabilidades y se presenta de una manera más clara y ordenada cada una de ellas.

Matriz de riesgos

En esta matriz se presenta la información de las vulnerabilidades encontradas (dichas vulnerabilidades son consideradas riesgos en la medida del daño que podrían tener para la Base de datos) correspondientes al nivel operativo de la auditoria con su respectivo nivel de criticidad asociado. A continuación, se presenta una versión reducida de la matriz, que puede consultarse en su totalidad en el Anexo A.

Tabla 4
Matriz de riesgos

Riesgo	*Criticidad*
Roles en la Base de datos	Alto
Encriptación	Medio
Usuarios huérfanos	Medio
Roles	Bajo
Permisos rol PUBLIC	Bajo
Permisos	Bajo
Permisos rol PUBLIC	Bajo
Permisos	Bajo
Cross-site Scripting (XSS)	Medio
Cross-site Scripting (XSS)	Medio
Cross-site Scripting (XSS)	Medio
Cross-site Scripting (XSS)	Medio
Cross-site Scripting (XSS)	Medio
Cross-site Scripting (XSS)	Medio
Cross-site Scripting (XSS)	Medio
Cross-site Scripting (XSS)	Medio
Prototype Pollution	Medio
Prototype Pollution	Alto
Command Injection	Alta

Prototype Pollution	Alta
Regular Expression Denial of Service (ReDoS)	Media
Cross-site Scripting (XSS)	Alta
Prototype Pollution	Alta
Clickjacking	Medio
Cross-site Scripting (XSS)	Medio
Denial of Service (DoS)	Medio
JSONP Callback Attack	Medio

Para determinar el nivel de criticidad de los riesgos estimados, se realiza una ponderación teniendo en cuenta la probabilidad que tienen estos riesgos para materializarse y el impacto que tiene sobre la seguridad en la Base de datos. Con dicho objetivo claro, se realizó la ponderación con base en la siguiente tabla de probabilidad de ocurrencia adaptada del modelo presentado por MAGERIT en el libro Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.

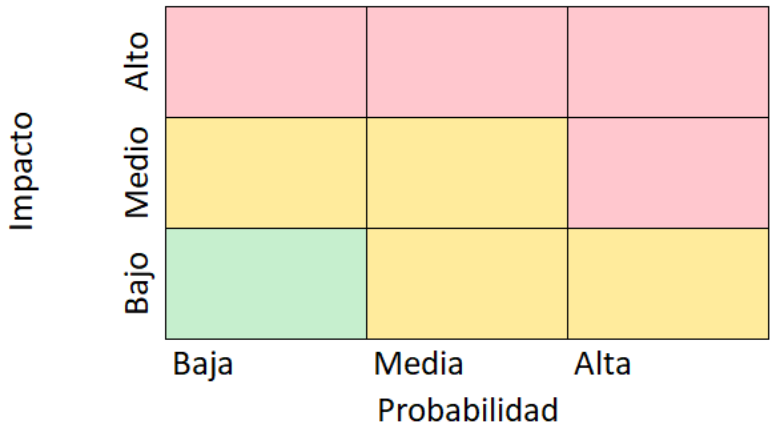
Tabla 5
Probabilidad de ocurrencia

Alta	Frecuente	Mensualmente
Media	Normal	Una vez al año
Baja	Poco Frecuente	Cada varios años

Nota: Adaptado de MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro I - Método

A continuación se muestra la matriz probabilidad-impacto realizada para tal fin, donde el área roja corresponde al nivel de criticidad alto, el Area amarilla al medio y el Area verde corresponde a un nivel de criticidad bajo.

Figura 22
Matriz de probabilidad-impacto



Nota: Adaptado de MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro I – Método

Teniendo en cuenta los riesgos presentados anteriormente, se toman como prioritarios los riesgos catalogados como Altos y medios, para ser tratados y evaluados con mayor urgencia dado su impacto sobre la Base de datos.

Por otra parte, se presenta el cumplimiento y observaciones de los controles asociados a los riesgos de carácter estratégico y táctico correspondientes a los riesgos existentes en la norma ISO 27002 (Tabla 6).

