UNIVERSIDAD PERUANA LOS ANDES

FACULTAD DE INGENIERÍA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS Y COMPUTACIÓN

TESIS

IMPLEMENTACIÓN DE CONTROLES DE CONFIGURACIÓN DE SEGURIDAD EN LA BASE DE DATOS DE GPA BUSINESS SAC - LIMA 2022

PRESENTADO POR:

Bach. Jorge Luis Romero Santa Cruz

Líneas de investigación: Nuevas tecnologías y procesos

PARA OPTAR EL TÍTULO PROFESIONAL DE

INGENIERO DE SISTEMAS Y COMPUTACIÓN

HUANCAYO – PERÚ

2023

MG. JAIME HUMBERTO ORTIZ FERNANDEZ

ASESOR TEMÁTICO

DR. MAGNO TEÓFILO BALDEÓN TOVAR

ASESOR METODOLÓGICO

HOJA DE CONFORMIDAD DE LOS JURADOS

_____

DR. RUBÉN DARÍO TAPIA SILGUERA

PRESIDENTE

_____

MG. CAROL JOSEFINA FABIAN CORONEL

JURADO 01

_____

MG. WALTER DAVID ESTARES VENTOCILLA

JURADO 02

_____

MG. JUDYTH MARLENI ECHAVIGURIN TORRES

JURADO 03

_____

MG. LEONEL UNTIVEROS PEÑALOZA

SECRETARIO

DEDICATORIA:

Me complace dedicar este trabajo a mis padres Luis Romero Chacón y Julia Santa Cruz Huatuco, porque a través de su amor, paciencia, buenos valores ayudaron a trazar mi camino.

A mis hermanas, por su apoyo rotundo en cada instante de mi vida; a mi esposa por ser el apoyo incondicional en mi vida. Finalmente, a mis hijos quienes son mi motor que me ayudo alcanzar mis objetivos.

AGRADECIMIENTO:

Eternamente agradecido con Dios por ponerme personas que me apoyaron y me brindaron sus sugerencias para llevar a cabo y hacer todo lo posible que esta tesis contribuya a nuestra comunidad.

CONSTANCIA 031

DE SIMILITUD DE TRABAJOS DE INVESTIGACIÓN POR EL SOFTWARE DE PREVENCIÓN DE PLAGIO TURNITIN

La Dirección de Unidad de Investigación de la Facultad de Ingeniería, hace constar por la presente, que el informe final de tesis titulado:

"IMPLEMENTACIÓN DE CONTROLES DE CONFIGURACIÓN DE SEGURIDAD EN LA BASE DE DATOS DE GPA BUSINESS SAC – LIMA 2022".

Cuyo autor(es) : Jorge Luis, Romero Santa Cruz.

Facultad : Ingeniería

Escuela Profesional : Ingeniería de Sistemas y Computación

Asesor(a) : Mg. Jaime Humberto, Ortiz Fernandez
Dr. Magno Teófilo, Baldeón Tovar

Que, fue presentado con fecha 20.01.2023 y después de realizado el análisis correspondiente en el software de prevención de plagio Turnitin con fecha 23.01.2023; con la siguiente configuración de software de prevención de plagio Turnitin:

- [x] Excluye bibliografía.
- [x] Excluye citas.
- [x] Excluye cadenas menores de a 20 palabras.
- [ ] Otro criterio (especificar)

Dicho documento presenta un porcentaje de similitud de **26 %**. En tal sentido, de acuerdo a los criterios de porcentajes establecidos en el artículo N°11 del Reglamento de uso de software de prevención de plagio, el cual indica que no se debe superar el **30%**. Se declara, que el trabajo de investigación: si contiene un porcentaje aceptable de similitud. Observaciones: ninguna.

En señal de conformidad y verificación se firma y sella la presenta constancia.

Huancayo 30 de Enero del 2023

UNIVERSIDAD PERUANA LOS ANDES
DIRECCIÓN DE LA UNIDAD DE INVESTIGACIÓN
FACULTAD DE INGENIERÍA

Dr. Santiago Zevallos Salinas
Director de la Unidad de Investigación

ÍNDICE DE CONTENIDO

DEDICATORIA: v
AGRADECIMIENTO: vi
ÍNDICE DE CONTENIDO viii
RESUMEN xv
ABSTRACT xvi
INTRODUCCIÓN xvii
CAPITULO I: 18
EL PROBLEMA DE INVESTIGACIÓN 18
1.1. PLANTEAMIENTO DEL PROBLEMA 18
1.2. FORMULACIÓN Y SISTEMATIZACIÓN DEL PROBLEMA 19
1.2.1. Problema General 19
1.2.2. Problemas Específicos 20
1.3. JUSTIFICACIÓN 20
1.3.1. Social 20
1.3.2. Teórica 20
1.3.3. Metodológica 21
1.4. DELIMITACIONES 21
1.4.1. Espacial 21
1.4.2. Temporal 21
1.4.4. Económica 22
1.5. LIMITACIONES 22
1.6. OBJETIVOS 22
1.6.1. Objetivo General 22
1.6.2. Objetivos Específicos 22

CAPITULO II: 24
MARCO TEÓRICO 24
2.1. ANTECEDENTES 24
2.1.1. Internacionales 24
2.1.2. Nacionales 27
2.2. MARCO CONCEPTUAL 30
2.2.1. Controles de configuración de seguridad 30
2.2.2. Seguridad 31
2.2.3. Actualización del software de base de datos y configuración de parámetros 34
2.2.4. Configuración de parámetros de conexión, acceso, usuarios y asignación y/o revocación de privilegios 35
2.2.5. Configuración de parámetros de auditorías 35
2.2.6. Base de Datos 36
2.2.7. Disponibilidad 37
2.2.8. Confidencialidad 37
2.2.9. Integridad 38
2.3. DEFINICIÓN DE TÉRMINOS 38
2.3.1. Listener.ora 38
2.3.2. Malware 38
2.3.3. Parámetros generales de Base de Datos Oracle 38
2.3.4. Parche 38
2.3.5. Ransomware 39
2.3.6. SQL 39
2.3.7. Versión del parche del motor de BD 39
2.3.8. Vulnerabilidad y ataques informáticos 39
2.4. HIPÓTESIS 39

2.4.1. Hipótesis General 39
2.4.2. Hipótesis Específicas 39
2.5. VARIABLES 40
2.5.1. Definición conceptual de la variable 40
2.5.2. Definición operacional de la variable 40
CAPITULO III: 43
METODOLOGIA 43
3.1. MÉTODO DE INVESTIGACIÓN 43
3.2. TIPO DE INVESTIGACIÓN 43
3.3. NIVEL DE INVESTIGACIÓN 44
3.4. DISEÑO DE INVESTIGACIÓN 44
3.5. POBLACIÓN Y MUESTRA 44
3.5.1. Población 44
3.5.2. Muestra 45
3.6. TÉCNICAS E INSTRUMENTOS DE RECOLECCIÓN DE DATOS 45
3.6.1. Técnicas 45
3.6.2. Instrumentos 45
3.7. PROCESAMIENTO DE LA INFORMACIÓN 46
3.8. TÉCNICAS Y ANÁLISIS DE DATOS 46
3.8. ASPECTOS ETICOS DE LA INVESTIGACIÓN 47
RESULTADOS 48
4.1. DESCRIPCIÓN DEL DISEÑO TECNOLÓGICO 48
4.2. DESCRIPCIÓN DE RESULTADOS 49
4.2.1. Resultados preliminares de la prueba (Antes de la implementación de los controles de configuración de seguridad) 49
4.2.2. Resultados posteriores a la prueba (Después de la implementación de los controles de configuración de seguridad) 59

4.3. CONTRASTACIÓN DE HIPÓTESIS 67
4.3.1. Prueba de Normalidad 67
4.3.2. Resultados obtenidos 69
4.3.3. Prueba de la hipótesis general 72
4.3.4. Prueba de la primera hipótesis 73
4.3.5. Prueba de la segunda hipótesis 75
4.3.6. Prueba de la tercera hipótesis 76
CAPITULO V: 78
DISCUSIÓN DE RESULTADOS 78
RECOMENDACIONES 81
REFERENCIAS BIBLIOGRÁFICAS 82
ANEXOS 86
Anexo 1: Matriz de Consistencia 86
Anexo 2: Matriz de operacionalización de variables 88
Anexo 3: Matriz de operacionalización del instrumento 90
Anexo 4 Ficha de validez del instrumento 91
Anexo 5: Lista de Cotejo para la instancia de base de datos “bdgpadev” del ambiente de desarrollo de la empresa GPA Business SAC 92
Anexo 6: Lista de Cotejo para la instancia de base de datos “bdgpaqa” del ambiente de control de calidad de la empresa GPA Business SAC: 107
Anexo 7: Constancia de aplicación del instrumento 122
Anexo 8: Validez del Instrumento 123
Anexo 9: Consentimiento Informado 127
Anexo 10: Lista de Cotejo Pre Test de los controles de configuración de seguridad en la base de datos Oracle 19c en la instancia de base de datos “bdgpadev” del ambiente de desarrollo de la empresa GPA Business SAC. 128
Anexo 11: Lista de Cotejo Pre Test de los controles de configuración de seguridad en la base de datos Oracle 19c en la instancia de base de datos

“bdgpaqa” del ambiente de control de calidad de la empresa GPA Business SAC. 143

Anexo 12: Lista de Cotejo Post Test de los controles de configuración de seguridad en la base de datos Oracle 19c en la instancia de base de datos “bdgpadev” del ambiente de desarrollo de la empresa GPA Business SAC. 158

Anexo 13: Lista de Cotejo Post Test de los controles de configuración de seguridad en la base de datos Oracle 19c en la instancia de base de datos “bdgpaqa” del ambiente de control de calidad de la empresa GPA Business SAC. 173

ÍNDICE DE TABLAS

Tabla 1: Operacionalización de las variables 42
Tabla 2: Instancias de bases de datos Oracle 19c 45
Tabla 3: Estadísticas de fiabilidad 46
Tabla 4: Número de elementos de la variable 1 50
Tabla 5: Número de elementos de la primera dimensión 52
Tabla 6: Número de elementos de la segunda dimensión 54
Tabla 7: Número de elementos de la tercera dimensión 56
Tabla 8: Número de elementos de la variable 1 59
Tabla 9: Ítems no aplicado / aplicado de la Variable 1 en la instancia bdgpadev 59
Tabla 10: Ítems no aplicado / aplicado de la Variable 1 en la instancia bdgpaqa 60
Tabla 11: Número de elementos de la primera dimensión 61
Tabla 12: Ítems no aplicado / aplicado en la primera dimensión de la instancia bdgpadev 61
Tabla 13: Ítems no aplicado / aplicado en la primera dimensión de la instancia bdgpaqa 62
Tabla 14: Número de elementos de la segunda dimensión 63
Tabla 15: Ítems no aplicado / aplicado en la segunda dimensión de la instancia bdgpadev 63
Tabla 16: Ítems no aplicado / aplicado en la segunda dimensión de la instancia bdgpaqa 64
Tabla 17: Número de elementos de la tercera dimensión 65
Tabla 18: Ítems no aplicado / aplicado en la tercera dimensión de la instancia bdgpadev 66
Tabla 19: Ítems no aplicado / aplicado en la tercera dimensión de la instancia bdgpaqa 66
Tabla 20: Prueba de normalidad de la variable Controles de configuración de seguridad 69
Tabla 21: Prueba de normalidad de la primera dimensión Actualización del software de base de datos y configuración de parámetros 70
Tabla 22: Prueba de normalidad de la segunda dimensión Configuración de parámetros de conexión, acceso, usuarios y asignación y/o revocación de privilegios 71
Tabla 23: Prueba de normalidad de la tercera dimensión Configuración de parámetros de auditorías 71
Tabla 24: Prueba de rangos con signo de wilcoxon de la hipótesis general 73
Tabla 25: Significancia asintótica de la hipótesis general 73
Tabla 26: Prueba de rangos con signo de wilcoxon de la hipótesis específica 1 74
Tabla 27: Significancia asintótica de la hipótesis específica 1 74
Tabla 28: Prueba de rangos con signo de wilcoxon de la hipótesis específica 2 76
Tabla 29: Significancia asintótica de la hipótesis específica 2 76
Tabla 30: Prueba de rangos con signo de wilcoxon de la hipótesis específica 3 77
Tabla 31: Significancia asintótica de la hipótesis específica 3 77

ÍNDICE DE FIGURAS

Figura 1: Características de la Seguridad 33
Figura 2: Flujo de proceso de implantación 49
Figura 3: Ítems no aplicado / aplicado de la Variable 1 en la instancia bdgpadev 50
Figura 4: Ítems no aplicado / aplicado de la variable 1 en la instancia bdgpadev 50
Figura 5: Ítems no aplicado / aplicado en la variable 1 de la instancia bdgpaqa 51
Figura 6:Ítems no aplicado / aplicado de la variable 1 en la instancia bdgpaqa 51
Figura 7: Ítems no aplicado / aplicado en la primera dimensión de la instancia bdgpadev 52
Figura 8: Ítems no aplicado / aplicado de la primera dimensión en la instancia bdgpadev 52
Figura 9: Ítems no aplicado / aplicado en la primera dimensión de la instancia bdgpaqa 53
Figura 10: Ítems no aplicado / aplicado de la primera dimensión en la instancia bdgpaqa 53
Figura 11: Ítems no aplicado / aplicado en la segunda dimensión de la instancia bdgpadev 54
Figura 12: Ítems no aplicado / aplicado de la segunda dimensión en la instancia bdgpadev 55
Figura 13: Ítems no aplicado / aplicado en la segunda dimensión de la instancia bdgpaqa 55
Figura 14:Ítems no aplicado / aplicado de la segunda dimensión en la instancia bdgpaqa 56
Figura 15: Ítems no aplicado / aplicado en la tercera dimensión de la instancia bdgpadev 57
Figura 16: Ítems no aplicado / aplicado en la tercera dimensión de la instancia bdgpadev 57
Figura 17: Ítems no aplicado / aplicado en la tercera dimensión de la instancia bdgpaqa 58
Figura 18: Ítems no aplicado / aplicado en la tercera dimensión de la instancia bdgpaqa 58
Figura 19:Ítems no aplicado / aplicado de la variable 1 en la instancia bdgpadev 59
Figura 20:Ítems no aplicado / aplicado de la variable 1 en la instancia bdgpaqa 60
Figura 21: Ítems no aplicado / aplicado en la primera dimensión de la instancia bdgpadev 61
Figura 22: Ítems no aplicado / aplicado en la primera dimensión de la instancia bdgpaqa 62
Figura 23: Ítems no aplicado / aplicado en la segunda dimensión de la instancia bdgpadev 64
Figura 24: Ítems no aplicado / aplicado en la segunda dimensión de la instancia bdgpaqa 65
Figura 25: Ítems no aplicado / aplicado en la tercera dimensión de la instancia bdgpadev 66
Figura 26: Ítems no aplicado / aplicado en la tercera dimensión de la instancia bdgpaqa 67
Figura 27: Q-Q normal de Dif_v1post-v1pre 69
Figura 28: Q-Q normal de diferencia de la primera dimensión 70
Figura 29: Q-Q normal de diferencia de la segunda dimensión 71
Figura 30: Q-Q normal de diferencia de la tercera dimensión 72

RESUMEN

Este trabajo de investigación fue titulado: “IMPLEMENTACIÓN DE CONTROLES DE CONFIGURACIÓN DE SEGURIDAD EN LA BASE DE DATOS DE GPA BUSINESS SAC - LIMA 2022”, fue elaborado con la finalidad de obtener el título profesional de Ingeniero de Sistemas y Computación; además de demostrar que la implementación de controles de configuración de seguridad influye significativamente en la base de datos de la empresa GPA Business SAC.

El problema que dio origen fue ¿De qué manera la implementación de controles de configuración de seguridad influye en la base de datos de GPA Business SAC – Lima 2022? El objetivo general fue: Determinar de qué manera la implementación de controles de configuración de seguridad influye en la base de datos de la GPA Business SAC – Lima 2022, para ello, se tuvieron en cuenta aspectos clave de las variables de estudio. La hipótesis general fue: La implementación de controles de configuración de seguridad influye significativamente en la base de datos de GPA Business SAC – Lima 2022.

Básicamente, es una investigación cuantitativa, en la que se utiliza como método general el método científico y el tipo de investigación corresponde a una investigación aplicada, el diseño de investigación utilizado fue pre experimental, donde se implementó los controles de configuración de seguridad en la base de datos de GPA Business SAC.

Se utilizó la prueba estadística de Wilcoxon para comparar las hipótesis, lo que permitió determinar la influencia de los controles de configuración de seguridad en la base de datos de GPA Business SAC. Puesto que el p valor obtenido fue de 0,000 siendo menor que el nivel de significación de 0,05%, por lo tanto, la empresa GPA Business SAC puede mejorar significativamente la confidencialidad, disponibilidad e integridad de la información que aloja en su base de datos a través de la implementación.

Palabras claves: Controles de configuración, Seguridad, Base de datos.

ABSTRACT

This research work was entitled: "IMPLEMENTATION OF SECURITY CONFIGURATION CONTROLS IN THE GPA BUSINESS SAC'S DATABASE - LIMA 2022", was prepared with the purpose of obtaining the professional title of Systems and Computing Engineer; in addition to demonstrating that the implementation of security configuration controls significantly influences the database of the company GPA Business SAC.

The problem that gave rise was: How does the implementation of security configuration controls influence the GPA Business SAC's database – Lima 2022? The general objective was: To determine how the implementation of security configuration controls influences the GPA Business SAC's database - Lima 2022, for this, key aspects of the study variables were taken into account. The general hypothesis was: The implementation of security configuration controls significantly influences the GPA Business SAC's database – Lima 2022.

Basically, it is quantitative research, in which the scientific method is used as a general method and the type of research corresponds to applied research, the research design used was pre-experimental, where security configuration controls were implemented in the database of GPA Business SAC.

The Wilcoxon statistical test was used to compare the hypotheses, which allowed determining the influence of the security configuration controls in the GPA Business SAC's database. Since the p value obtained was 0.000, being less than the significance level of 0.05%, therefore, the company GPA Business SAC can significantly improve the confidentiality, availability and integrity of the information it hosts in its database through implementation.

INTRODUCCIÓN

Este proyecto de investigación se titula: “Implementación de controles de configuración de seguridad en la base de datos de GPA Business SAC”, con el problema de investigación: ¿De qué manera la implementación de controles de configuración de seguridad influye en la base de datos de GPA Business SAC?, Para dar solución a este problema de investigación, se logró el siguiente objetivo: Determinar de qué manera la implementación de controles de configuración de seguridad influye en la base de datos de la GPA Business SAC. planteando la solución al problema encontrado en la empresa. Los resultados que se obtienen con la implementación de controles de configuración de seguridad en la base de datos de la empresa son de beneficio para la empresa, para sus usuarios e investigadores al obtener nuevos conocimientos y experiencias.

Este estudio se divide en cinco capítulos, siendo su estructura la siguiente:

Capítulo I: Contiene el problema de investigación a partir del cual se desarrolló el planteamiento del problema, la formulación y sistematización del problema, la justificación, delimitaciones, limitaciones y los objetivos de la investigación. Capítulo II: Incluye el desarrollo del Marco Teórico presentando los antecedentes internacionales y nacionales, el marco conceptual, la definición de términos, la hipótesis y las variables de la investigación. Capítulo III: Cubre la Metodología de la Investigación, tipo, nivel, diseño, población y muestra de la investigación, técnicas e instrumentos de recolección de datos, procesamiento de la información, técnicas y análisis de datos. Capítulo IV: Contiene los resultados de la investigación. Capítulo V: contiene la discusión de resultados, conclusiones y recomendaciones. Finalmente se incluye las referencias bibliográficas y los anexos.

CAPITULO I:

EL PROBLEMA DE INVESTIGACIÓN

1.1. PLANTEAMIENTO DEL PROBLEMA

La globalización en el entorno de la tecnificación se incrementó en los últimos 20 años, lo cual nos ha habituado a utilizar los medios digitales, por ello tenemos el riesgo de ciber amenazas, ciberdelitos y ciber riesgo, para lo cual estos mecanismos de salvaguarda de la data renacen en la ciberseguridad. (Arroyo&Hernández, 2020).

Cada vez se hace más importante, que la entidad privada y pública y consiguientemente para la existencia habitual que conocemos; parte de este progreso aporta nuevos desafíos como son la defensa ante amenazas de ciberdelitos de complejidad variada, ataques que se despliegan escudriñando vulnerar la data informática del sector público o privado para desenlaces delictivos. (Bohórquez, 2020)

Según ESET Threat Report T3 2021, en el tercer trimestre del 2021, en Europa y Asia, los países que tuvieron mayores incidencias de ataques cibernéticos fueron España con un 7,8 %, Turquía con el 6,6 % y Japón con el 5,5 %. (p.22)

Mientras que, en el continente de América, de acuerdo con los datos de la telemetría de ESET, las empresas en Brasil fueron las más afectadas por malware con el 19% de todas las detecciones en Latinoamérica, seguidas por las de México (17,5%), Argentina (13,3%), Colombia (10,6%) y Perú (8,9%). (p.13)

De acuerdo a lo publicado en welivesecurity by ESET, esta ola de ataques afectó a varios organismos públicos de Costa Rica con los ataques del grupo Conti, que primero atacó al Ministerio de Hacienda de Costa Rica y luego extendió su ataque a otras entidades públicas, y también del Ransomware Hive, que atacó a la Caja Costarricense de Seguro Social

(CCSS). Por su parte, Conti también atacó a organismos públicos de Perú, mientras que en Argentina el Poder Judicial de Córdoba fue víctima de un ataque del Ransomware Play y el Ransomware Quantum atacó a agencias gubernamentales de República Dominicana.

En ese sentido, la Secretaria de Gobierno y Transformación Digital remite a las Entidades Privadas y Públicas del estado peruano, el Comunicado N°004-2022-PCM/SGTD/CNSD, por medio del cual indican las previsiones del caso que deben de implementar en el menor tiempo posible, teniendo dentro sus principales sugerencias, las siguientes:

- Se debe implementar un firewall de base de datos.
- Se debe implementar el monitoreo permanente de los servicios ofrecidos para garantizar su disponibilidad, así como también la trazabilidad de las operaciones.
- Cambiar de contraseñas a todos los usuarios de todas las plataformas.
- Realizar una revisión completa de los usuarios creados para cada uno de los sistemas informáticos y de comunicación.

Por lo antes indicado, la GPA Business SAC requiere la implementación de controles de configuración de seguridad que van influir significativamente en su base de datos, que le permitirá mejorar la confidencialidad, disponibilidad e integridad de la información que aloja en su base de datos y aunque la seguridad total es inalcanzable, mediante el presente proyecto se espera lograr un nivel de seguridad altamente satisfactorio, que minimice los riesgos a los que está expuesta la empresa y el impacto que ocasionarían si efectivamente se materializara algún ataque.

1.2. FORMULACIÓN Y SISTEMATIZACIÓN DEL PROBLEMA

1.2.1. Problema General

¿De qué manera la implementación de controles de configuración de seguridad influye en la base de datos de GPA Business SAC – Lima 2022?

1.2.2. Problemas Específicos

a) ¿De qué manera la implementación de controles de configuración de seguridad influye en la confidencialidad en la base de datos de GPA Business SAC – Lima 2022?
b) ¿De qué manera la implementación de controles de configuración de seguridad influye en la disponibilidad en la base de datos de GPA Business SAC – Lima 2022?
c) ¿De qué manera la implementación de controles de configuración de seguridad influye en la integridad en la base de datos de GPA Business SAC – Lima 2022?

1.3. JUSTIFICACIÓN

1.3.1. Social

La relevancia social de la investigación se sustenta en el beneficio de la empresa de elevar el control de configuración de seguridad en su base de datos, lo que permite que su información y la de sus clientes van a preservar su confidencialidad, integridad y disponibilidad. Por otro lado, esta investigación también sirve de guía a los administradores de base de datos, ingenieros, estudiantes de Ingeniería o profesionales de áreas afines que estén realizando actividades como administración de base de datos o que estén en prácticas de temáticas relacionadas con esta actividad, permitiéndoles aplicar los controles de configuración de seguridad como parte de las buenas prácticas para así reducir el grado de vulnerabilidad frente a un eventual ataque informático.

1.3.2. Teórica

La investigación, en su relevancia teórica, se basa en incrementar el conocimiento de cada uno de los controles de configuración de seguridad en una base de datos, verificando que la versión del parche siempre sea el vigente, que la configuración de los parámetros del listener.ora, los parámetros generales de la base de datos, los parámetros de conexión y acceso, parámetros de usuarios estén de acuerdo a lo recomendado, además de la

asignación y revocación de los privilegios justos y necesarios, finalmente verificar que se encuentren configurados los parámetros de auditoría tradicional y los parámetros de la auditoría unificada para obtener la trazabilidad de todas las actividades que se realiza en la base de datos. Además, esta investigación repercute en parte en el éxito de las empresas para mejorar su competitividad, ya que reducen el grado de vulnerabilidad ante ataques informáticos y se convierte en una guía primaria para futuros estudios de las mismas características debido a la obsolescencia e innovación tecnológica

1.3.3. Metodológica

La justificación metodológica de la investigación se basa en la aplicación de mecanismos de mejores prácticas de seguridad, estas recomendaciones de seguridad y protección de datos deben de incorporarse a las tareas diarias con el fin de reforzar nuestra postura general de seguridad, con la finalidad de garantizar significativamente la disponibilidad, integridad y confidencialidad de la información de la empresa GPA Business SAC, ya que es su activo más importante.

1.4. DELIMITACIONES

1.4.1. Espacial

El presente estudio y propuesta de Implementación de controles de configuración de seguridad en la base de datos será aplicado en la sede de GPA Business S.A.C. ubicado en la Asociación La Merced Mz “B” Lt “13” en el distrito de Ate Vitarte, provincia de Lima y departamento de Lima.

1.4.2. Temporal

La fecha correspondiente a considerar para el desarrollo del trabajo de investigación propuesto es de setiembre de 2022 hasta agosto de 2023.

1.4.4. Económica

La presente investigación tiene el carácter de autofinanciado por el investigador.

1.5. LIMITACIONES

Para el proceso de la investigación se encontró una serie de limitaciones que dificultaron el avance y desarrollo de la investigación, entre las limitaciones que se encontraron son las siguientes:

- Se tuvo dificultad con el acceso presencial al ambiente de desarrollo de la empresa GPA Business S.A.C.
- Se tuvo demora en la habilitación del acceso remoto al ambiente de desarrollo de la empresa GPA Business S.A.C.
- En el ambiente de desarrollo de la empresa GPA Business SAC tuvieron que recrear el servidor de base de datos del ambiente de producción.
- Se tuvo demora en la habilitación del acceso remoto al ambiente de control de calidad de la empresa GPA Business S.A.C.
- En el ambiente de control de calidad de la empresa GPA Business SAC tuvieron que recrear el servidor de base de datos del ambiente de producción.

1.6. OBJETIVOS

1.6.1. Objetivo General

Determinar de qué manera la implementación de controles de configuración de seguridad influye en la base de datos de la GPA Business SAC – Lima 2022.

1.6.2. Objetivos Específicos

a) Determinar de qué manera la implementación de controles de configuración de seguridad influye en la confidencialidad de la base de datos de GPA Business SAC – Lima 2022.

b) Determinar de qué manera la implementación de controles de configuración de seguridad influye en la disponibilidad de la base de datos de GPA Business SAC – Lima 2022.

c) Determinar de qué manera la implementación de controles de configuración de seguridad influye en la integridad de la base de datos de GPA Business SAC – Lima 2022.

CAPITULO II:

MARCO TEÓRICO

2.1. ANTECEDENTES

2.1.1. Internacionales

- **Paredes (2022) en su investigación "GUÍA DE IMPLEMENTACIÓN DE POLÍTICAS DE CONTROL PARA MITIGAR LOS CIBERATAQUES BASADOS EN EL MODELO CARDING EN LA COAC "RIOBAMBA LTDA", (tesis pregrado). Universidad Nacional de Chimborazo – Riobamba – Ecuador**; esta investigación desarrollo una guía de implementación de políticas de control para mitigar los ciberataques basados en el modelo Carding en la COAC "Riobamba Ltda." Este trabajo recolectó información crucial respecto a los parámetros de las metodologías ENISA y APCERT identificando lo más adecuados para el desarrollo de la guía. Luego de aplicar la técnica de recolección de información, se les logró un 40% para la identificación y análisis de riesgos., por otra parte, en las entrevistas con ejecutivos muestran evidencia de que los departamentos de tecnología tienen un 21% de efectividad en sus programas de seguridad cibernética, lo que tiene un impacto significativo en los riesgos asociados al modelo Carding. En la comparación entre métodos, ENISA obtuvo una puntuación de 19 puntos, correspondiente al 95% del criterio, mientras que APCERT obtuvo una puntuación de 15 puntos, correspondiente al 75%., por lo cual, empleó el método ENISA, el mismo que brindó

instrucciones detalladas para mitigar posibles ataques basados en el modelo Carding.

- **Vasquez (2021) en su tesis "CIBERSEGURIDAD BASADA EN ANALÍTICA PARA BASE DE DATOS ORACLE", (tesis maestría). Konrad Lorenz Fundación Universitaria – Bogotá, D.C. Colombia**; esta investigación clasificó el nivel de riesgo expuesto y automatizó la gestión del control del estado de una o más bases de datos Oracle, se apoyó en diferentes herramientas de analítica de datos que sirven para clasificar, predecir y automatizar. Investigó los estándares establecidos en diferentes organizaciones que vigilan y publican las mejores prácticas, siendo estas el insumo para construir una línea base de seguridad y a partir de ese proceso los diferentes datos obtenidos para asignar un estado de corrección de las vulnerabilidades encontradas y cruzarlas con la información obtenida de las publicaciones que genera la entidad NATIONAL VULNERABILITY DATABASE (NVD) a todos los productos de tecnología, utilizando en este caso las relacionadas con las bases de datos Oracle. Como resultado, el proyecto obtuvo niveles satisfactorios en el contexto desarrollado y dejó la posibilidad abierta para alcanzar un mejor rendimiento si se aplica en una o más organizaciones.
- **Barriga (2021) en su tesis "MÓDULO DE SEGURIDAD INFORMÁTICA APLICANDO LA AUTENTICACIÓN DE DOBLE FACTOR PARA LA EMPRESA HOME OFFICE S.A.S.", (tesis pregrado). Universidad Nacional de Chimborazo – Riobamba – Ecuador**; esta investigación implementó un módulo de seguridad informática mediante autenticación de dos factores para Home Office S.A.S., con el objetivo de administrar y autenticar la información de los usuarios, detectar, neutralizar ataques informáticos y garantizar el acceso exclusivo a sus usuarios autorizados. Utilizó varios métodos y metodologías en el desarrollo de

módulos informáticos, la metodología en cascada fue el análisis de factores de propiedad por información bibliográfica. La evaluación de los módulos de la computadora se realizó utilizando métodos Delphi bajo las métricas de seguridad del estándar ISO 25010. Se utilizaron dos ciclos para llevar a cabo este proceso. Como resultado, la primera interacción típicamente mostró un 83% de acuerdo y la segunda sesión mostró un 100% de acuerdo para todas las métricas, mejorando la seguridad informática de Home Office S.A.S.

- **Cifre (2020) en su tesis "MODELO DE SEGURIDAD PARA LA GESTIÓN DE VULNERABILIDADES DE SERVIDORES EN NUBES PRIVADAS", (tesis maestría). Universidad Tecnológica Nacional. Facultad Regional Santa Fe – Argentina**; esta investigación definió un modelo de seguridad para gestión de vulnerabilidades de servidores en Nubes privadas, que contemple lineamientos generales para el diseño de una política de seguridad donde se detalló roles de usuarios y documentación recomendada, un proceso de aseguramiento apoyado sobre actualizaciones, indicadores de vulnerabilidad basado en factores críticos de seguridad, y clasificó en niveles de seguridad fundamentada en la madurez de la organización. El propósito fue proponer especificaciones concretas de las actividades que se llevaron a cabo para realizar una adecuada gestión de vulnerabilidades siguiendo los lineamientos de los estándares internacionales ISO/IEC 27000 y O-ISM3, facilitando el proceso de certificación de ISO/IEC 27001 por parte de las organizaciones.
- **Flórez y Quintana (2018) en su tesis "SISTEMA DE DETECCIÓN DE ATAQUES INFORMÁTICOS A REDES DE DATOS EMPRESARIALES SOPORTADO EN HONEYPOTS", (tesis grado). Universidad de Cartagena Facultad de Ingeniería Programa de Ingeniería de Sistemas – Cartagena de Indias – Colombia**; esta investigación

implementó un sistema para simplificar el análisis de la información obtenida de ataques informáticos a redes de datos empresariales soportado en honeypots. Un honeypot es una herramienta de "engaño", diseñada para detectar a un atacante que intenta comprometer los sistemas de información electrónica de una organización. Si se implementa correctamente, un honeypot puede servir como un mecanismo de alerta temprana y un dispositivo avanzado de vigilancia de seguridad. Se puede usar para minimizar los riesgos de ataques a sistemas y redes de TI. Propuso el diseño y desarrollo de un sistema de detección de ataques informáticos a redes de datos empresariales utilizando honeypots para poder analizar, observar y rastrear los ataques de los intrusos o hackers en las redes empresariales, permitiéndole al administrador de TI aportar mejoras a los esquemas de seguridad de la empresa en la cual trabaja. Teniendo presente el principio de los honeypots expresado en la frase "CONOCE A TU ENEMIGO", podrá identificarlo, estudiarlo, conocer los servicios que más ataca, o los más vulnerables de la red atacada, siendo posible tomar medidas que permitan mitigar en cierto modo las vulnerabilidades existentes en cualquier entorno de red.

2.1.2. Nacionales

- **Castro (2022), en su tesis "ANÁLISIS COMPARATIVO DE ALGORITMOS DE APRENDIZAJE AUTOMÁTICO PARA IDENTIFICAR ATAQUES DE INYECCIÓN SQL A BASE DE DATOS EN APLICACIONES WEB". (tesis pregrado). Universidad Señor de Sipán**; esta investigación planteó un análisis comparativo de los algoritmos de aprendizaje automático para mitigar los ataques de inyección SQL, comprendió las etapas de clasificación de los algoritmos según su rendimiento en cuanto a precisión y de tipo de inyección SQL, realizó la extracción de los

datos para su procesamiento y aplicación de los algoritmos de aprendizaje automático seleccionados para el análisis de los datos clasificados. Para la clasificación de los ataques de inyección SQL a base de datos, construyó una tabla de clasificación por tipo de ataque y el nivel de riesgo que significan las firmas. La implementación de los algoritmos de aprendizaje automático lo realizó en el entorno de trabajo Jupiter Notebook y scikit-learn, utilizó Phyton con las librerías AdaBoost, SVM y Decision Tree que demostró ser un buen entorno porque evaluó la precisión de tres algoritmos de aprendizaje automático poniendo a prueba la data extraída después de recogerlo de los ataques realizados en un sitio web, finalmente, el algoritmo Decision Tree demostró una mejor precisión obteniendo el 100% al momento de realizar el análisis.

- **Díaz (2021), en su tesis: "MODELO DE PROCESOS PARA EL DESARROLLO DE SOFTWARE CON CARACTERÍSTICAS DE SEGURIDAD PARA VULNERABILIDADES MÁS RECURRENTES". (tesis pregrado). Universidad Señor de Sipán**; esta investigación planteó brindar una solución eficaz a las vulnerabilidades en el software que utiliza la nueva tecnología adquirida. Se basó en los modelos de procesos, para aplicar seguridad al software, utilizó OWASP SAMM y Microsoft-SDL, lo cual garantizo una protección alta a las vulnerabilidades de seguridad más recurrentes que fueron identificadas por OWASP, así también obtuvo las técnicas necesarias para evitar vulnerabilidades, información que sirvió de apoyo principal para el modelo de procesos y así evitar vulnerabilidades de manera eficaz en cada una de las etapas del ciclo de vida del desarrollo del software.
- **Dávila y Dextre (2021) en su tesis "PROPUESTA DE UNA IMPLEMENTACIÓN DE UN PROGRAMA DE GESTIÓN DE VULNERABILIDADES DE SEGURIDAD INFORMÁTICA PARA MITIGAR LOS SINIESTROS DE LA INFORMACIÓN EN EL**

POLICLÍNICO DE SALUD AMC ALIENADO A LA NTP-ISO/IEC 270001:2014 EN LA CIUDAD DE LIMA – 2021", (tesis pregrado). Universidad Tecnológica del Perú; esta investigación planteó un modelo de gestión, análisis y evaluación del estado de vulnerabilidades existentes en los activos de información del Policlínico de Salud AMC. Logrando una gestión adecuada de estos y con la garantía de que se cumplan los basados en la NTP ISO 27001:2014 usó los dominios del anexo A para contribuir en el proceso de gestión de vulnerabilidades. Esto le permitió conocer la realidad del Policlínico de salud AMC de tal forma que hizo un análisis y evaluación de las debilidades que se detectaron y determinó así su ciclo de vida. Luego, detectó y analizó las debilidades en AMC a través de herramientas de escaneos automatizados sobre la infraestructura de la entidad; finalmente, definió y estableció los controles del Anexo A de la norma indicada lo cual formó parte del proceso de gestión de vulnerabilidades.

- **Ramírez (2019) en sus tesis "IMPLEMENTACIÓN DE LINEAMIENTOS BASE DE SEGURIDAD EN BASE DE DATOS ORACLE Y SQL SERVER EN UNA ENTIDAD BANCARIA" (tesis pregrado). Universidad San Ignacio de Loyola;** esta investigación tuvo como objetivo la aplicación de líneas base de seguridad de base de datos para los motores Oracle y Microsoft SQL Server en los activos de base de datos de la entidad bancaria Falabella. Estos lineamientos base eran configuraciones de seguridad que fueron aplicados en los entornos de desarrollo y calidad y se encuentran bajo los criterios establecidos por CIS Benchmarks, desarrollado por Center for Internet Security (CIS), estándar global de las mejores prácticas reconocidas para proteger la seguridad de los sistemas de tecnologías de la información (TI).
- **Huincho (2019) en su tesis "SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA MEJORAR LA**

PROTECCIÓN INFORMÁTICA DE LA COMISARIA REGIÓN HUANCAVELICA". (tesis pregrado). Universidad Nacional Daniel Alcides Carrión; esta investigación se enfocó en la apreciación y análisis de un factor de riesgos que provino desde el interior de la institución, aseguró sus datos e información de valor con la ayuda de un Sistema de Gestión de Seguridad de la Información, conociendo, gestionando y minimizando los posibles riesgos que atenten contra la seguridad de la información que se puede encontrar en los correos electrónicos, páginas web, imágenes, bases de datos, faxes, contratos, presentaciones, documentos, entre otros, por lo que, el ciclo de vida de la información debe ser considerado. Este enfoque permite analizar y organizar la estructura del sistema de información, lo que facilita la determinación de procedimientos de trabajo para mantener su seguridad. Además, gestionó los riesgos a través de un Sistema de Gestión de Seguridad de la Información que le permitió preservar la confidencialidad, integridad y disponibilidad de la misma, en el interior de la empresa, ante sus clientes y ante las distintas partes interesadas del negocio. Esta implementación de SGSI le permitió un gran aumento en la seguridad de los activos de información de la comisaria de la región de Huancavelica., que garantizó que los riesgos de seguridad de información fueran conocidos, asumidos, gestionados y minimizados de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptable ante los cambios que se produzcan en los riesgos, en su entorno y las nuevas tecnologías.

2.2. MARCO CONCEPTUAL

2.2.1. Controles de configuración de seguridad

El término control proviene de un vocablo francés, controle. El cual tiene como significado comprobación, fiscalización o inspección.

Hoy en día la rápida evolución del entorno técnico requiere que las organizaciones adopten un conjunto mínimo de controles de

seguridad para proteger su información y sistemas de información. (Huincho, 2019, p.17).

Pese a que estar protegidos todo el tiempo no es factible, así como tener control de un zero day, sí es posible contar con todos los controles y medidas sobre las entidades será un apoyo clave para la contención y protección en estas situaciones. (Dávila y Dextre, 2021, p. 19).

CIS Benchmarks establece un conjunto de controles de seguridad de base de datos aplicables a plataformas Oracle versión 11g basado en su documento CIS Oracle Database 11g R2 Benchmark v2.0.0 (2016) y plataformas Oracle versión 12c basado en su documento CIS Oracle Database 12c Benchmark v1.1.0. (Ramírez, 2019, p. 19).

2.2.2. Seguridad

El término seguridad proviene de la palabra securitas del latín hace foco en la característica de seguro, es decir, realza la propiedad de algo donde no se registran peligros, daños ni riesgos. Una cosa segura es algo firme, cierto e indubitable.

Según la IS027002, “La seguridad de la información se puede caracterizar por la preservación de:

- Confidencialidad: asegura que el acceso a la información está adecuadamente autorizado.
- Integridad: Salvaguarda la precisión y completitud de la información y sus métodos de proceso.
- Disponibilidad: Asegura que los usuarios autorizados pueden acceder a la información cuando la necesitan”.

INFOSEC Glossary 2000: “Seguridad Informática son las medidas y controles que aseguran la confidencialidad, integridad y disponibilidad de los activos de los sistemas de información, incluyendo hardware, software, firmware y aquella información que procesan, almacenan y comunican”. De estas definiciones podemos deducir que los principales objetivos de la seguridad informática son:

- Confidencialidad: consiste en la capacidad de garantizar que la información, almacenada en el sistema informático o transmitido por la red, solamente va a estar disponible para aquellas personas autorizadas a acceder a dicha información, es decir, que, si los contenidos cayesen en manos ajenas, estas no podrían acceder a la información o a su interpretación.
- Disponibilidad: la definiremos como la capacidad de garantizar que tanto el sistema como los datos van a estar disponibles al usuario en todo momento. Pensemos, por ejemplo, en la importancia que tiene este objetivo para una empresa encargada de impartir ciclos formativos a distancia. Constantemente está recibiendo consultas, descargas a su sitio web, etc., por lo que siempre deberá estar disponible para sus usuarios.
- Integridad: diremos que es la capacidad de garantizar que los datos no han sido modificados desde su creación sin autorización. La información que disponemos es válida y consistente. Este objetivo es muy importante cuando estamos realizando trámites bancarios por Internet. Se deberá garantizar que ningún intruso pueda capturar y modificar los datos en tránsito.
- No repudio: este objetivo garantiza la participación de las partes en una comunicación. En toda comunicación, existe un emisor y un receptor, por lo que podemos distinguir dos tipos de no repudio: a) No repudio en origen: garantiza que la persona que envía el mensaje no puede negar que es el emisor del mismo, ya que el receptor tendrá pruebas del envío. b) No repudio en destino: El receptor no puede negar que recibió el mensaje, porque el emisor tiene pruebas de la recepción del mismo. Este servicio es muy importante en las transacciones comerciales por Internet, ya que incrementa la confianza entre las partes en las comunicaciones.

Figura 1: Características de la Seguridad
Fuente: Elaboración propia

Los siguientes mecanismos se utilizan para lograr los objetivos que se muestran en el diagrama anterior:

- Autenticación, que permite identificar al remitente del mensaje, al creador del documento o al dispositivo conectado a la red o servicio.
- Autorización, que controla el acceso del usuario a áreas restringidas, diversos dispositivos y servicios después de pasar el proceso de autorización.
- Auditoría, confirman la eficacia de las políticas o medidas de seguridad adoptadas.
- Encriptación, ayuda a ocultar la información transmitida a través de la red o almacenada en dispositivos, para que cualquier persona no autorizada sin un algoritmo y una clave pueda acceder a la información protegida.
- Realización de copias de seguridad e imágenes de respaldo, para que podamos recuperar la información perdida o dañada en caso de error.
- Antivirus, consiste en programas diseñados para protegerlo de las amenazas de virus.
- Cortafuegos o firewall, un programa que monitorea y previene intentos de conexión no deseados tanto desde su computadora a una red como viceversa.

- Servidores proxys, consiste en una computadora que ejecuta un software especializado que actúa como intermediario entre la red interna de una empresa y una red externa como Internet. Entre otras cosas, estos servidores verifican y autorizan el acceso de los usuarios a varios tipos de servicios como FTP (transferencia de archivos) y Web (acceso a páginas de Internet).
- Utilización de firma electrónica o certificado digital, son mecanismos para asegurar la identidad de las personas o sujetos, para evitar el no repudio al firmar declaraciones o documentos. Hoy en día, también se utilizan ampliamente para establecer una comunicación segura entre la computadora de un usuario y un servidor de Internet, como el sitio web de un banco.
- Un conjunto de leyes diseñadas para proteger los datos personales que exigen que las empresas mantengan su confidencialidad.