Tabla 6
Verificación de controles

POLÍTICAS DE SEGURIDAD.	Cumple		Observaciones
	Sí	No	
6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN.			
6.1.1 Asignación de responsabilidades para la seguridad de la información.	x		
6.1.2 Segregación de tareas.		x	No está definido claramente la segregación de tareas administrativas en la Base de datos
6.1.3 Contacto con las autoridades.	x		
6.1.5 Seguridad de la información en la gestión de proyectos.	x		
6.2 Dispositivos para movilidad y teletrabajo.	x		
6.2.1 Política de uso de dispositivos para movilidad.	x		
6.2.2 Teletrabajo.	x		
9. CONTROL DE ACCESOS.			
9.1.1 Política de control de accesos.		x	No existe una política clara en el control de accesos a la Base de datos Terridata
9.1.2 Control de acceso a las redes y servicios asociados.	x		
9.2 Gestión de acceso de usuario.		x	Los roles administrativos de la Base de datos no se encuentran bien definidos
9.2.1 Gestión de altas/bajas en el registro de usuarios.	x		
9.2.2 Gestión de los derechos de acceso asignados a usuarios.		x	Los usuarios de la Base de datos tienen privilegios poco claros
9.2.3 Gestión de los derechos de acceso con privilegios especiales.		x	Todos los usuarios de nivel administrativo poseen los mismos privilegios
9.2.4 Gestión de información confidencial de autenticación de usuarios.	x		
9.2.5 Revisión de los derechos de acceso de los usuarios.		x	Los derechos de acceso de la Base de datos no se encuentran bien definidos
9.2.6 Retirada o adaptación de los derechos de acceso	x		
9.3 Responsabilidades del usuario.	x		
9.3.1 Uso de información confidencial para la autenticación.	x		
9.4 Control de acceso a sistemas y aplicaciones.	x		

9.4.1 Restricción del acceso a la información.	x		
9.4.2 Procedimientos seguros de inicio de sesión.	x		
9.4.3 Gestión de contraseñas de usuario.	x		
9.4.4 Uso de herramientas de administración de sistemas.	x		
9.4.5 Control de acceso al código fuente de los programas.	x		
10. CIFRADO.			
10.1 Controles criptográficos.	x		
10.1.1 Política de uso de los controles criptográficos.	x		
10.1.2 Gestión de claves.	x		
12. SEGURIDAD EN LA OPERATIVA.			
12.1.1 Documentación de procedimientos de operación.		x	No existe una documentación actualizada de la operación de la Base de datos
12.1.2 Gestión de cambios.	x		
12.1.3 Gestión de capacidades.	x		
12.2 Protección contra código malicioso.	x		
12.2.1 Controles contra el código malicioso.	x		
12.3 Copias de seguridad.	x		
12.3.1 Copias de seguridad de la información.	x		
12.4 Registro de actividad y supervisión.		x	El manejo de la documentación se encuentra incompleto
12.4.1 Registro y gestión de eventos de actividad.	x		
12.4.2 Protección de los registros de información.	x		
12.6 Gestión de la vulnerabilidad técnica.		x	Existen varias políticas dentro del servidor del a Base de datos que no se alinean con la seguridad solicitada por el gestor
12.6.1 Gestión de las vulnerabilidades técnicas.		x	
12.6.2 Restricciones en la instalación de software.	x		
13. SEGURIDAD EN LAS TELECOMUNICACIONES.			
13.1.1 Controles de red.	x		
13.1.2 Mecanismos de seguridad asociados a servicios en red.	x		
13.1.3 Segregación de redes.	x		
13.2 Intercambio de información con partes externas.	x		
13.2.1 Políticas y procedimientos de intercambio de información.	x		
13.2.2 Acuerdos de intercambio.	x		
13.2.3 Mensajería electrónica.	x		

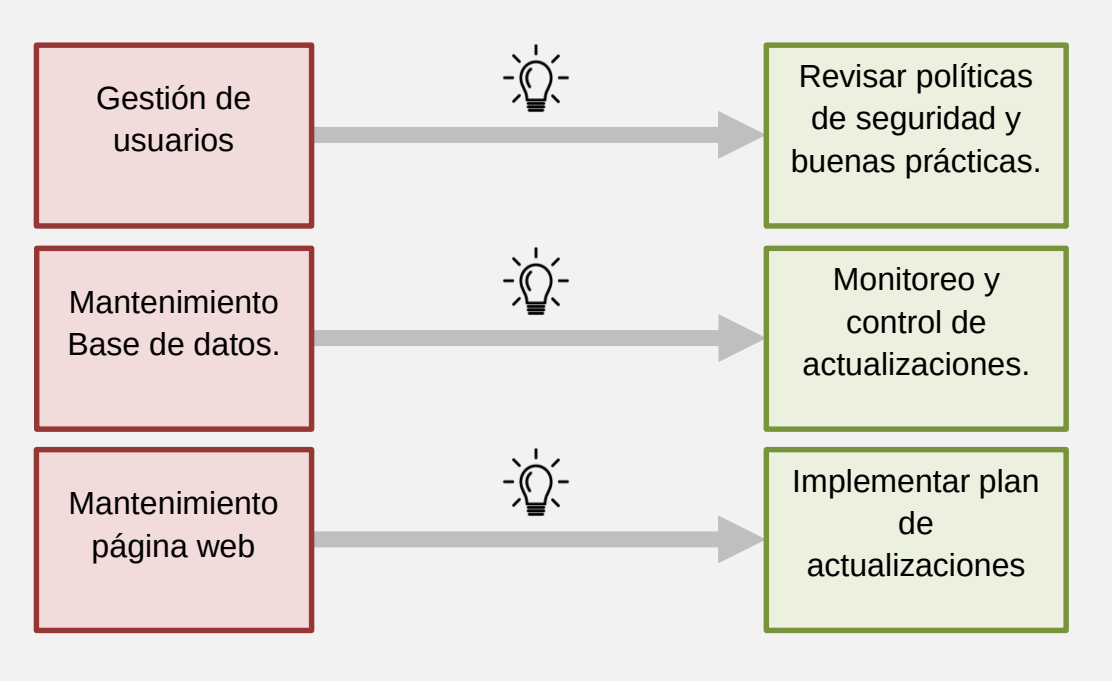
13.2.4 Acuerdos de confidencialidad y secreto.	x		
14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN			
14.1.1 Análisis y especificación de los requisitos de seguridad.	x		
14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas.	x		
14.1.3 Protección de las transacciones por redes telemáticas.	x		
16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.			
16.1 Gestión de incidentes de seguridad de la información y mejoras.	x		
16.1.1 Responsabilidades y procedimientos.	x		
16.1.2 Notificación de los eventos de seguridad de la información.	x		
16.1.3 Notificación de puntos débiles de la seguridad.		x	Existen varias políticas dentro del servidor del a Base de datos que no se alinean con la seguridad solicitada por el gestor
16.1.5 Respuesta a los incidentes de seguridad.	x		
16.1.6 Aprendizaje de los incidentes de seguridad de la información.	x		
17. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.			
17.1.1 Planificación de la continuidad de la seguridad de la información.	x		
17.1.2 Implantación de la continuidad de la seguridad de la información.	x		
17.2 Redundancias.	x		
18. CUMPLIMIENTO.			
18.1 Cumplimiento de los requisitos legales y contractuales.	x		
18.1.1 Identificación de la legislación aplicable.	x		
18.1.2 Derechos de propiedad intelectual (DPI).	x		
18.1.3 Protección de los registros de la organización.	x		
18.1.4 Protección de datos y privacidad de la información personal.	x		
18.1.5 Regulación de los controles criptográficos.	x		
18.2 Revisiones de la seguridad de la información.	x		
18.2.1 Revisión independiente de la seguridad de la información.	x		
18.2.2 Cumplimiento de las políticas y normas de seguridad.	x		
18.2.3 Comprobación del cumplimiento.	x		

Resultados y recomendaciones

A través de las diferentes pruebas y análisis realizados para la Base de datos Terridata y los controles establecidos por la norma ISO 27002, se detectan una gran cantidad de vulnerabilidades derivadas de una mala implementación de buenas prácticas al momento de realizar mantenimientos a la página web, o en el diseño y distribución de usuarios y roles en la Base de datos.

A continuación, se muestran las recomendaciones generadas con el fin de mejorar el estado de seguridad de la Base de datos y la página web donde esta implementada, ya que de esta depende el acceso a la Base de datos de Terridata.