Las organizaciones poseen información que deben proteger frente a riesgos y amenazas para asegurar el correcto funcionamiento de su negocio. Este tipo de información imprescindible para las empresas es lo que se denomina activo de información.

2.2.3. Actualización del software de base de datos y configuración de parámetros

Según Sánchez (2017), Instalar una base de datos implica conocer muy bien el funcionamiento de las bases de datos y la arquitectura del SGBD concreto que vamos a instalar.

Actualizaciones de seguridad: Al tratarse de entornos de 'software', es importante que los sistemas se actualicen con las últimas versiones que hayan sido validadas como correctas, para evitar ataques apoyados en posibles vulnerabilidades. (Cifre, 2020, p. 13).

2.2.4. Configuración de parámetros de conexión, acceso, usuarios y asignación y/o revocación de privilegios

Los SGBD ofrecen mecanismos para implantar restricciones de integridad en la base de datos. Estas restricciones van a proteger la base de datos contra daños accidentales. Los valores de los datos que se almacenan deben satisfacer ciertos tipos de restricciones de consistencia y reglas de integridad, que especificará el administrador de la base de datos. El SGBD puede determinar si se produce una violación de la restricción. (Vasquez, 2021, p. 18).

¿Qué se entiende por Autorización?, es el proceso que garantiza que los usuarios correctamente autenticados puedan acceder solo a aquellos recursos para los cuales el propietario les ha dado su aprobación. La autorización también se conoce como control de acceso, y estas dos palabras serán usadas de aquí en adelante como sinónimos dentro de este documento. El control de acceso puede ser utilizado en diferentes contextos como: proteger los archivos y carpetas en un equipo de cómputo, controlar el acceso a las bases de datos, preservar la información en las aplicaciones, este último es el alcance para este documento. (Cardona, 2021, p. 5).

2.2.5. Configuración de parámetros de auditorías

Con el análisis de la auditoría, tomar las respectivas medidas sobre los controles, procedimiento y normas que se tiene y que ha fallado, realizar las correcciones respectivas en la política, darla a conocer a los usuarios que interactúan con la base de datos. (Gómez, 2018, p. 77).

Un requisito de auditoría y de gran importancia para las investigaciones forenses es la aplicación de pistas de auditoría y la generación de trazabilidad de las actividades que afectan la integridad de los datos o la visualización de los datos sensibles. (Bonilla, 2017, p. 56)

2.2.6. Base de Datos

Definimos un Sistema Gestor de Bases de Datos o SGBD, también llamado DBMS (Data Base Management System) como una colección de datos relacionados entre sí, estructurados y organizados, y un conjunto de programas que acceden y gestionan esos datos. (Vasquez, 2021, p. 17).

Este componente se encarga de la permanencia de los datos del usuario con respecto al tiempo, se guarda toda la información sensible que sea administrada por el sistema de administración. (Flores y Quintana, 2018, p. 57).

Las bases de datos constituyen un sistema de proceso de datos cuyo objetivo básico es el de conservar información y mantenerla disponible para su acceso de forma eficiente. El interés de los usuarios por la información contenida en una base de datos es debido, a su significación en los procesos de toma de decisiones.

Las aplicaciones de bases de datos tienen cuatro componentes principales: datos, programas, dispositivos de almacenamiento y usuarios. Las principales ventajas que presentan respecto a los datos se refieren a su integración y la posibilidad de ser compartidos. Las bases de datos permiten la unificación de distintos ficheros de datos -integración- con eliminación de redundancias y repeticiones entre ellos. Los datos compartidos están accesibles por diversos usuarios, de forma aparentemente simultánea y para diferentes propósitos. Una misma base de datos puede ser percibida por distintos usuarios de forma variable.

Un Sistema Gestor de Base de Datos (SGBD) proporciona los siguientes mecanismos para garantizar la seguridad e integridad de los datos:

- Debe garantizar la protección de los datos contra accesos no autorizados, tanto intencionados como accidentales.

Debe controlar que sólo los usuarios autorizados accedan a la base de datos.

- Los SGBD ofrecen mecanismos para implantar restricciones de integridad en la base de datos. Estas restricciones van a proteger la base de datos contra daños accidentales. Los valores de los datos que se almacenan deben satisfacer ciertos tipos de restricciones de consistencia y reglas de integridad, que especificará el administrador de la base de datos. El SGBD puede determinar si se produce una violación de la restricción.
- Proporciona herramientas y mecanismos para la planificación y realización de copias de seguridad y restauración.
- Debe ser capaz de recuperar la base de datos llevándola a un estado consistente en caso de ocurrir algún suceso que la dañe.
- Debe asegurar el acceso concurrente y ofrecer mecanismos para conservar la consistencia de los datos en el caso de que varios usuarios actualicen la base de datos de forma concurrente. (Vasquez, 2021, p. 18).

2.2.7. Disponibilidad

Disponibilidad, se refiere a la propiedad de ser accesible y utilizable a demanda por una entidad autorizada. (Cardona, 2021, p. 23).

Acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran. (Nieves, 2017, p. 12).

2.2.8. Confidencialidad

Confidencialidad, que se entiende como la propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados. (Cardona, 2021, p. 23).

La información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados. (Nieves, 2017, p. 11).

2.2.9. Integridad

Integridad, se define como la propiedad de exactitud y completitud (Cardona, 2021, p. 23).

Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso. (Nieves, 2017, p. 11).

2.3. DEFINICIÓN DE TÉRMINOS

2.3.1. Listener.ora

Para obtener una conexión desde fuera del servidor donde está instalada la base de datos Oracle, se debe acceder al servicio denominado listener, este debe estar activado. o como se suele decir, el listener de Oracle debe estar escuchando. En pocas palabras es el puerto de escucha del servidor para atender las peticiones de los clientes.

2.3.2. Malware

Software malicioso que tiene como objetivo infiltrarse o dañar un sistema de información sin el consentimiento de su propietario. Se destacan virus, gusanos, troyanos, keyloggers, botnets, spyware, adware y ransomware. (Cifre, 2020, p. 97)

2.3.3. Parámetros generales de Base de Datos Oracle

La operación de la instancia de base de datos Oracle está gobernada por numerosos parámetros que están establecidos en archivos de configuración específicos. (Ramírez, 2019, p. 19).

2.3.4. Parche

Un parche es una pieza de software diseñado para actualizar un programa de computadora o sus datos de apoyo, para corregir o mejorar la misma. Esto incluye la fijación de las vulnerabilidades de seguridad y otros aspectos. Con este tipo de parches, generalmente llamados correcciones de errores, permite mejorar la facilidad de uso o el rendimiento. (Cifre, 2020, p. 97)

2.3.5. Ransomware

Tipo de malware que impide a los usuarios acceder a su sistema o a sus archivos personales y que exige el pago de un rescate para poder acceder de nuevo a ellos. (Cifre, 2020, p. 97)

2.3.6. SQL

El significado de las siglas en inglés Structured Query Languaje, lenguaje declarativo o de consulta estructurada de acceso a bases de datos relacionales. (Gomez, 2018, p. 13)

2.3.7. Versión del parche del motor de BD

Siempre que se publican actualizaciones de software para mejorar la seguridad de cualquier motor de base de datos. Si no se siguen o se aplican estas actualizaciones de software, el sistema será más vulnerable a los ataques. (Bonilla, 2017, p. 42)

2.3.8. Vulnerabilidad y ataques informáticos

Una vulnerabilidad es una debilidad o fallo en un sistema de información que pone en riesgo la seguridad de la información permitiendo que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad de la misma, por lo que es necesario encontrarlas y eliminarlas lo antes posible. Estas debilidades o fallas pueden tener distintos orígenes, entre los que se destacan: fallos de diseño, errores de configuración, carencias de procedimientos o limitaciones propias de la tecnología. (Cifre, 2020, p. 14)

2.4. HIPÓTESIS

2.4.1. Hipótesis General

La implementación de controles de configuración de seguridad influye significativamente en la base de datos de GPA Business SAC – Lima 2022.

2.4.2. Hipótesis Específicas

a) La implementación de controles de configuración de seguridad influye significativamente en la confidencialidad de la base de datos de GPA Business SAC – Lima 2022.

b) La implementación de controles de configuración de seguridad influye significativamente en la disponibilidad de la base de datos de GPA Business SAC – Lima 2022.

c) La implementación de controles de configuración de seguridad influye significativamente en la integridad de la base de datos de GPA Business SAC – Lima 2022.

2.5. VARIABLES

2.5.1. Definición conceptual de la variable

a) Controles de configuración de seguridad

Hoy en día la rápida evolución del entorno técnico requiere que las organizaciones adopten un conjunto mínimo de controles de seguridad para proteger su información y sistemas de información. (Huincho 2019).

b) Base de datos

Definimos un Sistema Gestor de Bases de Datos o SGBD, también llamado DBMS (Data Base Management System) como una colección de datos relacionados entre sí, estructurados y organizados, y un conjunto de programas que acceden y gestionan esos datos. (Vásquez 2021).

2.5.2. Definición operacional de la variable

a) Controles de configuración de seguridad

Corresponde a la operación de los numerosos parámetros que están establecidos en archivos de configuración específicos de una base de datos Oracle, estas configuraciones deberán ser consideradas y mantenidas cuidadosamente.

b) Base de Datos

Sistema de gestión de datos relacionales basado en SQL. Se diseñó y se optimizó para las aplicaciones web y puede utilizarse en cualquier plataforma. Dado que está diseñado para procesar millones de consultas y miles de transacciones, es una elección popular para las empresas de comercio electrónico.

2.5.3. La operacionalización de variables

Tabla 1: Operacionalización de variables

VARIABLES	DEFINICIÓN CONCEPTUAL	DEFINICIÓN OPERACIONAL	DIMENSIONES	INDICADORES	ÍTEMS	TIPO DE VARIABLES	INSTRUMENTOS
Controles de configuración de seguridad	Hoy en día la rápida evolución del entorno técnico requiere que las organizaciones adopten un conjunto mínimo de controles de seguridad para proteger su información y sistemas de información. (Huincho 2019)	Corresponde a la operación de los numerosos parámetros que están establecidos en archivos de configuración específicos de una base de datos Oracle, estas configuraciones deberán ser consideradas y mantenidas cuidadosamente	Actualización del software de base de datos y configuración de parámetros	• Versión del parche del motor de BD. • Configurar parámetros de listener. • Configurar parámetros generales de BD	1 2 y 3 4 al 19	Nominal cuantitativo	Lista de cotejo
			Configuración de parámetros de conexión, acceso, usuarios y asignación y/o revocación de privilegios	• Configurar parámetros de conexión y acceso. • Configurar parámetros de usuarios. • Asignar y/o revocar privilegios	20 al 28 29 al 34 35 al 76		
			Configuración de parámetros de auditorías.	• Configurar parámetros de auditoria tradicional. • Configurar parámetros de auditoría unificada	77 al 94 95 al 121		

Base de Datos	Definimos un Sistema Gestor de Bases de Datos o SGBD, también llamado DBMS (Data Base Management System) como una colección de datos relacionados entre sí, estructurados y organizados, y un conjunto de programas que acceden y gestionan esos datos. (Vásquez 2021)	Sistema de gestión de datos relacionales basado en SQL. Se diseñó y se optimizó para las aplicaciones web y puede utilizarse en cualquier plataforma. Dado que está diseñado para procesar millones de consultas y miles de transacciones, es una elección popular para las empresas de comercio electrónico.	Disponibilidad Confidencialidad Integridad	Grado de disponibilidad Grado de confidencialidad Grado de integridad	Del 2 al 19 Del 20 al 76 1 y del 77 al 121	Nominal cualitativo	Lista de cotejo

Tabla 1: Operacionalización de las variables

Fuente: Elaboración Propia

CAPITULO III:

METODOLOGIA

3.1. MÉTODO DE INVESTIGACIÓN

La investigación de acuerdo a sus objetivo y naturaleza se encuentra dentro del enfoque cuantitativo, debido a que los datos recolectados son numéricos y el método general que se utilizará será el método científico, ya que se hará uso de la metodología científica para lograr la meta de la investigación en este caso establecer la influencia de los controles de configuración de seguridad en la base de datos de la empresa GPA Business SAC. “Es el procedimiento que se sigue en la investigación, con el objetivo de descubrir las formas de existencia de los procesos objetivos, para desentrañar sus conexiones internas y externas, para generalizar y profundizar los conocimientos así adquiridos, para llegar a demostrarlos con rigor racional y para comprobarlos en el experimento y con las técnicas necesarias”. (Cabezas, Andrade y Torres, 2018)

3.2. TIPO DE INVESTIGACIÓN

El estudio corresponde a una investigación aplicada, ya que se manifiesta que la variable “Controles de configuración de seguridad” permitirá a la empresa GPA Business SAC tener instancias de base de datos significativamente seguras. “La teoría se encarga de resolver problemas prácticos, se basa en los hallazgos, descubrimientos y soluciones que se planteó en el objetivo del estudio, normalmente este tipo de investigación se utiliza en la medicina o ingenierías”. (Arias, 2021).

3.3. NIVEL DE INVESTIGACIÓN

El nivel de investigación que se utilizó fue el de carácter explicativo, de acuerdo a Arias “Este alcance tiene la característica de establecer causa – efecto entre sus variables”, (Arias, 2021).

Este estudio recopiló información sobre los controles de configuración de seguridad antes y después; para medir la variable y luego mostrar el nivel de importancia de seguridad que proporciona en las instancias de base de datos de la empresa GPA Business SAC.

3.4. DISEÑO DE INVESTIGACIÓN

El diseño de la investigación fue pre - experimental con un grupo de pre y post prueba. “Existen los estudios de un grupo con una sola medición. Se realiza la medición luego de aplicar el tratamiento en tiempos diferentes” (Arias, 2021)

M = O1 X O2

Donde:

M: Muestra (Instancias: bdgpadev, bdgpaqa)

O1: Observación (Pre test)

O2: Observación (Post test)

X: Manipulación de la variable Independiente

3.5. POBLACIÓN Y MUESTRA

3.5.1. Población

“La población es un conjunto de elementos con fines comunes de los cuales resulta las conclusiones más relevantes de una investigación” (Cabezas, Andrade y Torres, 2018).

La población se encuentra constituida por las tres instancias de bases de datos Oracle 19c de los ambientes de producción, control de calidad y desarrollo de la

empresa GPA Business SAC, como se muestra a continuación.

Tabla 2: Instancias de bases de datos Oracle 19c

Ambiente	Instancia BD	Motor BD	Versión	Esquema
Producción	bdgpaprd	Oracle	19.0	BD_GPA
Control de calidad	bdgpaqa	Oracle	19.0	BD_GPA
Desarrollo	bdgpadev	Oracle	19.0	BD_GPA

Tabla 2: Instancias de bases de datos Oracle 19c
Fuente: Elaboración propia

3.5.2. Muestra

Se aplicará la muestra no probabilística por conveniencia, considerando las instancias de base de datos “bdgpadev” del ambiente de desarrollo y la instancia de base de datos “bdgpaqa” del ambiente de control de calidad.

3.6. TÉCNICAS E INSTRUMENTOS DE RECOLECCIÓN DE DATOS

La técnica de investigación utilizada en el estudio es la observación y el instrumento utilizado fue la lista de cotejo, las mismas que se aplicaron a cada uno de los elementos de la muestra

3.6.1. Técnicas

Su centro de apoyo está en el proceso de investigación a las medidas numéricas, se fundamenta y utiliza la observación del proceso en forma de recolección de datos y los analiza para llegar a responder las preguntas que se plantean en un inicio de la investigación. (Cabezas, Andrade y Torres, 2018).

3.6.2. Instrumentos

Es un instrumento o herramienta de investigación que sirve a la observación. Llamada también hoja de chequeo o check list, consiste en una cédula u hoja de control, de verificación de la presencia o ausencia de conductas, secuencia de acciones, destrezas, competencias,

aspectos de salud, actividades sociales etc. (Ñaupas, Valdivia, Palacios y Romero. 2018).

3.7. PROCESAMIENTO DE LA INFORMACIÓN

Se utilizaron diversas herramientas de software para procesar la información:

Para el proceso de recolección de información se utilizó el software Toad versión 16.0, herramienta donde se ejecutó los scripts y se pudo recolectar las evidencias de la recolección de información.

Para el proceso de ingreso de los datos obtenidos y su respectiva evaluación se utilizó el Microsoft Excel 2019.

Asimismo, para realizar el procesamiento, análisis y calculo estadístico de los datos recolectados a través de la lista de cotejo, se utilizó el software SPSS (Statistical Package for Social Sciences) Versión 26.

3.8. TÉCNICAS Y ANÁLISIS DE DATOS

Se efectuó la ejecución de la recolección de información en las instancias de bases de datos del ambiente de desarrollo y control de calidad de la empresa GPA Business SAC y los datos obtenidos se trasladaron a la lista de cotejo, los mismos que fueron trasladados a la herramienta de cálculo estadístico SPSS para medir la confiabilidad del instrumento, a través del coeficiente de Kuder-Richardson, estadístico que permite calcular una medida de confiabilidad de la consistencia interna para las medidas con opciones dicotómicas. (No aplicado (0) - Aplicado (1)); obteniendo el siguiente resultado:

Estadísticas de fiabilidad

Alfa de Cronbach	N de elementos
1,000	2

Tabla 3: Estadísticas de fiabilidad
Fuente: Elaboración propia

Se llegó a la conclusión de que el instrumento utilizado es válido y sirve para el propósito de la investigación.

La validez del instrumento se realizó con la Ficha de Validez del Instrumento, para ello los jueces validaron la lista de cotejo de los controles de configuración de seguridad de las instancias de base de datos Oracle 19c de los ambientes de desarrollo y control de calidad de la empresa GPA Business SAC.

Se utilizó para procesar y analizar los datos obtenidos en el proceso de comparar los resultados del pretest, que son los resultados del proceso en su estado inicial, con los resultados del post test que son los resultados obtenidos después de implementar los controles de configuración de seguridad faltantes; se utilizaron estadísticas descriptivas como frecuencias y estadísticas inferenciales como las pruebas de Shapiro-Wilk y Wilcoxon.

3.8. ASPECTOS ETICOS DE LA INVESTIGACIÓN

La información utilizada en esta investigación fue obtenida con el uso del instrumento de investigación; la lista de cotejo para los controles de configuración de seguridad en la base de datos Oracle 19c para cada una de las instancias de base de datos del ambiente de desarrollo (bdgpadev) y del ambiente de control de calidad (bdgpaqa) de la empresa GPA Business SAC tanto en el pre test como en el post test; información que se procesó de forma adecuada sin adulteraciones, la misma que cuenta con la confidencialidad respectiva.

El investigador asume el compromiso de evidenciar información real y transparente, así mismo de brindar la confianza a la entidad de que los datos recolectados solo serán de uso para la presente investigación.

CAPITULO IV:

RESULTADOS

4.1. DESCRIPCIÓN DEL DISEÑO TECNOLÓGICO

GPA BUSINESS S.A.C. es una empresa consultora en tecnología, dedicada al desarrollo de herramientas tecnológicas para la optimización de todos los procesos que las empresas medianas y grandes requieren hoy para un desempeño competitivo. Cuenta con un equipo que está integrado por analistas, especialista IT, diseñadores y comunicadores.

Objetivo: Ser proveedores de las mejores marcas y brindar un buen asesoramiento en equipos informáticos y sistemas de circuito cerrado.

Misión: Ser socio estratégico para sus empresas clientes, trabajando en conjunto para obtener estándares acordes a su realidad con los mejores equipos de cómputo y cámaras de vigilancia.

Visión: Ser una empresa que se desarrolle de forma confiable, segura, sólida, flexible y rentable, construyendo el cambio en la era del conocimiento, con la audacia y calidad humana de su gente, con una gestión que se anticipe y se adapte al cambio, aprenda de la experiencia e innove permanentemente.

Para el presente trabajo de investigación la unidad de análisis es la instancia de base de datos que aloja la información del sistema informático de la empresa GPA Business SAC.

La instancia de base de datos almacena la información de los procesos de negocio en el esquema de base de datos “BD_GPA”, preservando su integridad, confiabilidad y disponibilidad del activo más importante de la empresa GPA Business SAC.

Los ambientes de desarrollo, control de calidad y producción cuentan con una instancia de base de datos cada una, estas se encuentran

homologadas sobre el mismo sistema operativo (Windows) el cual está certificado por el fabricante del motor de base de datos. (Oracle).

La lista de cotejo fue generada en base al documento “CIS Oracle 19c Benchmark” recomendado por CIS Security Benchmarks y que se encuentra disponible en su página web.

Los controles de configuración de seguridad forman parte del estándar global de las mejores prácticas reconocidas para proteger la seguridad de los sistemas de tecnologías de la información de los diversos ataques informáticos más dominantes.

Se muestra el flujo del proceso para la implementación de los controles de configuración de seguridad en la base de datos de la empresa GPA Business SAC:

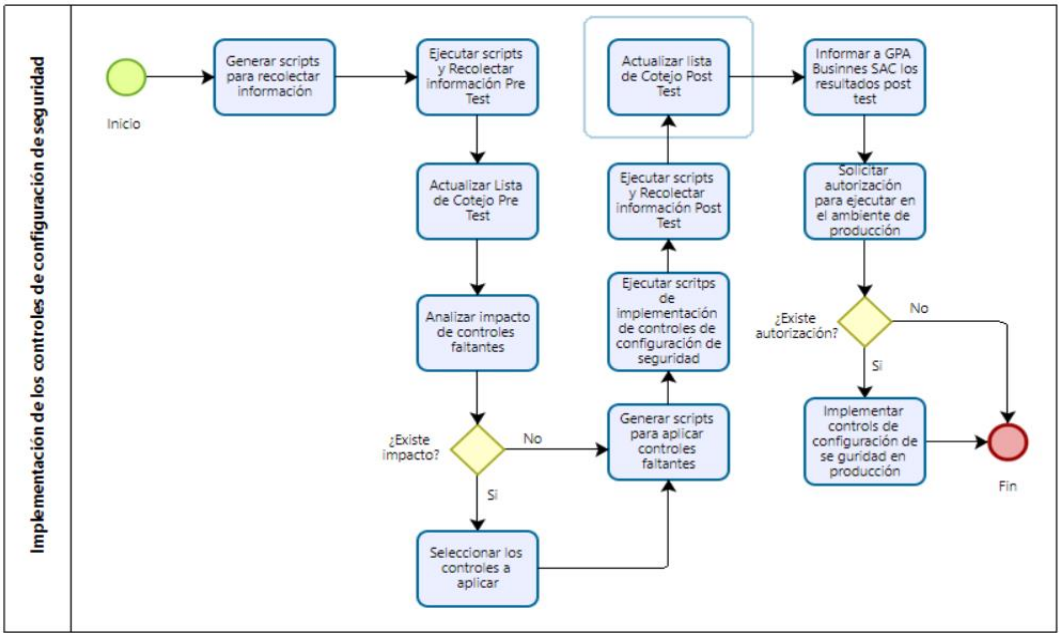

Figura 2: Flujo de proceso de implantación
Fuente: Elaboración propia

4.2. DESCRIPCIÓN DE RESULTADOS

4.2.1. Resultados preliminares de la prueba (Antes de la implementación de los controles de configuración de seguridad)

Variable: Controles de configuración de seguridad

Está conformada por tres dimensiones, cada dimensión tiene sus indicadores y cada indicador tiene los ítems que permite la medición respectiva. Para la medición de la variable uno hay un total de ciento

veintiún ítems que se encuentran distribuidos entre las dimensiones y estas a su vez en cada uno de los indicadores que las conforman.

Instancia		**bdgpadev**	**bdgpaqa**
Variable 1		Controles de configuración de seguridad	Controles de configuración de seguridad
N	Válido	121	121
	Perdidos	0	0

Tabla 4: Número de elementos de la variable 1
Fuente: Matriz de operacionalización de variables

Tabla de Frecuencias Pre Test de la variable Controles de configuración de seguridad en la instancia bdgpadev

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	No aplicado	67	55,4	55,4	55,4
	Aplicado	54	44,6	44,6	100,0
	Total	121	100,0	100,0	

Figura 3: Ítems no aplicado / aplicado de la Variable 1 en la instancia bdgpadev
Fuente: Lista de cotejo pre test instancia bdgpadev

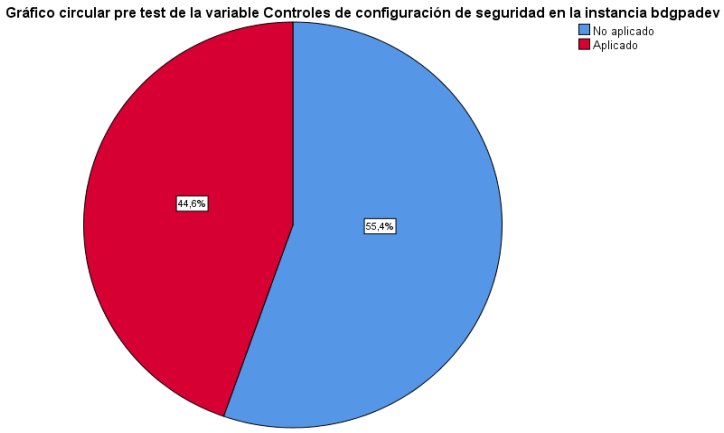

Figura 4: Ítems no aplicado / aplicado de la variable 1 en la instancia bdgpadev
Fuente: Lista de cotejo pre test instancia bdgpadev

En las figuras 3 y 4 se muestra los resultados que se han obtenido en la recolección de información del pre test de la variable Controles de configuración de seguridad, obteniendo los siguientes resultados: el 55.4% de los controles de configuración de seguridad no se encuentran aplicados en la instancia de base de datos (bdgpadev) del ambiente de desarrollo. Por otro lado, el 44.6% de los controles de configuración de seguridad si se encuentran aplicados en la instancia de base de datos (bdgpadev) del ambiente de desarrollo.

Tabla de Frecuencias Pre Test de la variable Controles de configuración de seguridad en la instancia bdgpaqa

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	No aplicado	67	55,4	55,4	55,4
	Aplicado	54	44,6	44,6	100,0
	Total	121	100,0	100,0	

Figura 5: Ítems no aplicado / aplicado en la variable 1 de la instancia bdgpaqa
Fuente: Lista de cotejo pre test instancia bdgpaqa

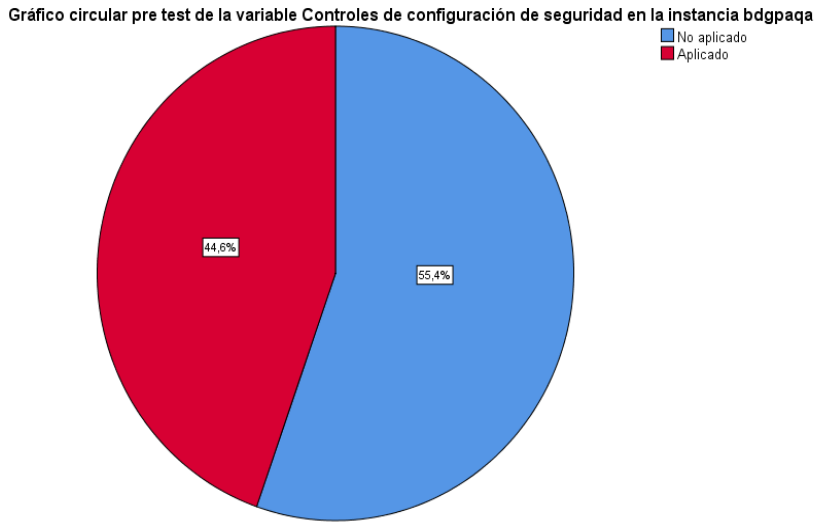

Figura 6:Ítems no aplicado / aplicado de la variable 1 en la instancia bdgpaqa
Fuente: Lista de cotejo pre test instancia bdgpaqa

En las figuras 5 y 6 se puede observar los resultados que se han obtenido en la recolección de información del pretest de la variable Controles de configuración de seguridad, obteniendo los siguientes resultados: el 55.4% de los controles de configuración de seguridad no se encuentran aplicados en la instancia de base de datos (bdgpaqa) del ambiente de control de calidad. Por otro lado, el 44.6% de los controles de configuración de seguridad si se encuentran aplicados en la instancia de base de datos (bdgpaqa) del ambiente de control de calidad.

Dimensión: Actualización del software de base de datos y configuración de parámetros

La primera dimensión “Actualización del software de base de datos y configuración de parámetros” está conformada por tres indicadores. Para la medición de los indicadores hay un total de diecinueve ítems, conformados desde el ítem 1 hasta el ítem 19.

Instancia		bdgpadev	bdgpaqa
Dimensión		Actualización del software de base de datos y configuración de parámetros	Actualización del software de base de datos y configuración de parámetros
N	Válido	19	19
	Perdidos	0	0

Tabla 5: Número de elementos de la primera dimensión
Fuente: Matriz de operacionalización de variables

Tabla de Frecuencias Pre Test de la dimensión Actualización del software de base de datos y configuración de parámetros en la instancia bdgpadev

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	No aplicado	8	42,1	42,1	42,1
	Aplicado	11	57,9	57,9	100,0
	Total	19	100,0	100,0	

Figura 7: Ítems no aplicado / aplicado en la primera dimensión de la instancia bdgpadev
Fuente: Lista de cotejo pre test instancia bdgpadev

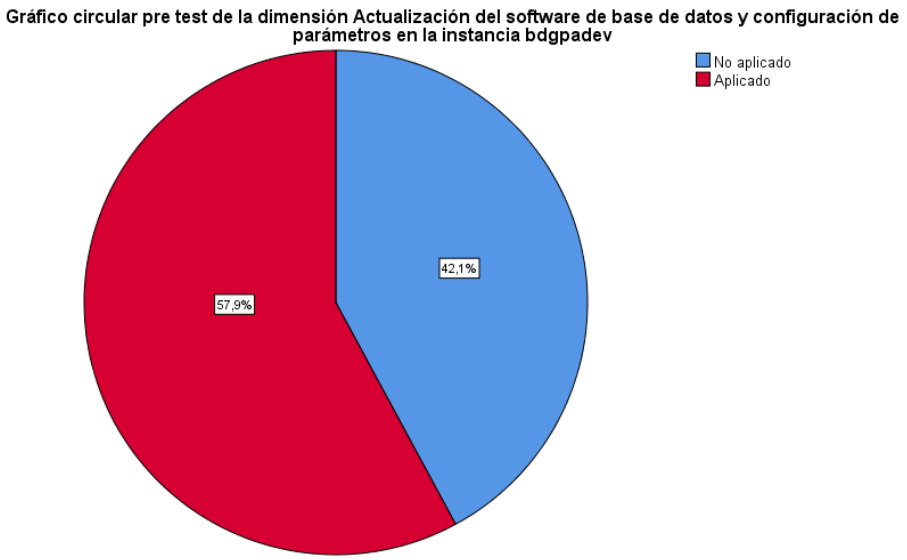

Figura 8: Ítems no aplicado / aplicado de la primera dimensión en la instancia bdgpadev
Fuente: Lista de cotejo pre test instancia bdgpadev

En las figuras 7 y 8 se puede observar los resultados que se han obtenido en la recolección de información del pretest de la dimensión Actualización del software de base de datos y configuración de

parámetros, obteniendo los siguientes resultados: el 57.9% de los controles de configuración de seguridad si se encuentran aplicados en la instancia de base de datos (bdgpadev) del ambiente de desarrollo. Por otro lado, el 42.1% de los controles de configuración de seguridad no se encuentran aplicados en la instancia de base de datos (bdgpadev) del ambiente de desarrollo.

Tabla de Frecuencias Pre Test de la dimensión Actualización del software de base de datos y configuración de parámetros en la instancia bdgpaqa

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	No aplicado	8	42,1	42,1	42,1
	Aplicado	11	57,9	57,9	100,0
	Total	19	100,0	100,0	

Figura 9: Ítems no aplicado / aplicado en la primera dimensión de la instancia bdgpaqa
Fuente: Lista de cotejo pre test instancia bdgpaqa

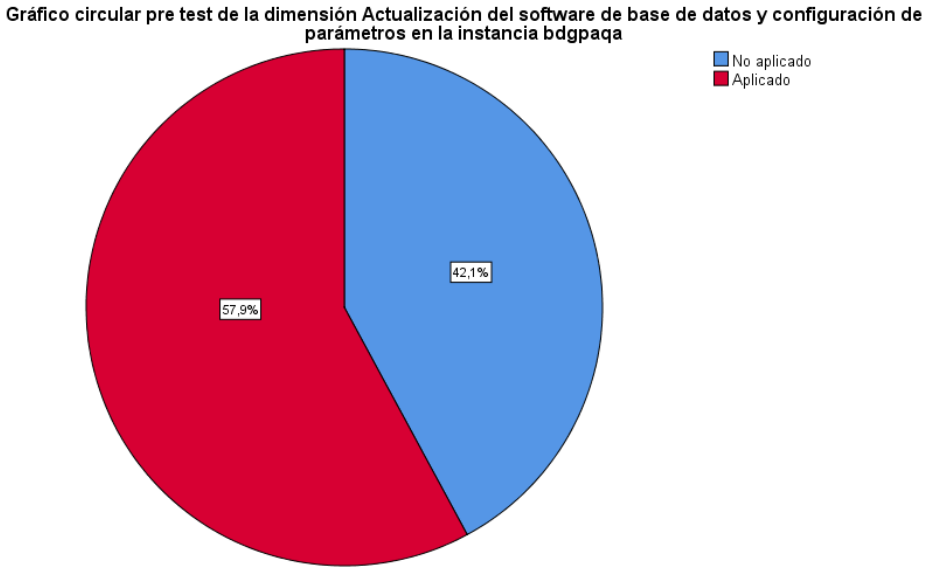

Figura 10: Ítems no aplicado / aplicado de la primera dimensión en la instancia bdgpaqa
Fuente: Lista de cotejo pre test instancia bdgpaqa

En las figuras 9 y 10 se puede observar los resultados que se han obtenido en la recolección de información del pretest de la dimensión Actualización del software de base de datos y configuración de parámetros, obteniendo los siguientes resultados: el 57.9% de los controles de configuración de seguridad si se encuentran aplicados

en la instancia de base de datos (bdgpaqa) del ambiente de control de calidad. Por otro lado, el 42.1% de los controles de configuración de seguridad no se encuentran aplicados en la instancia de base de datos (bdgpaqa) del ambiente de control de calidad.

Dimensión: Configuración de parámetros de conexión, acceso, usuarios y asignación y/o revocación de privilegios

La segunda dimensión “Configuración de parámetros de conexión, acceso, usuarios y asignación y/o revocación de privilegios” está conformada por tres indicadores. Para la medición de los indicadores hay un total de cincuenta y siete ítems, conformados desde el ítem 20 hasta el ítem 76.

Instancia		**bdgpadev**	**bdgpaqa**
Dimensión		Configuración de parámetros de conexión, acceso, usuarios y asignación y/o revocación de privilegios	Configuración de parámetros de conexión, acceso, usuarios y asignación y/o revocación de privilegios
N	Válido	57	57
	Perdidos	0	0

Tabla 6: Número de elementos de la segunda dimensión
Fuente: Matriz de operacionalización de variables

Tabla de Frecuencias Pre Test de la dimensión Configuración de parámetros de conexión, acceso, usuarios y asignación y/o revocación de privilegios en la instancia bdgpadev

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	No aplicado	30	52,6	52,6	52,6
	Aplicado	27	47,4	47,4	100,0
	Total	57	100,0	100,0	

Figura 11: Ítems no aplicado / aplicado en la segunda dimensión de la instancia bdgpadev
Fuente: Lista de cotejo pre test instancia bdgpadev

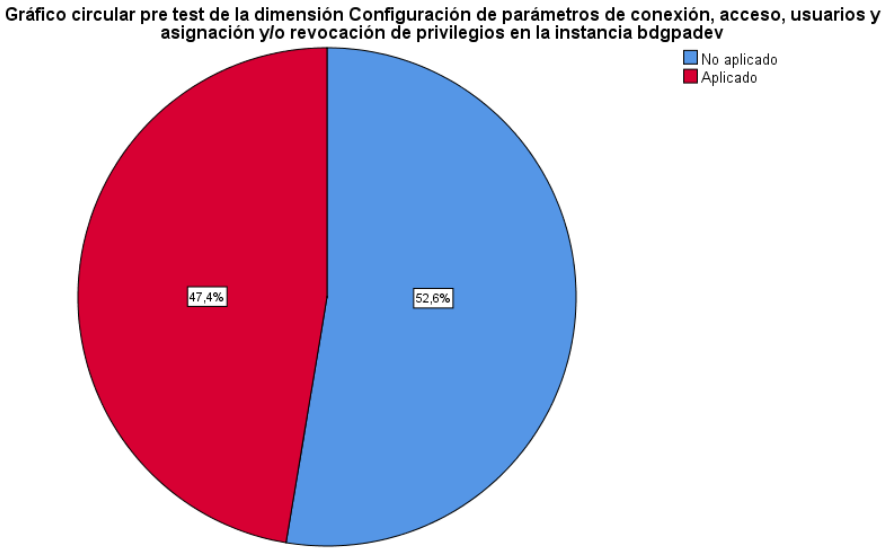

Figura 12: Ítems no aplicado / aplicado de la segunda dimensión en la instancia bdgpadev
Fuente: Lista de cotejo pre test instancia bdgpadev

En las figuras 11 y 12 se puede observar los resultados que se han obtenido en la recolección de información del pretest de la dimensión Configuración de parámetros de conexión, acceso, usuarios y asignación y/o revocación de privilegios, obteniendo los siguientes resultados: el 52.6% de los controles de configuración de seguridad no se encuentran aplicados en la instancia de base de datos (bdgpadev) del ambiente de desarrollo. Por otro lado, el 47.4% de los controles de configuración de seguridad si se encuentran aplicados en la instancia de base de datos (bdgpadev) del ambiente de desarrollo.

Tabla de Frecuencias Pre Test de la dimensión Configuración de parámetros de conexión, acceso, usuarios y asignación y/o revocación de privilegios en la instancia bdgpaqa

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	No aplicado	30	52,6	52,6	52,6
	Aplicado	27	47,4	47,4	100,0
	Total	57	100,0	100,0	

Figura 13: Ítems no aplicado / aplicado en la segunda dimensión de la instancia bdgpaqa
Fuente: Lista de cotejo pre test instancia bdgpaqa

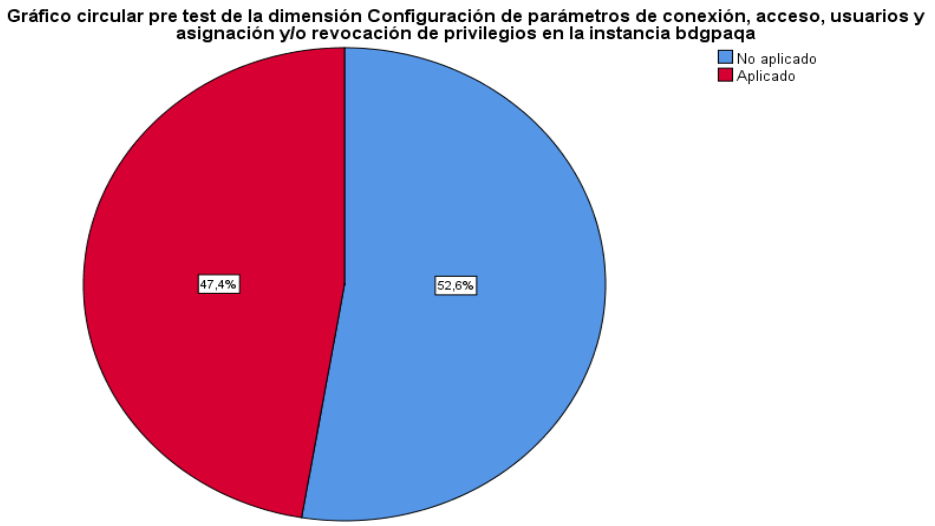

Figura 14:Ítems no aplicado / aplicado de la segunda dimensión en la instancia bdgpaqa
Fuente: Lista de cotejo pre test instancia bdgpaqa

En las figuras 13 y 14 se puede observar los resultados que se han obtenido en la recolección de información del pretest de la dimensión Configuración de parámetros de conexión, acceso, usuarios y asignación y/o revocación de privilegios, obteniendo los siguientes resultados: el 52.6% de los controles de configuración de seguridad no se encuentran aplicados en la instancia de base de datos (bdgpaqa) del ambiente de control de calidad. Por otro lado, el 47.4% de los controles de configuración de seguridad si se encuentran aplicados en la instancia de base de datos (bdgpaqa) del ambiente de control de calidad.

Dimensión: Configuración de parámetros de auditorías

La tercera dimensión “Configuración de parámetros de auditorías” está conformada por dos indicadores. Para la medición de los indicadores hay un total de cuarenta y cinco ítems, conformados desde el ítem 77 hasta el ítem 121.

Instancia		**bdgpadev**	**bdgpaqa**
Dimensión		Configuración de parámetros de auditorías	Configuración de parámetros de auditorías
N	Válido	45	45
	Perdidos	0	0

Tabla 7: Número de elementos de la tercera dimensión
Fuente: Matriz de operacionalización de variables

Tabla de Frecuencias Pre Test de la dimensión Configuración de parámetros de auditorías en la instancia bdgpadev

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	No aplicado	29	64,4	64,4	64,4
	Aplicado	16	35,6	35,6	100,0
	Total	45	100,0	100,0	

Figura 15: Ítems no aplicado / aplicado en la tercera dimensión de la instancia bdgpadev
Fuente: Lista de cotejo pre test instancia bdgpadev

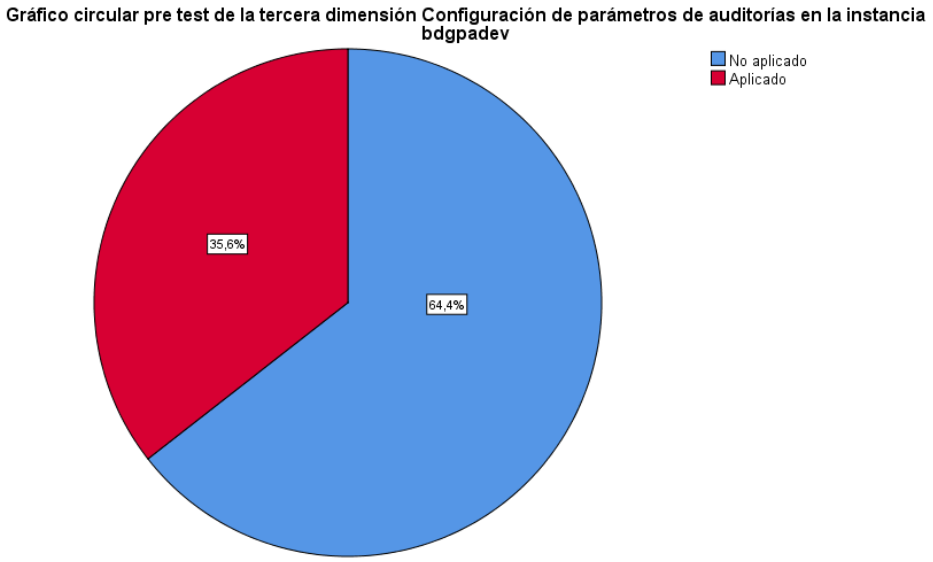

Figura 16: Ítems no aplicado / aplicado en la tercera dimensión de la instancia bdgpadev
Fuente: Lista de cotejo pre test instancia bdgpadev

En las figuras 15 y 16 se puede observar los resultados que se han obtenido en la recolección de información del pretest de la dimensión Configuración de parámetros de auditorías, obteniendo los siguientes resultados: el 64.4% de los controles de configuración de seguridad no se encuentran aplicados en la instancia de base de datos (bdgpadev) del ambiente de desarrollo. Por otro lado, el 35.6% de los controles de configuración de seguridad si se encuentran aplicados en la instancia de base de datos (bdgpadev) del ambiente de desarrollo.