Figura 23
Recomendaciones



Fuente: elaboración propia

Gestión de usuarios:

En relación a la gestión de usuarios, se recomiendan distintas prácticas que permitan minimizar los riesgos asociados a una mala gestión de los mismos. A continuación, se presentan dichas recomendaciones.

Tabla 7
Recomendaciones gestión de usuarios

Recomendación	Controles	Periodicidad
Utilizar privilegios de administrador solo cuando sea necesario.	Verificar privilegios de la BD	Semanal
Minimizar el número de administradores.	Monitoreo de usuarios con privilegios administrativos	Mensual
Evitar la dependencia del grupo de Windows incorporado \ administradores.	Verificar políticas de seguridad de la Base de datos	Semestral
Usar roles de servidor definidos por el usuario en lugar de otorgar acceso a individuos.		
Desactivar la opción Cross-Database Ownership Chaining a menos que se implementen varias Base de datos en una sola unidad.		
Migrar el uso a confianza selectiva en lugar de usar la propiedad TRUSTWORTHY.		
Utilizar roles de servidor definidos por el usuario como alternativa a la asignación de privilegios de nivel de servidor a usuarios individuales.	Monitoreo de usuarios con privilegios administrativos	Mensual

Los usuarios miembros de los roles fijos db_owner y db_accessadmin, pueden otorgar acceso a usuarios sin el consentimiento ni los permisos del administrador de SQL Server. Se recomienda generar una delegación de control de acceso para los usuarios y realizar auditorías periódicas de los permisos de los mismos.	Monitorear los privilegios de acceso y los roles establecidos para la BD	Semanal

Mantenimiento de la Base de datos:

Como primera medida, se recomienda habilitar la característica Transparent Database Encryption (TDE), con la cual se encripta toda la Base de datos, permitiendo encriptar a su vez datos y archivos de registro. Por otra parte, se generan una serie de recomendaciones que definen el control y la revisión de posibles problemas derivados de la actualización de los datos y modificaciones en las tablas.

Tabla 8
Recomendaciones mantenimiento

Recomendación	Controles	Periodicidad
Detener servicios no utilizados de SQL Server como 'Integration Services', 'Analysis Services' o 'Reporting Services'.	Monitoreo estado de la BD	Diario
Ejecutar copias de seguridad parciales cada semana y completas cada mes.		Semanal/mensual
Limpiar datos al realizar la copia de seguridad completa.		Mensual
Indexar de nuevo los datos al finalizar la limpieza de datos.		Mensual
Realizar pruebas de restauración con el fin de determinar el tiempo de indisponibilidad de la Base de datos.		Mensual

Mantenimiento del sitio web:

Se recomienda ejecutar un plan de actualización de la página web, ya que muchas de las librerías que se emplearon para su implementación se encuentran desactualizadas desde hace varios años, poniendo en peligro la integridad de la Base de datos, de la página y de las personas que la visitan.

Conclusiones

Es importante conocer el funcionamiento del sistema Gestor de Base de datos, ya que de él dependen los lineamientos administrativos para usuarios, grupos de usuarios y permisos en la Base de datos.

A través de la auditoria de sistemas de información aplicada para las Base de datos, es posible alinear los resultados y las recomendaciones con los estándares nacionales e internacionales que garanticen la integridad y seguridad de la información.

Realizar auditorías con base en buenas prácticas permite identificar los riesgos asociados al incumplimiento de las mismas, garantizando que la Base de datos esté acorde al estándar.

La Base de datos Terridata no posee un diseño eficiente en términos de seguridad, dado que la mayoría de usuarios son predeterminados, y los usuarios creados para esta comparten los mismos permisos.

Uno de los principales riesgos encontrados deriva de la mala distribución de roles y los permisos asociados a estos, poniendo en riesgo la integridad de la Base de datos.

Se encontraron más riesgos de los esperados teniendo en cuenta la importancia de la entidad y la confidencialidad con la que esta debe manejar la información.

Se deben implementar políticas de actualización para la página web, dado que algunas de sus librerías están desactualizadas, derivando en graves riesgos para los usuarios, la página web y la misma Base de datos.

Referencias

Beauchemin, B. (2012). *SQL Server 2012 Security Best Practices - Operational and Administrative Tasks.* Obtenido de https://go.microsoft.com/fwlink/?LinkID=31629

Departamento Nacional de Planeación. (2019). *Manual y políticas de seguridad de la información.* Bogotá.

Digicert. (2021). *¿Qué son SSL,TLS y HTTPS?* Obtenido de Digicert: https://www.websecurity.digicert.com/es/es/security-topics/what-is-ssl-tls-https

Esic. (Enero de 2018). *Modelo entidad relación: descripción y aplicaciones*. Obtenido de Esic: https://www.esic.edu/rethink/tecnologia/modelo-entidad-relacion-descripcion-aplicaciones

IBM. (2009). *Consulta de SQL, Volumen 1.* Obtenido de http://ftpmirror.your.org/pub/misc/ftp.software.ibm.com/ps/products/db2/info/vr95/pdf/es_ES/db2s1z952.pdf

ISO2700.es. (Octubre de 2013). *ISO/IEC 27002:2013. 14 DOMINIOS, 35 OBJETIVOS DE CONTROL Y 114 CONTROLES* . Obtenido de ISO2700.es: https://www.iso27000.es/assets/files/ControlesISO27002-2013.pdf

ISO27000.es. (2021). *Serie "27000"*. Obtenido de ISO27000.es: https://www.iso27000.es/iso27000.html

Ivanti. (2021). *Microsoft SQL Server Database Maintenance*. Obtenido de Ivanti: https://help.ivanti.com/iv/help/en_US/isec/94/Topics/SQL-Server-Database-Maintenance.htm

MAGERIT – versión 3.0. (Metodología de Análisis y Gestión). Madrid: Ministerio de Hacienda y Administraciones Públicas. Obtenido de https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

Marín, R. (16 de Abril de 2019). *Los gestores de bases de datos más usados en la actualidad.* Obtenido de Revista digital Inesem: https://revistadigital.inesem.es/informatica-y-tics/los-gestores-de-bases-de-datos-mas-usados/

Microsoft. (Agosto de 2016). *Bases de datos independientes*. Obtenido de Microsoft: https://docs.microsoft.com/es-es/sql/relational-databases/databases/contained-databases?view=sql-server-ver15

Microsoft. (21 de 06 de 2019). *Securing SQL Server*. Obtenido de Microsoft: https://docs.microsoft.com/en-us/sql/relational-databases/security/securing-sql-server?view=sql-server-ver15

Microsoft. (03 de Junio de 2020). *Database-Level Roles*. Obtenido de Microsoft: https://docs.microsoft.com/en-us/sql/relational-databases/security/authentication-access/database-level-roles?view=sql-server-ver15

Microsoft. (Abril de 26 de 2021). *Vulnerability assessment for SQL Server*. Obtenido de Microsoft: 26

MinTIC. (2016). *Seguridad y privacidad de la información .* MinTIC, Gobierno. Obtenido de https://mintic.gov.co/gestionti/615/articles-5482_G15_Auditoria.pdf

Nielsen, P., White, M., & Parui, U. (2009). *Microsoft SQL Server 2008 Bible.* New York, UNITED STATES: John Wiley & Sons, Incorporated. Obtenido de http://ebookcentral.proquest.com/lib/bibliotecausta-ebooks/detail.action?docID=455849

Oracle. (2021). *¿Qué es una base de datos relacional?* Obtenido de Oracle: https://www.oracle.com/co/database/what-is-a-relational-database/

Oracle. (2021). *MySQL Database Service*. Obtenido de Oracle: MySQL Database Service

Saucedo Mejía , S., Gutierrez Diaz de León, L. A., Ayala López, A., & Lozoya Arandia, J. (2014). *Metodología para Auditar Bases de Datos fundamentada en Estándares y.* Universidad de Guadalajara. Obtenido de https://www.iiis.org/cds2014/cd2014sci/cisci_2014/paperspdf/ca899my.pdf