Tabla de Frecuencias Pre Test de la dimensión Configuración de parámetros de auditorías en la instancia bdgpaqa

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	No aplicado	29	64,4	64,4	64,4
	Aplicado	16	35,6	35,6	100,0
	Total	45	100,0	100,0	

Figura 17: Ítems no aplicado / aplicado en la tercera dimensión de la instancia bdgpaqa
Fuente: Lista de cotejo pre test instancia bdgpaqa

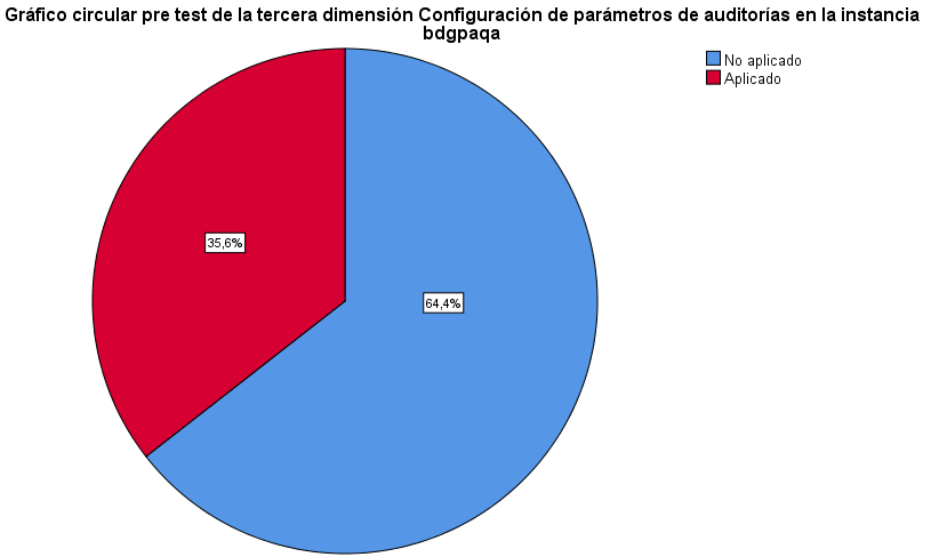

Figura 18: Ítems no aplicado / aplicado en la tercera dimensión de la instancia bdgpaqa
Fuente: Lista de cotejo pre test instancia bdgpaqa

En las figuras 17 y 18 se puede observar los resultados que se han obtenido en la recolección de información del pretest de la dimensión Configuración de parámetros de auditorías, obteniendo los siguientes resultados: el 64.4% de los controles de configuración de seguridad no se encuentran aplicados en la instancia de base de datos (bdgpaqa) del ambiente de control de calidad. Por otro lado, el 35.6% de los controles de configuración de seguridad si se encuentran aplicados en la instancia de base de datos (bdgpaqa) del ambiente de control de calidad.

4.2.2. Resultados posteriores a la prueba (Después de la implementación de los controles de configuración de seguridad)

Variable: Controles de configuración de seguridad

Como se indicó en el numeral anterior, está conformada por tres dimensiones, cada dimensión tiene sus indicadores y cada indicador tiene los ítems que permite la medición respectiva. Para la medición de la variable uno hay un total de ciento veintiún ítems que se encuentran distribuidos entre las dimensiones y estas a su vez en cada uno de los indicadores que las conforman.

Instancia		**bdgpadev**	**bdgpaqa**
Variable 1		Controles de configuración de seguridad	Controles de configuración de seguridad
N	Válido	121	121
	Perdidos	0	0

Tabla 8: Número de elementos de la variable 1
Fuente: Matriz de operacionalización de variables

Tabla de Frecuencias Post Test de la variable Controles de configuración de seguridad en la instancia bdgpadev

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	No aplicado	0	0,0	0,	0,0
	Aplicado	121	100,0	100,0	100,0
	Total	121	100,0	100,0	

Tabla 9: Ítems no aplicado / aplicado de la Variable 1 en la instancia bdgpadev
Fuente: Lista de cotejo post test instancia bdgpadev

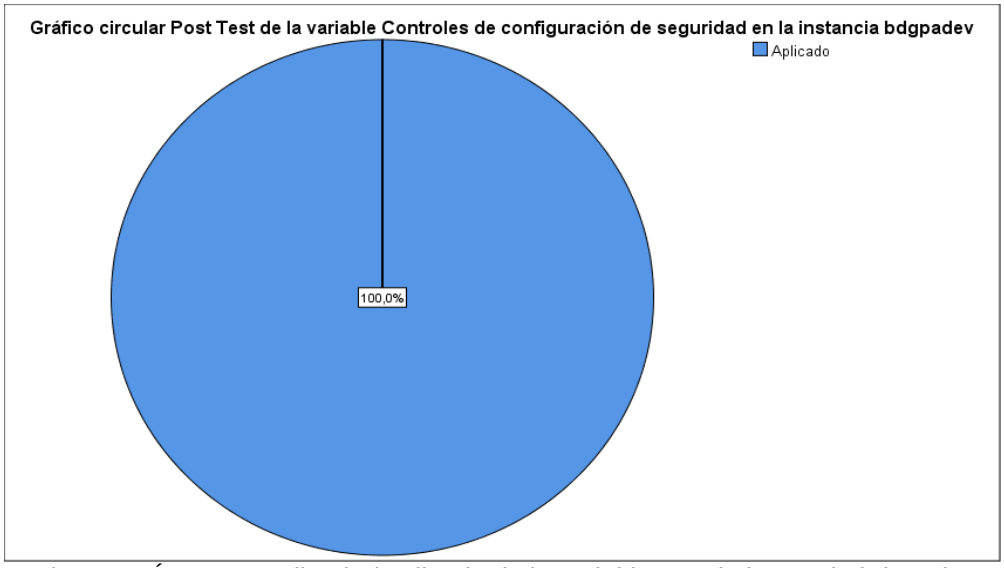

Figura 19:Ítems no aplicado / aplicado de la variable 1 en la instancia bdgpadev
Fuente: Lista de cotejo post test instancia bdgpadev

En la tabla 9 y figura 19 se muestra los resultados obtenidos a partir de la información recopilada del post test de la variable Controles de configuración de seguridad, obteniendo los siguientes resultados: el 100.0% de los controles de configuración de seguridad si se encuentran aplicados en la instancia de base de datos (bdgpadev) del ambiente de desarrollo. Por otro lado, el 0.0% de los controles de configuración de seguridad no se encuentran aplicados en la instancia de base de datos (bdgpadev) del ambiente de desarrollo.

Tabla de Frecuencias Post Test de la variable Controles de configuración de seguridad en la instancia bdgpaqa

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	No aplicado	0	0,0	0,	0,0
	Aplicado	121	100,0	100,0	100,0
	Total	121	100,0	100,0	

Tabla 10: Ítems no aplicado / aplicado de la Variable 1 en la instancia bdgpaqa
Fuente: Lista de cotejo post test instancia bdgpaqa

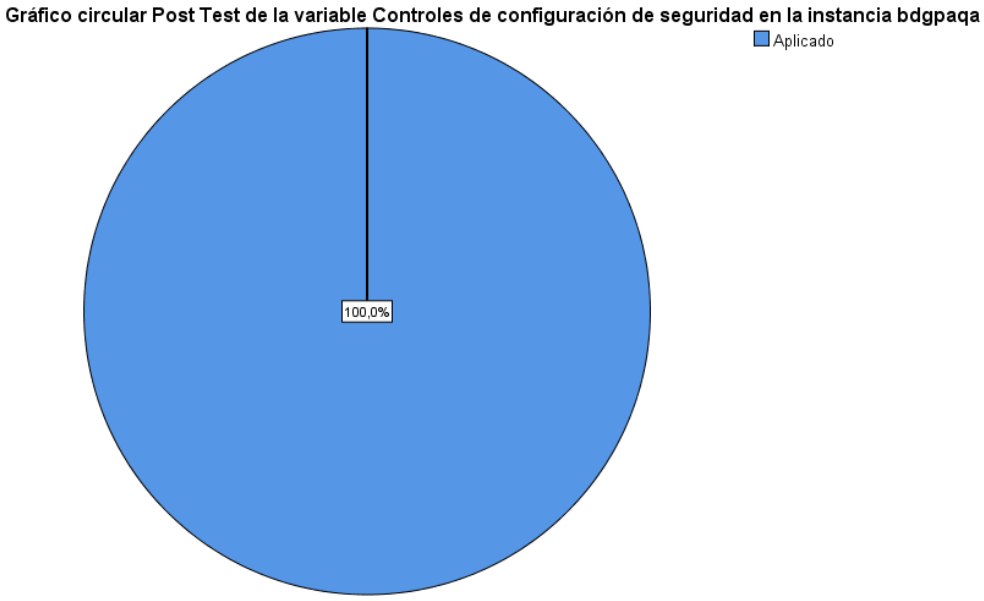

Figura 20:Ítems no aplicado / aplicado de la variable 1 en la instancia bdgpaqa
Fuente: Lista de cotejo post test instancia bdgpaqa

En la tabla 10 y figura 20 se muestra los resultados obtenidos a partir de la información recopilada del post test de la variable Controles de configuración de seguridad, obteniendo los siguientes resultados: el 100.0% de los controles de configuración de seguridad si se encuentran aplicados en la instancia de base de datos (bdgpaqa) del

ambiente de control de calidad. Por otro lado, el 0.0% de los controles de configuración de seguridad no se encuentran aplicados en la instancia de base de datos (bdgpaqa) del ambiente de control de calidad.

Dimensión: Actualización del software de base de datos y configuración de parámetros

La primera dimensión “Actualización del software de base de datos y configuración de parámetros” está conformada por tres indicadores. Para la medición de los indicadores hay un total de diecinueve ítems, conformados desde el ítem 1 hasta el ítem 19.

Instancia		**bdgpadev**	**bdgpaqa**
Dimensión		Actualización del software de base de datos y configuración de parámetros	Actualización del software de base de datos y configuración de parámetros
N	Válido	19	19
	Perdidos	0	0

Tabla 11: Número de elementos de la primera dimensión
Fuente: Matriz de operacionalización de variables

Tabla de Frecuencias Post Test de la dimensión Actualización del software de base de datos y configuración de parámetros en la instancia bdgpadev

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	No aplicado	0	0,0	0,0	0,0
	Aplicado	19	100,0	100,0	100,0
	Total	19	100,0	100,0	

Tabla 12: Ítems no aplicado / aplicado en la primera dimensión de la instancia bdgpadev
Fuente: Lista de cotejo post test instancia bdgpadev

Figura 21: Ítems no aplicado / aplicado en la primera dimensión de la instancia bdgpadev
Fuente: Lista de cotejo post test instancia bdgpadev

En la tabla 12 y figura 21 se muestra los resultados obtenidos a partir de la información recopilada del post test de la dimensión Actualización del software de base de datos y configuración de parámetros, obteniendo los siguientes resultados: el 100.0% de los controles de configuración de seguridad si se encuentran aplicados en la instancia de base de datos (bdgpadev) del ambiente de desarrollo. Por otro lado, el 0.0% de los controles de configuración de seguridad no se encuentran aplicados en la instancia de base de datos (bdgpadev) del ambiente de desarrollo.

Tabla de Frecuencias Post Test de la dimensión Actualización del software de base de datos y configuración de parámetros en la instancia bdgpaqa

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	No aplicado	0	0,0	0,0	0,0
	Aplicado	19	100,0	100,0	100,0
	Total	19	100,0	100,0	

Tabla 13: Ítems no aplicado / aplicado en la primera dimensión de la instancia bdgpaqa
Fuente: Lista de cotejo post test instancia bdgpaqa

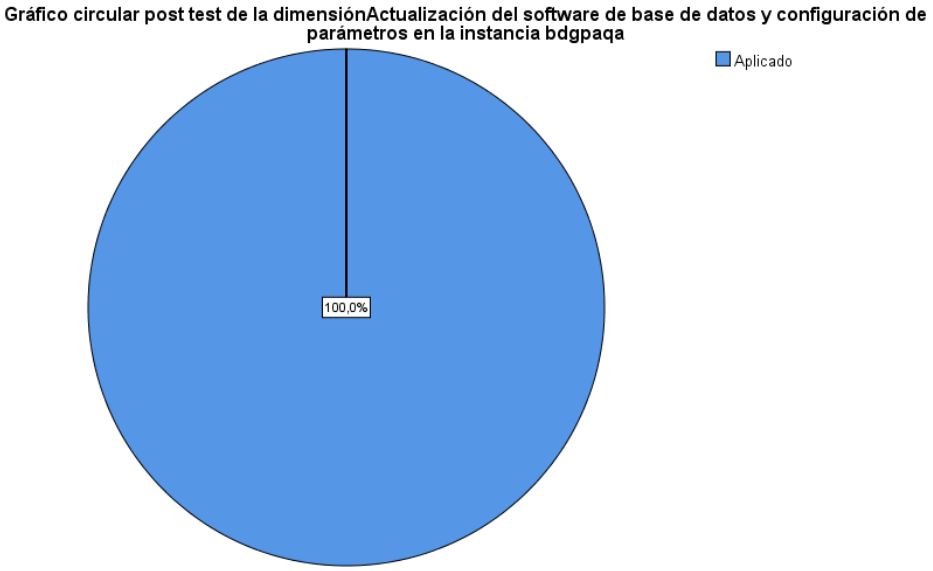

Figura 22: Ítems no aplicado / aplicado en la primera dimensión de la instancia bdgpaqa
Fuente: Lista de cotejo post test instancia bdgpaqa

En la tabla 13 y figura 22 se muestra los resultados obtenidos a partir de la información recopilada del post test de la dimensión Actualización del software de base de datos y configuración de

parámetros, obteniendo los siguientes resultados: el 100.0% de los controles de configuración de seguridad si se encuentran aplicados en la instancia de base de datos (bdgpaqa) del ambiente de control de calidad. Por otro lado, el 0.0% de los controles de configuración de seguridad no se encuentran aplicados en la instancia de base de datos (bdgpaqa) del ambiente de control de calidad.

Dimensión: Configuración de parámetros de conexión, acceso, usuarios y asignación y/o revocación de privilegios

La segunda dimensión es la "Configuración de parámetros de conexión, acceso, usuarios y asignación y/o revocación de privilegios" está conformada por tres indicadores. Para la medición de los indicadores hay un total de cincuenta y siete ítems, conformados desde el ítem 20 hasta el ítem 76.

Instancia		**bdgpadev**	**bdgpaqa**
Dimensión		Configuración de parámetros de conexión, acceso, usuarios y asignación y/o revocación de privilegios	Configuración de parámetros de conexión, acceso, usuarios y asignación y/o revocación de privilegios
N	Válido	57	57
	Perdidos	0	0

Tabla 14: Número de elementos de la segunda dimensión
Fuente: Matriz de operacionalización de variables

Tabla de Frecuencias Post Test de la dimensión Configuración de parámetros de conexión, acceso, usuarios y asignación y/o revocación de privilegios en la instancia bdgpadev

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	No aplicado	0	0,0	0,0	0,0
	Aplicado	57	100,0	100,0	100,0
	Total	57	100,0	100,0	

Tabla 15: Ítems no aplicado / aplicado en la segunda dimensión de la instancia bdgpadev
Fuente: Lista de cotejo post test instancia bdgpadev

Figura 23: Ítems no aplicado / aplicado en la segunda dimensión de la instancia bdgpadev

Fuente: Lista de cotejo post test instancia bdgpadev

En la tabla 15 y figura 23 se muestra los resultados obtenidos a partir de la información recopilada del post test de la dimensión Configuración de parámetros de conexión, acceso, usuarios y asignación y/o revocación de privilegios, obteniendo los siguientes resultados: el 100.0% de los controles de configuración de seguridad si se encuentran aplicados en la instancia de base de datos (bdgpadev) del ambiente de desarrollo. Por otro lado, el 0.0% de los controles de configuración de seguridad no se encuentran aplicados en la instancia de base de datos (bdgpadev) del ambiente de desarrollo.

Tabla de Frecuencias Post Test de la dimensión Configuración de parámetros de conexión, acceso, usuarios y asignación y/o revocación de privilegios en la instancia bdgpaqa

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	No aplicado	0	0,0	0,0	0,0
	Aplicado	57	100,0	100,0	100,0
	Total	57	100,0	100,0	

Tabla 16: Ítems no aplicado / aplicado en la segunda dimensión de la instancia bdgpaqa

Fuente: Lista de cotejo post test instancia bdgpaqa

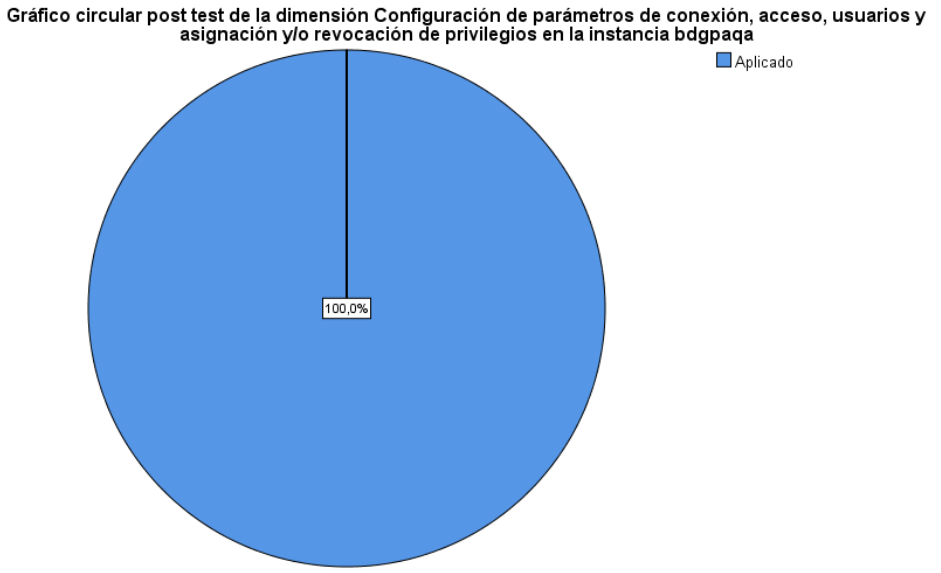

Figura 24: Ítems no aplicado / aplicado en la segunda dimensión de la instancia bdgpaqa
Fuente: Lista de cotejo post test instancia bdgpaqa

En la tabla 16 y figura 24 se muestra los resultados obtenidos a partir de la información recopilada del post test de la dimensión Configuración de parámetros de conexión, acceso, usuarios y asignación y/o revocación de privilegios, obteniendo los siguientes resultados: el 100.0% de los controles de configuración de seguridad si se encuentran aplicados en la instancia de base de datos (bdgpaqa) del ambiente de control de calidad. Por otro lado, el 0.0% de los controles de configuración de seguridad no se encuentran aplicados en la instancia de base de datos (bdgpaqa) del ambiente de control de calidad.

Dimensión: Configuración de parámetros de auditorías

La tercera dimensión es la "Configuración de parámetros de auditorías" está conformada por dos indicadores. Para la medición de los indicadores hay un total de cuarenta y cinco ítems, conformados desde el ítem 77 hasta el ítem 121.

Instancia		**bdgpadev**	**bdgpaqa**
Dimensión		Configuración de parámetros de auditorías	Configuración de parámetros de auditorías
N	Válido	45	45
	Perdidos	0	0

Tabla 17: Número de elementos de la tercera dimensión
Fuente: Matriz de operacionalización de variables

Tabla de Frecuencias Post Test de la dimensión Configuración de parámetros de auditorías en la bdgpadev

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	No aplicado	0	0,0	0,0	0,0
	Aplicado	45	100,0	100,0	100,0
	Total	45	100,0	100,0	

Tabla 18: Ítems no aplicado / aplicado en la tercera dimensión de la instancia bdgpadev
Fuente: Lista de cotejo post test instancia bdgpadev

Figura 25: Ítems no aplicado / aplicado en la tercera dimensión de la instancia bdgpadev
Fuente: Lista de cotejo post test instancia bdgpadev

En la tabla 18 y figura 25 se muestra los resultados obtenidos a partir de la información recopilada del post test de la dimensión Configuración de parámetros de auditorías, obteniendo los siguientes resultados: el 100.0% de los controles de configuración de seguridad si se encuentran aplicados en la instancia de base de datos (bdgpadev) del ambiente de desarrollo. Por otro lado, el 0.0% de los controles de configuración de seguridad no se encuentran aplicados en la instancia de base de datos (bdgpadev) del ambiente de desarrollo.

Tabla de Frecuencias Post Test de la dimensión Configuración de parámetros de auditorías en la bdgpaqa

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	No aplicado	0	0,0	0,0	0,0
	Aplicado	45	100,0	100,0	100,0
	Total	45	100,0	100,0	

Tabla 19: Ítems no aplicado / aplicado en la tercera dimensión de la instancia bdgpaqa
Fuente: Lista de cotejo post test instancia bdgpaqa

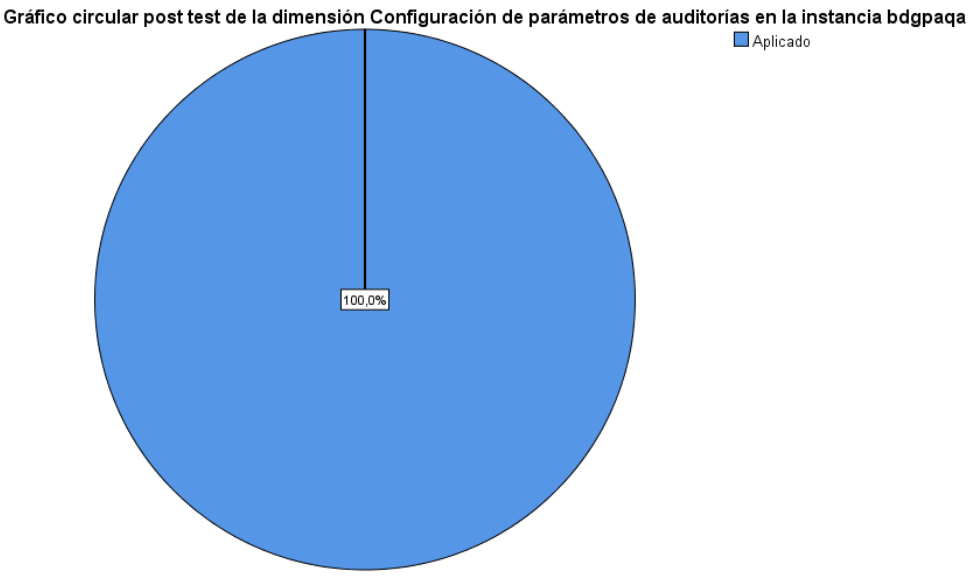

Figura 26: Ítems no aplicado / aplicado en la tercera dimensión de la instancia bdgpaqa
Fuente: Lista de cotejo post test instancia bdgpaqa

En la tabla 19 y figura 26 se muestra los resultados obtenidos a partir de la información recopilada del post test de la dimensión Configuración de parámetros de auditorías, obteniendo los siguientes resultados: el 100.0% de los controles de configuración de seguridad si se encuentran aplicados en la instancia de base de datos (bdgpaqa) del ambiente de control de calidad. Por otro lado, el 0.0% de los controles de configuración de seguridad no se encuentran aplicados en la instancia de base de datos (bdgpaqa) del ambiente de control de calidad.

4.3. CONTRASTACIÓN DE HIPÓTESIS

4.3.1. Prueba de Normalidad

Se realizó la prueba de normalidad para la diferencia de la información recolectada del post test menos la información recolectada en el pre test, esto se realizó para la variable uno, para cada uno de sus tres indicadores y para cada instancia de base de datos que conforma la muestra de la investigación:

Diferencia entre la variable controles de configuración de seguridad post test menos controles de configuración de seguridad pre test de las instancias de base de datos bdgpadev y bdgpaqa:

Teniendo en cuenta la cantidad de 121 ítems que conforma la muestra de la instancia bdgpadev y bdgpaqa respectivamente. Como es mayor a 50, se considera la prueba de normalidad de Kolmogorov-Smirnov.

Diferencia entre la primera dimensión Actualización del software de base de datos y configuración de parámetros post test menos Actualización del software de base de datos y configuración de parámetros pre test de las instancias de base de datos bdgpadev y bdgpaqa:

Teniendo en cuenta la cantidad de 19 ítems que conforma la muestra de las instancias bdgpadev y bdgpaqa respectivamente. Como es menor a 50, se considera la prueba de normalidad de Shapiro-Wilk.

Diferencia entre la segunda dimensión Configuración de parámetros de conexión, acceso, usuarios y asignación y/o revocación de privilegios post test menos Configuración de parámetros de conexión, acceso, usuarios y asignación y/o revocación de privilegios pre test de las instancias de base de datos bdgpadev y bdgpaqa:

Teniendo en cuenta la cantidad de 57 ítems que conforma la muestra de las instancias bdgpadev y bdgpaqa respectivamente. Como es mayor a 50, se considera la prueba de normalidad de Kolmogorov-Smirnov.

Diferencia entre la tercera dimensión Configuración de parámetros de auditorías post test menos Configuración de parámetros de auditorías pre test de las instancias de base de datos bdgpadev y bdgpaqa:

Teniendo en cuenta la cantidad de 45 ítems que conforma la muestra de las instancias bdgpadev y bdgpaqa respectivamente. Como es menor a 50, se considera la prueba de normalidad de Shapiro-Wilk.

Todas estas pruebas se realizaron utilizando el programa SPSS 26.0 teniendo en cuenta el nivel de confiabilidad del 95%.

Si sig < 0.05 entonces adopta una distribución no normal.

Si sig ≥ 0.05 entonces adopta una distribución normal.

Donde sig = nivel crítico del contraste

4.3.2. Resultados obtenidos

Para la prueba de normalidad de la variable Controles de configuración de seguridad se utilizó el criterio de Kolmogorov-Smimov y como resultado se obtuvieron los siguientes datos:

Prueba de normalidad

	Kolmogorov-Smirnov[a]		
	Estadístico	gl	Sig.
Dif_v1post_v1pre	,368	121	,000

a. Corrección de significación de Lilliefors

Tabla 20: Prueba de normalidad de la variable Controles de configuración de seguridad
Fuente: Elaboración propia

En la tabla 20 se observa el resultado obtenido en el porcentaje de Controles de configuración de seguridad se obtuvo el valor de ,000 y como este dato es menor a 0.05; esto concluye que los datos provienen de una distribución no normal.

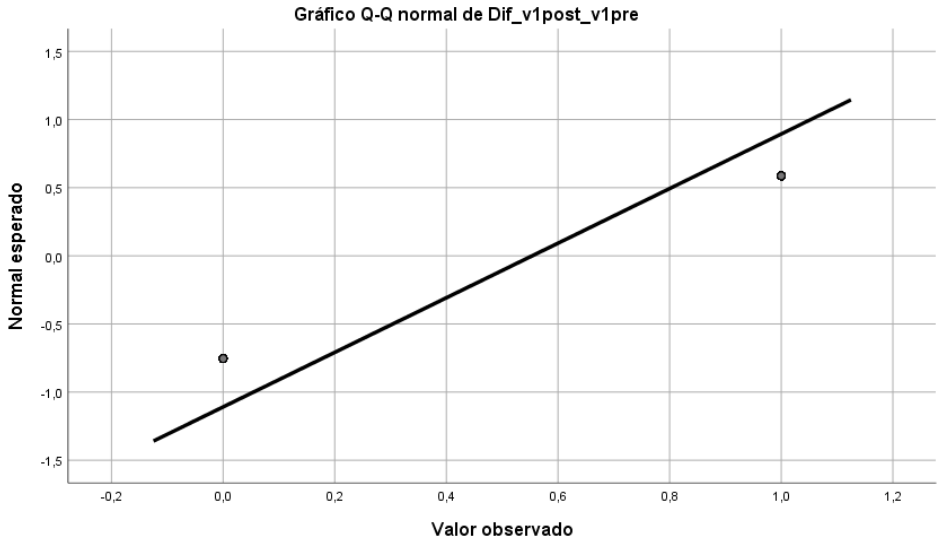

Figura 27: Q-Q normal de Dif_v1post-v1pre
Fuente: Elaboración propia

Para la prueba de normalidad de la primera dimensión Actualización del software de base de datos y configuración de parámetros se utilizó el criterio de Shapiro-Wilk y como resultado se obtuvieron los siguientes datos:

Prueba de normalidad

	Shapiro-Wilk		
	Estadístico	gl	Sig.
Diferencia de la primera dimensión	,633	19	,000

a. Corrección de significación de Lilliefors

Tabla 21: Prueba de normalidad de la primera dimensión Actualización del software de base de datos y configuración de parámetros
Fuente: Elaboración propia

En la tabla 21 se observa el resultado obtenido en el porcentaje de Actualización del software de base de datos y configuración de parámetros se obtuvo el valor de ,000 y como este dato es menor a 0.05; esto concluye que los datos provienen de una distribución no normal.

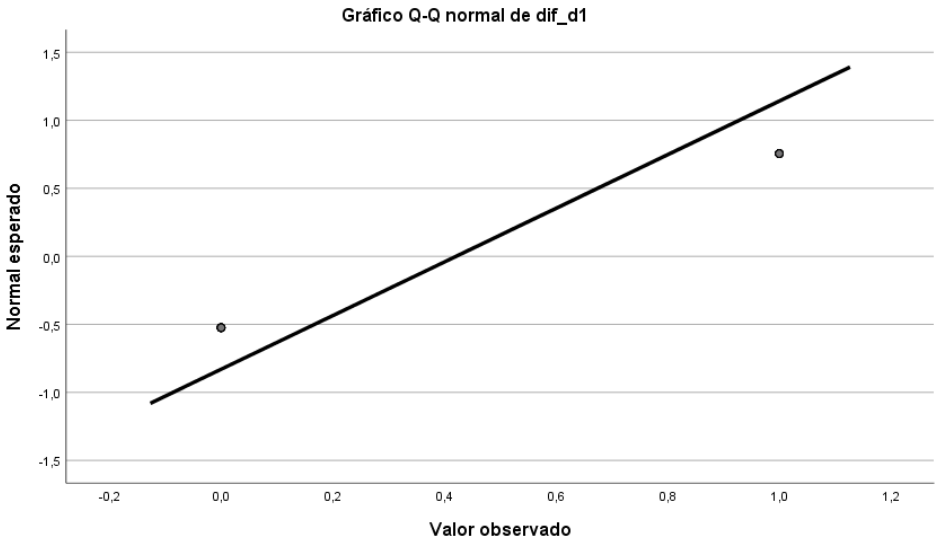

Figura 28: Q-Q normal de diferencia de la primera dimensión
Fuente: Elaboración propia

Para la prueba de normalidad de la segunda dimensión Configuración de parámetros de conexión, acceso, usuarios y asignación y/o revocación de privilegios se utilizó el criterio de Kolmogorov-Smimov y como resultado se obtuvieron los siguientes datos:

Prueba de normalidad

	Kolmogorov-Smirnov[a]		
	Estadístico	gl	Sig.
Diferencia de la segunda dimensión	,353	57	,000

a. Corrección de significación de Lilliefors

Tabla 22: Prueba de normalidad de la segunda dimensión Configuración de parámetros de conexión, acceso, usuarios y asignación y/o revocación de privilegios
Fuente: Elaboración propia

En la tabla 22 se observa el resultado obtenido en el porcentaje de Configuración de parámetros de conexión, acceso, usuarios y asignación y/o revocación de privilegios se obtuvo el valor de ,000 y como este dato es menor a 0.05; esto concluye que los datos provienen de una distribución no normal

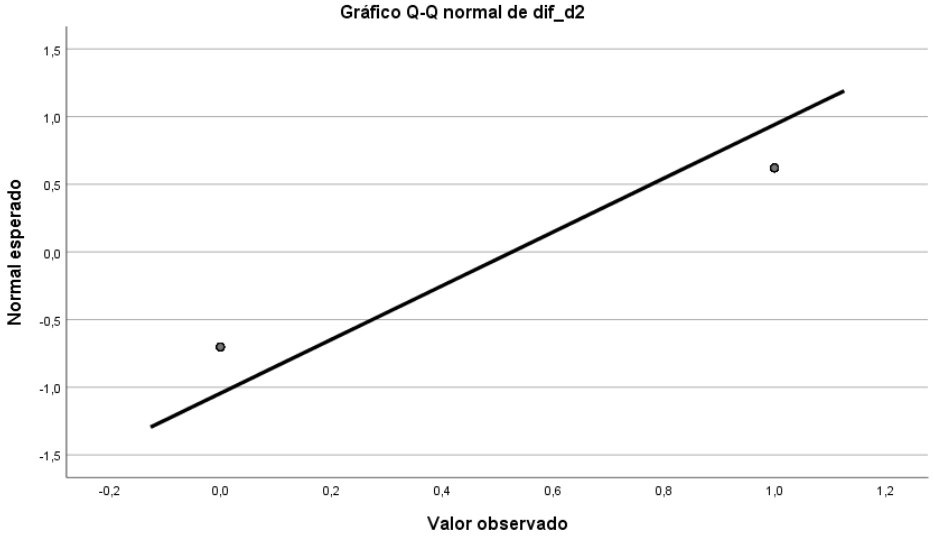

Figura 29: Q-Q normal de diferencia de la segunda dimensión
Fuente: Elaboración propia

Para la prueba de normalidad de la tercera dimensión Configuración de parámetros de auditorías se utilizó el criterio de Shapiro-Wilk y como resultado se obtuvieron los siguientes datos:

Prueba de normalidad

	Shapiro-Wilk		
	Estadístico	gl	Sig.
Diferencia de la tercera dimensión	,606	45	,000

a. Corrección de significación de Lilliefors

Tabla 23: Prueba de normalidad de la tercera dimensión Configuración de parámetros de auditorías
Fuente: Elaboración propia

En la tabla 23 se observa el resultado obtenido en el porcentaje de Configuración de parámetros de auditorías se obtuvo el valor de ,000 y como este dato es menor a 0.05; esto concluye que los datos provienen de una distribución no normal.

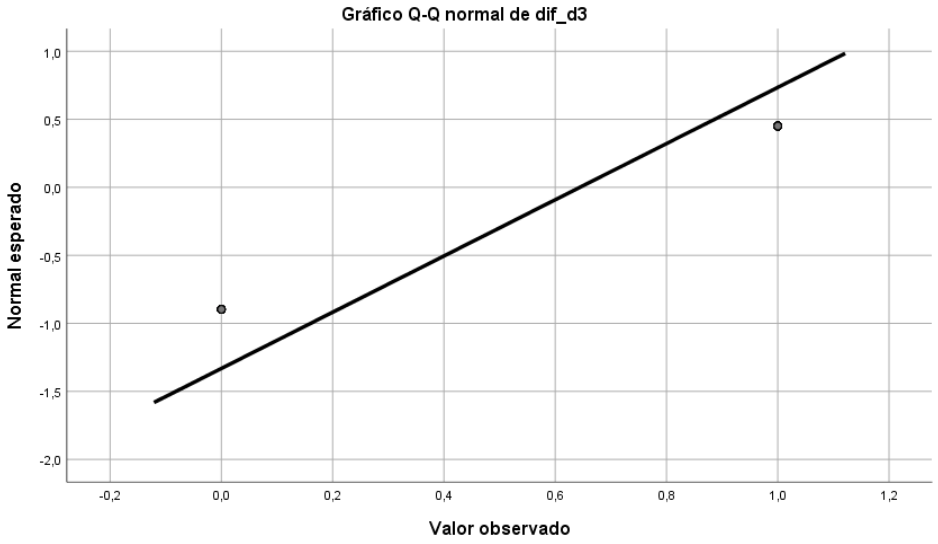

Figura 30: Q-Q normal de diferencia de la tercera dimensión
Fuente: Elaboración propia

4.3.3. Prueba de la hipótesis general

La implementación de controles de configuración de seguridad influye significativamente en la base de datos de GPA Business SAC.

a. Planteamiento de la hipótesis:

Hipótesis nula (Ho): La implementación de controles de configuración de seguridad no influye significativamente en la base de datos de GPA Business SAC.

Ho: μpre prueba = μpost prueba

Hipótesis alterna (H1): La implementación de controles de configuración de seguridad influye significativamente en la base de datos de GPA Business SAC

Ha: μpre prueba ≠ μpost prueba

b. Nivel de significancia o riesgo

El nivel utilizado en el diseño pre experimental es bilateral es de α= 0,05, (el tipo de prueba: es bilateral).

α=0,05 (bilateral α = 0,025)

c. Estadígrafo de prueba

El estadígrafo de prueba más apropiado para la presente tesis es el Test de Wilcoxon.

Prueba de rangos con signo de Wilcoxon

Rangos

		N	Rango promedio	Suma de rangos
Post Test – Pre-Test	Rangos negativos	0[a]	,00	,00
	Rangos positivos	67[b]	34,00	2278,00
	Empates	54[c]		
	Total	121		

a. Post Test < Pre-Test
b. Post Test > Pre-Test
c. Post Test = Pre-Test

Tabla 24: Prueba de rangos con signo de wilcoxon de la hipótesis general
Fuente: Elaboración propia

Estadísticos de prueba[a]

	Post Test – Pre Test
Z	-8,185[b]
Sig. asintótica(bilateral)	,000

a. Prueba de rangos con signo de Wilcoxon
b. Se basa en rangos negativos.

Tabla 25: Significancia asintótica de la hipótesis general
Fuente: Elaboración propia

d. Regla de decisión estadística

Puesto que el p valor 0,000 es menor que el nivel de significación de 0,05%. En consecuencia, se rechaza la hipótesis nula (H0) y se acepta la hipótesis alterna (H1).

e. Conclusión estadística

Finalmente se concluye que; la implementación de controles de configuración de seguridad influye significativamente en la base de datos de GPA Business SAC.

4.3.4. Prueba de la primera hipótesis

La implementación de controles de configuración de seguridad influye significativamente en la confidencialidad de la base de datos de GPA Business SAC.

a. Planteamiento de la hipótesis:

Hipótesis nula (Ho): La implementación de controles de configuración de seguridad no influye significativamente en la confidencialidad de la base de datos de GPA Business SAC.

Ho: μpre prueba = μpost prueba

Hipótesis alterna (H1): La implementación de controles de configuración de seguridad influye significativamente en la confidencialidad de la base de datos de GPA Business SAC.

Ha: μpre prueba ≠ μpost prueba

b. Nivel de significancia o riesgo

El nivel utilizado en el diseño pre experimental es bilateral es de α= 0,05, (el tipo de prueba: es bilateral).

α=0,05 (bilateral α = 0,025)

c. Estadígrafo de prueba

El estadígrafo de prueba más apropiado para la presente tesis es el Test de Wilcoxon.

Prueba de rangos con signo de Wilcoxon

Rangos

		N	Rango promedio	Suma de rangos
D1_Post_Test - D1_Pre_Test	Rangos negativos	0[a]	,00	,00
	Rangos positivos	8[b]	4,50	36,00
	Empates	11[c]		
	Total	19		

a. D1_Post_Test < D1_Pre_Test

b. D1_Post_Test > D1_Pre_Test

c. D1_Post_Test = D1_Pre_Test

Tabla 26: Prueba de rangos con signo de wilcoxon de la hipótesis específica 1
Fuente: Elaboración propia

Estadísticos de prueba[a]

	D1_Post_Test - D1_Pre_Test
Z	-2,828[b]
Sig. asintótica(bilateral)	,005

a. Prueba de rangos con signo de Wilcoxon

b. Se basa en rangos negativos.

Tabla 27: Significancia asintótica de la hipótesis específica 1
Fuente: Elaboración propia

d. Regla de decisión estadística

Puesto que el p valor 0,000 es menor que el nivel de significación de 0,05%. En consecuencia, se rechaza la hipótesis nula (H0) y se acepta la hipótesis alterna (H1).

e. Conclusión estadística

Finalmente se concluye que; la implementación de controles de configuración de seguridad influye significativamente en la confidencialidad de la base de datos de GPA Business SAC.

4.3.5. Prueba de la segunda hipótesis

La implementación de controles de configuración de seguridad influye significativamente en la disponibilidad de la base de datos de GPA Business SAC.

a. Planteamiento de la hipótesis:

Hipótesis nula (Ho): La implementación de controles de configuración de seguridad no influye significativamente en la disponibilidad de la base de datos de GPA Business SAC

Ho: µpre prueba = µpost prueba

Hipótesis alterna (H1): La implementación de controles de configuración de seguridad influye significativamente en la disponibilidad de la base de datos de GPA Business SAC.

Ha: µpre prueba ≠ µpost prueba

b. Nivel de significancia o riesgo

El nivel utilizado en el diseño pre experimental es bilateral es de α= 0,05, (el tipo de prueba: es bilateral).

α=0,05 (bilateral α = 0,025)

c. Estadígrafo de prueba

El estadígrafo de prueba más apropiado para la presente tesis es el Test de Wilcoxon.

Prueba de rangos con signo de Wilcoxon

Rangos

		N	Rango promedio	Suma de rangos
D2_Post_Test - D2_Pre_Test	Rangos negativos	0[a]	,00	,00
	Rangos positivos	30[b]	15,50	465,00

	Empates	27[c]		
	Total	57		

a. D2_Post_Test < D2_Pre_Test
b. D2_Post_Test > D2_Pre_Test
c. D2_Post_Test = D2_Pre_Test

Tabla 28: Prueba de rangos con signo de wilcoxon de la hipótesis específica 2
Fuente: Elaboración propia

Estadísticos de prueba[a]

	D2_Post_Test - D2_Pre_Test
Z	-5,477[b]
Sig. asintótica(bilateral)	,000

a. Prueba de rangos con signo de Wilcoxon

b. Se basa en rangos negativos.

Tabla 29: Significancia asintótica de la hipótesis específica 2
Fuente: Elaboración propia

d. Regla de decisión estadística

Puesto que el p valor 0,000 es menor que el nivel de significación de 0,05%. En consecuencia, se rechaza la hipótesis nula (H0) y se acepta la hipótesis alterna (H1).

e. Conclusión estadística

Finalmente se concluye que; la implementación de controles de configuración de seguridad influye significativamente en la disponibilidad de la base de datos de GPA Business SAC.

4.3.6. Prueba de la tercera hipótesis

La implementación de controles de configuración de seguridad influye significativamente en la integridad de la base de datos de GPA Business SAC.

a. Planteamiento de la hipótesis:

Hipótesis nula (Ho): La implementación de controles de configuración de seguridad no influye significativamente en la integridad de la base de datos de GPA Business SAC.

Ho: µpre prueba = µpost prueba

Hipótesis alterna (H1): La implementación de controles de configuración de seguridad influye significativamente en la integridad de la base de datos de GPA Business SAC.

Ha: µpre prueba ≠ µpost prueba

b. Nivel de significancia o riesgo

El nivel utilizado en el diseño pre experimental es bilateral es de α= 0,05, (el tipo de prueba: es bilateral).

α=0,05 (bilateral α = 0,025)

c. Estadígrafo de prueba

El estadígrafo de prueba más apropiado para la presente tesis es el Test de Wilcoxon.

Prueba de rangos con signo de Wilcoxon

Rangos

		N	Rango promedio	Suma de rangos
D3_Post_Test - D3_Pre_Test	Rangos negativos	0[a]	,00	,00
	Rangos positivos	29[b]	15,00	435,00
	Empates	16[c]		
	Total	45		

a. D3_Post_Test < D3_Pre_Test
b. D3_Post_Test > D3_Pre_Test
c. D3_Post_Test = D3_Pre_Test

Tabla 30: Prueba de rangos con signo de wilcoxon de la hipótesis específica 3
Fuente: Elaboración propia

Estadísticos de prueba[a]

	D3_Post_Test - D3_Pre_Test
Z	-5,385[b]
Sig. asintótica(bilateral)	,000

a. Prueba de rangos con signo de Wilcoxon
b. Se basa en rangos negativos.

Tabla 31: Significancia asintótica de la hipótesis específica 3
Fuente: Elaboración propia

d. Regla de decisión estadística

Puesto que el p valor 0,000 es menor que el nivel de significación de 0,05%. En consecuencia, se rechaza la hipótesis nula (H0) y se acepta la hipótesis alterna (H1).

e. Conclusión estadística

Finalmente se concluye que; la implementación de controles de configuración de seguridad influye significativamente en la integridad de la base de datos de GPA Business SAC

CAPITULO V:
DISCUSIÓN DE RESULTADOS

Con los resultados obtenidos se evidencia que la implementación de controles de configuración de seguridad en la base de datos de la empresa GPA Business SAC, influye significativamente en incrementar el nivel de seguridad de las instancias de base de datos ante un eventual ataque informático, debido a que se elevó el grado de disponibilidad, confidencialidad e integridad de la base de datos de la empresa GPA Business SAC protegiendo su activo más importante de la organización ante un eventual ataque informático.

Respecto a la actualización del software de base de datos y configuración de parámetros se confirmó que la implementación de los controles de configuración de seguridad ha mejorado en la actualización del software de base de datos y configuración de parámetros en un 42.1%, debido a que hubo una mejora en la actualización del software de base de datos y configuración de parámetros en el post test logrando la implementación al 100%, respecto a la implementación encontrada en el pre test de 57,9% de controles de configuración de seguridad aplicados. Así mismo se obtuvo que el p valor fue 0,000 y fue menor que el nivel de significación de 0,05%. En consecuencia, se rechazó la hipótesis nula (H0) y se aceptó la hipótesis alterna (H1), por tanto, se afirma que. la implementación de controles de configuración de seguridad influye significativamente en la confidencialidad de la base de datos de GPA Business SAC.