Anexo A

Matriz de riesgos

Riesgo	Descripción	Causa	Consecuencia	Criticidad	Plan de acción
Roles en la Base de datos	Se encuentra una vulnerabilidad en la definición y distribución de los roles y permisos dentro de la Base de datos	Mala organización	Alterar los privilegios y permisos de los roles, exponiendo información confidencial	Alto	Reestructuración de los permisos y privilegios de los roles que se encuentran en la Base de datos
Encriptación	La opción para habilitar el cifrado de datos transparente (TDE) se encuentra desactivada	Falta de protección de los datos en reposo	Información en riesgo de divulgación	Medio	Habilitar y comprobar el funcionamiento del TDE
Usuarios huérfanos	Se encuentra que en la Base de datos existen usuarios huérfanos que pueden dar acceso a atacantes potenciales	Configuración incorrecta	Atacantes potenciales pueden heredar permisos en la Base de datos utilizando estos usuarios	Medio	Eliminar completamente estos usuarios de la Base de datos
Roles	Se encuentra una vulnerabilidad en la definición y distribución de los roles	Configuración incorrecta	Dificulta la gestión de la Base de datos	Bajo	Eliminar miembros que no deberían tener acceso a la función de Base de datos
Permisos rol PUBLIC	Se encuentra que se han otorgado permisos excesivos a roles públicos	Mala gestión de los usuarios	Se frustra la correcta construcción de la separación de funciones y permisos	Bajo	Revisar y cambiar los permisos otorgados a roles públicos
Permisos	Se encuentra que se han otorgado permisos a usuarios directamente	Mala gestión de la herramienta	Información en riesgo de divulgación	Bajo	Realizar una gestión de control de acceso centralizada a teniendo en cuenta al grupo de administradores
Permisos rol PUBLIC	Se encuentra que se han otorgado permisos	Mala gestión de los usuarios	Se frustra la correcta construcción de la separación de	Bajo	Revisar y cambiar los permisos

	excesivos a roles públicos		funciones y permisos		otorgados a roles públicos
Permisos	Se encuentra que se han otorgado permisos a usuarios directamente	Mala gestión de la herramienta	Información en riesgo de divulgación	Bajo	Realizar una gestión de control de acceso centralizada a teniendo en cuenta al grupo de administradores
Cross-site Scripting (XSS)	Las versiones afectadas de este paquete son vulnerables a Cross-site Scripting (XSS) a través del atributo tooltip data-viewport.	Mantenimiento deficiente	Un atacante puede insertar el código malicioso en la aplicación Un atacante puede enviar un enlace malicioso externamente desde la aplicación del sitio web vulnerable a un usuario Un atacante puede generar un ataque mediante Phishing Un atacante inyecta código que parece seguro, pero luego es reescrito y modificado por el navegador, mientras analiza el marcado.	Medio	Actualizar bootstrap a la versión 3.4.0 o superior.
Cross-site Scripting (XSS)	Las versiones afectadas de este paquete son vulnerables a Cross-site Scripting (XSS) a través de la propiedad de destino de configuración via affix.	Mantenimiento deficiente	Un atacante puede insertar el código malicioso en la aplicación Un atacante puede enviar un enlace malicioso externamente desde la aplicación del sitio web	Medio	Actualizar bootstrap a la versión 3.4.0 o superior.

			vulnerable a un usuario		
			Un atacante puede generar un ataque mediante Phishing		
			Un atacante inyecta código que parece seguro, pero luego es reescrito y modificado por el navegador, mientras analiza el marcado.		
Cross-site Scripting (XSS)	Las versiones afectadas de este paquete son vulnerables a Cross-site Scripting (XSS) a través del data-target attribute.	Mantenimiento deficiente	Un atacante puede insertar el código malicioso en la aplicación	Medio	Actualizar bootstrap a la versión 3.4.0, 4.0.0-beta.2 o superior
			Un atacante puede enviar un enlace malicioso externamente desde la aplicación del sitio web vulnerable a un usuario		
			Un atacante puede generar un ataque mediante Phishing		
			Un atacante inyecta código que parece seguro, pero luego es reescrito y modificado por el navegador, mientras analiza el marcado.		
Cross-site Scripting (XSS)	Las versiones afectadas de este paquete son vulnerables a Cross-site	Mantenimiento deficiente	Un atacante puede insertar el código malicioso en la aplicación	Medio	Actualizar bootstrap a la versión 3.4.1, 4.3.1 o superior.

	Scripting (XSS) en las propiedades de plantillas data-template, data-content y data-title properties of tooltip/popover...		Un atacante puede enviar un enlace malicioso externamente desde la aplicación del sitio web vulnerable a un usuario Un atacante puede generar un ataque mediante Phishing Un atacante inyecta código que parece seguro, pero luego es reescrito y modificado por el navegador, mientras analiza el marcado.		
Cross-site Scripting (XSS)	Las versiones afectadas de este paquete son vulnerables a Cross-site Scripting (XSS) a través de los complementos tooltip, collapse y scrollspy.	Mantenimiento deficiente	Un atacante puede insertar el código malicioso en la aplicación Un atacante puede enviar un enlace malicioso externamente desde la aplicación del sitio web vulnerable a un usuario Un atacante puede generar un ataque mediante Phishing Un atacante inyecta código que parece seguro, pero luego es reescrito y modificado por el navegador, mientras analiza el marcado.	Medio	Actualizar bootstrap a la versión 3.4.0, 4.1.2 o superior

Cross-site Scripting (XSS)	Las versiones afectadas de este paquete son vulnerables a Cross-site Scripting (XSS) Pasando HTML que contiene elementos <option> de fuentes no confiables	Mantenimiento deficiente	Un atacante puede insertar el código malicioso en la aplicación Un atacante puede enviar un enlace malicioso externamente desde la aplicación del sitio web vulnerable a un usuario Un atacante puede generar un ataque mediante Phishing Un atacante inyecta código que parece seguro, pero luego es reescrito y modificado por el navegador, mientras analiza el marcado.	Medio	Actualice jquery a la versión 3.5.0 o superior.
Cross-site Scripting (XSS)	Las versiones afectadas de este paquete son vulnerables a Cross-site Scripting (XSS). Pueden pasar HTML de fuentes no confiable.	Mantenimiento deficiente	Un atacante puede insertar el código malicioso en la aplicación Un atacante puede enviar un enlace malicioso externamente desde la aplicación del sitio web vulnerable a un usuario Un atacante puede generar un ataque mediante Phishing Un atacante inyecta código que parece seguro, pero luego es	Medio	Actualice jquery a la versión 3.5.0 o superior.

			reescrito y modificado por el navegador, mientras analiza el marcado.		
Cross-site Scripting (XSS)	Las versiones afectadas de este paquete son vulnerables a los ataques de Cross-site Scripting (XSS) cuando se realiza una solicitud ajax entre dominios sin la opción dataType que hace que se ejecuten respuestas de texto / javascript.	Mantenimiento deficiente	Un atacante puede insertar el código malicioso en la aplicación Un atacante puede enviar un enlace malicioso externamente desde la aplicación del sitio web vulnerable a un usuario Un atacante puede generar un ataque mediante Phishing Un atacante inyecta código que parece seguro, pero luego es reescrito y modificado por el navegador, mientras analiza el marcado.	Medio	Actualice jquery a la versión 1.12.2, 2.2.2, 3.0.0 o superior.
Prototype Pollution	Las versiones afectadas de este paquete son vulnerables a la contaminación de prototipos. Se puede engañar a la función extend para que modifique el prototipo de	Mantenimiento deficiente	Un atacante puede efectuar un ataque tipo DoS Un atacante puede realizar la ejecución remota de código.	Medio	Actualizar jquery a la versión 3.4.0 o superior.

	Object cuando el atacante controla parte de la estructura que se pasa a esta función.		Un atacante puede contaminar las propiedades en las que se basa el código base por su valor informativo, incluidas las propiedades de seguridad como las cookies o los tokens.		
Prototype Pollution	Las versiones afectadas de este paquete son vulnerables a la contaminación de prototipos en zipObjectDeep debido a una solución incompleta para CVE-2020-8203.	Mantenimiento deficiente	Un atacante puede efectuar un ataque tipo DoS Un atacante puede realizar la ejecución remota de código. Un atacante puede contaminar las propiedades en las que se basa el código base por su valor informativo, incluidas las propiedades de seguridad como las cookies o los tokens.	Alto	Actualizar lodash a la versión 4.17.20 o superior.
Command Injection	Las versiones afectadas de este paquete son vulnerables a la inyección de comandos a través de template	Mantenimiento deficiente	Un atacante puede usar transmisiones inseguras de datos del usuario, como cookies y formularios, para inyectar un comando en el shell del sistema en un servidor web. El atacante puede aprovechar los privilegios de la	Alta	Actualizar a la versión lodash@4.17.21.