Respecto a la configuración de parámetros de conexión, acceso, usuarios y asignación y/o revocación de privilegios se confirmó que la implementación de los controles de configuración de seguridad ha mejorado en la configuración de parámetros de conexión, acceso, usuarios y asignación y/o revocación de privilegios en un 52.6%, debido a que hubo una mejora en la configuración de

parámetros de conexión, acceso, usuarios y asignación y/o revocación de privilegios en el post test logrando la implementación al 100%, respecto a la implementación encontrada en el pre test de 47,4% de controles de configuración de seguridad aplicados. Así mismo se obtuvo que el p valor fue 0,000 y fue menor que el nivel de significación de 0,05%. En consecuencia, se rechazó la hipótesis nula (H0) y se aceptó la hipótesis alterna (H1), por tanto, se afirma que. la implementación de controles de configuración de seguridad influye significativamente en la disponibilidad de la base de datos de GPA Business SAC.

Respecto a la configuración de parámetros de auditorías se confirmó que la implementación de los controles de configuración de seguridad ha mejorado en la configuración de parámetros de auditorías en un 64.4%, debido a que hubo una mejora en la configuración de parámetros de auditorías en el post test logrando la implementación al 100%, respecto a la implementación encontrada en el pre test de 35.6% de controles de configuración de seguridad aplicados. Así mismo se obtuvo que el p valor fue 0,000 y fue menor que el nivel de significación de 0,05%. En consecuencia, se rechazó la hipótesis nula (H0) y se aceptó la hipótesis alterna (H1), por tanto, se afirma que. la implementación de controles de configuración de seguridad influye significativamente en la integridad de la base de datos de GPA Business SAC.

Los resultados de la investigación se complementan con los hallazgos de Paredes (2022) quien en su investigación desarrollo una guía de implementación de políticas de control para mitigar los ciberataques basados en el modelo Carding en la COAC Riobamba LTDA, también se concuerda con Vasquez (2021) quien en su investigación Ciberseguridad basada en analítica para base de datos Oracle clasifico el nivel de riesgo expuesto y automatizo la gestión del control del estado de las bases de datos Oracle, así mismo se concuerda con Ramírez (2019) quien en su investigación realizó la implementación de lineamientos base de seguridad en base de datos Oracle y SQL Server en una entidad bancaria.

Es importante que este trabajo se implemente en otras empresas que utilizan motores de base de datos Oracle, y sea realizado por un administrador de base de datos para que garantice la implementación.

CONCLUSIONES

1. Se concluye que en la actualización del software de base de datos y configuración de parámetros de la empresa GPA Business SAC, antes de implementar los controles de configuración de seguridad se obtuvo un promedio de 57,9% y con los controles de configuración de seguridad implementados se obtuvo un promedio de 100%, por lo que se observa un aumento de 42.1%, por lo tanto, se afirma la hipótesis de que la implementación de controles de configuración de seguridad influye significativamente en la confidencialidad de la base de datos de GPA Business SAC.

2. Se concluye que en la configuración de parámetros de conexión, acceso, usuarios y asignación y/o revocación de privilegios de la empresa GPA Business SAC, antes de implementar los controles de configuración de seguridad se obtuvo un promedio de 47,4% y con los controles de configuración de seguridad implementados se obtuvo un promedio de 100%, por lo que se observa un aumento de 52.6%, por lo tanto, se afirma la hipótesis de que la implementación de controles de configuración de seguridad influye significativamente en la disponibilidad de la base de datos de GPA Business SAC.

3. Se concluye que en la configuración de parámetros de auditorías de la empresa GPA Business SAC, antes de implementar los controles de configuración de seguridad se obtuvo un promedio de 35,6% y con los controles de configuración de seguridad implementados se obtuvo un promedio de 100%, por lo que se observa un aumento de 64.4%, por lo tanto, se afirma la hipótesis de que la implementación de controles de configuración de seguridad influye significativamente en la integridad de la base de datos de GPA Business SAC.

4. Finalmente, con los resultados obtenidos de las dimensiones se afirma la hipótesis general de que la implementación de controles de configuración de seguridad influye significativamente en la base de datos de GPA Business SAC.

RECOMENDACIONES

1. Para los futuros investigadores es recomendable tener en cuenta la dimensión Actualización del software de base de datos y configuración de parámetros. Con el propósito de incrementar significativamente la seguridad de la instancia de base de datos respecto a la confidencialidad del activo más importante de las organizaciones.

2. Para los futuros investigadores es recomendable tener en cuenta la dimensión Configuración de parámetros de conexión, acceso, usuarios y asignación y/o revocación de privilegios. Con el propósito de incrementar significativamente la seguridad de la instancia de base de datos respecto a la disponibilidad del activo más importante de las organizaciones.

3. Para los futuros investigadores es recomendable tener en cuenta la dimensión Configuración de parámetros de auditorías. Con el propósito de incrementar significativamente la seguridad de la instancia de base de datos respecto a la integridad del activo más importante de las organizaciones.

4. Se recomienda que las nuevas instancias de bases de datos a crear cuenten con la implementación de los controles de configuración de seguridad y sobre esa base recién realizar el despliegue de sus nuevos sistemas informáticos.

5. Se recomienda a los futuros investigadores estar atentos a las publicaciones que realiza CIS Benchmarks, con la finalidad de mantenerse al día respecto a los controles de seguridad de base de datos aplicables a las distintas plataformas de base de datos.

REFERENCIAS BIBLIOGRÁFICAS

ACIS Asociación Colombiana de Ingenieros de Sistemas. Malware: la principal preocupación de las empresas de América Latina. [Fecha de consulta 13 de setiembre de 2022]. Disponible en: https://acis.org.co/portal/content/noticiasdelsector/malware-la-principal-preocupaci%C3%B3n-de-las-empresas-de-am%C3%A9rica-latina

Arroyo Guardeño, D., Gayoso Martínez, V., & Hernández Encinas, L. (2020). Ciberseguridad. CSIC.

Barriga, B. (2021). Módulo de seguridad informática aplicando la autenticación de doble factor para la empresa Home Office S.A.S., (tesis de pregrado) Universidad Nacional de Chimborazo – Riobamba – Ecuador. Recuperado de: file:///D:/Titulo/2%20Tesis/03%20Tesis%20Internacionales/8.-Informe%20Final%20del%20Proyecto%20de%20Investigacion%20Byron%20Barriga.pdf

Bohórquez, A. (2021). Ciberseguridad y su relación en la gestión de tecnologías de información en la empresa I & T Electric, Lima 2020. Recuperado de: https://hdl.handle.net/20.500.12692/63128

Bonilla, C. (2017) Elaboración de una metodología de detección y mitigación de vulnerabilidades de base de datos y su incidencia en la seguridad de la información de la empresa Automekano CÍA. LTDA, de la ciudad de Ambato, (tesis de grado) Universidad Técnica de Ambato – Ecuador. Recuperado de: https://repositorio.uta.edu.ec/handle/123456789/24534

Cabezas E., Andrade D.; y Torres J. (2018). *Introducción a la metodología de la investigación científica. Universidad de las Fuerzas Armadas*. Recuperado de: http://repositorio.espe.edu.ec/jspui/bitstream/21000/15424/1/Introduccion%20a%20la%20Metodologia%20de%20la%20investigacion%20cientifica.pdf

Cardona, P. (2021). Diseño de un modelo centralizado de autorizaciones para mejorar la seguridad en aplicaciones desarrolladas a la medida, (tesis de grado) Instituto Tecnológico Metropolitano – Medellín – Colombia. Recuperado de: https://repositorio.itm.edu.co/handle/20.500.12622/4680

Castro, L. (2022). Análisis comparativo de algoritmos de aprendizaje automático para identificar ataques de inyección sql a base de datos en aplicaciones web, (tesis de pregrado) Universidad Señor de Sipán – Pimente – Perú. Recuperado de: https://repositorio.uss.edu.pe/bitstream/handle/20.500.12802/9320/Castro%20Fern%c3%a1ndez%2c%20Levi%20Ronald.pdf?sequence=1&isAllowed=y

Center for Internet Security (2022). Oracle Database 19c Benchmark versión 1.0.0 Recuperada de https://www.cisecurity.org/benchmark/oracle_database

CFGM. Seguridad Informática – IHMC Public Cmaps (2) Recuperado de: https://cursa.ihmc.us/rid=1L86VJF89-23G253D-JQC5/Conceptos%20B%C3%A1sicos%20de%20Seguridad%20de%20la%20Informaci%C3%B3n.ppsx

Cifre, S. (2020). Modelo de seguridad para la gestión de vulnerabilidades de servidores en nubes privadas. (tesis de postgrado) Universidad Tecnológica Nacional. Facultad Regional Santa Fe – Argentina. Recuperado de: https://ria.utn.edu.ar/bitstream/handle/20.500.12272/6050/Tesis%20de%20

Maestri%cc%81a%20-%20Cifre%20Simo%cc%81n.pdf?sequence=1&isAllowed=y
Cifuentes, G. (2014). Análisis de seguridad en base de datos: Aplicación Oracle versión 11G. (tesis de postgrado) Universidad de las Fuerzas Armadas – Sangolqui – Ecuador. Recuperado de: http://repositorio.espe.edu.ec/xmlui/handle/21000/8373
Dávila A. y Dextre B. (2021). Propuesta de una implementación de un programa de gestión de vulnerabilidades de seguridad informática para mitigar los siniestros de la información en el policlínico de salud AMC alienado a la NTP-ISO/IEC 270001:2014 en la ciudad de Lima – 2021, (tesis de pregrado) Universidad Tecnológica del Peru – Lima – Perú. Recuperado de: https://repositorio.utp.edu.pe/handle/20.500.12867/4906
Definición.de. Definición de Control. [en línea] [Fecha de consulta: 13 de setiembre del 2022]. Disponible en https://definicion.de/control/
Definición.de. Definición de Seguridad. [en línea] [Fecha de consulta: 13 de setiembre del 2022]. Disponible en https://definicion.de/?s=seguridad
Díaz, R. (2021). Modelo de procesos para el desarrollo de software con características de seguridad para vulnerabilidades más recurrentes, (tesis de pregrado) Universidad Señor de Sipán – Pimentel – Perú. Recuperado de: https://repositorio.uss.edu.pe/handle/20.500.12802/9221
Florez, I. y Quintana, J. (2018). Sistema de detección de ataques informáticos a redes de datos empresariales soportado en Honeypots, (tesis de pregrado) Universidad de Cartagena Facultad de Ingeniería Programa de Ingeniería de Sistemas – Cartagena de Indias – Colombia. Recuperado de: https://repositorio.unicartagena.edu.co/bitstream/handle/11227/8498/TESIS%20FLOREZ-%20MANQUINTANA.pdf?sequence=1&isAllowed=y
Gámez, M. (2002). Una valoración de las amenazas y propuesta para mejorar la seguridad de los depósitos de datos, (tesis de grado) Instituto Tecnológico de Costa Rica – Cartago – Costa Rica. Recuperado en: https://repositoriotec.tec.ac.cr/handle/2238/213
Gomez, Y. (2018). Estudio de Seguridad en base de datos SQL y NoSQL, (tesis de postgrado) Universidad Nacional Abierta y a Distancia – Bogotá D.C. – Colombia. Recuperado de: https://repository.unad.edu.co/bitstream/handle/10596/21429/52488191.pdf?sequence=4&isAllowed=y
Huincho, W. (2019). Sistema de gestión de seguridad de la información para mejorar la protección informática de la comisaria región Huancavelica, (tesis de pregrado) Universidad Nacional Daniel Alcides Carrión – Cerro de Pasco – Perú. Recuperado de: http://repositorio.undac.edu.pe/handle/undac/2017
IGS Integral Group Solution. Procedimiento-gestión-de-parches-y-actualizaciones. [en línea] [Fecha de consulta: 03 de octubre de 2022]. Disponible en: https://www.igroupsolution.com/wp-content/uploads/2021/10/Procedimiento-gestion-de-parches-y-actualizaciones.pdf
INCIBE - INSTITUTO NACIONAL DE CIBERSEGURIDAD. Vulnerabilidad. [en línea] [Fecha de consulta: 10 de noviembre 2022] Disponible en: https://www.incibe.es/aprendeciberseguridad/vulnerabilidad

ISO 27002 (2022). *El portal de ISO 27000 en español*. Recuperada de http://www.iso27000.es/iso27000.html

JorgeSanchez.net. Manual de Administración de Bases de Datos. [en línea] [Fecha de consulta: 03 de octubre de 2022]. Disponible en: https://jorgesanchez.net/manuales/abd/instalacion-oracle.html

Nieves, A. (2017). Diseño de un sistema de gestión de la seguridad de la información (SGSI) basados en la Norma ISO/IEC 27001:2013. (tesis de grado) Institución Universitaria Politécnico Grancolombiano – Colombia. Recuperado en: https://alejandria.poligran.edu.co/handle/10823/994

Ñaupas, H., Valdivia, M., Palacios, J. y Romero, H. (2018) Metodología de la investigación Cuantitativa – Cualitativa y Redacción de la Tesis. 5ª. Edición. Bogotá. Ediciones de la U. Recuperado de: https://edicionesdelau.com/wp-content/uploads/2018/09/Anexos-Metodologia_%C3%91aupas_5aEd.pdf

OCI, Seguridad de las bases de datos. [en línea] [Fecha de consulta: 23 de setiembre del 2022]. Disponible en https://www.oracle.com/pe/security/database-security/

OCI, ¿Qué es la seguridad de datos? [en línea] [Fecha de consulta: 23 de setiembre del 2022]. Disponible en https://www.oracle.com/pe/security/database-security/what-is-data-security/

Palacios Martínez, Ignacio (dir.), Rosa Alonso Alonso, Mario Cal Varela, Yolanda Calvo Benzies, Francisco Xabier Fernández Polo, Lidia Gómez García, Paula López Rúa, Yonay Rodríguez Rodríguez & José Ramón Varela Pérez. 2019. Diccionario electrónico de enseñanza y aprendizaje de lenguas. ISBN 978-84-09-10971-5. [en línea] [Fecha de consulta: 25 de setiembre del 2022]. Disponible en https://www.dicenlen.eu/es/diccionario/entradas/coeficientes-fiabilidad-kuder-richardson

Paredes, K. (2022). Guía de implementación de políticas de control para mitigar los ciberataques basados en el modelo carding en la COAC “Riobamba LTDA.”, (tesis de pregrado) Universidad Nacional de Chimborazo – Riobamba – Ecuador. Recuperado de: http://dspace.unach.edu.ec/bitstream/51000/8918/1/Paredes%20D.%2c%20%20Karen%20V.%20%282022%29%20GU%c3%8dA%20DE%20IMPLEMENTACI%c3%93N%20DE%20POL%c3%8dTICAS%20%281%29.pdf

Ramírez, J. (2019), Implementación de lineamientos base de seguridad en bases de datos Oracle y SQL Server en una entidad bancaria, (tesis de pregrado) Universidad Sn Ignacio de Loyola – Perú. Recuperado de: https://repositorio.usil.edu.pe/server/api/core/bitstreams/f93832ed-9541-4442-9849-6281172d7bed/content

Soy un DBA. El listener de Oracle. [en línea] [Fecha de consulta: 13 de noviembre del 2022]. Disponible en https://soyundba.com/2021/07/07/el-listener-de-oracle/

Vasques, R. (2021). Ciberseguridad basada en analítica para bases de datos Oracle, (tesis de postgrado) Konrad Lorenz Fundación Universitaria – Bogotá, D.C. Colombia. Recuperado de: https://repositorio.konradlorenz.edu.co/flip/index.jsp?pdf=/bitstream/handle/001/4967/617201002-Tesis.pdf?sequence=1&isAllowed=y

Welivesecurity, by ESET. Ataque del ransomware LockBit afectó al Poder Judicial de Chile. [en línea] [Fecha de consulta: 13 de setiembre del 2022]. Disponible

en https://www.welivesecurity.com/la-es/2022/09/28/ataque-ransomware-lockbit-poder-judicial-chile/

Welivesecurity, ESET Security Report 2021: para conocer el panorama de la seguridad corporativa en la región [en línea] [fecha de consulta: 16 de setiembre del 2022]. Recuperado de: https://www.welivesecurity.com/wp-content/uploads/2021/06/ESET-security-report-LATAM2021.pdf

Welivesecurity, ESET Security Report 2022: para conocer el panorama de la seguridad corporativa en la región [en línea] [fecha de consulta: 16 de setiembre del 2022]. Recuperado de: https://www.welivesecurity.com/wp-content/uploads/2022/07/ESET-security-report-LATAM-2022.pdf

Welivesecurity, ESET Threat Report T3 2021: para conocer el panorama de las amenazas y desde la perspectiva de expertos en investigación y detección [en línea] [fecha de consulta: 16 de setiembre del 2022]. Recuperado de: https://www.welivesecurity.com/wp-content/uploads/2022/02/eset_threat_report_t32021.pdf

ANEXOS

Anexo 1: Matriz de Consistencia

Título: "Implementación de controles de configuración de seguridad en la base de datos de GPA Business SAC. Lima 2022"

PROBLEMAS	OBJETIVOS	HIPÓTESIS	VARIABLES	DIMENSIONES	MÉTODO
General: ¿De qué manera la implementación de controles de configuración de seguridad influye en la base de datos de GPA Business SAC?	**General:** Determinar de qué manera la implementación de controles de configuración de seguridad influye en la base de datos de GPA Business SAC.	**General:** La implementación de controles de configuración de seguridad influye significativamente en la base de datos de GPA Business SAC.	Controles de configuración de seguridad	Actualización de software de base de datos y parametrización Configuración de parámetros de conexión, acceso, usuarios y asignación y/o revocación de privilegios. Configuración de parámetros de auditorías	**Método de investigación:** Método científico **Tipo de investigación:** Investigación aplicada **Nivel de investigación**: Nivel explicativo **Diseño de la investigación**: Pre experimental M = O1 X O2 Donde: M: Muestra (Instancias bdgpadev y bdgpaqa) O1: Observación (Pre test) O2: Observación (Post test) X: Manipulación de la primera variable
Específicos a) ¿De qué manera la implementación de controles de configuración de seguridad influye en la confidencialidad en la base de datos de GPA Business SAC?	**Específicos** a) Determinar de qué manera la implementación de controles de configuración de seguridad influye en la confidencialidad en la base de datos de GPA Business SAC	**Específicos** a) La implementación de controles de configuración de seguridad influye significativamente en la confidencialidad de la base de datos de GPA Business SAC.			

b) ¿De qué manera la implementación de controles de configuración de seguridad influye en la disponibilidad en la base de datos de GPA Business SAC? c) ¿De qué manera la implementación de controles de configuración de seguridad influye en la integridad en la base de datos de GPA Business SAC?	b) Determinar de qué manera la implementación de controles de configuración de seguridad influye en la disponibilidad en la base de datos de GPA Business SAC. c) Determinar de qué manera la implementación de controles de configuración de seguridad influye en la integridad la base de datos de GPA Business SAC.	b) La implementación de controles de configuración de seguridad influye significativamente en la disponibilidad de la base de datos de GPA Business SAC. c) La implementación de controles de configuración de seguridad influye significativamente en la integridad de la base de datos de GPA Business SAC.	Base de datos	Disponibilidad Confidencialidad Integridad	**Población y Muestra**: **Población** Las tres instancias de bases de datos de la empresa GPA Business SAC. **Muestra** Se aplicará la muestra no probabilística por conveniencia, considerando las instancias de base de datos **bdgpadev** del ambiente de desarrollo y **bdgpaqa** del ambiente de control de calidad. **Técnicas de recopilación de datos:** - Observación **Instrumento de investigación** - Lista de cotejo **Procesamiento de información** El software ofimático que se utilizará para el procesamiento de la información será Microsoft Excel 2016. Asimismo, para realizar el procesamiento y análisis de la información recolectada, se empleará el software SPSS (Statistical Package for Social Sciences) Versión 26.

Anexo 2: Matriz de operacionalización de variables

VARIABLES	DEFINICIÓN CONCEPTUAL	DEFINICIÓN OPERACIONAL	DIMENSIONES	INDICADORES	ÍTEMS	TIPO DE VARIABLES	INSTRUMENTOS
Controles de configuración de seguridad	Hoy en día la rápida evolución del entorno técnico requiere que las organizaciones adopten un conjunto mínimo de controles de seguridad para proteger su información y sistemas de información. (Huincho 2019)	Corresponde a la operación de los numerosos parámetros que están establecidos en archivos de configuración específicos de una base de datos Oracle, estas configuraciones deberán ser consideradas y mantenidas cuidadosamente.	Actualización del software de base de datos y configuración de parámetros	• Versión del parche del motor de BD. • Configurar parámetros de listener. • Configurar parámetros generales de BD.	1 2 y 3 Del 4 al 19	Nominal cuantitativo	Lista de cotejo
			Configuración de parámetros de conexión, acceso, usuarios y asignación y/o revocación de privilegios	• Configurar parámetros de conexión y acceso. • Configurar parámetros de usuarios. • Asignar y/o revocar privilegios.	Del 20 al 28 Del 29 al 34 Del 35 al 76		
			Configuración de parámetros de auditorías	• Configurar parámetros de auditoria tradicional. • Configurar parámetros de auditoría unificada	Del 77 al 94 Del 95 al 121		

Base de datos	Definimos un Sistema Gestor de Bases de Datos o SGBD, también llamado DBMS (Data Base Management System) como una colección de datos relacionados entre sí, estructurados y organizados, y un conjunto de programas que acceden y gestionan esos datos. (Vásquez 2021)	Sistema de gestión de datos relacionales basado en SQL. Se diseñó y se optimizó para las aplicaciones web y puede utilizarse en cualquier plataforma. Dado que está diseñado para procesar millones de consultas y miles de transacciones, es una elección popular para de las empresas de comercio electrónico.	Disponibilidad Confidencialidad Integridad	Grado de disponibilidad verdadero / falso Grado de confidencialidad verdadero / falso Grado de integridad verdadero / falso	Del 2 al 19 Del 20 al 76 1 y del 77 al 121	Nominal cualitativo	Lista de cotejo

Anexo 3: Matriz de operacionalización del instrumento

VARIABLE	DIMENSIONES	INDICADORES	ÍTEMS	RESPUESTA
Controles de configuración de seguridad	**D1:** Actualización del software de base de datos y configuración de parámetros	Versión del parche del motor de BD. Configurar parámetros de listener. Configurar parámetros generales de BD.	1 2 y 3 Del 4 al 19	Escala: No aplicado = 0 Aplicado = 1
	D2: Configuración de parámetros de conexión, acceso, usuarios y asignación y/o revocación de privilegios	Configurar parámetros de conexión y acceso. Configurar parámetros de usuarios. Asignar y/o revocar privilegios	Del 20 al 28 Del 29 al 34 Del 35 y 76	
	D3: Configuración de parámetros de auditorías.	Configurar parámetros de auditoria tradicional. Configurar parámetros de auditoría unificada	Del 77 al 94 Del 95 al 121	

VARIABLE	DIMENSIONES	INDICADORES	ÍTEMS	RESPUESTA
Base de datos	**D1:** Disponibilidad	Grado de disponibilidad	Del 2 al 19	Escala: No aplicado = 0 Aplicado = 1
	D2: Confidencialidad	Grado de confidencialidad	Del 20 al 76	
	D3: Integridad	Grado de integridad	1 y del 77 al 121	

Anexo 4 Ficha de validez del instrumento

UNIVERSIDAD PERUANA LOS ANDES

FICHA DE VALIDEZ DEL INSTRUMENTO

JUICIO DE EXPERTO

Nombre del Instrumento: Lista de Cotejo para los controles de configuración de seguridad en la base de datos Oracle 19c

Nombre del investigador**:** Jorge Luis Romero Santa Cruz

Título**:** Implementación de controles de configuración de seguridad en la base de datos de GPA Business SAC – Lima 2022.

Instrucción: Luego de analizar y cotejar el instrumento de investigación "Lista de cotejo" con la matriz de consistencia del presente, le solicito que, en base a su criterio y experiencia profesional, valide dicho instrumento para su aplicación.

CRITERIOS		VALORACIÓN		OBSERVACIÓN
		SI	NO	
1. **CLARIDAD**	Esta formulado con lenguaje claro y apropiado.			
2. **OBJETIVIDAD**	Esta expresado en conductas observables.			
3. **PERTINENCIA**	Adecuado al avance de la ciencia y la pedagogía.			
4. **ORGANIZACIÓN**	Existe una organización lógica.			
5. **SUFICIENCIA**	Comprende los aspectos de cantidad y calidad.			
6. **ADECUACIÓN**	Adecuado para valorar en constructo o variable a medir.			
7. **CONSISTENCIA**	Basado en aspectos teóricos y científicos.			
8. **COHERENCIA**	Entre las dimensiones, indicadores y los ítems.			
9. **METODOLOGÍA**	La estrategia responde al propósito de la medición.			
10. **SIGNIFICATIVIDAD**	Es útil y adecuado para la investigación.			

CRITERIO DE VALORACIÓN DEL JUEZ:

Procede su aplicación ( )

No procede su aplicación ( )

Nombres y apellidos del juez:	
Dirección:	
Título profesional:	
Grado académico:	
Número del DNI:	Número de celular:

……

Lima, …… de …… del 2022

Anexo 5: Lista de Cotejo para la instancia de base de datos "bdgpadev" del ambiente de desarrollo de la empresa GPA Business SAC:

Escala: No aplicado = 0; Aplicado = 1

V1.1 Actualización del software de base de datos y configuración de parámetros				
V1.1.1: Versión del parche del motor de BD				
Ítem	**Controles / Parámetros**	**Acción**	**Escala**	**Observación**
1	PATCH	Asegurar que esté aplicado el último parche generado por el fabricante para mitigar la posibilidad de vulnerabilidad en la base de datos Oracle.		
V1.1.2: Configurar parámetros de listener				
2	EXTPROC	Asegurar que dicho parámetro no esté presente en el archivo listener.ora para evitar que algunas librerías del sistema operativo puedan ser invocadas por la base de datos.		
3	ADMIN_RESTRICTIONS	Asegurar que ese parámetro esté presente en el archivo listener.ora para evitar que usuarios no administradores puedan alterar en tiempo real los parámetros del archivo.		
V1.1.3: Configurar parámetros generales de BD				
4	AUDIT_SYS_OPERATIONS	Asegurar que se configure este parámetro con el valor de TRUE va permitir conocer las actividades realizadas por la cuenta administradora SYS. Las operaciones se registrarán en la tabla SYS.AUD$. Va a requerir reinicio de la base de datos.		
5	AUDIT_TRAIL	Asegurar que se configure este parámetro con los valores de DB, EXTENDED, OS, XML, EXTENDED, DB, XML; va permitir habilitar las funciones básicas de auditoría, además de recopilar datos para solucionar problemas y valiosos registros forenses.		
6	GLOBAL_NAMES	Asegurar que se configure este parámetro con el valor de TRUE va permitir conectarse remotamente a otra base de datos a través de un único nombre de enlace entre las bases de datos.		
7	OS_ROLES	Asegurar que se configure este parámetro con el valor de FALSE para evitar que el sistema operativo use grupos externos para la administración de la base de datos.		
8	REMOTE_LISTENER	Asegurar que se configure este parámetro con el valor NULL para evitar establecer un oyente válido en un sistema separado, a menos que estén utilizando un RAC.		

9	REMOTE_LOGIN_PASSWORDFILE	Asegurar que se configure este parámetro con el valor de NONE para evitar conexiones privilegiadas no seguras a la base de datos.		
10	REMOTE_OS_AUTHENT	Asegurar que se configure este parámetro con el valor de FALSE para evitar suplantación de conexiones y permita otorgar privilegios a un usuario no autorizado del sistema operativo y este pueda realizar conexiones.		
11	REMOTE_OS_ROLES	Asegurar que se configure este parámetro con el valor de FALSE para evitar que usuarios del sistema operativo tengan permisos para la administración de la base de datos.		
12	SEC_CASE_SENSITIVE_LOGON	Asegurar que se configure este parámetro con el valor de TRUE para aumentar el conjunto de caracteres que se pueden elegir para las contraseñas, lo que evita a los ataques de contraseña de fuerza bruta.		
13	SEC_MAX_FAILED_LOGIN_ATTEMPTS	Asegurar que se configure este parámetro con el valor de 3 o menos, determina cuántos inicios de sesión fallidos se permitirán, antes de que la instancia cierre la conexión de inicio de sesión.		
14	SEC_PROTOCOL_ERROR_FURTHER_ACTION	Asegurar que se configure este parámetro con el valor de (DROP,3) permitirá que se corte una conexión después de tres paquetes defectuosos o con formato incorrecto.		
15	SEC_PROTOCOL_ERROR_TRACE_ACTION	Asegurar que se configure este parámetro con el valor de LOG, permite el registro de los acontecimientos que pasa en la instancia de base de datos.		
16	SEC_RETURN_SERVER_RELEASE_BANNER	Asegurar que se configure este parámetro con el valor de FALSE para evitar que la base de datos devuelva información sobre el número de versión del parche aplicado.		
17	SQL92_SECURITY	Asegurar que se configure este parámetro con el valor de TRUE para evitar la divulgación de información involuntaria asegurándose de que solo los usuarios que ya tienen el privilegio SELECT puedan ejecutar sentencias que les permite obtener los valores almacenados.		
18	TRACE_FILES_PUBLIC	Asegurar que se configure este parámetro con el valor de FALSE para evitar que el archivo de rastreo del sistema sea legible.		
19	RESOURCE_LIMIT	Asegurar que se configure este parámetro con el valor de TRUE determina si se aplican límites de recursos en los perfiles de base de datos.		
V.1.2. Configuración de parámetros de conexión, acceso, usuarios y asignación y/o revocación de privilegios				
V.1.2.1. Configurar parámetros de conexión y acceso				
Ítem	**Control**	**Acción**	**Escala**	**Observación**

20	FAILED_LOGIN_ATTEMPTS	Asegurar que se configure este parámetro con el valor de 5 o menos, determina cuántos intentos fallidos de inicio de sesión se permite antes de que el sistema bloquee la cuenta del usuario.		
21	PASSWORD_LOCK_TIME	Asegurar que se configure este parámetro con el valor de 1 determina cuántos días deben pasar para que la cuenta se desbloqué después de que se haya producido el número establecido de intentos fallidos en el inicio de sesión.		
22	PASSWORD_LIFE_TIME	Asegurar que se configure este parámetro con el valor de 90 o menos para determinar cuánto tiempo se puede usar una contraseña antes de que el usuario pueda cambiarla.		
23	PASSWORD_REUSE_MAX	Asegurar que se configure este parámetro con el valor de 20 o más, para determinar cuántas contraseñas diferentes se deben usar antes de que el usuario pueda reutilizar una contraseña anterior.		
24	PASSWORD_REUSE_TIME	Asegurar que se configure este parámetro con el valor de 365 o más, para determina la cantidad de tiempo en días que debe pasar antes de que se pueda reutilizar la misma contraseña.		
25	PASSWORD_GRACE_TIME	Asegurar que se configure este parámetro con el valor de 5 o menos, para determinar cuántos días puede un usuario tener una contraseña vencida, antes que la sesión del usuario se bloque automáticamente.		
26	PASSWORD_VERIFY_FUNCTIO N	Asegurar que se configure este parámetro en todos los Profiles, para determinar las reglas de complejidad de contraseñas (casos mixtos con dígitos y caracteres especiales), bloquear las combinaciones simples y aplicar cambios a las configuraciones de historial logrando frustrar potencialmente los inicios de sesión no autorizados.		
27	SESSIONS_PER_USER	Asegurar que se configure este parámetro con el valor de 10 o menos, para determinar el número máximo de sesiones de un usuario ayudando a prevenir el mal uso de recursos a nivel de memoria o ataques de denegación de servicio intencionales.		
28	INACTIVE_ACCOUNT_TIME	Asegurar que se configure este parámetro con el valor de 120 o menos, para determinar el número máximo de días de inactividad (sin inicios de sesión en absoluto) después de lo cual la cuenta se bloqueará.		
V.1.2.2. Configurar parámetros de usuarios				
29	Credenciales por defecto (DEFAULT PASSWORDS)	Asegurar que todas las credenciales por defecto sean modificadas, para evitar que cualquier atacante con acceso a la base de datos puede autenticarse con una cuenta predeterminada utilizando una credencial por efecto.		

30	Esquemas de ejemplo (SAMPLE DATA)	Asegurar que todos los esquemas de muestra (BI o HR o IX o OE o PM o SCOTT o SH) sean removidos del ambiente de producción, para evitar que puedan ser utilizados para lanzar exploits contra el ambiente de producción.		
31	DBA_USERS.AUTHENTICATION_TYPE	Asegurar que esté campo no contenga el valor de EXTERNAL, para evitar que un usuario remoto del sistema operativo pueda tener acceso a la base de datos con autorización completa.		
32	Usuarios sin profile por defecto (DEFAULT PROFILE)	Asegurar que los usuarios no tengan asignado el profile por defecto (DEFAULT), debido a que cuenta con configuraciones ilimitadas que a menudo son requeridas por el usuario administrador, tales configuraciones ilimitadas deben reservarse estrictamente y no aplicarse a usuarios innecesarios.		
33	SYS.USER$MIG	Asegurar que la tabla sys.user$mig sea eliminada al inicio de una migración, para evitar que su información pueda llegar hacer conocida por un atacante.		
34	Enlaces públicos (PUBLIC DATABASE LINKS)	Asegurar que no exista enlaces públicos de bases de datos para evitar que cualquier usuario pueda logra una conexión a la base de datos para consultar, actualizar, insertar, eliminar datos en una base de datos remota.		
V.1.2.3. Asignar y/o revocar privilegios				
35	DBMS_LDAP - UTL_INADDR	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de las tablas DBMS_LDAP y UTL_INADDR para evitar la creación de errores especialmente diseñados o él envió de información vía DNS al exterior.		
36	UTL_TCP	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de la tabla UTL_TCP para evitar que usuarios no autorizados envíen datos arbitrarios desde el servidor de base de datos.		
37	UTL_MAIL - UTL_SMTP	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de las tablas UTL_MAIL y UTL_SMTP para evitar que un usuario no autorizado corrompa el SMTP, función para aceptar o generar correo no deseado que puede resultar en una denegación de servicio debido a la saturación de la red		
38	UTL_DBWS	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de la tabla UTL_DBWS para evitar que un usuario no autorizado corrompa el HTTP flujo utilizado para transportar los protocolos que comunican la instancia basada en la web.		

39	UTL_ORAMTS - UTL_HTTP	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de las tablas UTL_ORAMTS y UTL_HTTP para evitar él envió de información (sensible) a sitios web.		
40	HTTPURITYPE	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de la tabla HTTPURITYPE para evitar el filtrado de información de la base de datos a un destino externo por HTTP.		
41	DBMS_ADVISOR	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de la tabla DBMS_ADVISOR para evitar que un usuario no autorizado corrompa archivos del sistema operativo o componentes fundamentales de la base de datos.		
42	DBMS_LOB	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de la tabla DBMS_LOB para evitar que subprogramas puedan manipular, leer, escribir en BLOB, CLOB, NCLOB, BFILE y LOB temporales		
43	UTL_FILE	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de la tabla UTL_FILE para evitar que un usuario pueda leer y escribir archivos ubicados en el servidor donde está instalada la instancia de base de datos.		
44	DBMS_CRYPTO	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de la tabla DBMS_CRYPTO para evitar la ejecución de procedimientos de criptografía que puede potencialmente comprometer una porción o la totalidad de los datos.		
45	DBMS_OBFUSCATION_TOOLKIT	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de la tabla DBMS_OBFUSCATION_TOOLKIT para evitar que la herramienta que determina la fuerza del algoritmo de cifrado sea utilizada para cifrar los datos de la aplicación.		
46	DBMS_RANDOM	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de la tabla DBMS_RANDOM para evitar que una aplicación no autorizada genere números aleatorios.		
47	DBMS_JAVA - DBMS_JAVA_TEST	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de las tablas DBMS_JAVA y DBMS_JAVA_TEST para evitar que un atacante ejecute comandos del sistema operativo desde la base de datos.		
48	DBMS_JOB	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de la tabla DBMS_JOB para evitar que un usuario no autorizado inhabilite o sobrecargue la cola de trabajos.		

49	DBMS_SCHEDULER	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de la tabla DBMS_SCHEDULER para evitar que un usuario no autorizado ejecute trabajos de la base de datos o del sistema operativo.		
50	DBMS_SQL	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de la tabla DBMS_SQL para evitar la escalada de privilegios si no se realiza la validación de entrada adecuadamente.		
51	DBMS_XMLGEN	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de la tabla DBMS_XMLGEN para evitar la búsqueda de información confidencial en toda la base de datos. Información como números de tarjetas de crédito.		
52	DBMS_XMLQUERY, DBMS_XMLSAVE, DBMS_XMLSTORE, DBMS_AW, OWA_UTIL y DBMS_REDACT	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de las tablas DBMS_XMLQUERY, DBMS_XMLSAVE, DBMS_XMLSTORE, DBMS_AW, OWA_UTIL y DBMS_REDACT para evitar que usuarios malintencionados pueden aprovechar este paquete como una función de inyección auxiliar en un ataque de inyección SQL.		
53	DBMS_BACKUP_RESTORE	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de la tabla DBMS_BACKUP_RESTORE para evitar el acceso a los archivos del sistema operativo.		
54	DBMS_FILE_TRANSFER	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de la tabla DBMS_FILE_TRANSFER para evitar transferir archivos desde un servidor de base de datos a otro sin autorización para hacerlo.		
55	DBMS_SYS_SQL	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de la tabla DBMS_SYS_SQL para evitar que un usuario ejecute código como un usuario diferente sin ingresar credenciales válidas.		
56	DBMS_REPCAT_SQL_UTL, INITJVMAUX, DBMS_AQADM_SYS, DBMS_STREAMS_RPC y LTADM	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de las tablas DBMS_REPCAT_SQL_UTL, INITJVMAUX, DBMS_AQADM_SYS, DBMS_STREAMS_RPC y LTADM para evitar que un usuario no autorizado ejecute SQL comandos como un usuario SYS.		
57	DBMS_PRVTAQIM	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de la tabla DBMS_PRVTAQIM para evitar que un usuario no autorizado escale privilegios por cualquier instrucción SQL y que podría ejecutarse como usuario SYS.		
58	DBMS_IJOB y DBMS_PDB_EXEC_SQL	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de las tablas DBMS_IJOB y DBMS_PDB_EXEC_SQL para evitar que un atacante cambie de identidad utilizando un nombre de usuario diferente para ejecutar un trabajo de base de datos.		

59	SYS.AUD$	Asegurar que usuarios no autorizados tengan privilegios sobre la tabla SYS.AUD$ para que no permita distorsión en los registros de auditoría, escondiendo actividades no autorizadas.		
60	SYS.DBA_%	Asegurar que el privilegio PUBLIC sea revocado de todas las tablas sensibles del usuario SYS que sean encontradas en la vista DBA_% para evitar que usuarios no autorizados puedan manipular los datos confidenciales.		
61	CDB_LOCAL_ADMINAUTH$, DEFAULT_PWD$, ENC$, HISTGRM$, HIST_HEAD$, LINK$, PDB_SYNC$, SCHEDULER$_CREDENTIAL, USER$, USER_HISTORY$ y XS$VERIFIERS	Asegurar que el privilegio ALL sea revocado de las tablas CDB_LOCAL_ADMINAUTH$, DEFAULT_PWD$, ENC$, HISTGRM$, HIST_HEAD$, LINK$, PDB_SYNC$, SCHEDULER$_CREDENTIAL, USER$, USER_HISTORY$ y XS$VERIFIERS del usuario SYS para evitar que usuarios no autorizados puedan manipular los datos sensibles y confidenciales.		
62	%ANY%	Asegurar que los privilegios tipo %ANY% sean revocados de todos los objetos no autorizados de la base de dato para evitar que usuarios no autorizados puedan manipular los datos confidenciales o dañen el catálogo de datos.		
63	ADMIN_OPTION	Asegurar que de la tabla DBA_SYS_PRIVS.% se revoke los privilegios no autorizados donde el campo ADMIN_OPTION sea igual a YES para evitar que los usuarios puedan otorgar sus mismos privilegios a otros usuarios.		
64	EXECUTE ANY PROCEDURE	Asegurar que el privilegio EXECUTE ANY PROCEDURE sea revocado de los esquemas OUTLN y DBSNMP para evitar que tenga más privilegios de los necesarios.		
65	SELECT ANY DICTIONARY	Asegurar que este privilegio sea revocado de cuentas no administrativas para evitar que un usuario no autorizado pueda recopilar información sobre la base de datos a través del diccionario de datos objetos. La información recopilada podría utilizarse potencialmente para explotar la base de datos.		
66	SELECT ANY TABLE	Asegurar que este privilegio sea revocado de cuentas no administrativas para evitar que un usuario no autorizado pueda visualizar sin autorización información sensible.		
67	AUDIT SYSTEM	Asegurar que este privilegio sea revocado de cuentas no administrativas para evita que un usuario no autorizado pueda alterar las actividades de auditoria programadas, como deshabilitar la creación de pistas de auditoría.		

68	EXEMPT ACCESS POLICY	Asegurar que este privilegio sea revocado de cuentas no administrativas para evitar que un usuario no autorizado pueda acceder a todas las filas de una tabla independientemente de los bloqueos de seguridad a nivel de fila.		
69	BECOME USER	Asegurar que este privilegio sea revocado de cuentas no administrativas para evitar que un usuario no autorizado pueda usar privilegios otorgados a otro usuario,		
70	CREATE PROCEDURE	Asegurar que este privilegio sea revocado de cuentas no administrativas para evitar que un usuario no autorizado pueda crear procedimientos no autorizados que facilitan el robo de datos o la denegación de servicio al corromper las tablas de datos.		
71	ALTER SYSTEM	Asegurar que este privilegio sea revocado de cuentas no administrativas para evitar que un usuario no autorizado pueda modificar las operaciones en ejecución de la instancia.		
72	CREATE ANY LIBRARY y CREATE LIBRARY	Asegurar que estos privilegios sean revocados de cuentas no administrativas para evitar que un usuario no autorizado pueda crear objetos que están asociados a las bibliotecas compartidas.		
73	GRANT ANY OBJECT PRIVILEGE, GRANT ANY ROLE y GRANT ANY PRIVILEGE	Asegurar que estos privilegios sean revocados de cuentas no administrativas para evitar que un usuario no autorizado pueda acceder o cambiar datos confidenciales, o dañar el catálogo de datos debido a un potencial daño al acceso de instancia.		
74	SELECT_CATALOG_ROLE	Asegurar que este rol sea revocado de cuentas no administrativas para evitar que un usuario no autorizado pueda divulgar todos los datos del diccionario.		
75	EXECUTE_CATALOG_ROLE	Asegurar que este rol sea revocado de cuentas no administrativas para evitar que un usuario no autorizado pueda interrumpir las operaciones mediante la inicialización de procedimientos no autorizados.		
76	DBA	Asegurar que este rol sea revocado de cuentas no administrativas para evitar que un usuario no autorizado pueda generar una gran cantidad de problemas innecesarios. Este privilegio abre la puerta a violaciones de datos, violaciones de integridad y condiciones de denegación de servicio.		
V.1.3 Configuración de parámetros de auditorías				
V.1.3.1 Configurar parámetros de auditoria tradicional				

77	AUDIT_OPTION = USER	Asegurar que la tabla DBA_STMT_AUDIT_OPTS contenga un registro donde el campo AUDIT_OPTION sea igual a USER va a permitir auditar todas las actividades que realicen en la base de datos.		
78	AUDIT_OPTION = ROLE	Asegurar que la tabla DBA_STMT_AUDIT_OPTS contenga un registro donde el campo AUDIT_OPTION sea igual a ROLE va a permitir auditar todos los intentos, exitosos o no, de crear, descartar, modificar o establecer roles.		
79	AUDIT_OPTION = SYSTEM GRANT	Asegurar que la tabla DBA_STMT_AUDIT_OPTS contenga un registro donde el campo AUDIT_OPTION sea igual a SYSTEM GRANT va a permitir auditar cualquier intento, exitoso o no, para otorgar o revocar cualquier privilegio o función del sistema, independientemente del privilegio en poder del usuario que intenta la operación.		
80	AUDIT_OPTION = PROFILE	Asegurar que la tabla DBA_STMT_AUDIT_OPTS contenga un registro donde el campo AUDIT_OPTION sea igual a PROFILE va a permitir auditar todos los intentos, exitosos o no, de crear, descartar o alterar cualquier perfil.		
81	AUDIT_OPTION = DATABASE LINK	Asegurar que la tabla DBA_STMT_AUDIT_OPTS contenga un registro donde el campo AUDIT_OPTION sea igual a DATABASE LINK va a permitir auditar todas las actividades en los enlaces de la base de datos.		
82	AUDIT_OPTION = PUBLIC DATABASE LINK	Asegurar que la tabla DBA_STMT_AUDIT_OPTS contenga un registro donde el campo AUDIT_OPTION sea igual a PUBLIC DATABASE LINK va a permitir auditar todas las actividades del usuario que impliquen la creación, alteración o eliminación de los enlaces públicos.		
83	AUDIT_OPTION = PUBLIC SYNONYM	Asegurar que la tabla DBA_STMT_AUDIT_OPTS contenga un registro donde el campo AUDIT_OPTION sea igual a PUBLIC SYNONYM va a permitir auditar todas las actividades del usuario que impliquen la creación, alteración o eliminación de los sinónimos públicos.		
84	AUDIT_OPTION = SYNONYM	Asegurar que la tabla DBA_STMT_AUDIT_OPTS contenga un registro donde el campo AUDIT_OPTION sea igual a SYNONYM va a permitir auditar todas las actividades del usuario que impliquen la creación, alteración o eliminación de los sinónimos públicos.		
85	AUDIT_OPTION = DIRECTORY	Asegurar que la tabla DBA_STMT_AUDIT_OPTS contenga un registro donde el campo AUDIT_OPTION sea igual a DIRECTORY va		

		a permitir auditar todas las actividades del usuario que impliquen la creación, alteración o eliminación de un directorio.		
86	AUDIT_OPTION = SELECT ANY DICTIONARY	Asegurar que la tabla DBA_STMT_AUDIT_OPTS contenga un registro donde el campo AUDIT_OPTION sea igual a SELECT ANY DICTIONARY va a permitir auditar todas las actividades del usuario relacionadas con esta capacidad.		
87	AUDIT_OPTION = GRANT ANY OBJECT PRIVILEGE	Asegurar que la tabla DBA_STMT_AUDIT_OPTS contenga un registro donde el campo AUDIT_OPTION sea igual a GRANT ANY OBJECT PRIVILEGE va a permitir para auditar todas las actividades del usuario relacionadas con otorgar o revocar cualquier privilegio de objeto, que incluye privilegios sobre tablas, directorios, modelos de minería.		
88	AUDIT_OPTION = GRANT ANY PRIVILEGE	Asegurar que la tabla DBA_STMT_AUDIT_OPTS contenga un registro donde el campo AUDIT_OPTION sea igual a GRANT ANY PRIVILEGE va a permitir auditar todas las actividades del usuario administrador relacionadas con cambiar la seguridad infraestructura, para eliminar, agregar, modificar usuarios y más.		
89	AUDIT_OPTION = DROP ANY PROCEDURE	Asegurar que la tabla DBA_STMT_AUDIT_OPTS contenga un registro donde el campo AUDIT_OPTION sea igual a DROP ANY PROCEDURE va a permitir auditar todas las actividades del usuario que impliquen la eliminación de procedimientos.		
90	SYS.AUD$	Asegurar que el privilegio ALL este habilitado en la tabla SYS.AUD$ va proporcionar pruebas forenses desde el inicio de actividades no autorizadas.		
91	AUDIT_OPTION = PROCEDURE	Asegurar que la tabla DBA_STMT_AUDIT_OPTS contenga un registro donde el campo AUDIT_OPTION sea igual a PROCEDURE va a permitir auditar todas las actividades del usuario que impliquen la creación, alteración o eliminación de un procedimiento.		
92	AUDIT_OPTION = ALTER SYSTEM	Asegurar que la tabla DBA_STMT_AUDIT_OPTS contenga un registro donde el campo AUDIT_OPTION sea igual a ALTER SYSTEM va permitir auditar cualquier intento no autorizado de alterar el sistema, estos registros pueden ser muy útiles.		
93	AUDIT_OPTION = TRIGGER	Asegurar que la tabla DBA_STMT_AUDIT_OPTS contenga un registro donde el campo AUDIT_OPTION sea igual a TRIGGER va a permitir auditar todas las actividades del usuario que impliquen la creación, alteración o eliminación de un trigger.		

94	AUDIT_OPTION = CREATE SESSION	Asegurar que la tabla DBA_STMT_AUDIT_OPTS contenga un registro donde el campo AUDIT_OPTION sea igual a CREATE SESSION va a permitir auditar todos los intentos de conexión a la base de datos, ya sea con éxito o no, así como las desconexiones/cierres de sesión de auditoría.		
V.1.3.2 Configurar parámetros de auditoría unificada				
95	CREATE USER	Asegurar habilitar la auditoría de la instrucción CREATE USER va permitir el registro de todas las creaciones de cuentas ya sean exitosas o no, emitidas por los usuarios independientemente de los privilegios que tienen los usuarios.		
96	ALTER USER	Asegurar habilitar la auditoría de la instrucción ALTER USER va permitir el registro de todos los cambios de contraseña, bloqueo de cuentas. También va registrar los cambios de propiedades de los usuarios, Profiles, tablespaces por defecto o temporales y las cuotas de espacio en los tablespaces ya sean exitosas o no, emitidas por los usuarios independientemente de los privilegios que tienen los usuarios.		
97	DROP USER	Asegurar habilitar la auditoría de la instrucción DROP USER va permitir el registro de todas las eliminaciones de cuentas o esquemas de la base de datos ya sean exitosas o no, emitidas por los usuarios independientemente de los privilegios que tienen los usuarios.		
98	CREATE ROLE	Asegurar habilitar la auditoría de la instrucción CREATE ROLE va permitir el registro de todas las creaciones de colecciones de privilegios de sistema, privilegios de objetos que se otorgan a los usuarios o a otros roles ya sean exitosas o no, emitidas por los usuarios independientemente de los privilegios que tienen los usuarios.		
99	ALTER ROLE	Asegurar habilitar la auditoría de la instrucción ALTER ROLE va permitir el registro de todos los movimientos que se realizan en la colección de privilegios de sistema, privilegios de objetos que se otorgan a los usuarios o a otros roles ya sean exitosas o no, emitidas por los usuarios independientemente de los privilegios que tienen los usuarios.		
100	DROP ROLE	Asegurar habilitar la auditoría de la instrucción DROP ROLE va permitir el registro de todas las eliminaciones de colecciones de privilegios de sistema, privilegios de objetos que se otorgan a los usuarios o a otros roles ya sean exitosas o no, emitidas por los		

		usuarios independientemente de los privilegios que tienen los usuarios.		
101	GRANT	Asegurar habilitar la auditoría de la instrucción GRANT va permitir el registro de todas las otorgaciones de privilegios a los usuarios o a otros roles ya sean exitosas o no, emitidas por los usuarios independientemente de los privilegios que tienen los usuarios		
102	REVOKE	Asegurar habilitar la auditoría de la instrucción REVOKE va permitir el registro de todas las revocatorias de privilegios a los usuarios o a otros roles ya sean exitosas o no, emitidas por los usuarios independientemente de los privilegios que tienen los usuarios		
103	CREATE PROFILE	Asegurar habilitar la auditoría de la instrucción CREATE PROFILE va permitir el registro de todas las creaciones de políticas de contraseñas, como reglas de complejidad de contraseñas, restricciones de reutilización y límites de uso de recursos ya sean exitosas o no, emitidas por los usuarios independientemente de los privilegios que tienen los usuarios.		
104	ALTER PROFILE	Asegurar habilitar la auditoría de la instrucción ALTER PROFILE va permitir el registro de todas las modificaciones de políticas de contraseñas, como reglas de complejidad de contraseñas, restricciones de reutilización y límites de uso de recursos ya sean exitosas o no, emitidas por los usuarios independientemente de los privilegios que tienen los usuarios.		
105	DROP PROFILE	Asegurar habilitar la auditoría de la instrucción DROP PROFILE va permitir el registro de todas las modificaciones de políticas de contraseñas, como reglas de complejidad de contraseñas, restricciones de reutilización y límites de uso de recursos ya sean exitosas o no, emitidas por los usuarios independientemente de los privilegios que tienen los usuarios		
106	CREATE DATABASE LINK	Asegurar habilitar la auditoría de la instrucción CREATE DATABASE LINK va permitir el registro de todas las creaciones de los enlaces para establecer conexiones de base de datos a base de datos, estas conexiones están disponibles sin autenticación ya sean exitosas o no, emitidas por los usuarios independientemente de los privilegios que tienen los usuarios.		
107	ALTER DATABASE LINK	Asegurar habilitar la auditoría de la instrucción ALTER DATABASE LINK va permitir el registro de todas las modificaciones de los enlaces para establecer conexiones de base de datos a base de datos, estas		

		conexiones están disponibles sin autenticación ya sean exitosas o no, emitidas por los usuarios independientemente de los privilegios que tienen los usuarios		
108	DROP DATABASE LINK	Asegurar habilitar la auditoría de la instrucción ALTER DATABASE LINK va permitir el registro de todas las eliminaciones de los enlaces para establecer conexiones de base de datos a base de datos, estas conexiones están disponibles sin autenticación ya sean exitosas o no, emitidas por los usuarios independientemente de los privilegios que tienen los usuarios		
109	CREATE SYNONYM	Asegurar habilitar la auditoría de la instrucción CREATE SYNONYM va permitir el registro de todas las creaciones de un nombre alternativo para un objeto de base de datos como tabla, vista, procedimiento, objeto java o incluso otro sinónimo ya sean exitosas o no, emitidas por los usuarios independientemente de los privilegios que tienen los usuarios.		
110	ALTER SYNONYM	Asegurar habilitar la auditoría de la instrucción ALTER SYNONYM va permitir el registro de todas las modificaciones de un nombre alternativo para un objeto de base de datos como tabla, vista, procedimiento, objeto java o incluso otro sinónimo ya sean exitosas o no, emitidas por los usuarios independientemente de los privilegios que tienen los usuarios		
111	DROP SYNONYM	Asegurar habilitar la auditoría de la instrucción DROP SYNONYM va permitir el registro de todas las eliminaciones de un nombre alternativo para un objeto de base de datos como tabla, vista, procedimiento, objeto java o incluso otro sinónimo ya sean exitosas o no, emitidas por los usuarios independientemente de los privilegios que tienen los usuarios		
112	SELECT ANY DICTIONARY	Asegurar habilitar la auditoría de la instrucción SELECT ANY DICTIONARY va permitir el registro de todas las acciones que realizan los usuarios cuando vean la definición de los objetos de esquemas, de los objetos del diccionario de datos, incluido en vistas DBA_, vistas V$, vistas X$ y tablas SYS subyacentes como TAB$ y OBJ		
113	AUDSYS.AUD$UNIFIED	Asegurar habilitar la auditoría de la instrucción AUDSYS.AUD$UNIFIED va permitir el registro de todos los intentos de acceso a AUDSYS.AUD$UNIFIED, ya sea con éxito o sin éxito, independientemente de los privilegios que tengan los usuarios para emitir dichas declaraciones		

114	CREATE PROCEDURE /FUNCTION / PACKAGE / PACKAGE BODY	Asegurar habilitar la auditoría de las instrucciones CREATE PROCEDURE / FUNCTION / PACKAGE / PACKAGE BODY va permitir el registro de todas las creaciones de estas instrucciones comerciales que se encuentran definido por código PL/SQL y sentencias SQL contenidas dentro de estos objetos, ya sean instrucciones satisfactorias o no satisfactorias emitidos por los usuarios independientemente de los privilegios que tengan los usuarios para emitir tales declaraciones		
115	ALTER PROCEDURE / FUNCTION / PACKAGE / PACKAGE BODY	Asegurar habilitar la auditoría de las instrucciones ALTER PROCEDURE / FUNCTION / PACKAGE / PACKAGE BODY va permitir el registro de todas las modificaciones de estas instrucciones comerciales que se encuentran definido por código PL/SQL y sentencias SQL contenidas dentro de estos objetos, ya sean instrucciones satisfactorias o no satisfactorias emitidos por los usuarios independientemente de los privilegios que tengan los usuarios para emitir tales declaraciones		
116	DROP PROCEDURE / FUNCTION / PACKAGE / PACKAGE BODY	Asegurar habilitar la auditoría de las instrucciones DROP PROCEDURE / FUNCTION / PACKAGE / PACKAGE BODY va permitir el registro de todas las eliminaciones de estas instrucciones comerciales que se encuentran definido por código PL/SQL y sentencias SQL contenidas dentro de estos objetos, ya sean instrucciones satisfactorias o no satisfactorias emitidos por los usuarios independientemente de los privilegios que tengan los usuarios para emitir tales declaraciones		
117	ALTER SYSTEM	Asegurar habilitar la auditoría de la instrucción ALTER SYSTEM va permitir el registro de todas las modificaciones al cambiar la configuración de la instancia que podría afectar la postura de seguridad, rendimiento o funcionamiento normal de la base de datos. Además, se registrarán la ejecución de los comandos de sistema operativo, ya sean exitosas o no, realizadas por los usuarios independientemente de sus privilegios.		
118	CREATE TRIGGER	Asegurar habilitar la auditoría de la instrucción CREATE TRIGGER va permitir el registro de todas las creaciones de los disparadores que contienen código para realizar validaciones o hacer cumplir restricciones críticas sobre los datos ya sean exitosas o no, ejecutadas por los usuarios independientemente de los privilegios que tienen los usuarios.		

119	ALTER TRIGGER	Asegurar habilitar la auditoría de la instrucción ALTER TRIGGER va permitir el registro de todas las modificaciones de los disparadores que contienen código para realizar validaciones o hacer cumplir restricciones críticas sobre los datos ya sean exitosas o no, ejecutadas por los usuarios independientemente de los privilegios que tienen los usuarios		
120	DROP TRIGGER	Asegurar habilitar la auditoría de la instrucción DROP TRIGGER va permitir el registro de todas las eliminaciones de los disparadores que contienen código para realizar validaciones o hacer cumplir restricciones críticas sobre los datos ya sean exitosas o no, ejecutadas por los usuarios independientemente de los privilegios que tienen los usuarios		
121	LOGON / LOGOFF	Asegurar habilitar la auditoría de la instrucción LOGON / LOGOFF va permitir el registro de todas los inicios o cierres de sesión que realicen los usuarios independientemente de sus privilegios		

Anexo 6: Lista de Cotejo para la instancia de base de datos "bdgpaqa" del ambiente de control de calidad de la empresa GPA Business SAC:

Escala: No aplicado = 0; Aplicado = 1

V1.1 Actualización del software de base de datos y configuración de parámetros				
V1.1.1: Versión del parche del motor de BD				
Ítem	**Controles / Parámetros**	**Acción**	**Escala**	**Observación**
1	PATCH	Asegurar que esté aplicado el último parche generado por el fabricante para mitigar la posibilidad de vulnerabilidad en la base de datos Oracle.		
V1.1.2: Configurar parámetros de listener				
2	EXTPROC	Asegurar que dicho parámetro no esté presente en el archivo listener.ora para evitar que algunas librerías del sistema operativo puedan ser invocadas por la base de datos.		
3	ADMIN_RESTRICTIONS	Asegurar que ese parámetro esté presente en el archivo listener.ora para evitar que usuarios no administradores puedan alterar en tiempo real los parámetros del archivo.		
V1.1.3: Configurar parámetros generales de BD				
4	AUDIT_SYS_OPERATIONS	Asegurar que se configure este parámetro con el valor de TRUE va permitir conocer las actividades realizadas por la cuenta administradora SYS. Las operaciones se registrarán en la tabla SYS.AUD$. Va a requerir reinicio de la base de datos.		
5	AUDIT_TRAIL	Asegurar que se configure este parámetro con los valores de DB, EXTENDED, OS, XML, EXTENDED, DB, XML; va permitir habilitar las funciones básicas de auditoría, además de recopilar datos para solucionar problemas y valiosos registros forenses.		
6	GLOBAL_NAMES	Asegurar que se configure este parámetro con el valor de TRUE va permitir conectarse remotamente a otra base de datos a través de un único nombre de enlace entre las bases de datos.		
7	OS_ROLES	Asegurar que se configure este parámetro con el valor de FALSE para evitar que el sistema operativo use grupos externos para la administración de la base de datos.		
8	REMOTE_LISTENER	Asegurar que se configure este parámetro con el valor NULL para evitar establecer un oyente válido en un sistema separado, a menos que estén utilizando un RAC.		

9	REMOTE_LOGIN_PASSWORDFILE	Asegurar que se configure este parámetro con el valor de NONE para evitar conexiones privilegiadas no seguras a la base de datos.		
10	REMOTE_OS_AUTHENT	Asegurar que se configure este parámetro con el valor de FALSE para evitar suplantación de conexiones y permita otorgar privilegios a un usuario no autorizado del sistema operativo y este pueda realizar conexiones.		
11	REMOTE_OS_ROLES	Asegurar que se configure este parámetro con el valor de FALSE para evitar que usuarios del sistema operativo tengan permisos para la administración de la base de datos.		
12	SEC_CASE_SENSITIVE_LOGON	Asegurar que se configure este parámetro con el valor de TRUE para aumentar el conjunto de caracteres que se pueden elegir para las contraseñas, lo que evita a los ataques de contraseña de fuerza bruta.		
13	SEC_MAX_FAILED_LOGIN_ATTEMPTS	Asegurar que se configure este parámetro con el valor de 3 o menos, determina cuántos inicios de sesión fallidos se permitirán, antes de que la instancia cierre la conexión de inicio de sesión.		
14	SEC_PROTOCOL_ERROR_FURTHER_ACTION	Asegurar que se configure este parámetro con el valor de (DROP,3) permitirá que se corte una conexión después de tres paquetes defectuosos o con formato incorrecto.		
15	SEC_PROTOCOL_ERROR_TRACE_ACTION	Asegurar que se configure este parámetro con el valor de LOG, permite el registro de los acontecimientos que pasa en la instancia de base de datos.		
16	SEC_RETURN_SERVER_RELEASE_BANNER	Asegurar que se configure este parámetro con el valor de FALSE para evitar que la base de datos devuelva información sobre el número de versión del parche aplicado.		
17	SQL92_SECURITY	Asegurar que se configure este parámetro con el valor de TRUE para evitar la divulgación de información involuntaria asegurándose de que solo los usuarios que ya tienen el privilegio SELECT puedan ejecutar sentencias que les permite obtener los valores almacenados.		
18	TRACE_FILES_PUBLIC	Asegurar que se configure este parámetro con el valor de FALSE para evitar que el archivo de rastreo del sistema sea legible.		
19	RESOURCE_LIMIT	Asegurar que se configure este parámetro con el valor de TRUE determina si se aplican límites de recursos en los perfiles de base de datos.		
V.1.2. Configuración de parámetros de conexión, acceso, usuarios y asignación y/o revocación de privilegios				
V.1.2.1. Configurar parámetros de conexión y acceso				
Ítem	**Control**	**Acción**	**Escala**	**Observación**

20	FAILED_LOGIN_ATTEMPTS	Asegurar que se configure este parámetro con el valor de 5 o menos, determina cuántos intentos fallidos de inicio de sesión se permite antes de que el sistema bloquee la cuenta del usuario.		
21	PASSWORD_LOCK_TIME	Asegurar que se configure este parámetro con el valor de 1 determina cuántos días deben pasar para que la cuenta se desbloqué después de que se haya producido el número establecido de intentos fallidos en el inicio de sesión.		
22	PASSWORD_LIFE_TIME	Asegurar que se configure este parámetro con el valor de 90 o menos para determinar cuánto tiempo se puede usar una contraseña antes de que el usuario pueda cambiarla.		
23	PASSWORD_REUSE_MAX	Asegurar que se configure este parámetro con el valor de 20 o más, para determinar cuántas contraseñas diferentes se deben usar antes de que el usuario pueda reutilizar una contraseña anterior.		
24	PASSWORD_REUSE_TIME	Asegurar que se configure este parámetro con el valor de 365 o más, para determina la cantidad de tiempo en días que debe pasar antes de que se pueda reutilizar la misma contraseña.		
25	PASSWORD_GRACE_TIME	Asegurar que se configure este parámetro con el valor de 5 o menos, para determinar cuántos días puede un usuario tener una contraseña vencida, antes que la sesión del usuario se bloque automáticamente.		
26	PASSWORD_VERIFY_FUNCTIO N	Asegurar que se configure este parámetro en todos los Profiles, para determinar las reglas de complejidad de contraseñas (casos mixtos con dígitos y caracteres especiales), bloquear las combinaciones simples y aplicar cambios a las configuraciones de historial logrando frustrar potencialmente los inicios de sesión no autorizados.		
27	SESSIONS_PER_USER	Asegurar que se configure este parámetro con el valor de 10 o menos, para determinar el número máximo de sesiones de un usuario ayudando a prevenir el mal uso de recursos a nivel de memoria o ataques de denegación de servicio intencionales.		
28	INACTIVE_ACCOUNT_TIME	Asegurar que se configure este parámetro con el valor de 120 o menos, para determinar el número máximo de días de inactividad (sin inicios de sesión en absoluto) después de lo cual la cuenta se bloqueará.		
V.1.2.2. Configurar parámetros de usuarios				
29	Credenciales por defecto (DEFAULT PASSWORDS)	Asegurar que todas las credenciales por defecto sean modificadas, para evitar que cualquier atacante con acceso a la base de datos		

		puede autenticarse con una cuenta predeterminada utilizando una credencial por efecto.		
30	Esquemas de ejemplo (SAMPLE DATA)	Asegurar que todos los esquemas de muestra (BI o HR o IX o OE o PM o SCOTT o SH) sean removidos del ambiente de producción, para evitar que puedan ser utilizados para lanzar exploits contra el ambiente de producción.		
31	DBA_USERS.AUTHENTICATION_TYPE	Asegurar que esté campo no contenga el valor de EXTERNAL, para evitar que un usuario remoto del sistema operativo pueda tener acceso a la base de datos con autorización completa.		
32	Usuarios sin profile por defecto (DEFAULT PROFILE)	Asegurar que los usuarios no tengan asignado el profile por defecto (DEFAULT), debido a que cuenta con configuraciones ilimitadas que a menudo son requeridas por el usuario administrador, tales configuraciones ilimitadas deben reservarse estrictamente y no aplicarse a usuarios innecesarios.		
33	SYS.USER$MIG	Asegurar que la tabla sys.user$mig sea eliminada al inicio de una migración, para evitar que su información pueda llegar hacer conocida por un atacante.		
34	Enlaces públicos (PUBLIC DATABASE LINKS)	Asegurar que no exista enlaces públicos de bases de datos para evitar que cualquier usuario pueda logra una conexión a la base de datos para consultar, actualizar, insertar, eliminar datos en una base de datos remota.		
V.1.2.3. Asignar y/o revocar privilegios				
35	DBMS_LDAP - UTL_INADDR	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de las tablas DBMS_LDAP y UTL_INADDR para evitar la creación de errores especialmente diseñados o él envió de información vía DNS al exterior.		
36	UTL_TCP	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de la tabla UTL_TCP para evitar que usuarios no autorizados envíen datos arbitrarios desde el servidor de base de datos.		
37	UTL_MAIL - UTL_SMTP	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de las tablas UTL_MAIL y UTL_SMTP para evitar que un usuario no autorizado corrompa el SMTP, función para aceptar o generar correo no deseado que puede resultar en una denegación de servicio debido a la saturación de la red		
38	UTL_DBWS	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de la tabla UTL_DBWS para evitar que un usuario no autorizado corrompa		

		el HTTP flujo utilizado para transportar los protocolos que comunican la instancia basada en la web.		
39	UTL_ORAMTS - UTL_HTTP	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de las tablas UTL_ORAMTS y UTL_HTTP para evitar él envió de información (sensible) a sitios web.		
40	HTTPURITYPE	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de la tabla HTTPURITYPE para evitar el filtrado de información de la base de datos a un destino externo por HTTP.		
41	DBMS_ADVISOR	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de la tabla DBMS_ADVISOR para evitar que un usuario no autorizado corrompa archivos del sistema operativo o componentes fundamentales de la base de datos.		
42	DBMS_LOB	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de la tabla DBMS_LOB para evitar que subprogramas puedan manipular, leer, escribir en BLOB, CLOB, NCLOB, BFILE y LOB temporales		
43	UTL_FILE	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de la tabla UTL_FILE para evitar que un usuario pueda leer y escribir archivos ubicados en el servidor donde está instalada la instancia de base de datos.		
44	DBMS_CRYPTO	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de la tabla DBMS_CRYPTO para evitar la ejecución de procedimientos de criptografía que puede potencialmente comprometer una porción o la totalidad de los datos.		
45	DBMS_OBFUSCATION_TOOLKIT	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de la tabla DBMS_OBFUSCATION_TOOLKIT para evitar que la herramienta que determina la fuerza del algoritmo de cifrado sea utilizada para cifrar los datos de la aplicación.		
46	DBMS_RANDOM	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de la tabla DBMS_RANDOM para evitar que una aplicación no autorizada genere números aleatorios.		
47	DBMS_JAVA - DBMS_JAVA_TEST	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de las tablas DBMS_JAVA y DBMS_JAVA_TEST para evitar que un atacante ejecute comandos del sistema operativo desde la base de datos.		

48	DBMS_JOB	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de la tabla DBMS_JOB para evitar que un usuario no autorizado inhabilite o sobrecargue la cola de trabajos.		
49	DBMS_SCHEDULER	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de la tabla DBMS_SCHEDULER para evitar que un usuario no autorizado ejecute trabajos de la base de datos o del sistema operativo.		
50	DBMS_SQL	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de la tabla DBMS_SQL para evitar la escalada de privilegios si no se realiza la validación de entrada adecuadamente.		
51	DBMS_XMLGEN	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de la tabla DBMS_XMLGEN para evitar la búsqueda de información confidencial en toda la base de datos. Información como números de tarjetas de crédito.		
52	DBMS_XMLQUERY, DBMS_XMLSAVE, DBMS_XMLSTORE, DBMS_AW, OWA_UTIL y DBMS_REDACT	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de las tablas DBMS_XMLQUERY, DBMS_XMLSAVE, DBMS_XMLSTORE, DBMS_AW, OWA_UTIL y DBMS_REDACT para evitar que usuarios malintencionados pueden aprovechar este paquete como una función de inyección auxiliar en un ataque de inyección SQL.		
53	DBMS_BACKUP_RESTORE	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de la tabla DBMS_BACKUP_RESTORE para evitar el acceso a los archivos del sistema operativo.		
54	DBMS_FILE_TRANSFER	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de la tabla DBMS_FILE_TRANSFER para evitar transferir archivos desde un servidor de base de datos a otro sin autorización para hacerlo.		
55	DBMS_SYS_SQL	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de la tabla DBMS_SYS_SQL para evitar que un usuario ejecute código como un usuario diferente sin ingresar credenciales válidas.		
56	DBMS_REPCAT_SQL_UTL, INITJVMAUX, DBMS_AQADM_SYS, DBMS_STREAMS_RPC y LTADM	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de las tablas DBMS_REPCAT_SQL_UTL, INITJVMAUX, DBMS_AQADM_SYS, DBMS_STREAMS_RPC y LTADM para evitar que un usuario no autorizado ejecute SQL comandos como un usuario SYS.		
57	DBMS_PRVTAQIM	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de la tabla DBMS_PRVTAQIM para evitar que un usuario no autorizado escale privilegios por cualquier instrucción SQL y que podría ejecutarse como usuario SYS.		

58	DBMS_IJOB y DBMS_PDB_EXEC_SQL	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de las tablas DBMS_IJOB y DBMS_PDB_EXEC_SQL para evitar que un atacante cambie de identidad utilizando un nombre de usuario diferente para ejecutar un trabajo de base de datos.		
59	SYS.AUD$	Asegurar que usuarios no autorizados tengan privilegios sobre la tabla SYS.AUD$ para que no permita distorsión en los registros de auditoría, escondiendo actividades no autorizadas.		
60	SYS.DBA_%	Asegurar que el privilegio PUBLIC sea revocado de todas las tablas sensibles del usuario SYS que sean encontradas en la vista DBA_% para evitar que usuarios no autorizados puedan manipular los datos confidenciales.		
61	CDB_LOCAL_ADMINAUTH$, DEFAULT_PWD$, ENC$, HISTGRM$, HIST_HEAD$, LINK$, PDB_SYNC$, SCHEDULER$_CREDENTIAL, USER$, USER_HISTORY$ y XS$VERIFIERS	Asegurar que el privilegio ALL sea revocado de las tablas CDB_LOCAL_ADMINAUTH$, DEFAULT_PWD$, ENC$, HISTGRM$, HIST_HEAD$, LINK$, PDB_SYNC$, SCHEDULER$_CREDENTIAL, USER$, USER_HISTORY$ y XS$VERIFIERS del usuario SYS para evitar que usuarios no autorizados puedan manipular los datos sensibles y confidenciales.		
62	%ANY%	Asegurar que los privilegios tipo %ANY% sean revocados de todos los objetos no autorizados de la base de dato para evitar que usuarios no autorizados puedan manipular los datos confidenciales o dañen el catálogo de datos.		
63	ADMIN_OPTION	Asegurar que de la tabla DBA_SYS_PRIVS.% se revoke los privilegios no autorizados donde el campo ADMIN_OPTION sea igual a YES para evitar que los usuarios puedan otorgar sus mismos privilegios a otros usuarios.		
64	EXECUTE ANY PROCEDURE	Asegurar que el privilegio EXECUTE ANY PROCEDURE sea revocado de los esquemas OUTLN y DBSNMP para evitar que tenga más privilegios de los necesarios.		
65	SELECT ANY DICTIONARY	Asegurar que este privilegio sea revocado de cuentas no administrativas para evitar que un usuario no autorizado pueda recopilar información sobre la base de datos a través del diccionario de datos objetos. La información recopilada podría utilizarse potencialmente para explotar la base de datos.		

66	SELECT ANY TABLE	Asegurar que este privilegio sea revocado de cuentas no administrativas para evitar que un usuario no autorizado pueda visualizar sin autorización información sensible.		
67	AUDIT SYSTEM	Asegurar que este privilegio sea revocado de cuentas no administrativas para evita que un usuario no autorizado pueda alterar las actividades de auditoria programadas, como deshabilitar la creación de pistas de auditoría.		
68	EXEMPT ACCESS POLICY	Asegurar que este privilegio sea revocado de cuentas no administrativas para evitar que un usuario no autorizado pueda acceder a todas las filas de una tabla independientemente de los bloqueos de seguridad a nivel de fila.		
69	BECOME USER	Asegurar que este privilegio sea revocado de cuentas no administrativas para evitar que un usuario no autorizado pueda usar privilegios otorgados a otro usuario,		
70	CREATE PROCEDURE	Asegurar que este privilegio sea revocado de cuentas no administrativas para evitar que un usuario no autorizado pueda crear procedimientos no autorizados que facilitan el robo de datos o la denegación de servicio al corromper las tablas de datos.		
71	ALTER SYSTEM	Asegurar que este privilegio sea revocado de cuentas no administrativas para evitar que un usuario no autorizado pueda modificar las operaciones en ejecución de la instancia.		
72	CREATE ANY LIBRARY y CREATE LIBRARY	Asegurar que estos privilegios sean revocados de cuentas no administrativas para evitar que un usuario no autorizado pueda crear objetos que están asociados a las bibliotecas compartidas.		
73	GRANT ANY OBJECT PRIVILEGE, GRANT ANY ROLE y GRANT ANY PRIVILEGE	Asegurar que estos privilegios sean revocados de cuentas no administrativas para evitar que un usuario no autorizado pueda acceder o cambiar datos confidenciales, o dañar el catálogo de datos debido a un potencial daño al acceso de instancia.		
74	SELECT_CATALOG_ROLE	Asegurar que este rol sea revocado de cuentas no administrativas para evitar que un usuario no autorizado pueda divulgar todos los datos del diccionario.		
75	EXECUTE_CATALOG_ROLE	Asegurar que este rol sea revocado de cuentas no administrativas para evitar que un usuario no autorizado pueda interrumpir las operaciones mediante la inicialización de procedimientos no autorizados.		

76	DBA	Asegurar que este rol sea revocado de cuentas no administrativas para evitar que un usuario no autorizado pueda generar una gran cantidad de problemas innecesarios. Este privilegio abre la puerta a violaciones de datos, violaciones de integridad y condiciones de denegación de servicio.		
V.1.3 Configuración de parámetros de auditorías				
V.1.3.1 Configurar parámetros de auditoria tradicional				
77	AUDIT_OPTION = USER	Asegurar que la tabla DBA_STMT_AUDIT_OPTS contenga un registro donde el campo AUDIT_OPTION sea igual a USER va a permitir auditar todas las actividades que realicen en la base de datos.		
78	AUDIT_OPTION = ROLE	Asegurar que la tabla DBA_STMT_AUDIT_OPTS contenga un registro donde el campo AUDIT_OPTION sea igual a ROLE va a permitir auditar todos los intentos, exitosos o no, de crear, descartar, modificar o establecer roles.		
79	AUDIT_OPTION = SYSTEM GRANT	Asegurar que la tabla DBA_STMT_AUDIT_OPTS contenga un registro donde el campo AUDIT_OPTION sea igual a SYSTEM GRANT va a permitir auditar cualquier intento, exitoso o no, para otorgar o revocar cualquier privilegio o función del sistema, independientemente del privilegio en poder del usuario que intenta la operación.		
80	AUDIT_OPTION = PROFILE	Asegurar que la tabla DBA_STMT_AUDIT_OPTS contenga un registro donde el campo AUDIT_OPTION sea igual a PROFILE va a permitir auditar todos los intentos, exitosos o no, de crear, descartar o alterar cualquier perfil.		
81	AUDIT_OPTION = DATABASE LINK	Asegurar que la tabla DBA_STMT_AUDIT_OPTS contenga un registro donde el campo AUDIT_OPTION sea igual a DATABASE LINK va a permitir auditar todas las actividades en los enlaces de la base de datos.		
82	AUDIT_OPTION = PUBLIC DATABASE LINK	Asegurar que la tabla DBA_STMT_AUDIT_OPTS contenga un registro donde el campo AUDIT_OPTION sea igual a PUBLIC DATABASE LINK va a permitir auditar todas las actividades del usuario que impliquen la creación, alteración o eliminación de los enlaces públicos.		
83	AUDIT_OPTION = PUBLIC SYNONYM	Asegurar que la tabla DBA_STMT_AUDIT_OPTS contenga un registro donde el campo AUDIT_OPTION sea igual a PUBLIC SYNONYM va a permitir auditar todas las actividades del usuario que		

		impliquen la creación, alteración o eliminación de los sinónimos públicos.		
84	AUDIT_OPTION = SYNONYM	Asegurar que la tabla DBA_STMT_AUDIT_OPTS contenga un registro donde el campo AUDIT_OPTION sea igual a SYNONYM va a permitir auditar todas las actividades del usuario que impliquen la creación, alteración o eliminación de los sinónimos públicos.		
85	AUDIT_OPTION = DIRECTORY	Asegurar que la tabla DBA_STMT_AUDIT_OPTS contenga un registro donde el campo AUDIT_OPTION sea igual a DIRECTORY va a permitir auditar todas las actividades del usuario que impliquen la creación, alteración o eliminación de un directorio.		
86	AUDIT_OPTION = SELECT ANY DICTIONARY	Asegurar que la tabla DBA_STMT_AUDIT_OPTS contenga un registro donde el campo AUDIT_OPTION sea igual a SELECT ANY DICTIONARY va a permitir auditar todas las actividades del usuario relacionadas con esta capacidad.		
87	AUDIT_OPTION = GRANT ANY OBJECT PRIVILEGE	Asegurar que la tabla DBA_STMT_AUDIT_OPTS contenga un registro donde el campo AUDIT_OPTION sea igual a GRANT ANY OBJECT PRIVILEGE va a permitir para auditar todas las actividades del usuario relacionadas con otorgar o revocar cualquier privilegio de objeto, que incluye privilegios sobre tablas, directorios, modelos de minería.		
88	AUDIT_OPTION = GRANT ANY PRIVILEGE	Asegurar que la tabla DBA_STMT_AUDIT_OPTS contenga un registro donde el campo AUDIT_OPTION sea igual a GRANT ANY PRIVILEGE va a permitir auditar todas las actividades del usuario administrador relacionadas con cambiar la seguridad infraestructura, para eliminar, agregar, modificar usuarios y más.		
89	AUDIT_OPTION = DROP ANY PROCEDURE	Asegurar que la tabla DBA_STMT_AUDIT_OPTS contenga un registro donde el campo AUDIT_OPTION sea igual a DROP ANY PROCEDURE va a permitir auditar todas las actividades del usuario que impliquen la eliminación de procedimientos.		
90	SYS.AUD$	Asegurar que el privilegio ALL este habilitado en la tabla SYS.AUD$ va proporcionar pruebas forenses desde el inicio de actividades no autorizadas.		
91	AUDIT_OPTION = PROCEDURE	Asegurar que la tabla DBA_STMT_AUDIT_OPTS contenga un registro donde el campo AUDIT_OPTION sea igual a PROCEDURE va a permitir auditar todas las actividades del usuario que impliquen la creación, alteración o eliminación de un procedimiento.		

92	AUDIT_OPTION = ALTER SYSTEM	Asegurar que la tabla DBA_STMT_AUDIT_OPTS contenga un registro donde el campo AUDIT_OPTION sea igual a ALTER SYSTEM va permitir auditar cualquier intento no autorizado de alterar el sistema, estos registros pueden ser muy útiles.		
93	AUDIT_OPTION = TRIGGER	Asegurar que la tabla DBA_STMT_AUDIT_OPTS contenga un registro donde el campo AUDIT_OPTION sea igual a TRIGGER va a permitir auditar todas las actividades del usuario que impliquen la creación, alteración o eliminación de un trigger.		
94	AUDIT_OPTION = CREATE SESSION	Asegurar que la tabla DBA_STMT_AUDIT_OPTS contenga un registro donde el campo AUDIT_OPTION sea igual a CREATE SESSION va a permitir auditar todos los intentos de conexión a la base de datos, ya sea con éxito o no, así como las desconexiones/cierres de sesión de auditoría.		
V.1.3.2 Configurar parámetros de auditoría unificada				
95	CREATE USER	Asegurar habilitar la auditoría de la instrucción CREATE USER va permitir el registro de todas las creaciones de cuentas ya sean exitosas o no, emitidas por los usuarios independientemente de los privilegios que tienen los usuarios.		
96	ALTER USER	Asegurar habilitar la auditoría de la instrucción ALTER USER va permitir el registro de todos los cambios de contraseña, bloqueo de cuentas. También va registrar los cambios de propiedades de los usuarios, Profiles, tablespaces por defecto o temporales y las cuotas de espacio en los tablespaces ya sean exitosas o no, emitidas por los usuarios independientemente de los privilegios que tienen los usuarios.		
97	DROP USER	Asegurar habilitar la auditoría de la instrucción DROP USER va permitir el registro de todas las eliminaciones de cuentas o esquemas de la base de datos ya sean exitosas o no, emitidas por los usuarios independientemente de los privilegios que tienen los usuarios.		
98	CREATE ROLE	Asegurar habilitar la auditoría de la instrucción CREATE ROLE va permitir el registro de todas las creaciones de colecciones de privilegios de sistema, privilegios de objetos que se otorgan a los usuarios o a otros roles ya sean exitosas o no, emitidas por los usuarios independientemente de los privilegios que tienen los usuarios.		

99	ALTER ROLE	Asegurar habilitar la auditoría de la instrucción ALTER ROLE va permitir el registro de todos los movimientos que se realizan en la colección de privilegios de sistema, privilegios de objetos que se otorgan a los usuarios o a otros roles ya sean exitosas o no, emitidas por los usuarios independientemente de los privilegios que tienen los usuarios.		
100	DROP ROLE	Asegurar habilitar la auditoría de la instrucción DROP ROLE va permitir el registro de todas las eliminaciones de colecciones de privilegios de sistema, privilegios de objetos que se otorgan a los usuarios o a otros roles ya sean exitosas o no, emitidas por los usuarios independientemente de los privilegios que tienen los usuarios.		
101	GRANT	Asegurar habilitar la auditoría de la instrucción GRANT va permitir el registro de todas las otorgaciones de privilegios a los usuarios o a otros roles ya sean exitosas o no, emitidas por los usuarios independientemente de los privilegios que tienen los usuarios		
102	REVOKE	Asegurar habilitar la auditoría de la instrucción REVOKE va permitir el registro de todas las revocatorias de privilegios a los usuarios o a otros roles ya sean exitosas o no, emitidas por los usuarios independientemente de los privilegios que tienen los usuarios		
103	CREATE PROFILE	Asegurar habilitar la auditoría de la instrucción CREATE PROFILE va permitir el registro de todas las creaciones de políticas de contraseñas, como reglas de complejidad de contraseñas, restricciones de reutilización y límites de uso de recursos ya sean exitosas o no, emitidas por los usuarios independientemente de los privilegios que tienen los usuarios.		
104	ALTER PROFILE	Asegurar habilitar la auditoría de la instrucción ALTER PROFILE va permitir el registro de todas las modificaciones de políticas de contraseñas, como reglas de complejidad de contraseñas, restricciones de reutilización y límites de uso de recursos ya sean exitosas o no, emitidas por los usuarios independientemente de los privilegios que tienen los usuarios.		
105	DROP PROFILE	Asegurar habilitar la auditoría de la instrucción DROP PROFILE va permitir el registro de todas las modificaciones de políticas de contraseñas, como reglas de complejidad de contraseñas, restricciones de reutilización y límites de uso de recursos ya sean		

		exitosas o no, emitidas por los usuarios independientemente de los privilegios que tienen los usuarios		
106	CREATE DATABASE LINK	Asegurar habilitar la auditoría de la instrucción CREATE DATABASE LINK va permitir el registro de todas las creaciones de los enlaces para establecer conexiones de base de datos a base de datos, estas conexiones están disponibles sin autenticación ya sean exitosas o no, emitidas por los usuarios independientemente de los privilegios que tienen los usuarios.		
107	ALTER DATABASE LINK	Asegurar habilitar la auditoría de la instrucción ALTER DATABASE LINK va permitir el registro de todas las modificaciones de los enlaces para establecer conexiones de base de datos a base de datos, estas conexiones están disponibles sin autenticación ya sean exitosas o no, emitidas por los usuarios independientemente de los privilegios que tienen los usuarios		
108	DROP DATABASE LINK	Asegurar habilitar la auditoría de la instrucción ALTER DATABASE LINK va permitir el registro de todas las eliminaciones de los enlaces para establecer conexiones de base de datos a base de datos, estas conexiones están disponibles sin autenticación ya sean exitosas o no, emitidas por los usuarios independientemente de los privilegios que tienen los usuarios		
109	CREATE SYNONYM	Asegurar habilitar la auditoría de la instrucción CREATE SYNONYM va permitir el registro de todas las creaciones de un nombre alternativo para un objeto de base de datos como tabla, vista, procedimiento, objeto java o incluso otro sinónimo ya sean exitosas o no, emitidas por los usuarios independientemente de los privilegios que tienen los usuarios.		
110	ALTER SYNONYM	Asegurar habilitar la auditoría de la instrucción ALTER SYNONYM va permitir el registro de todas las modificaciones de un nombre alternativo para un objeto de base de datos como tabla, vista, procedimiento, objeto java o incluso otro sinónimo ya sean exitosas o no, emitidas por los usuarios independientemente de los privilegios que tienen los usuarios		
111	DROP SYNONYM	Asegurar habilitar la auditoría de la instrucción DROP SYNONYM va permitir el registro de todas las eliminaciones de un nombre alternativo para un objeto de base de datos como tabla, vista, procedimiento, objeto java o incluso otro sinónimo ya sean exitosas o no, emitidas por		

		los usuarios independientemente de los privilegios que tienen los usuarios		
112	SELECT ANY DICTIONARY	Asegurar habilitar la auditoría de la instrucción SELECT ANY DICTIONARY va permitir el registro de todas las acciones que realizan los usuarios cuando vean la definición de los objetos de esquemas, de los objetos del diccionario de datos, incluido en vistas DBA_, vistas V$, vistas X$ y tablas SYS subyacentes como TAB$ y OBJ		
113	AUDSYS.AUD$UNIFIED	Asegurar habilitar la auditoría de la instrucción AUDSYS.AUD$UNIFIED va permitir el registro de todos los intentos de acceso a AUDSYS.AUD$UNIFIED, ya sea con éxito o sin éxito, independientemente de los privilegios que tengan los usuarios para emitir dichas declaraciones		
114	CREATE PROCEDURE /FUNCTION / PACKAGE / PACKAGE BODY	Asegurar habilitar la auditoría de las instrucciones CREATE PROCEDURE / FUNCTION / PACKAGE / PACKAGE BODY va permitir el registro de todas las creaciones de estas instrucciones comerciales que se encuentran definido por código PL/SQL y sentencias SQL contenidas dentro de estos objetos, ya sean instrucciones satisfactorias o no satisfactorias emitidos por los usuarios independientemente de los privilegios que tengan los usuarios para emitir tales declaraciones		
115	ALTER PROCEDURE / FUNCTION / PACKAGE / PACKAGE BODY	Asegurar habilitar la auditoría de las instrucciones ALTER PROCEDURE / FUNCTION / PACKAGE / PACKAGE BODY va permitir el registro de todas las modificaciones de estas instrucciones comerciales que se encuentran definido por código PL/SQL y sentencias SQL contenidas dentro de estos objetos, ya sean instrucciones satisfactorias o no satisfactorias emitidos por los usuarios independientemente de los privilegios que tengan los usuarios para emitir tales declaraciones		
116	DROP PROCEDURE / FUNCTION / PACKAGE / PACKAGE BODY	Asegurar habilitar la auditoría de las instrucciones DROP PROCEDURE / FUNCTION / PACKAGE / PACKAGE BODY va permitir el registro de todas las eliminaciones de estas instrucciones comerciales que se encuentran definido por código PL/SQL y sentencias SQL contenidas dentro de estos objetos, ya sean instrucciones satisfactorias o no satisfactorias emitidos por los usuarios independientemente de los privilegios que tengan los usuarios para emitir tales declaraciones		

117	ALTER SYSTEM	Asegurar habilitar la auditoría de la instrucción ALTER SYSTEM va permitir el registro de todas las modificaciones al cambiar la configuración de la instancia que podría afectar la postura de seguridad, rendimiento o funcionamiento normal de la base de datos. Además, se registrarán la ejecución de los comandos de sistema operativo, ya sean exitosas o no, realizadas por los usuarios independientemente de sus privilegios.		
118	CREATE TRIGGER	Asegurar habilitar la auditoría de la instrucción CREATE TRIGGER va permitir el registro de todas las creaciones de los disparadores que contienen código para realizar validaciones o hacer cumplir restricciones críticas sobre los datos ya sean exitosas o no, ejecutadas por los usuarios independientemente de los privilegios que tienen los usuarios.		
119	ALTER TRIGGER	Asegurar habilitar la auditoría de la instrucción ALTER TRIGGER va permitir el registro de todas las modificaciones de los disparadores que contienen código para realizar validaciones o hacer cumplir restricciones críticas sobre los datos ya sean exitosas o no, ejecutadas por los usuarios independientemente de los privilegios que tienen los usuarios		
120	DROP TRIGGER	Asegurar habilitar la auditoría de la instrucción DROP TRIGGER va permitir el registro de todas las eliminaciones de los disparadores que contienen código para realizar validaciones o hacer cumplir restricciones críticas sobre los datos ya sean exitosas o no, ejecutadas por los usuarios independientemente de los privilegios que tienen los usuarios		
121	LOGON / LOGOFF	Asegurar habilitar la auditoría de la instrucción LOGON / LOGOFF va permitir el registro de todas los inicios o cierres de sesión que realicen los usuarios independientemente de sus privilegios		

Anexo 7: Constancia de aplicación del instrumento

CONSTANCIA DE APLICACIÓN

YO, ING. Lopez Leiva Yoel Walter, con DNI N° 41752134, Gerente General de la empresa GPA Business SAC con RUC 20518404963, por medio del presente constato la recolección de datos para la investigación titulada: **"Implementación de controles de configuración de seguridad en la base de datos de GPA Business SAC – Lima 2022"**, considerando los siguientes puntos:

1. PROCEDIMIENTO REALIZADO: Se efectuó una lista de cotejo para la observación y posteriormente se realizará una tabulación y análisis de los resultados obtenidos, con el fin de determinar la viabilidad de la investigación.
2. CONFIDENCIALIDAD: Sólo el investigador y el comité a interpretar tendrán acceso a los datos, su identificación no aparecerá en ningún informe ni publicación resultante del presente estudio.
3. PARTICIPACIÓN VOLUNTARIA: La participación en el estudio es libre y voluntaria. Usted puede negarse a participar o puede interrumpir su participación en cualquier momento durante el estudio.