			aplicación vulnerable para comprometer el servidor.		
Prototype Pollution	Las versiones afectadas de este paquete son vulnerables a la modificación de la función de utilidades y ZipObjectDeep. Si un atacante puede controlar parte de la estructura que se pasa a esta función, podría agregar o modificar una propiedad existente.	Mantenimiento deficiente	Un atacante puede efectuar un ataque tipo DoS Un atacante puede realizar la ejecución remota de código. Un atacante puede contaminar las propiedades en las que se basa el código base por su valor informativo, incluidas las propiedades de seguridad como las cookies o los tokens.	Alta	Actualizar a la versión lodash@4.17.21.
Regular Expression Denial of Service (ReDoS)	Las versiones afectadas de este paquete son vulnerables a la Denegación de servicio de expresión regular (ReDoS) a través de las funciones toNumber, trim y trimEnd.	Mantenimiento deficiente	Un atacante puede ejecutar ataques de denegación de servicio DoS	Media	Actualizar a la versión lodash@4.17.21.
Cross-site Scripting (XSS)	Las versiones afectadas de este paquete son vulnerables a Cross-site Scripting (XSS). XSS puede activarse en aplicaciones AngularJS que desinfectan fragmentos de HTML controlados por	Mantenimiento deficiente	Un atacante puede insertar el código malicioso en la aplicación Un atacante puede enviar un enlace malicioso externamente desde la aplicación del sitio web vulnerable a un usuario	Alta	Actualizar a la versión angular@1.8.0.

	el usuario antes de pasarlos a métodos JQLite como JQLite.prepend, JQLite.after, JQLite.append, JQLite.replaceWith, JQLite.append, new JQLite y angular.element.		Un atacante puede generar un ataque mediante Phishing Un atacante inyecta código que parece seguro, pero luego es reescrito y modificado por el navegador, mientras analiza el marcado.		
Prototype Pollution	Las versiones afectadas de este paquete son vulnerables. La función merge () podría ser engañada para agregar o modificar propiedades de Object.prototype usando un payload __proto__.	Mantenimiento deficiente	Un atacante puede efectuar un ataque tipo DoS Un atacante puede realizar la ejecución remota de código. Un atacante puede contaminar las propiedades en las que se basa el código base por su valor informativo, incluidas las propiedades de seguridad como las cookies o los tokens.	Alta	Actualizar a la versión angular@1.7.9.
Clickjacking	Las versiones afectadas de este paquete son vulnerables a Clickjacking. Al habilitar la configuración de SVG sin tomar otras precauciones, puede exponer su aplicación a ataques de	Mantenimiento deficiente	Un atacante puede aprovechar la página para realizar ataques tipo Phishing	Medio	Actualizar a la versión angular@1.5.0.

	secuestro de clics.				
Cross-site Scripting (XSS)	Las versiones afectadas de este paquete son vulnerables a Cross-site Scripting (XSS). El servicio $ http, <option> elements <select>permite solicitudes JSONP con URL que no son de confianza, que podrían ser explotadas por un atacante.	Mantenimiento deficiente	Un atacante puede insertar el código malicioso en la aplicación Un atacante puede enviar un enlace malicioso externamente desde la aplicación del sitio web vulnerable a un usuario Un atacante puede generar un ataque mediante Phishing Un atacante inyecta código que parece seguro, pero luego es reescrito y modificado por el navegador, mientras analiza el marcado.	Medio	Actualizar a la versión angular@1.6.3.
Denial of Service (DoS)	Las versiones afectadas de este paquete son vulnerables a la denegación de servicio (DoS)	Mantenimiento deficiente	Un atacante puede efectuar un ataque tipo DoS	Medio	Actualizar a la versión angular@1.6.3.
JSONP Callback Attack	Las versiones afectadas de este paquete son vulnerables al JSONP Callback Attack a través de JSONP. JSONP	Mantenimiento deficiente	Un atacante puede utilizar esta vulnerabilidad como método para solicitar datos de un servidor que reside en un dominio diferente al del cliente.	Medio	Actualizar a la versión angular@1.6.3.