En señal de conformidad de otorgar constatación para la presente investigación firmo a continuación.

Yoel W. Lopez Leiva
GERENTE GENERAL
GPA BUSINESS S.A.C

ING. Lopez Leiva Yoel Walter
DNI: 41752134

Anexo 8: Validez del Instrumento

UNIVERSIDAD PERUANA LOS ANDES

FICHA DE VALIDEZ DEL INSTRUMENTO

JUICIO DE EXPERTO

Nombre del Instrumento: Lista de Cotejo para los controles de configuración de seguridad en la base de datos Oracle 19c

Nombre del investigador: Jorge Luis Romero Santa Cruz

Título: Implementación de controles de configuración de seguridad en la base de datos de GPA Business SAC – Lima 2022.

Instrucción: Luego de analizar y cotejar el instrumento de investigación "Lista de cotejo" con la matriz de consistencia del presente, le solicito que, en base a su criterio y experiencia profesional, valide dicho instrumento para su aplicación.

CRITERIOS		VALORACIÓN		OBSERVACIÒN
		SI	NO	
1. CLARIDAD	Esta formulado con lenguaje claro y apropiado.	X		
2. OBJETIVIDAD	Esta expresado en conductas observables.	X		
3. PERTINENCIA	Adecuado al avance de la ciencia y la pedagogía.	X		
4. ORGANIZACIÓN	Existe una organización lógica.	X		
5. SUFICIENCIA	Comprende los aspectos de cantidad y calidad.	X		
6. ADECUACIÓN	Adecuado para valorar en constructo o variable a medir.	X		
7. CONSISTENCIA	Basado en aspectos teóricos y científicos.	X		
8. COHERENCIA	Entre las dimensiones, indicadores y los ítems.	X		
9. METODOLOGÍA	La estrategia responde al propósito de la medición.	X		
10. SIGNIFICATIVIDAD	Es útil y adecuado para la investigación.	X		

CRITERIO DE VALORACIÓN DEL JUEZ:

Procede su aplicación (X)

No procede su aplicación ( )

Nombres y apellidos del juez: Katerine Patricia Ramos Pacheco	
Dirección: Paso de los andes 693	
Título profesional: Ingeniera de Sistemas	
Grado académico: Titulada - Colegiada	
Número del DNI: 46897043	Número de celular: 957353151

Lima, 30 de diciembre del 2022

UNIVERSIDAD PERUANA LOS ANDES

FICHA DE VALIDEZ DEL INSTRUMENTO

JUICIO DE EXPERTO

Nombre del Instrumento: Lista de Cotejo para los controles de configuración de seguridad en la base de datos Oracle 19c

Nombre del investigador: Jorge Luis Romero Santa Cruz

Título: Implementación de controles de configuración de seguridad en la base de datos de GPA Business SAC – Lima 2022.

Instrucción: Luego de analizar y cotejar el instrumento de investigación "Lista de cotejo" con la matriz de consistencia del presente, le solicito que, en base a su criterio y experiencia profesional, valide dicho instrumento para su aplicación.

CRITERIOS		VALORACIÓN		OBSERVACIÒN
		SI	NO	
1. CLARIDAD	Esta formulado con lenguaje claro y apropiado.	X		
2. OBJETIVIDAD	Esta expresado en conductas observables.	X		
3. PERTINENCIA	Adecuado al avance de la ciencia y la pedagogía.	X		
4. ORGANIZACIÓN	Existe una organización lógica.	X		
5. SUFICIENCIA	Comprende los aspectos de cantidad y calidad.	X		
6. ADECUACIÓN	Adecuado para valorar en constructo o variable a medir.	X		
7. CONSISTENCIA	Basado en aspectos teóricos y científicos.	X		
8. COHERENCIA	Entre las dimensiones, indicadores y los ítems.	X		
9. METODOLOGÍA	La estrategia responde al propósito de la medición.	X		
10. SIGNIFICATIVIDAD	Es útil y adecuado para la investigación.	X		

CRITERIO DE VALORACIÓN DEL JUEZ:

Procede su aplicación (X)

No procede su aplicación ( )

Nombres y apellidos del juez: IVAN URQUIAGA HUAMAN	
Dirección: BRASIL 1636	
Título profesional: INGENIERO DE SISTEMAS	
Grado académico: TITULADO	
Número del DNI: 42959703	Número de celular: 989406716

Lima, 30 de diciembre del 2022

UNIVERSIDAD PERUANA LOS ANDES

FICHA DE VALIDEZ DEL INSTRUMENTO

JUICIO DE EXPERTO

Nombre del Instrumento: Lista de Cotejo para los controles de configuración de seguridad en la base de datos Oracle 19c

Nombre del investigador: Jorge Luis Romero Santa Cruz

Título: Implementación de controles de configuración de seguridad en la base de datos de GPA Business SAC – Lima 2022.

Instrucción: Luego de analizar y cotejar el instrumento de investigación "Lista de cotejo" con la matriz de consistencia del presente, le solicito que, en base a su criterio y experiencia profesional, valide dicho instrumento para su aplicación.

CRITERIOS		VALORACIÓN		OBSERVACIÒN
		SI	NO	
1. CLARIDAD	Esta formulado con lenguaje claro y apropiado.	X		–
2. OBJETIVIDAD	Esta expresado en conductas observables.	X		–
3. PERTINENCIA	Adecuado al avance de la ciencia y la pedagogía.	X		–
4. ORGANIZACIÓN	Existe una organización lógica.	X		–
5. SUFICIENCIA	Comprende los aspectos de cantidad y calidad.	X		–
6. ADECUACIÓN	Adecuado para valorar en constructo o variable a medir.	X		–
7. CONSISTENCIA	Basado en aspectos teóricos y científicos.	X		–
8. COHERENCIA	Entre las dimensiones, indicadores y los ítems.	X		–
9. METODOLOGÍA	La estrategia responde al propósito de la medición.	X		–
10. SIGNIFICATIVIDAD	Es útil y adecuado para la investigación.	X		–

CRITERIO DE VALORACIÓN DEL JUEZ:

Procede su aplicación (X)

No procede su aplicación ( )

Nombres y apellidos del juez: Genaro Alonso Pardo Mauricio	
Dirección: Urb. Paraíso del Norte 2da Etapa Mz A Lt. 27 - Huandoy, S.M.P.	
Título profesional: Ingeniero de Sistemas	
Grado académico: Bachiller en Ingeniería de Sistemas	
Número del DNI: 72445680	Número de celular: 987607266

Alonso Pardo

Lima, 30 de Diciembre del 2022

UNIVERSIDAD PERUANA LOS ANDES

UPLA

FICHA DE VALIDEZ DEL INSTRUMENTO

JUICIO DE EXPERTO

Nombre del Instrumento: Lista de Cotejo para los controles de configuración de seguridad en la base de datos Oracle 19c

Nombre del investigador: Jorge Luis Romero Santa Cruz

Título: Implementación de controles de configuración de seguridad en la base de datos de GPA Business SAC – Lima 2022.

Instrucción: Luego de analizar y cotejar el instrumento de investigación "Lista de cotejo" con la matriz de consistencia del presente, le solicito que, en base a su criterio y experiencia profesional, valide dicho instrumento para su aplicación.

CRITERIOS		VALORACIÓN		OBSERVACIÒN
		SI	NO	
1. CLARIDAD	Esta formulado con lenguaje claro y apropiado.	X		–
2. OBJETIVIDAD	Esta expresado en conductas observables.	X		–
3. PERTINENCIA	Adecuado al avance de la ciencia y la pedagogia.	X		–
4. ORGANIZACIÓN	Existe una organización lógica.	X		–
5. SUFICIENCIA	Comprende los aspectos de cantidad y calidad.	X		–
6. ADECUACIÓN	Adecuado para valorar en constructo o variable a medir.	X		–
7. CONSISTENCIA	Basado en aspectos teóricos y científicos.	X		–
8. COHERENCIA	Entre las dimensiones, indicadores y los items.	X		–
9. METODOLOGÍA	La estrategia responde al propósito de la medición.	X		–
10. SIGNIFICATIVIDAD	Es útil y adecuado para la investigación.	X		–

CRITERIO DE VALORACIÓN DEL JUEZ:

Procede su aplicación (X)

No procede su aplicación ( )

Nombres y apellidos del juez: ALVIN ENRIQUE ROMERO MORENO	
Dirección: CALLE SAN FELIPE 188 URB. STA. FELICIA, LA MOLINA	
Título profesional: INGENIERO DE COMPUTACION Y SISTEMAS	
Grado académico: BACHILLER EN ING. DE COMPUTACION Y SISTEMAS	
Número del DNI: 40536689	Número de celular: 990599050

Lima, 30 de DICIEMBRE del 2022

Anexo 9: Consentimiento Informado

CONSENTIMIENTO INFORMADO

YO, ING. Lopez Leiva Yoel Walter, con DNI N° 41752134, por medio del presente autorizo el uso de mi información de GPA Business SAC en la investigación titulada: "**Implementación de controles de configuración de seguridad en la base de datos de GPA Business SAC – Lima 2022**", considerando los siguientes puntos:

1. PROCEDIMIENTO A SEGUIR: Se efectuará una lista de cotejo, posteriormente se realizará una tabulación y análisis de los resultados obtenidos, con el fin de determinar la viabilidad de la investigación.
2. CONFIDENCIALIDAD: Sólo el investigador y el comité a interpretar tendrán acceso a los datos, su identificación no aparecerá en ningún informe ni publicación resultante del presente estudio.
3. PARTICIPACIÓN VOLUNTARIA: La participación en el estudio es libre y voluntaria. Usted puede negarse a participar o puede interrumpir su participación en cualquier momento durante el estudio.

En señal de conformidad de otorgar el consentimiento para la presente investigación firmo a continuación.

Yoel W. Lopez Leiva
GERENTE GENERAL
GPA BUSINESS S.A.C

ING. Lopez Leiva Yoel Walter
DNI: 41752134

Anexo 10: Lista de Cotejo Pre Test de los controles de configuración de seguridad en la base de datos Oracle 19c en la instancia de base de datos "bdgpadev" del ambiente de desarrollo de la empresa GPA Business SAC.

Escala: No aplicado = 0 – Aplicado = 1

V1.1 Actualización del software de base de datos y configuración de parámetros				
V1.1.1: Versión del parche del motor de BD				
Ítem	**Controles / Parámetros**	**Acción**	**Escala**	**Observación**
1	PATCH	Asegurar que esté aplicado el último parche generado por el fabricante para mitigar la posibilidad de vulnerabilidad en la base de datos Oracle.	0	No aplicado
V1.1.2: Configurar parámetros de listener				
2	EXTPROC	Asegurar que dicho parámetro no esté presente en el archivo listener.ora para evitar que algunas librerías del sistema operativo puedan ser invocadas por la base de datos.	0	No aplicado
3	ADMIN_RESTRICTIONS	Asegurar que ese parámetro esté presente en el archivo listener.ora para evitar que usuarios no administradores puedan alterar en tiempo real los parámetros del archivo.	0	No aplicado
V1.1.3: Configurar parámetros generales de BD				
4	AUDIT_SYS_OPERATIONS	Asegurar que se configure este parámetro con el valor de TRUE va permitir conocer las actividades realizadas por la cuenta administradora SYS. Las operaciones se registrarán en la tabla SYS.AUD$. Va a requerir reinicio de la base de datos.	1	Aplicado
5	AUDIT_TRAIL	Asegurar que se configure este parámetro con los valores de DB, EXTENDED, OS, XML, EXTENDED, DB, XML; va permitir habilitar las funciones básicas de auditoría, además de recopilar datos para solucionar problemas y valiosos registros forenses.	0	Aplicado
6	GLOBAL_NAMES	Asegurar que se configure este parámetro con el valor de TRUE va permitir conectarse remotamente a otra base de datos a través de un único nombre de enlace entre las bases de datos.	0	No aplicado
7	OS_ROLES	Asegurar que se configure este parámetro con el valor de FALSE para evitar que el sistema operativo use grupos externos para la administración de la base de datos.	1	Aplicado
8	REMOTE_LISTENER	Asegurar que se configure este parámetro con el valor NULL para evitar establecer un oyente válido en un sistema separado, a menos que estén utilizando un RAC.	1	Aplicado

9	REMOTE_LOGIN_PASSWORDFILE	Asegurar que se configure este parámetro con el valor de NONE para evitar conexiones privilegiadas no seguras a la base de datos.	0	No aplicado
10	REMOTE_OS_AUTHENT	Asegurar que se configure este parámetro con el valor de FALSE para evitar suplantación de conexiones y permita otorgar privilegios a un usuario no autorizado del sistema operativo y este pueda realizar conexiones.	1	Aplicado
11	REMOTE_OS_ROLES	Asegurar que se configure este parámetro con el valor de FALSE para evitar que usuarios del sistema operativo tengan permisos para la administración de la base de datos.	1	Aplicado
12	SEC_CASE_SENSITIVE_LOGON	Asegurar que se configure este parámetro con el valor de TRUE para aumentar el conjunto de caracteres que se pueden elegir para las contraseñas, lo que evita a los ataques de contraseña de fuerza bruta.	1	Aplicado
13	SEC_MAX_FAILED_LOGIN_ATTEMPTS	Asegurar que se configure este parámetro con el valor de 3 o menos, determina cuántos inicios de sesión fallidos se permitirán, antes de que la instancia cierre la conexión de inicio de sesión.	1	Aplicado
14	SEC_PROTOCOL_ERROR_FURTHER_ACTION	Asegurar que se configure este parámetro con el valor de (DROP,3) permitirá que se corte una conexión después de tres paquetes defectuosos o con formato incorrecto.	1	Aplicado
15	SEC_PROTOCOL_ERROR_TRACE_ACTION	Asegurar que se configure este parámetro con el valor de LOG, permite el registro de los acontecimientos que pasa en la instancia de base de datos.	0	No aplicado
16	SEC_RETURN_SERVER_RELEASE_BANNER	Asegurar que se configure este parámetro con el valor de FALSE para evitar que la base de datos devuelva información sobre el número de versión del parche aplicado.	1	Aplicado
17	SQL92_SECURITY	Asegurar que se configure este parámetro con el valor de TRUE para evitar la divulgación de información involuntaria asegurándose de que solo los usuarios que ya tienen el privilegio SELECT puedan ejecutar sentencias que les permite obtener los valores almacenados.	1	Aplicado
18	TRACE_FILES_PUBLIC	Asegurar que se configure este parámetro con el valor de FALSE para evitar que el archivo de rastreo del sistema sea legible.	0	No aplicado
19	RESOURCE_LIMIT	Asegurar que se configure este parámetro con el valor de TRUE determina si se aplican límites de recursos en los perfiles de base de datos.	1	Aplicado
V.1.2. Configuración de parámetros de conexión, acceso, usuarios y asignación y/o revocación de privilegios				
V.1.2.1. Configurar parámetros de conexión y acceso				
Ítem	**Control**	**Acción**	**Escala**	**Observación**

20	FAILED_LOGIN_ATTEMPTS	Asegurar que se configure este parámetro con el valor de 5 o menos, determina cuántos intentos fallidos de inicio de sesión se permite antes de que el sistema bloquee la cuenta del usuario.	0	No aplicado
21	PASSWORD_LOCK_TIME	Asegurar que se configure este parámetro con el valor de 1 determina cuántos días deben pasar para que la cuenta se desbloqué después de que se haya producido el número establecido de intentos fallidos en el inicio de sesión.	0	No aplicado
22	PASSWORD_LIFE_TIME	Asegurar que se configure este parámetro con el valor de 90 o menos para determinar cuánto tiempo se puede usar una contraseña antes de que el usuario pueda cambiarla.	0	No aplicado
23	PASSWORD_REUSE_MAX	Asegurar que se configure este parámetro con el valor de 20 o más, para determinar cuántas contraseñas diferentes se deben usar antes de que el usuario pueda reutilizar una contraseña anterior.	0	No aplicado
24	PASSWORD_REUSE_TIME	Asegurar que se configure este parámetro con el valor de 365 o más, para determina la cantidad de tiempo en días que debe pasar antes de que se pueda reutilizar la misma contraseña.	0	No aplicado
25	PASSWORD_GRACE_TIME	Asegurar que se configure este parámetro con el valor de 5 o menos, para determinar cuántos días puede un usuario tener una contraseña vencida, antes que la sesión del usuario se bloque automáticamente.	0	No aplicado
26	PASSWORD_VERIFY_FUNCTIO N	Asegurar que se configure este parámetro en todos los Profiles, para determinar las reglas de complejidad de contraseñas (casos mixtos con dígitos y caracteres especiales), bloquear las combinaciones simples y aplicar cambios a las configuraciones de historial logrando frustrar potencialmente los inicios de sesión no autorizados.	0	No aplicado
27	SESSIONS_PER_USER	Asegurar que se configure este parámetro con el valor de 10 o menos, para determinar el número máximo de sesiones de un usuario ayudando a prevenir el mal uso de recursos a nivel de memoria o ataques de denegación de servicio intencionales.	0	No aplicado
28	INACTIVE_ACCOUNT_TIME	Asegurar que se configure este parámetro con el valor de 120 o menos, para determinar el número máximo de días de inactividad (sin inicios de sesión en absoluto) después de lo cual la cuenta se bloqueará.	0	No aplicado
V.1.2.2. Configurar parámetros de usuarios				
29	Credenciales por defecto (DEFAULT PASSWORDS)	Asegurar que todas las credenciales por defecto sean modificadas, para evitar que cualquier atacante con acceso a la base de datos	1	Aplicado

		puede autenticarse con una cuenta predeterminada utilizando una credencial por efecto.		
30	Esquemas de ejemplo (SAMPLE DATA)	Asegurar que todos los esquemas de muestra (BI o HR o IX o OE o PM o SCOTT o SH) sean removidos del ambiente de producción, para evitar que puedan ser utilizados para lanzar exploits contra el ambiente de producción.	0	No aplicado
31	DBA_USERS.AUTHENTICATION_TYPE	Asegurar que esté campo no contenga el valor de EXTERNAL, para evitar que un usuario remoto del sistema operativo pueda tener acceso a la base de datos con autorización completa.	1	Aplicado
32	Usuarios sin profile por defecto (DEFAULT PROFILE)	Asegurar que los usuarios no tengan asignado el profile por defecto (DEFAULT), debido a que cuenta con configuraciones ilimitadas que a menudo son requeridas por el usuario administrador, tales configuraciones ilimitadas deben reservarse estrictamente y no aplicarse a usuarios innecesarios.	1	No aplicado
33	SYS.USER$MIG	Asegurar que la tabla sys.user$mig sea eliminada al inicio de una migración, para evitar que su información pueda llegar hacer conocida por un atacante.	1	Aplicado
34	Enlaces públicos (PUBLIC DATABASE LINKS)	Asegurar que no exista enlaces públicos de bases de datos para evitar que cualquier usuario pueda logra una conexión a la base de datos para consultar, actualizar, insertar, eliminar datos en una base de datos remota.	0	No aplicado
V.1.2.3. Asignar y/o revocar privilegios				
35	DBMS_LDAP - UTL_INADDR	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de las tablas DBMS_LDAP y UTL_INADDR para evitar la creación de errores especialmente diseñados o él envió de información vía DNS al exterior.	0	No aplicado
36	UTL_TCP	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de la tabla UTL_TCP para evitar que usuarios no autorizados envíen datos arbitrarios desde el servidor de base de datos.	0	No aplicado
37	UTL_MAIL - UTL_SMTP	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de las tablas UTL_MAIL y UTL_SMTP para evitar que un usuario no autorizado corrompa el SMTP, función para aceptar o generar correo no deseado que puede resultar en una denegación de servicio debido a la saturación de la red	0	No aplicado
38	UTL_DBWS	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de la tabla UTL_DBWS para evitar que un usuario no autorizado corrompa	1	Aplicado

		el HTTP flujo utilizado para transportar los protocolos que comunican la instancia basada en la web.		
39	UTL_ORAMTS - UTL_HTTP	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de las tablas UTL_ORAMTS y UTL_HTTP para evitar él envió de información (sensible) a sitios web.	0	No aplicado
40	HTTPURITYPE	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de la tabla HTTPURITYPE para evitar el filtrado de información de la base de datos a un destino externo por HTTP.	0	No aplicado
41	DBMS_ADVISOR	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de la tabla DBMS_ADVISOR para evitar que un usuario no autorizado corrompa archivos del sistema operativo o componentes fundamentales de la base de datos.	0	No aplicado
42	DBMS_LOB	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de la tabla DBMS_LOB para evitar que subprogramas puedan manipular, leer, escribir en BLOB, CLOB, NCLOB, BFILE y LOB temporales	0	No aplicado
43	UTL_FILE	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de la tabla UTL_FILE para evitar que un usuario pueda leer y escribir archivos ubicados en el servidor donde está instalada la instancia de base de datos.	0	No aplicado
44	DBMS_CRYPTO	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de la tabla DBMS_CRYPTO para evitar la ejecución de procedimientos de criptografía que puede potencialmente comprometer una porción o la totalidad de los datos.	1	Aplicado
45	DBMS_OBFUSCATION_TOOLKIT	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de la tabla DBMS_OBFUSCATION_TOOLKIT para evitar que la herramienta que determina la fuerza del algoritmo de cifrado sea utilizada para cifrar los datos de la aplicación.	0	No aplicado
46	DBMS_RANDOM	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de la tabla DBMS_RANDOM para evitar que una aplicación no autorizada genere números aleatorios.	0	No aplicado
47	DBMS_JAVA - DBMS_JAVA_TEST	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de las tablas DBMS_JAVA y DBMS_JAVA_TEST para evitar que un atacante ejecute comandos del sistema operativo desde la base de datos.	0	No aplicado

48	DBMS_JOB	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de la tabla DBMS_JOB para evitar que un usuario no autorizado inhabilite o sobrecargue la cola de trabajos.	0	No aplicado
49	DBMS_SCHEDULER	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de la tabla DBMS_SCHEDULER para evitar que un usuario no autorizado ejecute trabajos de la base de datos o del sistema operativo.	0	No aplicado
50	DBMS_SQL	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de la tabla DBMS_SQL para evitar la escalada de privilegios si no se realiza la validación de entrada adecuadamente.	0	No aplicado
51	DBMS_XMLGEN	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de la tabla DBMS_XMLGEN para evitar la búsqueda de información confidencial en toda la base de datos. Información como números de tarjetas de crédito.	0	No aplicado
52	DBMS_XMLQUERY, DBMS_XMLSAVE, DBMS_XMLSTORE, DBMS_AW, OWA_UTIL y DBMS_REDACT	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de las tablas DBMS_XMLQUERY, DBMS_XMLSAVE, DBMS_XMLSTORE, DBMS_AW, OWA_UTIL y DBMS_REDACT para evitar que usuarios malintencionados pueden aprovechar este paquete como una función de inyección auxiliar en un ataque de inyección SQL.	0	No aplicado
53	DBMS_BACKUP_RESTORE	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de la tabla DBMS_BACKUP_RESTORE para evitar el acceso a los archivos del sistema operativo.	1	Aplicado
54	DBMS_FILE_TRANSFER	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de la tabla DBMS_FILE_TRANSFER para evitar transferir archivos desde un servidor de base de datos a otro sin autorización para hacerlo.	1	Aplicado
55	DBMS_SYS_SQL	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de la tabla DBMS_SYS_SQL para evitar que un usuario ejecute código como un usuario diferente sin ingresar credenciales válidas.	1	Aplicado
56	DBMS_REPCAT_SQL_UTL, INITJVMAUX, DBMS_AQADM_SYS, DBMS_STREAMS_RPC y LTADM	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de las tablas DBMS_REPCAT_SQL_UTL, INITJVMAUX, DBMS_AQADM_SYS, DBMS_STREAMS_RPC y LTADM para evitar que un usuario no autorizado ejecute SQL comandos como un usuario SYS.	1	Aplicado
57	DBMS_PRVTAQIM	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de la tabla DBMS_PRVTAQIM para evitar que un usuario no autorizado escale privilegios por cualquier instrucción SQL y que podría ejecutarse como usuario SYS.	1	Aplicado

58	DBMS_IJOB y DBMS_PDB_EXEC_SQL	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de las tablas DBMS_IJOB y DBMS_PDB_EXEC_SQL para evitar que un atacante cambie de identidad utilizando un nombre de usuario diferente para ejecutar un trabajo de base de datos.	1	Aplicado
59	SYS.AUD$	Asegurar que usuarios no autorizados tengan privilegios sobre la tabla SYS.AUD$ para que no permita distorsión en los registros de auditoría, escondiendo actividades no autorizadas.	1	Aplicado
60	SYS.DBA_%	Asegurar que el privilegio PUBLIC sea revocado de todas las tablas sensibles del usuario SYS que sean encontradas en la vista DBA_% para evitar que usuarios no autorizados puedan manipular los datos confidenciales.	0	No aplicado
61	CDB_LOCAL_ADMINAUTH$, DEFAULT_PWD$, ENC$, HISTGRM$, HIST_HEAD$, LINK$, PDB_SYNC$, SCHEDULER$_CREDENTIAL, USER$, USER_HISTORY$ y XS$VERIFIERS	Asegurar que el privilegio ALL sea revocado de las tablas CDB_LOCAL_ADMINAUTH$, DEFAULT_PWD$, ENC$, HISTGRM$, HIST_HEAD$, LINK$, PDB_SYNC$, SCHEDULER$_CREDENTIAL, USER$, USER_HISTORY$ y XS$VERIFIERS del usuario SYS para evitar que usuarios no autorizados puedan manipular los datos sensibles y confidenciales.	1	Aplicado
62	%ANY%	Asegurar que los privilegios tipo %ANY% sean revocados de todos los objetos no autorizados de la base de dato para evitar que usuarios no autorizados puedan manipular los datos confidenciales o dañen el catálogo de datos.	0	No aplicado
63	ADMIN_OPTION	Asegurar que de la tabla DBA_SYS_PRIVS.% se revoke los privilegios no autorizados donde el campo ADMIN_OPTION sea igual a YES para evitar que los usuarios puedan otorgar sus mismos privilegios a otros usuarios.	1	Aplicado
64	EXECUTE ANY PROCEDURE	Asegurar que el privilegio EXECUTE ANY PROCEDURE sea revocado de los esquemas OUTLN y DBSNMP para evitar que tenga más privilegios de los necesarios.	1	Aplicado
65	SELECT ANY DICTIONARY	Asegurar que este privilegio sea revocado de cuentas no administrativas para evitar que un usuario no autorizado pueda recopilar información sobre la base de datos a través del diccionario de datos objetos. La información recopilada podría utilizarse potencialmente para explotar la base de datos.	0	No aplicado

66	SELECT ANY TABLE	Asegurar que este privilegio sea revocado de cuentas no administrativas para evitar que un usuario no autorizado pueda visualizar sin autorización información sensible.	1	Aplicado
67	AUDIT SYSTEM	Asegurar que este privilegio sea revocado de cuentas no administrativas para evita que un usuario no autorizado pueda alterar las actividades de auditoria programadas, como deshabilitar la creación de pistas de auditoría.	1	Aplicado
68	EXEMPT ACCESS POLICY	Asegurar que este privilegio sea revocado de cuentas no administrativas para evitar que un usuario no autorizado pueda acceder a todas las filas de una tabla independientemente de los bloqueos de seguridad a nivel de fila.	1	Aplicado
69	BECOME USER	Asegurar que este privilegio sea revocado de cuentas no administrativas para evitar que un usuario no autorizado pueda usar privilegios otorgados a otro usuario,	1	Aplicado
70	CREATE PROCEDURE	Asegurar que este privilegio sea revocado de cuentas no administrativas para evitar que un usuario no autorizado pueda crear procedimientos no autorizados que facilitan el robo de datos o la denegación de servicio al corromper las tablas de datos.	1	Aplicado
71	ALTER SYSTEM	Asegurar que este privilegio sea revocado de cuentas no administrativas para evitar que un usuario no autorizado pueda modificar las operaciones en ejecución de la instancia.	1	Aplicado
72	CREATE ANY LIBRARY y CREATE LIBRARY	Asegurar que estos privilegios sean revocados de cuentas no administrativas para evitar que un usuario no autorizado pueda crear objetos que están asociados a las bibliotecas compartidas.	1	Aplicado
73	GRANT ANY OBJECT PRIVILEGE, GRANT ANY ROLE y GRANT ANY PRIVILEGE	Asegurar que estos privilegios sean revocados de cuentas no administrativas para evitar que un usuario no autorizado pueda acceder o cambiar datos confidenciales, o dañar el catálogo de datos debido a un potencial daño al acceso de instancia.	1	Aplicado
74	SELECT_CATALOG_ROLE	Asegurar que este rol sea revocado de cuentas no administrativas para evitar que un usuario no autorizado pueda divulgar todos los datos del diccionario.	1	Aplicado
75	EXECUTE_CATALOG_ROLE	Asegurar que este rol sea revocado de cuentas no administrativas para evitar que un usuario no autorizado pueda interrumpir las operaciones mediante la inicialización de procedimientos no autorizados.	1	Aplicado

76	DBA	Asegurar que este rol sea revocado de cuentas no administrativas para evitar que un usuario no autorizado pueda generar una gran cantidad de problemas innecesarios. Este privilegio abre la puerta a violaciones de datos, violaciones de integridad y condiciones de denegación de servicio.	1	Aplicado
V.1.3 Configuración de parámetros de auditorías				
V.1.3.1 Configurar parámetros de auditoria tradicional				
77	AUDIT_OPTION = USER	Asegurar que la tabla DBA_STMT_AUDIT_OPTS contenga un registro donde el campo AUDIT_OPTION sea igual a USER va a permitir auditar todas las actividades que realicen en la base de datos.	0	No aplicado
78	AUDIT_OPTION = ROLE	Asegurar que la tabla DBA_STMT_AUDIT_OPTS contenga un registro donde el campo AUDIT_OPTION sea igual a ROLE va a permitir auditar todos los intentos, exitosos o no, de crear, descartar, modificar o establecer roles.	0	No aplicado
79	AUDIT_OPTION = SYSTEM GRANT	Asegurar que la tabla DBA_STMT_AUDIT_OPTS contenga un registro donde el campo AUDIT_OPTION sea igual a SYSTEM GRANT va a permitir auditar cualquier intento, exitoso o no, para otorgar o revocar cualquier privilegio o función del sistema, independientemente del privilegio en poder del usuario que intenta la operación.	0	No aplicado
80	AUDIT_OPTION = PROFILE	Asegurar que la tabla DBA_STMT_AUDIT_OPTS contenga un registro donde el campo AUDIT_OPTION sea igual a PROFILE va a permitir auditar todos los intentos, exitosos o no, de crear, descartar o alterar cualquier perfil.	0	No aplicado
81	AUDIT_OPTION = DATABASE LINK	Asegurar que la tabla DBA_STMT_AUDIT_OPTS contenga un registro donde el campo AUDIT_OPTION sea igual a DATABASE LINK va a permitir auditar todas las actividades en los enlaces de la base de datos.	0	No aplicado
82	AUDIT_OPTION = PUBLIC DATABASE LINK	Asegurar que la tabla DBA_STMT_AUDIT_OPTS contenga un registro donde el campo AUDIT_OPTION sea igual a PUBLIC DATABASE LINK va a permitir auditar todas las actividades del usuario que impliquen la creación, alteración o eliminación de los enlaces públicos.	0	No aplicado
83	AUDIT_OPTION = PUBLIC SYNONYM	Asegurar que la tabla DBA_STMT_AUDIT_OPTS contenga un registro donde el campo AUDIT_OPTION sea igual a PUBLIC SYNONYM va a permitir auditar todas las actividades del usuario que	0	No aplicado

		impliquen la creación, alteración o eliminación de los sinónimos públicos.		
84	AUDIT_OPTION = SYNONYM	Asegurar que la tabla DBA_STMT_AUDIT_OPTS contenga un registro donde el campo AUDIT_OPTION sea igual a SYNONYM va a permitir auditar todas las actividades del usuario que impliquen la creación, alteración o eliminación de los sinónimos públicos.	0	No aplicado
85	AUDIT_OPTION = DIRECTORY	Asegurar que la tabla DBA_STMT_AUDIT_OPTS contenga un registro donde el campo AUDIT_OPTION sea igual a DIRECTORY va a permitir auditar todas las actividades del usuario que impliquen la creación, alteración o eliminación de un directorio.	0	No aplicado
86	AUDIT_OPTION = SELECT ANY DICTIONARY	Asegurar que la tabla DBA_STMT_AUDIT_OPTS contenga un registro donde el campo AUDIT_OPTION sea igual a SELECT ANY DICTIONARY va a permitir auditar todas las actividades del usuario relacionadas con esta capacidad.	0	No aplicado
87	AUDIT_OPTION = GRANT ANY OBJECT PRIVILEGE	Asegurar que la tabla DBA_STMT_AUDIT_OPTS contenga un registro donde el campo AUDIT_OPTION sea igual a GRANT ANY OBJECT PRIVILEGE va a permitir para auditar todas las actividades del usuario relacionadas con otorgar o revocar cualquier privilegio de objeto, que incluye privilegios sobre tablas, directorios, modelos de minería.	0	No aplicado
88	AUDIT_OPTION = GRANT ANY PRIVILEGE	Asegurar que la tabla DBA_STMT_AUDIT_OPTS contenga un registro donde el campo AUDIT_OPTION sea igual a GRANT ANY PRIVILEGE va a permitir auditar todas las actividades del usuario administrador relacionadas con cambiar la seguridad infraestructura, para eliminar, agregar, modificar usuarios y más.	0	No aplicado
89	AUDIT_OPTION = DROP ANY PROCEDURE	Asegurar que la tabla DBA_STMT_AUDIT_OPTS contenga un registro donde el campo AUDIT_OPTION sea igual a DROP ANY PROCEDURE va a permitir auditar todas las actividades del usuario que impliquen la eliminación de procedimientos.	0	No aplicado
90	SYS.AUD$	Asegurar que el privilegio ALL este habilitado en la tabla SYS.AUD$ va proporcionar pruebas forenses desde el inicio de actividades no autorizadas.	0	No aplicado
91	AUDIT_OPTION = PROCEDURE	Asegurar que la tabla DBA_STMT_AUDIT_OPTS contenga un registro donde el campo AUDIT_OPTION sea igual a PROCEDURE va a permitir auditar todas las actividades del usuario que impliquen la creación, alteración o eliminación de un procedimiento.	0	No aplicado

92	AUDIT_OPTION = ALTER SYSTEM	Asegurar que la tabla DBA_STMT_AUDIT_OPTS contenga un registro donde el campo AUDIT_OPTION sea igual a ALTER SYSTEM va permitir auditar cualquier intento no autorizado de alterar el sistema, estos registros pueden ser muy útiles.	0	No aplicado
93	AUDIT_OPTION = TRIGGER	Asegurar que la tabla DBA_STMT_AUDIT_OPTS contenga un registro donde el campo AUDIT_OPTION sea igual a TRIGGER va a permitir auditar todas las actividades del usuario que impliquen la creación, alteración o eliminación de un trigger.	0	No aplicado
94	AUDIT_OPTION = CREATE SESSION	Asegurar que la tabla DBA_STMT_AUDIT_OPTS contenga un registro donde el campo AUDIT_OPTION sea igual a CREATE SESSION va a permitir auditar todos los intentos de conexión a la base de datos, ya sea con éxito o no, así como las desconexiones/cierres de sesión de auditoría.	0	No aplicado
V.1.3.2 Configurar parámetros de auditoría unificada				
95	CREATE USER	Asegurar habilitar la auditoría de la instrucción CREATE USER va permitir el registro de todas las creaciones de cuentas ya sean exitosas o no, emitidas por los usuarios independientemente de los privilegios que tienen los usuarios.	1	Aplicado
96	ALTER USER	Asegurar habilitar la auditoría de la instrucción ALTER USER va permitir el registro de todos los cambios de contraseña, bloqueo de cuentas. También va registrar los cambios de propiedades de los usuarios, Profiles, tablespaces por defecto o temporales y las cuotas de espacio en los tablespaces ya sean exitosas o no, emitidas por los usuarios independientemente de los privilegios que tienen los usuarios.	0	No aplicado
97	DROP USER	Asegurar habilitar la auditoría de la instrucción DROP USER va permitir el registro de todas las eliminaciones de cuentas o esquemas de la base de datos ya sean exitosas o no, emitidas por los usuarios independientemente de los privilegios que tienen los usuarios.	1	Aplicado
98	CREATE ROLE	Asegurar habilitar la auditoría de la instrucción CREATE ROLE va permitir el registro de todas las creaciones de colecciones de privilegios de sistema, privilegios de objetos que se otorgan a los usuarios o a otros roles ya sean exitosas o no, emitidas por los usuarios independientemente de los privilegios que tienen los usuarios.	0	No aplicado

99	ALTER ROLE	Asegurar habilitar la auditoría de la instrucción ALTER ROLE va permitir el registro de todos los movimientos que se realizan en la colección de privilegios de sistema, privilegios de objetos que se otorgan a los usuarios o a otros roles ya sean exitosas o no, emitidas por los usuarios independientemente de los privilegios que tienen los usuarios.	0	No aplicado
100	DROP ROLE	Asegurar habilitar la auditoría de la instrucción DROP ROLE va permitir el registro de todas las eliminaciones de colecciones de privilegios de sistema, privilegios de objetos que se otorgan a los usuarios o a otros roles ya sean exitosas o no, emitidas por los usuarios independientemente de los privilegios que tienen los usuarios.	0	No aplicado
101	GRANT	Asegurar habilitar la auditoría de la instrucción GRANT va permitir el registro de todas las otorgaciones de privilegios a los usuarios o a otros roles ya sean exitosas o no, emitidas por los usuarios independientemente de los privilegios que tienen los usuarios	1	Aplicado
102	REVOKE	Asegurar habilitar la auditoría de la instrucción REVOKE va permitir el registro de todas las revocatorias de privilegios a los usuarios o a otros roles ya sean exitosas o no, emitidas por los usuarios independientemente de los privilegios que tienen los usuarios	1	Aplicado
103	CREATE PROFILE	Asegurar habilitar la auditoría de la instrucción CREATE PROFILE va permitir el registro de todas las creaciones de políticas de contraseñas, como reglas de complejidad de contraseñas, restricciones de reutilización y límites de uso de recursos ya sean exitosas o no, emitidas por los usuarios independientemente de los privilegios que tienen los usuarios.	0	No aplicado
104	ALTER PROFILE	Asegurar habilitar la auditoría de la instrucción ALTER PROFILE va permitir el registro de todas las modificaciones de políticas de contraseñas, como reglas de complejidad de contraseñas, restricciones de reutilización y límites de uso de recursos ya sean exitosas o no, emitidas por los usuarios independientemente de los privilegios que tienen los usuarios.	0	No aplicado
105	DROP PROFILE	Asegurar habilitar la auditoría de la instrucción DROP PROFILE va permitir el registro de todas las modificaciones de políticas de contraseñas, como reglas de complejidad de contraseñas, restricciones de reutilización y límites de uso de recursos ya sean	0	No aplicado

		exitosas o no, emitidas por los usuarios independientemente de los privilegios que tienen los usuarios		
106	CREATE DATABASE LINK	Asegurar habilitar la auditoría de la instrucción CREATE DATABASE LINK va permitir el registro de todas las creaciones de los enlaces para establecer conexiones de base de datos a base de datos, estas conexiones están disponibles sin autenticación ya sean exitosas o no, emitidas por los usuarios independientemente de los privilegios que tienen los usuarios.	0	No aplicado
107	ALTER DATABASE LINK	Asegurar habilitar la auditoría de la instrucción ALTER DATABASE LINK va permitir el registro de todas las modificaciones de los enlaces para establecer conexiones de base de datos a base de datos, estas conexiones están disponibles sin autenticación ya sean exitosas o no, emitidas por los usuarios independientemente de los privilegios que tienen los usuarios	0	No aplicado
108	DROP DATABASE LINK	Asegurar habilitar la auditoría de la instrucción ALTER DATABASE LINK va permitir el registro de todas las eliminaciones de los enlaces para establecer conexiones de base de datos a base de datos, estas conexiones están disponibles sin autenticación ya sean exitosas o no, emitidas por los usuarios independientemente de los privilegios que tienen los usuarios	0	No aplicado
109	CREATE SYNONYM	Asegurar habilitar la auditoría de la instrucción CREATE SYNONYM va permitir el registro de todas las creaciones de un nombre alternativo para un objeto de base de datos como tabla, vista, procedimiento, objeto java o incluso otro sinónimo ya sean exitosas o no, emitidas por los usuarios independientemente de los privilegios que tienen los usuarios.	1	Aplicado
110	ALTER SYNONYM	Asegurar habilitar la auditoría de la instrucción ALTER SYNONYM va permitir el registro de todas las modificaciones de un nombre alternativo para un objeto de base de datos como tabla, vista, procedimiento, objeto java o incluso otro sinónimo ya sean exitosas o no, emitidas por los usuarios independientemente de los privilegios que tienen los usuarios	1	Aplicado
111	DROP SYNONYM	Asegurar habilitar la auditoría de la instrucción DROP SYNONYM va permitir el registro de todas las eliminaciones de un nombre alternativo para un objeto de base de datos como tabla, vista, procedimiento, objeto java o incluso otro sinónimo ya sean exitosas o no, emitidas por	1	Aplicado

		los usuarios independientemente de los privilegios que tienen los usuarios		
112	SELECT ANY DICTIONARY	Asegurar habilitar la auditoría de la instrucción SELECT ANY DICTIONARY va permitir el registro de todas las acciones que realizan los usuarios cuando vean la definición de los objetos de esquemas, de los objetos del diccionario de datos, incluido en vistas DBA_, vistas V$, vistas X$ y tablas SYS subyacentes como TAB$ y OBJ	1	Aplicado
113	AUDSYS.AUD$UNIFIED	Asegurar habilitar la auditoría de la instrucción AUDSYS.AUD$UNIFIED va permitir el registro de todos los intentos de acceso a AUDSYS.AUD$UNIFIED, ya sea con éxito o sin éxito, independientemente de los privilegios que tengan los usuarios para emitir dichas declaraciones	1	Aplicado
114	CREATE PROCEDURE /FUNCTION / PACKAGE / PACKAGE BODY	Asegurar habilitar la auditoría de las instrucciones CREATE PROCEDURE / FUNCTION / PACKAGE / PACKAGE BODY va permitir el registro de todas las creaciones de estas instrucciones comerciales que se encuentran definido por código PL/SQL y sentencias SQL contenidas dentro de estos objetos, ya sean instrucciones satisfactorias o no satisfactorias emitidos por los usuarios independientemente de los privilegios que tengan los usuarios para emitir tales declaraciones	1	Aplicado
115	ALTER PROCEDURE / FUNCTION / PACKAGE / PACKAGE BODY	Asegurar habilitar la auditoría de las instrucciones ALTER PROCEDURE / FUNCTION / PACKAGE / PACKAGE BODY va permitir el registro de todas las modificaciones de estas instrucciones comerciales que se encuentran definido por código PL/SQL y sentencias SQL contenidas dentro de estos objetos, ya sean instrucciones satisfactorias o no satisfactorias emitidos por los usuarios independientemente de los privilegios que tengan los usuarios para emitir tales declaraciones	1	Aplicado
116	DROP PROCEDURE / FUNCTION / PACKAGE / PACKAGE BODY	Asegurar habilitar la auditoría de las instrucciones DROP PROCEDURE / FUNCTION / PACKAGE / PACKAGE BODY va permitir el registro de todas las eliminaciones de estas instrucciones comerciales que se encuentran definido por código PL/SQL y sentencias SQL contenidas dentro de estos objetos, ya sean instrucciones satisfactorias o no satisfactorias emitidos por los usuarios independientemente de los privilegios que tengan los usuarios para emitir tales declaraciones	1	Aplicado

117	ALTER SYSTEM	Asegurar habilitar la auditoría de la instrucción ALTER SYSTEM va permitir el registro de todas las modificaciones al cambiar la configuración de la instancia que podría afectar la postura de seguridad, rendimiento o funcionamiento normal de la base de datos. Además, se registrarán la ejecución de los comandos de sistema operativo, ya sean exitosas o no, realizadas por los usuarios independientemente de sus privilegios.	0	No aplicado
118	CREATE TRIGGER	Asegurar habilitar la auditoría de la instrucción CREATE TRIGGER va permitir el registro de todas las creaciones de los disparadores que contienen código para realizar validaciones o hacer cumplir restricciones críticas sobre los datos ya sean exitosas o no, ejecutadas por los usuarios independientemente de los privilegios que tienen los usuarios.	1	Aplicado
119	ALTER TRIGGER	Asegurar habilitar la auditoría de la instrucción ALTER TRIGGER va permitir el registro de todas las modificaciones de los disparadores que contienen código para realizar validaciones o hacer cumplir restricciones críticas sobre los datos ya sean exitosas o no, ejecutadas por los usuarios independientemente de los privilegios que tienen los usuarios	1	Aplicado
120	DROP TRIGGER	Asegurar habilitar la auditoría de la instrucción DROP TRIGGER va permitir el registro de todas las eliminaciones de los disparadores que contienen código para realizar validaciones o hacer cumplir restricciones críticas sobre los datos ya sean exitosas o no, ejecutadas por los usuarios independientemente de los privilegios que tienen los usuarios	1	Aplicado
121	LOGON / LOGOFF	Asegurar habilitar la auditoría de la instrucción LOGON / LOGOFF va permitir el registro de todas los inicios o cierres de sesión que realicen los usuarios independientemente de sus privilegios	1	Aplicado

Anexo 11: Lista de Cotejo Pre Test de los controles de configuración de seguridad en la base de datos Oracle 19c en la instancia de base de datos "bdgpaqa" del ambiente de control de calidad de la empresa GPA Business SAC.

Escala: No aplicado = 0 – Aplicado = 1

V1.1 Actualización del software de base de datos y configuración de parámetros				
V1.1.1: Versión del parche del motor de BD				
Ítem	**Controles / Parámetros**	**Acción**	**Escala**	**Observación**
1	PATCH	Asegurar que esté aplicado el último parche generado por el fabricante para mitigar la posibilidad de vulnerabilidad en la base de datos Oracle.	0	No aplicado
V1.1.2: Configurar parámetros de listener				
2	EXTPROC	Asegurar que dicho parámetro no esté presente en el archivo listener.ora para evitar que algunas librerías del sistema operativo puedan ser invocadas por la base de datos.	0	No aplicado
3	ADMIN_RESTRICTIONS	Asegurar que ese parámetro esté presente en el archivo listener.ora para evitar que usuarios no administradores puedan alterar en tiempo real los parámetros del archivo.	0	No aplicado
V1.1.3: Configurar parámetros generales de BD				
4	AUDIT_SYS_OPERATIONS	Asegurar que se configure este parámetro con el valor de TRUE va permitir conocer las actividades realizadas por la cuenta administradora SYS. Las operaciones se registrarán en la tabla SYS.AUD$. Va a requerir reinicio de la base de datos.	1	Aplicado
5	AUDIT_TRAIL	Asegurar que se configure este parámetro con los valores de DB, EXTENDED, OS, XML, EXTENDED, DB, XML; va permitir habilitar las funciones básicas de auditoría, además de recopilar datos para solucionar problemas y valiosos registros forenses.	0	Aplicado
6	GLOBAL_NAMES	Asegurar que se configure este parámetro con el valor de TRUE va permitir conectarse remotamente a otra base de datos a través de un único nombre de enlace entre las bases de datos.	0	No aplicado
7	OS_ROLES	Asegurar que se configure este parámetro con el valor de FALSE para evitar que el sistema operativo use grupos externos para la administración de la base de datos.	1	Aplicado

8	REMOTE_LISTENER	Asegurar que se configure este parámetro con el valor NULL para evitar establecer un oyente válido en un sistema separado, a menos que estén utilizando un RAC.	1	Aplicado
9	REMOTE_LOGIN_PASSWORDFILE	Asegurar que se configure este parámetro con el valor de NONE para evitar conexiones privilegiadas no seguras a la base de datos.	0	No aplicado
10	REMOTE_OS_AUTHENT	Asegurar que se configure este parámetro con el valor de FALSE para evitar suplantación de conexiones y permita otorgar privilegios a un usuario no autorizado del sistema operativo y este pueda realizar conexiones.	1	Aplicado
11	REMOTE_OS_ROLES	Asegurar que se configure este parámetro con el valor de FALSE para evitar que usuarios del sistema operativo tengan permisos para la administración de la base de datos.	1	Aplicado
12	SEC_CASE_SENSITIVE_LOGON	Asegurar que se configure este parámetro con el valor de TRUE para aumentar el conjunto de caracteres que se pueden elegir para las contraseñas, lo que evita a los ataques de contraseña de fuerza bruta.	1	Aplicado
13	SEC_MAX_FAILED_LOGIN_ATTEMPTS	Asegurar que se configure este parámetro con el valor de 3 o menos, determina cuántos inicios de sesión fallidos se permitirán, antes de que la instancia cierre la conexión de inicio de sesión.	1	Aplicado
14	SEC_PROTOCOL_ERROR_FURTHER_ACTION	Asegurar que se configure este parámetro con el valor de (DROP,3) permitirá que se corte una conexión después de tres paquetes defectuosos o con formato incorrecto.	1	Aplicado
15	SEC_PROTOCOL_ERROR_TRACE_ACTION	Asegurar que se configure este parámetro con el valor de LOG, permite el registro de los acontecimientos que pasa en la instancia de base de datos.	0	No aplicado
16	SEC_RETURN_SERVER_RELEASE_BANNER	Asegurar que se configure este parámetro con el valor de FALSE para evitar que la base de datos devuelva información sobre el número de versión del parche aplicado.	1	Aplicado
17	SQL92_SECURITY	Asegurar que se configure este parámetro con el valor de TRUE para evitar la divulgación de información involuntaria asegurándose de que solo los usuarios que ya tienen el privilegio SELECT puedan ejecutar sentencias que les permite obtener los valores almacenados.	1	Aplicado
18	TRACE_FILES_PUBLIC	Asegurar que se configure este parámetro con el valor de FALSE para evitar que el archivo de rastreo del sistema sea legible.	0	No aplicado
19	RESOURCE_LIMIT	Asegurar que se configure este parámetro con el valor de TRUE determina si se aplican límites de recursos en los perfiles de base de datos.	1	Aplicado

V.1.2. Configuración de parámetros de conexión, acceso, usuarios y asignación y/o revocación de privilegios				
V.1.2.1. Configurar parámetros de conexión y acceso				
Ítem	**Control**	**Acción**	**Escala**	**Observación**
20	FAILED_LOGIN_ATTEMPTS	Asegurar que se configure este parámetro con el valor de 5 o menos, determina cuántos intentos fallidos de inicio de sesión se permite antes de que el sistema bloquee la cuenta del usuario.	0	No aplicado
21	PASSWORD_LOCK_TIME	Asegurar que se configure este parámetro con el valor de 1 determina cuántos días deben pasar para que la cuenta se desbloqué después de que se haya producido el número establecido de intentos fallidos en el inicio de sesión.	0	No aplicado
22	PASSWORD_LIFE_TIME	Asegurar que se configure este parámetro con el valor de 90 o menos para determinar cuánto tiempo se puede usar una contraseña antes de que el usuario pueda cambiarla.	0	No aplicado
23	PASSWORD_REUSE_MAX	Asegurar que se configure este parámetro con el valor de 20 o más, para determinar cuántas contraseñas diferentes se deben usar antes de que el usuario pueda reutilizar una contraseña anterior.	0	No aplicado
24	PASSWORD_REUSE_TIME	Asegurar que se configure este parámetro con el valor de 365 o más, para determina la cantidad de tiempo en días que debe pasar antes de que se pueda reutilizar la misma contraseña.	0	No aplicado
25	PASSWORD_GRACE_TIME	Asegurar que se configure este parámetro con el valor de 5 o menos, para determinar cuántos días puede un usuario tener una contraseña vencida, antes que la sesión del usuario se bloque automáticamente.	0	No aplicado
26	PASSWORD_VERIFY_FUNCTION	Asegurar que se configure este parámetro en todos los Profiles, para determinar las reglas de complejidad de contraseñas (casos mixtos con dígitos y caracteres especiales), bloquear las combinaciones simples y aplicar cambios a las configuraciones de historial logrando frustrar potencialmente los inicios de sesión no autorizados.	0	No aplicado
27	SESSIONS_PER_USER	Asegurar que se configure este parámetro con el valor de 10 o menos, para determinar el número máximo de sesiones de un usuario ayudando a prevenir el mal uso de recursos a nivel de memoria o ataques de denegación de servicio intencionales.	0	No aplicado
28	INACTIVE_ACCOUNT_TIME	Asegurar que se configure este parámetro con el valor de 120 o menos, para determinar el número máximo de días de inactividad (sin inicios de sesión en absoluto) después de lo cual la cuenta se bloqueará.	0	No aplicado
V.1.2.2. Configurar parámetros de usuarios				

29	Credenciales por defecto (DEFAULT PASSWORDS)	Asegurar que todas las credenciales por defecto sean modificadas, para evitar que cualquier atacante con acceso a la base de datos puede autenticarse con una cuenta predeterminada utilizando una credencial por efecto.	1	Aplicado
30	Esquemas de ejemplo (SAMPLE DATA)	Asegurar que todos los esquemas de muestra (BI o HR o IX o OE o PM o SCOTT o SH) sean removidos del ambiente de producción, para evitar que puedan ser utilizados para lanzar exploits contra el ambiente de producción.	0	No aplicado
31	DBA_USERS.AUTHENTICATION_TYPE	Asegurar que esté campo no contenga el valor de EXTERNAL, para evitar que un usuario remoto del sistema operativo pueda tener acceso a la base de datos con autorización completa.	1	Aplicado
32	Usuarios sin profile por defecto (DEFAULT PROFILE)	Asegurar que los usuarios no tengan asignado el profile por defecto (DEFAULT), debido a que cuenta con configuraciones ilimitadas que a menudo son requeridas por el usuario administrador, tales configuraciones ilimitadas deben reservarse estrictamente y no aplicarse a usuarios innecesarios.	1	No aplicado
33	SYS.USER$MIG	Asegurar que la tabla sys.user$mig sea eliminada al inicio de una migración, para evitar que su información pueda llegar hacer conocida por un atacante.	1	Aplicado
34	Enlaces públicos (PUBLIC DATABASE LINKS)	Asegurar que no exista enlaces públicos de bases de datos para evitar que cualquier usuario pueda logra una conexión a la base de datos para consultar, actualizar, insertar, eliminar datos en una base de datos remota.	0	No aplicado
V.1.2.3. Asignar y/o revocar privilegios				
35	DBMS_LDAP - UTL_INADDR	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de las tablas DBMS_LDAP y UTL_INADDR para evitar la creación de errores especialmente diseñados o él envió de información vía DNS al exterior.	0	No aplicado
36	UTL_TCP	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de la tabla UTL_TCP para evitar que usuarios no autorizados envíen datos arbitrarios desde el servidor de base de datos.	0	No aplicado
37	UTL_MAIL - UTL_SMTP	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de las tablas UTL_MAIL y UTL_SMTP para evitar que un usuario no autorizado corrompa el SMTP, función para aceptar o generar correo no deseado que puede resultar en una denegación de servicio debido a la saturación de la red	0	No aplicado

38	UTL_DBWS	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de la tabla UTL_DBWS para evitar que un usuario no autorizado corrompa el HTTP flujo utilizado para transportar los protocolos que comunican la instancia basada en la web.	1	Aplicado
39	UTL_ORAMTS - UTL_HTTP	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de las tablas UTL_ORAMTS y UTL_HTTP para evitar él envió de información (sensible) a sitios web.	0	No aplicado
40	HTTPURITYPE	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de la tabla HTTPURITYPE para evitar el filtrado de información de la base de datos a un destino externo por HTTP.	0	No aplicado
41	DBMS_ADVISOR	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de la tabla DBMS_ADVISOR para evitar que un usuario no autorizado corrompa archivos del sistema operativo o componentes fundamentales de la base de datos.	0	No aplicado
42	DBMS_LOB	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de la tabla DBMS_LOB para evitar que subprogramas puedan manipular, leer, escribir en BLOB, CLOB, NCLOB, BFILE y LOB temporales	0	No aplicado
43	UTL_FILE	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de la tabla UTL_FILE para evitar que un usuario pueda leer y escribir archivos ubicados en el servidor donde está instalada la instancia de base de datos.	0	No aplicado
44	DBMS_CRYPTO	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de la tabla DBMS_CRYPTO para evitar la ejecución de procedimientos de criptografía que puede potencialmente comprometer una porción o la totalidad de los datos.	1	Aplicado
45	DBMS_OBFUSCATION_TOOLKIT	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de la tabla DBMS_OBFUSCATION_TOOLKIT para evitar que la herramienta que determina la fuerza del algoritmo de cifrado sea utilizada para cifrar los datos de la aplicación.	0	No aplicado
46	DBMS_RANDOM	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de la tabla DBMS_RANDOM para evitar que una aplicación no autorizada genere números aleatorios.	0	No aplicado
47	DBMS_JAVA - DBMS_JAVA_TEST	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de las tablas DBMS_JAVA y DBMS_JAVA_TEST para evitar que un atacante ejecute comandos del sistema operativo desde la base de datos.	0	No aplicado

48	DBMS_JOB	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de la tabla DBMS_JOB para evitar que un usuario no autorizado inhabilite o sobrecargue la cola de trabajos.	0	No aplicado
49	DBMS_SCHEDULER	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de la tabla DBMS_SCHEDULER para evitar que un usuario no autorizado ejecute trabajos de la base de datos o del sistema operativo.	0	No aplicado
50	DBMS_SQL	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de la tabla DBMS_SQL para evitar la escalada de privilegios si no se realiza la validación de entrada adecuadamente.	0	No aplicado
51	DBMS_XMLGEN	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de la tabla DBMS_XMLGEN para evitar la búsqueda de información confidencial en toda la base de datos. Información como números de tarjetas de crédito.	0	No aplicado
52	DBMS_XMLQUERY, DBMS_XMLSAVE, DBMS_XMLSTORE, DBMS_AW, OWA_UTIL y DBMS_REDACT	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de las tablas DBMS_XMLQUERY, DBMS_XMLSAVE, DBMS_XMLSTORE, DBMS_AW, OWA_UTIL y DBMS_REDACT para evitar que usuarios malintencionados pueden aprovechar este paquete como una función de inyección auxiliar en un ataque de inyección SQL.	0	No aplicado
53	DBMS_BACKUP_RESTORE	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de la tabla DBMS_BACKUP_RESTORE para evitar el acceso a los archivos del sistema operativo.	1	Aplicado
54	DBMS_FILE_TRANSFER	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de la tabla DBMS_FILE_TRANSFER para evitar transferir archivos desde un servidor de base de datos a otro sin autorización para hacerlo.	1	Aplicado
55	DBMS_SYS_SQL	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de la tabla DBMS_SYS_SQL para evitar que un usuario ejecute código como un usuario diferente sin ingresar credenciales válidas.	1	Aplicado
56	DBMS_REPCAT_SQL_UTL, INITJVMAUX, DBMS_AQADM_SYS, DBMS_STREAMS_RPC y LTADM	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de las tablas DBMS_REPCAT_SQL_UTL, INITJVMAUX, DBMS_AQADM_SYS, DBMS_STREAMS_RPC y LTADM para evitar que un usuario no autorizado ejecute SQL comandos como un usuario SYS.	1	Aplicado
57	DBMS_PRVTAQIM	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de la tabla DBMS_PRVTAQIM para evitar que un usuario no autorizado escale privilegios por cualquier instrucción SQL y que podría ejecutarse como usuario SYS.	1	Aplicado

58	DBMS_IJOB y DBMS_PDB_EXEC_SQL	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de las tablas DBMS_IJOB y DBMS_PDB_EXEC_SQL para evitar que un atacante cambie de identidad utilizando un nombre de usuario diferente para ejecutar un trabajo de base de datos.	1	Aplicado
59	SYS.AUD$	Asegurar que usuarios no autorizados tengan privilegios sobre la tabla SYS.AUD$ para que no permita distorsión en los registros de auditoría, escondiendo actividades no autorizadas.	1	Aplicado
60	SYS.DBA_%	Asegurar que el privilegio PUBLIC sea revocado de todas las tablas sensibles del usuario SYS que sean encontradas en la vista DBA_% para evitar que usuarios no autorizados puedan manipular los datos confidenciales.	0	No aplicado
61	CDB_LOCAL_ADMINAUTH$, DEFAULT_PWD$, ENC$, HISTGRM$, HIST_HEAD$, LINK$, PDB_SYNC$, SCHEDULER$_CREDENTIAL, USER$, USER_HISTORY$ y XS$VERIFIERS	Asegurar que el privilegio ALL sea revocado de las tablas CDB_LOCAL_ADMINAUTH$, DEFAULT_PWD$, ENC$, HISTGRM$, HIST_HEAD$, LINK$, PDB_SYNC$, SCHEDULER$_CREDENTIAL, USER$, USER_HISTORY$ y XS$VERIFIERS del usuario SYS para evitar que usuarios no autorizados puedan manipular los datos sensibles y confidenciales.	1	Aplicado
62	%ANY%	Asegurar que los privilegios tipo %ANY% sean revocados de todos los objetos no autorizados de la base de dato para evitar que usuarios no autorizados puedan manipular los datos confidenciales o dañen el catálogo de datos.	0	No aplicado
63	ADMIN_OPTION	Asegurar que de la tabla DBA_SYS_PRIVS.% se revoke los privilegios no autorizados donde el campo ADMIN_OPTION sea igual a YES para evitar que los usuarios puedan otorgar sus mismos privilegios a otros usuarios.	1	Aplicado
64	EXECUTE ANY PROCEDURE	Asegurar que el privilegio EXECUTE ANY PROCEDURE sea revocado de los esquemas OUTLN y DBSNMP para evitar que tenga más privilegios de los necesarios.	1	Aplicado
65	SELECT ANY DICTIONARY	Asegurar que este privilegio sea revocado de cuentas no administrativas para evitar que un usuario no autorizado pueda recopilar información sobre la base de datos a través del diccionario de datos objetos. La información recopilada podría utilizarse potencialmente para explotar la base de datos.	0	No aplicado

66	SELECT ANY TABLE	Asegurar que este privilegio sea revocado de cuentas no administrativas para evitar que un usuario no autorizado pueda visualizar sin autorización información sensible.	1	Aplicado
67	AUDIT SYSTEM	Asegurar que este privilegio sea revocado de cuentas no administrativas para evita que un usuario no autorizado pueda alterar las actividades de auditoria programadas, como deshabilitar la creación de pistas de auditoría.	1	Aplicado
68	EXEMPT ACCESS POLICY	Asegurar que este privilegio sea revocado de cuentas no administrativas para evitar que un usuario no autorizado pueda acceder a todas las filas de una tabla independientemente de los bloqueos de seguridad a nivel de fila.	1	Aplicado
69	BECOME USER	Asegurar que este privilegio sea revocado de cuentas no administrativas para evitar que un usuario no autorizado pueda usar privilegios otorgados a otro usuario,	1	Aplicado
70	CREATE PROCEDURE	Asegurar que este privilegio sea revocado de cuentas no administrativas para evitar que un usuario no autorizado pueda crear procedimientos no autorizados que facilitan el robo de datos o la denegación de servicio al corromper las tablas de datos.	1	Aplicado
71	ALTER SYSTEM	Asegurar que este privilegio sea revocado de cuentas no administrativas para evitar que un usuario no autorizado pueda modificar las operaciones en ejecución de la instancia.	1	Aplicado
72	CREATE ANY LIBRARY y CREATE LIBRARY	Asegurar que estos privilegios sean revocados de cuentas no administrativas para evitar que un usuario no autorizado pueda crear objetos que están asociados a las bibliotecas compartidas.	1	Aplicado
73	GRANT ANY OBJECT PRIVILEGE, GRANT ANY ROLE y GRANT ANY PRIVILEGE	Asegurar que estos privilegios sean revocados de cuentas no administrativas para evitar que un usuario no autorizado pueda acceder o cambiar datos confidenciales, o dañar el catálogo de datos debido a un potencial daño al acceso de instancia.	1	Aplicado
74	SELECT_CATALOG_ROLE	Asegurar que este rol sea revocado de cuentas no administrativas para evitar que un usuario no autorizado pueda divulgar todos los datos del diccionario.	1	Aplicado
75	EXECUTE_CATALOG_ROLE	Asegurar que este rol sea revocado de cuentas no administrativas para evitar que un usuario no autorizado pueda interrumpir las operaciones mediante la inicialización de procedimientos no autorizados.	1	Aplicado

76	DBA	Asegurar que este rol sea revocado de cuentas no administrativas para evitar que un usuario no autorizado pueda generar una gran cantidad de problemas innecesarios. Este privilegio abre la puerta a violaciones de datos, violaciones de integridad y condiciones de denegación de servicio.	1	Aplicado
V.1.3 Configuración de parámetros de auditorías				
V.1.3.1 Configurar parámetros de auditoria tradicional				
77	AUDIT_OPTION = USER	Asegurar que la tabla DBA_STMT_AUDIT_OPTS contenga un registro donde el campo AUDIT_OPTION sea igual a USER va a permitir auditar todas las actividades que realicen en la base de datos.	0	No aplicado
78	AUDIT_OPTION = ROLE	Asegurar que la tabla DBA_STMT_AUDIT_OPTS contenga un registro donde el campo AUDIT_OPTION sea igual a ROLE va a permitir auditar todos los intentos, exitosos o no, de crear, descartar, modificar o establecer roles.	0	No aplicado
79	AUDIT_OPTION = SYSTEM GRANT	Asegurar que la tabla DBA_STMT_AUDIT_OPTS contenga un registro donde el campo AUDIT_OPTION sea igual a SYSTEM GRANT va a permitir auditar cualquier intento, exitoso o no, para otorgar o revocar cualquier privilegio o función del sistema, independientemente del privilegio en poder del usuario que intenta la operación.	0	No aplicado
80	AUDIT_OPTION = PROFILE	Asegurar que la tabla DBA_STMT_AUDIT_OPTS contenga un registro donde el campo AUDIT_OPTION sea igual a PROFILE va a permitir auditar todos los intentos, exitosos o no, de crear, descartar o alterar cualquier perfil.	0	No aplicado
81	AUDIT_OPTION = DATABASE LINK	Asegurar que la tabla DBA_STMT_AUDIT_OPTS contenga un registro donde el campo AUDIT_OPTION sea igual a DATABASE LINK va a permitir auditar todas las actividades en los enlaces de la base de datos.	0	No aplicado
82	AUDIT_OPTION = PUBLIC DATABASE LINK	Asegurar que la tabla DBA_STMT_AUDIT_OPTS contenga un registro donde el campo AUDIT_OPTION sea igual a PUBLIC DATABASE LINK va a permitir auditar todas las actividades del usuario que impliquen la creación, alteración o eliminación de los enlaces públicos.	0	No aplicado
83	AUDIT_OPTION = PUBLIC SYNONYM	Asegurar que la tabla DBA_STMT_AUDIT_OPTS contenga un registro donde el campo AUDIT_OPTION sea igual a PUBLIC SYNONYM va a permitir auditar todas las actividades del usuario que	0	No aplicado

		impliquen la creación, alteración o eliminación de los sinónimos públicos.		
84	AUDIT_OPTION = SYNONYM	Asegurar que la tabla DBA_STMT_AUDIT_OPTS contenga un registro donde el campo AUDIT_OPTION sea igual a SYNONYM va a permitir auditar todas las actividades del usuario que impliquen la creación, alteración o eliminación de los sinónimos públicos.	0	No aplicado
85	AUDIT_OPTION = DIRECTORY	Asegurar que la tabla DBA_STMT_AUDIT_OPTS contenga un registro donde el campo AUDIT_OPTION sea igual a DIRECTORY va a permitir auditar todas las actividades del usuario que impliquen la creación, alteración o eliminación de un directorio.	0	No aplicado
86	AUDIT_OPTION = SELECT ANY DICTIONARY	Asegurar que la tabla DBA_STMT_AUDIT_OPTS contenga un registro donde el campo AUDIT_OPTION sea igual a SELECT ANY DICTIONARY va a permitir auditar todas las actividades del usuario relacionadas con esta capacidad.	0	No aplicado
87	AUDIT_OPTION = GRANT ANY OBJECT PRIVILEGE	Asegurar que la tabla DBA_STMT_AUDIT_OPTS contenga un registro donde el campo AUDIT_OPTION sea igual a GRANT ANY OBJECT PRIVILEGE va a permitir para auditar todas las actividades del usuario relacionadas con otorgar o revocar cualquier privilegio de objeto, que incluye privilegios sobre tablas, directorios, modelos de minería.	0	No aplicado
88	AUDIT_OPTION = GRANT ANY PRIVILEGE	Asegurar que la tabla DBA_STMT_AUDIT_OPTS contenga un registro donde el campo AUDIT_OPTION sea igual a GRANT ANY PRIVILEGE va a permitir auditar todas las actividades del usuario administrador relacionadas con cambiar la seguridad infraestructura, para eliminar, agregar, modificar usuarios y más.	0	No aplicado
89	AUDIT_OPTION = DROP ANY PROCEDURE	Asegurar que la tabla DBA_STMT_AUDIT_OPTS contenga un registro donde el campo AUDIT_OPTION sea igual a DROP ANY PROCEDURE va a permitir auditar todas las actividades del usuario que impliquen la eliminación de procedimientos.	0	No aplicado
90	SYS.AUD$	Asegurar que el privilegio ALL este habilitado en la tabla SYS.AUD$ va proporcionar pruebas forenses desde el inicio de actividades no autorizadas.	0	No aplicado
91	AUDIT_OPTION = PROCEDURE	Asegurar que la tabla DBA_STMT_AUDIT_OPTS contenga un registro donde el campo AUDIT_OPTION sea igual a PROCEDURE va a permitir auditar todas las actividades del usuario que impliquen la creación, alteración o eliminación de un procedimiento.	0	No aplicado

92	AUDIT_OPTION = ALTER SYSTEM	Asegurar que la tabla DBA_STMT_AUDIT_OPTS contenga un registro donde el campo AUDIT_OPTION sea igual a ALTER SYSTEM va permitir auditar cualquier intento no autorizado de alterar el sistema, estos registros pueden ser muy útiles.	0	No aplicado
93	AUDIT_OPTION = TRIGGER	Asegurar que la tabla DBA_STMT_AUDIT_OPTS contenga un registro donde el campo AUDIT_OPTION sea igual a TRIGGER va a permitir auditar todas las actividades del usuario que impliquen la creación, alteración o eliminación de un trigger.	0	No aplicado
94	AUDIT_OPTION = CREATE SESSION	Asegurar que la tabla DBA_STMT_AUDIT_OPTS contenga un registro donde el campo AUDIT_OPTION sea igual a CREATE SESSION va a permitir auditar todos los intentos de conexión a la base de datos, ya sea con éxito o no, así como las desconexiones/cierres de sesión de auditoría.	0	No aplicado
V.1.3.2 Configurar parámetros de auditoría unificada				
95	CREATE USER	Asegurar habilitar la auditoría de la instrucción CREATE USER va permitir el registro de todas las creaciones de cuentas ya sean exitosas o no, emitidas por los usuarios independientemente de los privilegios que tienen los usuarios.	1	Aplicado
96	ALTER USER	Asegurar habilitar la auditoría de la instrucción ALTER USER va permitir el registro de todos los cambios de contraseña, bloqueo de cuentas. También va registrar los cambios de propiedades de los usuarios, Profiles, tablespaces por defecto o temporales y las cuotas de espacio en los tablespaces ya sean exitosas o no, emitidas por los usuarios independientemente de los privilegios que tienen los usuarios.	0	No aplicado
97	DROP USER	Asegurar habilitar la auditoría de la instrucción DROP USER va permitir el registro de todas las eliminaciones de cuentas o esquemas de la base de datos ya sean exitosas o no, emitidas por los usuarios independientemente de los privilegios que tienen los usuarios.	1	Aplicado
98	CREATE ROLE	Asegurar habilitar la auditoría de la instrucción CREATE ROLE va permitir el registro de todas las creaciones de colecciones de privilegios de sistema, privilegios de objetos que se otorgan a los usuarios o a otros roles ya sean exitosas o no, emitidas por los usuarios independientemente de los privilegios que tienen los usuarios.	0	No aplicado

99	ALTER ROLE	Asegurar habilitar la auditoría de la instrucción ALTER ROLE va permitir el registro de todos los movimientos que se realizan en la colección de privilegios de sistema, privilegios de objetos que se otorgan a los usuarios o a otros roles ya sean exitosas o no, emitidas por los usuarios independientemente de los privilegios que tienen los usuarios.	0	No aplicado
100	DROP ROLE	Asegurar habilitar la auditoría de la instrucción DROP ROLE va permitir el registro de todas las eliminaciones de colecciones de privilegios de sistema, privilegios de objetos que se otorgan a los usuarios o a otros roles ya sean exitosas o no, emitidas por los usuarios independientemente de los privilegios que tienen los usuarios.	0	No aplicado
101	GRANT	Asegurar habilitar la auditoría de la instrucción GRANT va permitir el registro de todas las otorgaciones de privilegios a los usuarios o a otros roles ya sean exitosas o no, emitidas por los usuarios independientemente de los privilegios que tienen los usuarios	1	Aplicado
102	REVOKE	Asegurar habilitar la auditoría de la instrucción REVOKE va permitir el registro de todas las revocatorias de privilegios a los usuarios o a otros roles ya sean exitosas o no, emitidas por los usuarios independientemente de los privilegios que tienen los usuarios	1	Aplicado
103	CREATE PROFILE	Asegurar habilitar la auditoría de la instrucción CREATE PROFILE va permitir el registro de todas las creaciones de políticas de contraseñas, como reglas de complejidad de contraseñas, restricciones de reutilización y límites de uso de recursos ya sean exitosas o no, emitidas por los usuarios independientemente de los privilegios que tienen los usuarios.	0	No aplicado
104	ALTER PROFILE	Asegurar habilitar la auditoría de la instrucción ALTER PROFILE va permitir el registro de todas las modificaciones de políticas de contraseñas, como reglas de complejidad de contraseñas, restricciones de reutilización y límites de uso de recursos ya sean exitosas o no, emitidas por los usuarios independientemente de los privilegios que tienen los usuarios.	0	No aplicado
105	DROP PROFILE	Asegurar habilitar la auditoría de la instrucción DROP PROFILE va permitir el registro de todas las modificaciones de políticas de contraseñas, como reglas de complejidad de contraseñas, restricciones de reutilización y límites de uso de recursos ya sean	0	No aplicado

		exitosas o no, emitidas por los usuarios independientemente de los privilegios que tienen los usuarios		
106	CREATE DATABASE LINK	Asegurar habilitar la auditoría de la instrucción CREATE DATABASE LINK va permitir el registro de todas las creaciones de los enlaces para establecer conexiones de base de datos a base de datos, estas conexiones están disponibles sin autenticación ya sean exitosas o no, emitidas por los usuarios independientemente de los privilegios que tienen los usuarios.	0	No aplicado
107	ALTER DATABASE LINK	Asegurar habilitar la auditoría de la instrucción ALTER DATABASE LINK va permitir el registro de todas las modificaciones de los enlaces para establecer conexiones de base de datos a base de datos, estas conexiones están disponibles sin autenticación ya sean exitosas o no, emitidas por los usuarios independientemente de los privilegios que tienen los usuarios	0	No aplicado
108	DROP DATABASE LINK	Asegurar habilitar la auditoría de la instrucción ALTER DATABASE LINK va permitir el registro de todas las eliminaciones de los enlaces para establecer conexiones de base de datos a base de datos, estas conexiones están disponibles sin autenticación ya sean exitosas o no, emitidas por los usuarios independientemente de los privilegios que tienen los usuarios	0	No aplicado
109	CREATE SYNONYM	Asegurar habilitar la auditoría de la instrucción CREATE SYNONYM va permitir el registro de todas las creaciones de un nombre alternativo para un objeto de base de datos como tabla, vista, procedimiento, objeto java o incluso otro sinónimo ya sean exitosas o no, emitidas por los usuarios independientemente de los privilegios que tienen los usuarios.	1	Aplicado
110	ALTER SYNONYM	Asegurar habilitar la auditoría de la instrucción ALTER SYNONYM va permitir el registro de todas las modificaciones de un nombre alternativo para un objeto de base de datos como tabla, vista, procedimiento, objeto java o incluso otro sinónimo ya sean exitosas o no, emitidas por los usuarios independientemente de los privilegios que tienen los usuarios	1	Aplicado
111	DROP SYNONYM	Asegurar habilitar la auditoría de la instrucción DROP SYNONYM va permitir el registro de todas las eliminaciones de un nombre alternativo para un objeto de base de datos como tabla, vista, procedimiento, objeto java o incluso otro sinónimo ya sean exitosas o no, emitidas por	1	Aplicado

		los usuarios independientemente de los privilegios que tienen los usuarios		
112	SELECT ANY DICTIONARY	Asegurar habilitar la auditoría de la instrucción SELECT ANY DICTIONARY va permitir el registro de todas las acciones que realizan los usuarios cuando vean la definición de los objetos de esquemas, de los objetos del diccionario de datos, incluido en vistas DBA_, vistas V$, vistas X$ y tablas SYS subyacentes como TAB$ y OBJ	1	Aplicado
113	AUDSYS.AUD$UNIFIED	Asegurar habilitar la auditoría de la instrucción AUDSYS.AUD$UNIFIED va permitir el registro de todos los intentos de acceso a AUDSYS.AUD$UNIFIED, ya sea con éxito o sin éxito, independientemente de los privilegios que tengan los usuarios para emitir dichas declaraciones	1	Aplicado
114	CREATE PROCEDURE /FUNCTION / PACKAGE / PACKAGE BODY	Asegurar habilitar la auditoría de las instrucciones CREATE PROCEDURE / FUNCTION / PACKAGE / PACKAGE BODY va permitir el registro de todas las creaciones de estas instrucciones comerciales que se encuentran definido por código PL/SQL y sentencias SQL contenidas dentro de estos objetos, ya sean instrucciones satisfactorias o no satisfactorias emitidos por los usuarios independientemente de los privilegios que tengan los usuarios para emitir tales declaraciones	1	Aplicado
115	ALTER PROCEDURE / FUNCTION / PACKAGE / PACKAGE BODY	Asegurar habilitar la auditoría de las instrucciones ALTER PROCEDURE / FUNCTION / PACKAGE / PACKAGE BODY va permitir el registro de todas las modificaciones de estas instrucciones comerciales que se encuentran definido por código PL/SQL y sentencias SQL contenidas dentro de estos objetos, ya sean instrucciones satisfactorias o no satisfactorias emitidos por los usuarios independientemente de los privilegios que tengan los usuarios para emitir tales declaraciones	1	Aplicado
116	DROP PROCEDURE / FUNCTION / PACKAGE / PACKAGE BODY	Asegurar habilitar la auditoría de las instrucciones DROP PROCEDURE / FUNCTION / PACKAGE / PACKAGE BODY va permitir el registro de todas las eliminaciones de estas instrucciones comerciales que se encuentran definido por código PL/SQL y sentencias SQL contenidas dentro de estos objetos, ya sean instrucciones satisfactorias o no satisfactorias emitidos por los usuarios independientemente de los privilegios que tengan los usuarios para emitir tales declaraciones	1	Aplicado

117	ALTER SYSTEM	Asegurar habilitar la auditoría de la instrucción ALTER SYSTEM va permitir el registro de todas las modificaciones al cambiar la configuración de la instancia que podría afectar la postura de seguridad, rendimiento o funcionamiento normal de la base de datos. Además, se registrarán la ejecución de los comandos de sistema operativo, ya sean exitosas o no, realizadas por los usuarios independientemente de sus privilegios.	0	No aplicado
118	CREATE TRIGGER	Asegurar habilitar la auditoría de la instrucción CREATE TRIGGER va permitir el registro de todas las creaciones de los disparadores que contienen código para realizar validaciones o hacer cumplir restricciones críticas sobre los datos ya sean exitosas o no, ejecutadas por los usuarios independientemente de los privilegios que tienen los usuarios.	1	Aplicado
119	ALTER TRIGGER	Asegurar habilitar la auditoría de la instrucción ALTER TRIGGER va permitir el registro de todas las modificaciones de los disparadores que contienen código para realizar validaciones o hacer cumplir restricciones críticas sobre los datos ya sean exitosas o no, ejecutadas por los usuarios independientemente de los privilegios que tienen los usuarios	1	Aplicado
120	DROP TRIGGER	Asegurar habilitar la auditoría de la instrucción DROP TRIGGER va permitir el registro de todas las eliminaciones de los disparadores que contienen código para realizar validaciones o hacer cumplir restricciones críticas sobre los datos ya sean exitosas o no, ejecutadas por los usuarios independientemente de los privilegios que tienen los usuarios	1	Aplicado
121	LOGON / LOGOFF	Asegurar habilitar la auditoría de la instrucción LOGON / LOGOFF va permitir el registro de todas los inicios o cierres de sesión que realicen los usuarios independientemente de sus privilegios	1	Aplicado

Anexo 12: Lista de Cotejo Post Test de los controles de configuración de seguridad en la base de datos Oracle 19c en la instancia de base de datos "bdgpadev" del ambiente de desarrollo de la empresa GPA Business SAC.

Escala: No aplicado = 0 – Aplicado = 1

V1.1 Actualización del software de base de datos y configuración de parámetros				
V1.1.1: Versión del parche del motor de BD				
Ítem	**Controles / Parámetros**	**Acción**	**Escala**	**Observación**
1	PATCH	Asegurar que esté aplicado el último parche generado por el fabricante para mitigar la posibilidad de vulnerabilidad en la base de datos Oracle.	1	Aplicado
V1.1.2: Configurar parámetros de listener				
2	EXTPROC	Asegurar que dicho parámetro no esté presente en el archivo listener.ora para evitar que algunas librerías del sistema operativo puedan ser invocadas por la base de datos.	1	Aplicado
3	ADMIN_RESTRICTIONS	Asegurar que ese parámetro esté presente en el archivo listener.ora para evitar que usuarios no administradores puedan alterar en tiempo real los parámetros del archivo.	1	Aplicado
V1.1.3: Configurar parámetros generales de BD				
4	AUDIT_SYS_OPERATIONS	Asegurar que se configure este parámetro con el valor de TRUE va permitir conocer las actividades realizadas por la cuenta administradora SYS. Las operaciones se registrarán en la tabla SYS.AUD$. Va a requerir reinicio de la base de datos.	1	Aplicado
5	AUDIT_TRAIL	Asegurar que se configure este parámetro con los valores de DB, EXTENDED, OS, XML, EXTENDED, DB, XML; va permitir habilitar las funciones básicas de auditoría, además de recopilar datos para solucionar problemas y valiosos registros forenses.	1	Aplicado
6	GLOBAL_NAMES	Asegurar que se configure este parámetro con el valor de TRUE va permitir conectarse remotamente a otra base de datos a través de un único nombre de enlace entre las bases de datos.	1	Aplicado
7	OS_ROLES	Asegurar que se configure este parámetro con el valor de FALSE para evitar que el sistema operativo use grupos externos para la administración de la base de datos.	1	Aplicado
8	REMOTE_LISTENER	Asegurar que se configure este parámetro con el valor NULL para evitar establecer un oyente válido en un sistema separado, a menos que estén utilizando un RAC.	1	Aplicado

9	REMOTE_LOGIN_PASSWORDFILE	Asegurar que se configure este parámetro con el valor de NONE para evitar conexiones privilegiadas no seguras a la base de datos.	1	Aplicado
10	REMOTE_OS_AUTHENT	Asegurar que se configure este parámetro con el valor de FALSE para evitar suplantación de conexiones y permita otorgar privilegios a un usuario no autorizado del sistema operativo y este pueda realizar conexiones.	1	Aplicado
11	REMOTE_OS_ROLES	Asegurar que se configure este parámetro con el valor de FALSE para evitar que usuarios del sistema operativo tengan permisos para la administración de la base de datos.	1	Aplicado
12	SEC_CASE_SENSITIVE_LOGON	Asegurar que se configure este parámetro con el valor de TRUE para aumentar el conjunto de caracteres que se pueden elegir para las contraseñas, lo que evita a los ataques de contraseña de fuerza bruta.	1	Aplicado
13	SEC_MAX_FAILED_LOGIN_ATTEMPTS	Asegurar que se configure este parámetro con el valor de 3 o menos, determina cuántos inicios de sesión fallidos se permitirán, antes de que la instancia cierre la conexión de inicio de sesión.	1	Aplicado
14	SEC_PROTOCOL_ERROR_FURTHER_ACTION	Asegurar que se configure este parámetro con el valor de (DROP,3) permitirá que se corte una conexión después de tres paquetes defectuosos o con formato incorrecto.	1	Aplicado
15	SEC_PROTOCOL_ERROR_TRACE_ACTION	Asegurar que se configure este parámetro con el valor de LOG, permite el registro de los acontecimientos que pasa en la instancia de base de datos.	1	Aplicado
16	SEC_RETURN_SERVER_RELEASE_BANNER	Asegurar que se configure este parámetro con el valor de FALSE para evitar que la base de datos devuelva información sobre el número de versión del parche aplicado.	1	Aplicado
17	SQL92_SECURITY	Asegurar que se configure este parámetro con el valor de TRUE para evitar la divulgación de información involuntaria asegurándose de que solo los usuarios que ya tienen el privilegio SELECT puedan ejecutar sentencias que les permite obtener los valores almacenados.	1	Aplicado
18	TRACE_FILES_PUBLIC	Asegurar que se configure este parámetro con el valor de FALSE para evitar que el archivo de rastreo del sistema sea legible.	1	Aplicado
19	RESOURCE_LIMIT	Asegurar que se configure este parámetro con el valor de TRUE determina si se aplican límites de recursos en los perfiles de base de datos.	1	Aplicado
V.1.2. Configuración de parámetros de conexión, acceso, usuarios y asignación y/o revocación de privilegios				
V.1.2.1. Configurar parámetros de conexión y acceso				
Ítem	**Control**	**Acción**	**Escala**	**Observación**

20	FAILED_LOGIN_ATTEMPTS	Asegurar que se configure este parámetro con el valor de 5 o menos, determina cuántos intentos fallidos de inicio de sesión se permite antes de que el sistema bloquee la cuenta del usuario.	1	Aplicado
21	PASSWORD_LOCK_TIME	Asegurar que se configure este parámetro con el valor de 1 determina cuántos días deben pasar para que la cuenta se desbloqué después de que se haya producido el número establecido de intentos fallidos en el inicio de sesión.	1	Aplicado
22	PASSWORD_LIFE_TIME	Asegurar que se configure este parámetro con el valor de 90 o menos para determinar cuánto tiempo se puede usar una contraseña antes de que el usuario pueda cambiarla.	1	Aplicado
23	PASSWORD_REUSE_MAX	Asegurar que se configure este parámetro con el valor de 20 o más, para determinar cuántas contraseñas diferentes se deben usar antes de que el usuario pueda reutilizar una contraseña anterior.	1	Aplicado
24	PASSWORD_REUSE_TIME	Asegurar que se configure este parámetro con el valor de 365 o más, para determina la cantidad de tiempo en días que debe pasar antes de que se pueda reutilizar la misma contraseña.	1	Aplicado
25	PASSWORD_GRACE_TIME	Asegurar que se configure este parámetro con el valor de 5 o menos, para determinar cuántos días puede un usuario tener una contraseña vencida, antes que la sesión del usuario se bloque automáticamente.	1	Aplicado
26	PASSWORD_VERIFY_FUNCTIO N	Asegurar que se configure este parámetro en todos los Profiles, para determinar las reglas de complejidad de contraseñas (casos mixtos con dígitos y caracteres especiales), bloquear las combinaciones simples y aplicar cambios a las configuraciones de historial logrando frustrar potencialmente los inicios de sesión no autorizados.	1	Aplicado
27	SESSIONS_PER_USER	Asegurar que se configure este parámetro con el valor de 10 o menos, para determinar el número máximo de sesiones de un usuario ayudando a prevenir el mal uso de recursos a nivel de memoria o ataques de denegación de servicio intencionales.	1	Aplicado
28	INACTIVE_ACCOUNT_TIME	Asegurar que se configure este parámetro con el valor de 120 o menos, para determinar el número máximo de días de inactividad (sin inicios de sesión en absoluto) después de lo cual la cuenta se bloqueará.	1	Aplicado
V.1.2.2. Configurar parámetros de usuarios				
29	Credenciales por defecto (DEFAULT PASSWORDS)	Asegurar que todas las credenciales por defecto sean modificadas, para evitar que cualquier atacante con acceso a la base de datos	1	Aplicado

		puede autenticarse con una cuenta predeterminada utilizando una credencial por efecto.		
30	Esquemas de ejemplo (SAMPLE DATA)	Asegurar que todos los esquemas de muestra (BI o HR o IX o OE o PM o SCOTT o SH) sean removidos del ambiente de producción, para evitar que puedan ser utilizados para lanzar exploits contra el ambiente de producción.	1	Aplicado
31	DBA_USERS.AUTHENTICATION_TYPE	Asegurar que esté campo no contenga el valor de EXTERNAL, para evitar que un usuario remoto del sistema operativo pueda tener acceso a la base de datos con autorización completa.	1	Aplicado
32	Usuarios sin profile por defecto (DEFAULT PROFILE)	Asegurar que los usuarios no tengan asignado el profile por defecto (DEFAULT), debido a que cuenta con configuraciones ilimitadas que a menudo son requeridas por el usuario administrador, tales configuraciones ilimitadas deben reservarse estrictamente y no aplicarse a usuarios innecesarios.	1	Aplicado
33	SYS.USER$MIG	Asegurar que la tabla sys.user$mig sea eliminada al inicio de una migración, para evitar que su información pueda llegar hacer conocida por un atacante.	1	Aplicado
34	Enlaces públicos (PUBLIC DATABASE LINKS)	Asegurar que no exista enlaces públicos de bases de datos para evitar que cualquier usuario pueda logra una conexión a la base de datos para consultar, actualizar, insertar, eliminar datos en una base de datos remota.	1	Aplicado
V.1.2.3. Asignar y/o revocar privilegios				
35	DBMS_LDAP - UTL_INADDR	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de las tablas DBMS_LDAP y UTL_INADDR para evitar la creación de errores especialmente diseñados o él envió de información vía DNS al exterior.	1	Aplicado
36	UTL_TCP	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de la tabla UTL_TCP para evitar que usuarios no autorizados envíen datos arbitrarios desde el servidor de base de datos.	1	Aplicado
37	UTL_MAIL - UTL_SMTP	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de las tablas UTL_MAIL y UTL_SMTP para evitar que un usuario no autorizado corrompa el SMTP, función para aceptar o generar correo no deseado que puede resultar en una denegación de servicio debido a la saturación de la red	1	Aplicado
38	UTL_DBWS	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de la tabla UTL_DBWS para evitar que un usuario no autorizado corrompa	1	Aplicado

		el HTTP flujo utilizado para transportar los protocolos que comunican la instancia basada en la web.		
39	UTL_ORAMTS - UTL_HTTP	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de las tablas UTL_ORAMTS y UTL_HTTP para evitar él envió de información (sensible) a sitios web.	1	Aplicado
40	HTTPURITYPE	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de la tabla HTTPURITYPE para evitar el filtrado de información de la base de datos a un destino externo por HTTP.	1	Aplicado
41	DBMS_ADVISOR	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de la tabla DBMS_ADVISOR para evitar que un usuario no autorizado corrompa archivos del sistema operativo o componentes fundamentales de la base de datos.	1	Aplicado
42	DBMS_LOB	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de la tabla DBMS_LOB para evitar que subprogramas puedan manipular, leer, escribir en BLOB, CLOB, NCLOB, BFILE y LOB temporales	1	Aplicado
43	UTL_FILE	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de la tabla UTL_FILE para evitar que un usuario pueda leer y escribir archivos ubicados en el servidor donde está instalada la instancia de base de datos.	1	Aplicado
44	DBMS_CRYPTO	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de la tabla DBMS_CRYPTO para evitar la ejecución de procedimientos de criptografía que puede potencialmente comprometer una porción o la totalidad de los datos.	1	Aplicado
45	DBMS_OBFUSCATION_TOOLKIT	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de la tabla DBMS_OBFUSCATION_TOOLKIT para evitar que la herramienta que determina la fuerza del algoritmo de cifrado sea utilizada para cifrar los datos de la aplicación.	1	Aplicado
46	DBMS_RANDOM	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de la tabla DBMS_RANDOM para evitar que una aplicación no autorizada genere números aleatorios.	1	Aplicado
47	DBMS_JAVA - DBMS_JAVA_TEST	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de las tablas DBMS_JAVA y DBMS_JAVA_TEST para evitar que un atacante ejecute comandos del sistema operativo desde la base de datos.	1	Aplicado

48	DBMS_JOB	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de la tabla DBMS_JOB para evitar que un usuario no autorizado inhabilite o sobrecargue la cola de trabajos.	1	Aplicado
49	DBMS_SCHEDULER	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de la tabla DBMS_SCHEDULER para evitar que un usuario no autorizado ejecute trabajos de la base de datos o del sistema operativo.	1	Aplicado
50	DBMS_SQL	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de la tabla DBMS_SQL para evitar la escalada de privilegios si no se realiza la validación de entrada adecuadamente.	1	Aplicado
51	DBMS_XMLGEN	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de la tabla DBMS_XMLGEN para evitar la búsqueda de información confidencial en toda la base de datos. Información como números de tarjetas de crédito.	1	Aplicado
52	DBMS_XMLQUERY, DBMS_XMLSAVE, DBMS_XMLSTORE, DBMS_AW, OWA_UTIL y DBMS_REDACT	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de las tablas DBMS_XMLQUERY, DBMS_XMLSAVE, DBMS_XMLSTORE, DBMS_AW, OWA_UTIL y DBMS_REDACT para evitar que usuarios malintencionados pueden aprovechar este paquete como una función de inyección auxiliar en un ataque de inyección SQL.	1	Aplicado
53	DBMS_BACKUP_RESTORE	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de la tabla DBMS_BACKUP_RESTORE para evitar el acceso a los archivos del sistema operativo.	1	Aplicado
54	DBMS_FILE_TRANSFER	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de la tabla DBMS_FILE_TRANSFER para evitar transferir archivos desde un servidor de base de datos a otro sin autorización para hacerlo.	1	Aplicado
55	DBMS_SYS_SQL	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de la tabla DBMS_SYS_SQL para evitar que un usuario ejecute código como un usuario diferente sin ingresar credenciales válidas.	1	Aplicado
56	DBMS_REPCAT_SQL_UTL, INITJVMAUX, DBMS_AQADM_SYS, DBMS_STREAMS_RPC y LTADM	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de las tablas DBMS_REPCAT_SQL_UTL, INITJVMAUX, DBMS_AQADM_SYS, DBMS_STREAMS_RPC y LTADM para evitar que un usuario no autorizado ejecute SQL comandos como un usuario SYS.	1	Aplicado
57	DBMS_PRVTAQIM	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de la tabla DBMS_PRVTAQIM para evitar que un usuario no autorizado escale privilegios por cualquier instrucción SQL y que podría ejecutarse como usuario SYS.	1	Aplicado

58	DBMS_IJOB y DBMS_PDB_EXEC_SQL	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de las tablas DBMS_IJOB y DBMS_PDB_EXEC_SQL para evitar que un atacante cambie de identidad utilizando un nombre de usuario diferente para ejecutar un trabajo de base de datos.	1	Aplicado
59	SYS.AUD$	Asegurar que usuarios no autorizados tengan privilegios sobre la tabla SYS.AUD$ para que no permita distorsión en los registros de auditoría, escondiendo actividades no autorizadas.	1	Aplicado
60	SYS.DBA_%	Asegurar que el privilegio PUBLIC sea revocado de todas las tablas sensibles del usuario SYS que sean encontradas en la vista DBA_% para evitar que usuarios no autorizados puedan manipular los datos confidenciales.	1	Aplicado
61	CDB_LOCAL_ADMINAUTH$, DEFAULT_PWD$, ENC$, HISTGRM$, HIST_HEAD$, LINK$, PDB_SYNC$, SCHEDULER$_CREDENTIAL, USER$, USER_HISTORY$ y XS$VERIFIERS	Asegurar que el privilegio ALL sea revocado de las tablas CDB_LOCAL_ADMINAUTH$, DEFAULT_PWD$, ENC$, HISTGRM$, HIST_HEAD$, LINK$, PDB_SYNC$, SCHEDULER$_CREDENTIAL, USER$, USER_HISTORY$ y XS$VERIFIERS del usuario SYS para evitar que usuarios no autorizados puedan manipular los datos sensibles y confidenciales.	1	Aplicado
62	%ANY%	Asegurar que los privilegios tipo %ANY% sean revocados de todos los objetos no autorizados de la base de dato para evitar que usuarios no autorizados puedan manipular los datos confidenciales o dañen el catálogo de datos.	1	Aplicado
63	ADMIN_OPTION	Asegurar que de la tabla DBA_SYS_PRIVS.% se revoke los privilegios no autorizados donde el campo ADMIN_OPTION sea igual a YES para evitar que los usuarios puedan otorgar sus mismos privilegios a otros usuarios.	1	Aplicado
64	EXECUTE ANY PROCEDURE	Asegurar que el privilegio EXECUTE ANY PROCEDURE sea revocado de los esquemas OUTLN y DBSNMP para evitar que tenga más privilegios de los necesarios.	1	Aplicado
65	SELECT ANY DICTIONARY	Asegurar que este privilegio sea revocado de cuentas no administrativas para evitar que un usuario no autorizado pueda recopilar información sobre la base de datos a través del diccionario de datos objetos. La información recopilada podría utilizarse potencialmente para explotar la base de datos.	1	Aplicado

66	SELECT ANY TABLE	Asegurar que este privilegio sea revocado de cuentas no administrativas para evitar que un usuario no autorizado pueda visualizar sin autorización información sensible.	1	Aplicado
67	AUDIT SYSTEM	Asegurar que este privilegio sea revocado de cuentas no administrativas para evita que un usuario no autorizado pueda alterar las actividades de auditoria programadas, como deshabilitar la creación de pistas de auditoría.	1	Aplicado
68	EXEMPT ACCESS POLICY	Asegurar que este privilegio sea revocado de cuentas no administrativas para evitar que un usuario no autorizado pueda acceder a todas las filas de una tabla independientemente de los bloqueos de seguridad a nivel de fila.	1	Aplicado
69	BECOME USER	Asegurar que este privilegio sea revocado de cuentas no administrativas para evitar que un usuario no autorizado pueda usar privilegios otorgados a otro usuario,	1	Aplicado
70	CREATE PROCEDURE	Asegurar que este privilegio sea revocado de cuentas no administrativas para evitar que un usuario no autorizado pueda crear procedimientos no autorizados que facilitan el robo de datos o la denegación de servicio al corromper las tablas de datos.	1	Aplicado
71	ALTER SYSTEM	Asegurar que este privilegio sea revocado de cuentas no administrativas para evitar que un usuario no autorizado pueda modificar las operaciones en ejecución de la instancia.	1	Aplicado
72	CREATE ANY LIBRARY y CREATE LIBRARY	Asegurar que estos privilegios sean revocados de cuentas no administrativas para evitar que un usuario no autorizado pueda crear objetos que están asociados a las bibliotecas compartidas.	1	Aplicado
73	GRANT ANY OBJECT PRIVILEGE, GRANT ANY ROLE y GRANT ANY PRIVILEGE	Asegurar que estos privilegios sean revocados de cuentas no administrativas para evitar que un usuario no autorizado pueda acceder o cambiar datos confidenciales, o dañar el catálogo de datos debido a un potencial daño al acceso de instancia.	1	Aplicado
74	SELECT_CATALOG_ROLE	Asegurar que este rol sea revocado de cuentas no administrativas para evitar que un usuario no autorizado pueda divulgar todos los datos del diccionario.	1	Aplicado
75	EXECUTE_CATALOG_ROLE	Asegurar que este rol sea revocado de cuentas no administrativas para evitar que un usuario no autorizado pueda interrumpir las operaciones mediante la inicialización de procedimientos no autorizados.	1	Aplicado

76	DBA	Asegurar que este rol sea revocado de cuentas no administrativas para evitar que un usuario no autorizado pueda generar una gran cantidad de problemas innecesarios. Este privilegio abre la puerta a violaciones de datos, violaciones de integridad y condiciones de denegación de servicio.	1	Aplicado
V.1.3 Configuración de parámetros de auditorías				
V.1.3.1 Configurar parámetros de auditoria tradicional				
77	AUDIT_OPTION = USER	Asegurar que la tabla DBA_STMT_AUDIT_OPTS contenga un registro donde el campo AUDIT_OPTION sea igual a USER va a permitir auditar todas las actividades que realicen en la base de datos.	1	Aplicado
78	AUDIT_OPTION = ROLE	Asegurar que la tabla DBA_STMT_AUDIT_OPTS contenga un registro donde el campo AUDIT_OPTION sea igual a ROLE va a permitir auditar todos los intentos, exitosos o no, de crear, descartar, modificar o establecer roles.	1	Aplicado
79	AUDIT_OPTION = SYSTEM GRANT	Asegurar que la tabla DBA_STMT_AUDIT_OPTS contenga un registro donde el campo AUDIT_OPTION sea igual a SYSTEM GRANT va a permitir auditar cualquier intento, exitoso o no, para otorgar o revocar cualquier privilegio o función del sistema, independientemente del privilegio en poder del usuario que intenta la operación.	1	Aplicado
80	AUDIT_OPTION = PROFILE	Asegurar que la tabla DBA_STMT_AUDIT_OPTS contenga un registro donde el campo AUDIT_OPTION sea igual a PROFILE va a permitir auditar todos los intentos, exitosos o no, de crear, descartar o alterar cualquier perfil.	1	Aplicado
81	AUDIT_OPTION = DATABASE LINK	Asegurar que la tabla DBA_STMT_AUDIT_OPTS contenga un registro donde el campo AUDIT_OPTION sea igual a DATABASE LINK va a permitir auditar todas las actividades en los enlaces de la base de datos.	1	Aplicado
82	AUDIT_OPTION = PUBLIC DATABASE LINK	Asegurar que la tabla DBA_STMT_AUDIT_OPTS contenga un registro donde el campo AUDIT_OPTION sea igual a PUBLIC DATABASE LINK va a permitir auditar todas las actividades del usuario que impliquen la creación, alteración o eliminación de los enlaces públicos.	1	Aplicado
83	AUDIT_OPTION = PUBLIC SYNONYM	Asegurar que la tabla DBA_STMT_AUDIT_OPTS contenga un registro donde el campo AUDIT_OPTION sea igual a PUBLIC SYNONYM va a permitir auditar todas las actividades del usuario que	1	Aplicado

		impliquen la creación, alteración o eliminación de los sinónimos públicos.		
84	AUDIT_OPTION = SYNONYM	Asegurar que la tabla DBA_STMT_AUDIT_OPTS contenga un registro donde el campo AUDIT_OPTION sea igual a SYNONYM va a permitir auditar todas las actividades del usuario que impliquen la creación, alteración o eliminación de los sinónimos públicos.	1	Aplicado
85	AUDIT_OPTION = DIRECTORY	Asegurar que la tabla DBA_STMT_AUDIT_OPTS contenga un registro donde el campo AUDIT_OPTION sea igual a DIRECTORY va a permitir auditar todas las actividades del usuario que impliquen la creación, alteración o eliminación de un directorio.	1	Aplicado
86	AUDIT_OPTION = SELECT ANY DICTIONARY	Asegurar que la tabla DBA_STMT_AUDIT_OPTS contenga un registro donde el campo AUDIT_OPTION sea igual a SELECT ANY DICTIONARY va a permitir auditar todas las actividades del usuario relacionadas con esta capacidad.	1	Aplicado
87	AUDIT_OPTION = GRANT ANY OBJECT PRIVILEGE	Asegurar que la tabla DBA_STMT_AUDIT_OPTS contenga un registro donde el campo AUDIT_OPTION sea igual a GRANT ANY OBJECT PRIVILEGE va a permitir para auditar todas las actividades del usuario relacionadas con otorgar o revocar cualquier privilegio de objeto, que incluye privilegios sobre tablas, directorios, modelos de minería.	1	Aplicado
88	AUDIT_OPTION = GRANT ANY PRIVILEGE	Asegurar que la tabla DBA_STMT_AUDIT_OPTS contenga un registro donde el campo AUDIT_OPTION sea igual a GRANT ANY PRIVILEGE va a permitir auditar todas las actividades del usuario administrador relacionadas con cambiar la seguridad infraestructura, para eliminar, agregar, modificar usuarios y más.	1	Aplicado
89	AUDIT_OPTION = DROP ANY PROCEDURE	Asegurar que la tabla DBA_STMT_AUDIT_OPTS contenga un registro donde el campo AUDIT_OPTION sea igual a DROP ANY PROCEDURE va a permitir auditar todas las actividades del usuario que impliquen la eliminación de procedimientos.	1	Aplicado
90	SYS.AUD$	Asegurar que el privilegio ALL este habilitado en la tabla SYS.AUD$ va proporcionar pruebas forenses desde el inicio de actividades no autorizadas.	1	Aplicado
91	AUDIT_OPTION = PROCEDURE	Asegurar que la tabla DBA_STMT_AUDIT_OPTS contenga un registro donde el campo AUDIT_OPTION sea igual a PROCEDURE va a permitir auditar todas las actividades del usuario que impliquen la creación, alteración o eliminación de un procedimiento.	1	Aplicado

92	AUDIT_OPTION = ALTER SYSTEM	Asegurar que la tabla DBA_STMT_AUDIT_OPTS contenga un registro donde el campo AUDIT_OPTION sea igual a ALTER SYSTEM va permitir auditar cualquier intento no autorizado de alterar el sistema, estos registros pueden ser muy útiles.	1	Aplicado
93	AUDIT_OPTION = TRIGGER	Asegurar que la tabla DBA_STMT_AUDIT_OPTS contenga un registro donde el campo AUDIT_OPTION sea igual a TRIGGER va a permitir auditar todas las actividades del usuario que impliquen la creación, alteración o eliminación de un trigger.	1	Aplicado
94	AUDIT_OPTION = CREATE SESSION	Asegurar que la tabla DBA_STMT_AUDIT_OPTS contenga un registro donde el campo AUDIT_OPTION sea igual a CREATE SESSION va a permitir auditar todos los intentos de conexión a la base de datos, ya sea con éxito o no, así como las desconexiones/cierres de sesión de auditoría.	1	Aplicado
V.1.3.2 Configurar parámetros de auditoría unificada				
95	CREATE USER	Asegurar habilitar la auditoría de la instrucción CREATE USER va permitir el registro de todas las creaciones de cuentas ya sean exitosas o no, emitidas por los usuarios independientemente de los privilegios que tienen los usuarios.	1	Aplicado
96	ALTER USER	Asegurar habilitar la auditoría de la instrucción ALTER USER va permitir el registro de todos los cambios de contraseña, bloqueo de cuentas. También va registrar los cambios de propiedades de los usuarios, Profiles, tablespaces por defecto o temporales y las cuotas de espacio en los tablespaces ya sean exitosas o no, emitidas por los usuarios independientemente de los privilegios que tienen los usuarios.	1	Aplicado
97	DROP USER	Asegurar habilitar la auditoría de la instrucción DROP USER va permitir el registro de todas las eliminaciones de cuentas o esquemas de la base de datos ya sean exitosas o no, emitidas por los usuarios independientemente de los privilegios que tienen los usuarios.	1	Aplicado
98	CREATE ROLE	Asegurar habilitar la auditoría de la instrucción CREATE ROLE va permitir el registro de todas las creaciones de colecciones de privilegios de sistema, privilegios de objetos que se otorgan a los usuarios o a otros roles ya sean exitosas o no, emitidas por los usuarios independientemente de los privilegios que tienen los usuarios.	1	Aplicado

99	ALTER ROLE	Asegurar habilitar la auditoría de la instrucción ALTER ROLE va permitir el registro de todos los movimientos que se realizan en la colección de privilegios de sistema, privilegios de objetos que se otorgan a los usuarios o a otros roles ya sean exitosas o no, emitidas por los usuarios independientemente de los privilegios que tienen los usuarios.	1	Aplicado
100	DROP ROLE	Asegurar habilitar la auditoría de la instrucción DROP ROLE va permitir el registro de todas las eliminaciones de colecciones de privilegios de sistema, privilegios de objetos que se otorgan a los usuarios o a otros roles ya sean exitosas o no, emitidas por los usuarios independientemente de los privilegios que tienen los usuarios.	1	Aplicado
101	GRANT	Asegurar habilitar la auditoría de la instrucción GRANT va permitir el registro de todas las otorgaciones de privilegios a los usuarios o a otros roles ya sean exitosas o no, emitidas por los usuarios independientemente de los privilegios que tienen los usuarios	1	Aplicado
102	REVOKE	Asegurar habilitar la auditoría de la instrucción REVOKE va permitir el registro de todas las revocatorias de privilegios a los usuarios o a otros roles ya sean exitosas o no, emitidas por los usuarios independientemente de los privilegios que tienen los usuarios	1	Aplicado
103	CREATE PROFILE	Asegurar habilitar la auditoría de la instrucción CREATE PROFILE va permitir el registro de todas las creaciones de políticas de contraseñas, como reglas de complejidad de contraseñas, restricciones de reutilización y límites de uso de recursos ya sean exitosas o no, emitidas por los usuarios independientemente de los privilegios que tienen los usuarios.	1	Aplicado
104	ALTER PROFILE	Asegurar habilitar la auditoría de la instrucción ALTER PROFILE va permitir el registro de todas las modificaciones de políticas de contraseñas, como reglas de complejidad de contraseñas, restricciones de reutilización y límites de uso de recursos ya sean exitosas o no, emitidas por los usuarios independientemente de los privilegios que tienen los usuarios.	1	Aplicado
105	DROP PROFILE	Asegurar habilitar la auditoría de la instrucción DROP PROFILE va permitir el registro de todas las modificaciones de políticas de contraseñas, como reglas de complejidad de contraseñas, restricciones de reutilización y límites de uso de recursos ya sean	1	Aplicado

		exitosas o no, emitidas por los usuarios independientemente de los privilegios que tienen los usuarios		
106	CREATE DATABASE LINK	Asegurar habilitar la auditoría de la instrucción CREATE DATABASE LINK va permitir el registro de todas las creaciones de los enlaces para establecer conexiones de base de datos a base de datos, estas conexiones están disponibles sin autenticación ya sean exitosas o no, emitidas por los usuarios independientemente de los privilegios que tienen los usuarios.	1	Aplicado
107	ALTER DATABASE LINK	Asegurar habilitar la auditoría de la instrucción ALTER DATABASE LINK va permitir el registro de todas las modificaciones de los enlaces para establecer conexiones de base de datos a base de datos, estas conexiones están disponibles sin autenticación ya sean exitosas o no, emitidas por los usuarios independientemente de los privilegios que tienen los usuarios	1	Aplicado
108	DROP DATABASE LINK	Asegurar habilitar la auditoría de la instrucción ALTER DATABASE LINK va permitir el registro de todas las eliminaciones de los enlaces para establecer conexiones de base de datos a base de datos, estas conexiones están disponibles sin autenticación ya sean exitosas o no, emitidas por los usuarios independientemente de los privilegios que tienen los usuarios	1	Aplicado
109	CREATE SYNONYM	Asegurar habilitar la auditoría de la instrucción CREATE SYNONYM va permitir el registro de todas las creaciones de un nombre alternativo para un objeto de base de datos como tabla, vista, procedimiento, objeto java o incluso otro sinónimo ya sean exitosas o no, emitidas por los usuarios independientemente de los privilegios que tienen los usuarios.	1	Aplicado
110	ALTER SYNONYM	Asegurar habilitar la auditoría de la instrucción ALTER SYNONYM va permitir el registro de todas las modificaciones de un nombre alternativo para un objeto de base de datos como tabla, vista, procedimiento, objeto java o incluso otro sinónimo ya sean exitosas o no, emitidas por los usuarios independientemente de los privilegios que tienen los usuarios	1	Aplicado
111	DROP SYNONYM	Asegurar habilitar la auditoría de la instrucción DROP SYNONYM va permitir el registro de todas las eliminaciones de un nombre alternativo para un objeto de base de datos como tabla, vista, procedimiento, objeto java o incluso otro sinónimo ya sean exitosas o no, emitidas por	1	Aplicado

		los usuarios independientemente de los privilegios que tienen los usuarios		
112	SELECT ANY DICTIONARY	Asegurar habilitar la auditoría de la instrucción SELECT ANY DICTIONARY va permitir el registro de todas las acciones que realizan los usuarios cuando vean la definición de los objetos de esquemas, de los objetos del diccionario de datos, incluido en vistas DBA_, vistas V$, vistas X$ y tablas SYS subyacentes como TAB$ y OBJ	1	Aplicado
113	AUDSYS.AUD$UNIFIED	Asegurar habilitar la auditoría de la instrucción AUDSYS.AUD$UNIFIED va permitir el registro de todos los intentos de acceso a AUDSYS.AUD$UNIFIED, ya sea con éxito o sin éxito, independientemente de los privilegios que tengan los usuarios para emitir dichas declaraciones	1	Aplicado
114	CREATE PROCEDURE /FUNCTION / PACKAGE / PACKAGE BODY	Asegurar habilitar la auditoría de las instrucciones CREATE PROCEDURE / FUNCTION / PACKAGE / PACKAGE BODY va permitir el registro de todas las creaciones de estas instrucciones comerciales que se encuentran definido por código PL/SQL y sentencias SQL contenidas dentro de estos objetos, ya sean instrucciones satisfactorias o no satisfactorias emitidos por los usuarios independientemente de los privilegios que tengan los usuarios para emitir tales declaraciones	1	Aplicado
115	ALTER PROCEDURE / FUNCTION / PACKAGE / PACKAGE BODY	Asegurar habilitar la auditoría de las instrucciones ALTER PROCEDURE / FUNCTION / PACKAGE / PACKAGE BODY va permitir el registro de todas las modificaciones de estas instrucciones comerciales que se encuentran definido por código PL/SQL y sentencias SQL contenidas dentro de estos objetos, ya sean instrucciones satisfactorias o no satisfactorias emitidos por los usuarios independientemente de los privilegios que tengan los usuarios para emitir tales declaraciones	1	Aplicado
116	DROP PROCEDURE / FUNCTION / PACKAGE / PACKAGE BODY	Asegurar habilitar la auditoría de las instrucciones DROP PROCEDURE / FUNCTION / PACKAGE / PACKAGE BODY va permitir el registro de todas las eliminaciones de estas instrucciones comerciales que se encuentran definido por código PL/SQL y sentencias SQL contenidas dentro de estos objetos, ya sean instrucciones satisfactorias o no satisfactorias emitidos por los usuarios independientemente de los privilegios que tengan los usuarios para emitir tales declaraciones	1	Aplicado

117	ALTER SYSTEM	Asegurar habilitar la auditoría de la instrucción ALTER SYSTEM va permitir el registro de todas las modificaciones al cambiar la configuración de la instancia que podría afectar la postura de seguridad, rendimiento o funcionamiento normal de la base de datos. Además, se registrarán la ejecución de los comandos de sistema operativo, ya sean exitosas o no, realizadas por los usuarios independientemente de sus privilegios.	1	Aplicado
118	CREATE TRIGGER	Asegurar habilitar la auditoría de la instrucción CREATE TRIGGER va permitir el registro de todas las creaciones de los disparadores que contienen código para realizar validaciones o hacer cumplir restricciones críticas sobre los datos ya sean exitosas o no, ejecutadas por los usuarios independientemente de los privilegios que tienen los usuarios.	1	Aplicado
119	ALTER TRIGGER	Asegurar habilitar la auditoría de la instrucción ALTER TRIGGER va permitir el registro de todas las modificaciones de los disparadores que contienen código para realizar validaciones o hacer cumplir restricciones críticas sobre los datos ya sean exitosas o no, ejecutadas por los usuarios independientemente de los privilegios que tienen los usuarios	1	Aplicado
120	DROP TRIGGER	Asegurar habilitar la auditoría de la instrucción DROP TRIGGER va permitir el registro de todas las eliminaciones de los disparadores que contienen código para realizar validaciones o hacer cumplir restricciones críticas sobre los datos ya sean exitosas o no, ejecutadas por los usuarios independientemente de los privilegios que tienen los usuarios	1	Aplicado
121	LOGON / LOGOFF	Asegurar habilitar la auditoría de la instrucción LOGON / LOGOFF va permitir el registro de todas los inicios o cierres de sesión que realicen los usuarios independientemente de sus privilegios	1	Aplicado

Anexo 13: Lista de Cotejo Post Test de los controles de configuración de seguridad en la base de datos Oracle 19c en la instancia de base de datos "bdgpaqa" del ambiente de control de calidad de la empresa GPA Business SAC.

Escala: No aplicado = 0 – Aplicado = 1

V1.1 Actualización del software de base de datos y configuración de parámetros				
V1.1.1: Versión del parche del motor de BD				
Ítem	**Controles / Parámetros**	**Acción**	**Escala**	**Observación**
1	PATCH	Asegurar que esté aplicado el último parche generado por el fabricante para mitigar la posibilidad de vulnerabilidad en la base de datos Oracle.	1	Aplicado
V1.1.2: Configurar parámetros de listener				
2	EXTPROC	Asegurar que dicho parámetro no esté presente en el archivo listener.ora para evitar que algunas librerías del sistema operativo puedan ser invocadas por la base de datos.	1	Aplicado
3	ADMIN_RESTRICTIONS	Asegurar que ese parámetro esté presente en el archivo listener.ora para evitar que usuarios no administradores puedan alterar en tiempo real los parámetros del archivo.	1	Aplicado
V1.1.3: Configurar parámetros generales de BD				
4	AUDIT_SYS_OPERATIONS	Asegurar que se configure este parámetro con el valor de TRUE va permitir conocer las actividades realizadas por la cuenta administradora SYS. Las operaciones se registrarán en la tabla SYS.AUD$. Va a requerir reinicio de la base de datos.	1	Aplicado
5	AUDIT_TRAIL	Asegurar que se configure este parámetro con los valores de DB, EXTENDED, OS, XML, EXTENDED, DB, XML; va permitir habilitar las funciones básicas de auditoría, además de recopilar datos para solucionar problemas y valiosos registros forenses.	1	Aplicado
6	GLOBAL_NAMES	Asegurar que se configure este parámetro con el valor de TRUE va permitir conectarse remotamente a otra base de datos a través de un único nombre de enlace entre las bases de datos.	1	Aplicado
7	OS_ROLES	Asegurar que se configure este parámetro con el valor de FALSE para evitar que el sistema operativo use grupos externos para la administración de la base de datos.	1	Aplicado

8	REMOTE_LISTENER	Asegurar que se configure este parámetro con el valor NULL para evitar establecer un oyente válido en un sistema separado, a menos que estén utilizando un RAC.	1	Aplicado
9	REMOTE_LOGIN_PASSWORDFILE	Asegurar que se configure este parámetro con el valor de NONE para evitar conexiones privilegiadas no seguras a la base de datos.	1	Aplicado
10	REMOTE_OS_AUTHENT	Asegurar que se configure este parámetro con el valor de FALSE para evitar suplantación de conexiones y permita otorgar privilegios a un usuario no autorizado del sistema operativo y este pueda realizar conexiones.	1	Aplicado
11	REMOTE_OS_ROLES	Asegurar que se configure este parámetro con el valor de FALSE para evitar que usuarios del sistema operativo tengan permisos para la administración de la base de datos.	1	Aplicado
12	SEC_CASE_SENSITIVE_LOGON	Asegurar que se configure este parámetro con el valor de TRUE para aumentar el conjunto de caracteres que se pueden elegir para las contraseñas, lo que evita a los ataques de contraseña de fuerza bruta.	1	Aplicado
13	SEC_MAX_FAILED_LOGIN_ATTEMPTS	Asegurar que se configure este parámetro con el valor de 3 o menos, determina cuántos inicios de sesión fallidos se permitirán, antes de que la instancia cierre la conexión de inicio de sesión.	1	Aplicado
14	SEC_PROTOCOL_ERROR_FURTHER_ACTION	Asegurar que se configure este parámetro con el valor de (DROP,3) permitirá que se corte una conexión después de tres paquetes defectuosos o con formato incorrecto.	1	Aplicado
15	SEC_PROTOCOL_ERROR_TRACE_ACTION	Asegurar que se configure este parámetro con el valor de LOG, permite el registro de los acontecimientos que pasa en la instancia de base de datos.	1	Aplicado
16	SEC_RETURN_SERVER_RELEASE_BANNER	Asegurar que se configure este parámetro con el valor de FALSE para evitar que la base de datos devuelva información sobre el número de versión del parche aplicado.	1	Aplicado
17	SQL92_SECURITY	Asegurar que se configure este parámetro con el valor de TRUE para evitar la divulgación de información involuntaria asegurándose de que solo los usuarios que ya tienen el privilegio SELECT puedan ejecutar sentencias que les permite obtener los valores almacenados.	1	Aplicado
18	TRACE_FILES_PUBLIC	Asegurar que se configure este parámetro con el valor de FALSE para evitar que el archivo de rastreo del sistema sea legible.	1	Aplicado
19	RESOURCE_LIMIT	Asegurar que se configure este parámetro con el valor de TRUE determina si se aplican límites de recursos en los perfiles de base de datos.	1	Aplicado

V.1.2. Configuración de parámetros de conexión, acceso, usuarios y asignación y/o revocación de privilegios				
V.1.2.1. Configurar parámetros de conexión y acceso				
Ítem	**Control**	**Acción**	**Escala**	**Observación**
20	FAILED_LOGIN_ATTEMPTS	Asegurar que se configure este parámetro con el valor de 5 o menos, determina cuántos intentos fallidos de inicio de sesión se permite antes de que el sistema bloquee la cuenta del usuario.	1	Aplicado
21	PASSWORD_LOCK_TIME	Asegurar que se configure este parámetro con el valor de 1 determina cuántos días deben pasar para que la cuenta se desbloqué después de que se haya producido el número establecido de intentos fallidos en el inicio de sesión.	1	Aplicado
22	PASSWORD_LIFE_TIME	Asegurar que se configure este parámetro con el valor de 90 o menos para determinar cuánto tiempo se puede usar una contraseña antes de que el usuario pueda cambiarla.	1	Aplicado
23	PASSWORD_REUSE_MAX	Asegurar que se configure este parámetro con el valor de 20 o más, para determinar cuántas contraseñas diferentes se deben usar antes de que el usuario pueda reutilizar una contraseña anterior.	1	Aplicado
24	PASSWORD_REUSE_TIME	Asegurar que se configure este parámetro con el valor de 365 o más, para determina la cantidad de tiempo en días que debe pasar antes de que se pueda reutilizar la misma contraseña.	1	Aplicado
25	PASSWORD_GRACE_TIME	Asegurar que se configure este parámetro con el valor de 5 o menos, para determinar cuántos días puede un usuario tener una contraseña vencida, antes que la sesión del usuario se bloque automáticamente.	1	Aplicado
26	PASSWORD_VERIFY_FUNCTION	Asegurar que se configure este parámetro en todos los Profiles, para determinar las reglas de complejidad de contraseñas (casos mixtos con dígitos y caracteres especiales), bloquear las combinaciones simples y aplicar cambios a las configuraciones de historial logrando frustrar potencialmente los inicios de sesión no autorizados.	1	Aplicado
27	SESSIONS_PER_USER	Asegurar que se configure este parámetro con el valor de 10 o menos, para determinar el número máximo de sesiones de un usuario ayudando a prevenir el mal uso de recursos a nivel de memoria o ataques de denegación de servicio intencionales.	1	Aplicado
28	INACTIVE_ACCOUNT_TIME	Asegurar que se configure este parámetro con el valor de 120 o menos, para determinar el número máximo de días de inactividad (sin inicios de sesión en absoluto) después de lo cual la cuenta se bloqueará.	1	Aplicado
V.1.2.2. Configurar parámetros de usuarios				

29	Credenciales por defecto (DEFAULT PASSWORDS)	Asegurar que todas las credenciales por defecto sean modificadas, para evitar que cualquier atacante con acceso a la base de datos puede autenticarse con una cuenta predeterminada utilizando una credencial por efecto.	1	Aplicado
30	Esquemas de ejemplo (SAMPLE DATA)	Asegurar que todos los esquemas de muestra (BI o HR o IX o OE o PM o SCOTT o SH) sean removidos del ambiente de producción, para evitar que puedan ser utilizados para lanzar exploits contra el ambiente de producción.	1	Aplicado
31	DBA_USERS.AUTHENTICATION_TYPE	Asegurar que esté campo no contenga el valor de EXTERNAL, para evitar que un usuario remoto del sistema operativo pueda tener acceso a la base de datos con autorización completa.	1	Aplicado
32	Usuarios sin profile por defecto (DEFAULT PROFILE)	Asegurar que los usuarios no tengan asignado el profile por defecto (DEFAULT), debido a que cuenta con configuraciones ilimitadas que a menudo son requeridas por el usuario administrador, tales configuraciones ilimitadas deben reservarse estrictamente y no aplicarse a usuarios innecesarios.	1	Aplicado
33	SYS.USER$MIG	Asegurar que la tabla sys.user$mig sea eliminada al inicio de una migración, para evitar que su información pueda llegar hacer conocida por un atacante.	1	Aplicado
34	Enlaces públicos (PUBLIC DATABASE LINKS)	Asegurar que no exista enlaces públicos de bases de datos para evitar que cualquier usuario pueda logra una conexión a la base de datos para consultar, actualizar, insertar, eliminar datos en una base de datos remota.	1	Aplicado
V.1.2.3. Asignar y/o revocar privilegios				
35	DBMS_LDAP - UTL_INADDR	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de las tablas DBMS_LDAP y UTL_INADDR para evitar la creación de errores especialmente diseñados o él envió de información vía DNS al exterior.	1	Aplicado
36	UTL_TCP	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de la tabla UTL_TCP para evitar que usuarios no autorizados envíen datos arbitrarios desde el servidor de base de datos.	1	Aplicado
37	UTL_MAIL - UTL_SMTP	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de las tablas UTL_MAIL y UTL_SMTP para evitar que un usuario no autorizado corrompa el SMTP, función para aceptar o generar correo no deseado que puede resultar en una denegación de servicio debido a la saturación de la red	1	Aplicado

38	UTL_DBWS	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de la tabla UTL_DBWS para evitar que un usuario no autorizado corrompa el HTTP flujo utilizado para transportar los protocolos que comunican la instancia basada en la web.	1	Aplicado
39	UTL_ORAMTS - UTL_HTTP	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de las tablas UTL_ORAMTS y UTL_HTTP para evitar él envió de información (sensible) a sitios web.	1	Aplicado
40	HTTPURITYPE	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de la tabla HTTPURITYPE para evitar el filtrado de información de la base de datos a un destino externo por HTTP.	1	Aplicado
41	DBMS_ADVISOR	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de la tabla DBMS_ADVISOR para evitar que un usuario no autorizado corrompa archivos del sistema operativo o componentes fundamentales de la base de datos.	1	Aplicado
42	DBMS_LOB	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de la tabla DBMS_LOB para evitar que subprogramas puedan manipular, leer, escribir en BLOB, CLOB, NCLOB, BFILE y LOB temporales	1	Aplicado
43	UTL_FILE	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de la tabla UTL_FILE para evitar que un usuario pueda leer y escribir archivos ubicados en el servidor donde está instalada la instancia de base de datos.	1	Aplicado
44	DBMS_CRYPTO	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de la tabla DBMS_CRYPTO para evitar la ejecución de procedimientos de criptografía que puede potencialmente comprometer una porción o la totalidad de los datos.	1	Aplicado
45	DBMS_OBFUSCATION_TOOLKIT	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de la tabla DBMS_OBFUSCATION_TOOLKIT para evitar que la herramienta que determina la fuerza del algoritmo de cifrado sea utilizada para cifrar los datos de la aplicación.	1	Aplicado
46	DBMS_RANDOM	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de la tabla DBMS_RANDOM para evitar que una aplicación no autorizada genere números aleatorios.	1	Aplicado
47	DBMS_JAVA - DBMS_JAVA_TEST	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de las tablas DBMS_JAVA y DBMS_JAVA_TEST para evitar que un atacante ejecute comandos del sistema operativo desde la base de datos.	1	Aplicado

48	DBMS_JOB	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de la tabla DBMS_JOB para evitar que un usuario no autorizado inhabilite o sobrecargue la cola de trabajos.	1	Aplicado
49	DBMS_SCHEDULER	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de la tabla DBMS_SCHEDULER para evitar que un usuario no autorizado ejecute trabajos de la base de datos o del sistema operativo.	1	Aplicado
50	DBMS_SQL	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de la tabla DBMS_SQL para evitar la escalada de privilegios si no se realiza la validación de entrada adecuadamente.	1	Aplicado
51	DBMS_XMLGEN	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de la tabla DBMS_XMLGEN para evitar la búsqueda de información confidencial en toda la base de datos. Información como números de tarjetas de crédito.	1	Aplicado
52	DBMS_XMLQUERY, DBMS_XMLSAVE, DBMS_XMLSTORE, DBMS_AW, OWA_UTIL y DBMS_REDACT	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de las tablas DBMS_XMLQUERY, DBMS_XMLSAVE, DBMS_XMLSTORE, DBMS_AW, OWA_UTIL y DBMS_REDACT para evitar que usuarios malintencionados pueden aprovechar este paquete como una función de inyección auxiliar en un ataque de inyección SQL.	1	Aplicado
53	DBMS_BACKUP_RESTORE	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de la tabla DBMS_BACKUP_RESTORE para evitar el acceso a los archivos del sistema operativo.	1	Aplicado
54	DBMS_FILE_TRANSFER	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de la tabla DBMS_FILE_TRANSFER para evitar transferir archivos desde un servidor de base de datos a otro sin autorización para hacerlo.	1	Aplicado
55	DBMS_SYS_SQL	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de la tabla DBMS_SYS_SQL para evitar que un usuario ejecute código como un usuario diferente sin ingresar credenciales válidas.	1	Aplicado
56	DBMS_REPCAT_SQL_UTL, INITJVMAUX, DBMS_AQADM_SYS, DBMS_STREAMS_RPC y LTADM	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de las tablas DBMS_REPCAT_SQL_UTL, INITJVMAUX, DBMS_AQADM_SYS, DBMS_STREAMS_RPC y LTADM para evitar que un usuario no autorizado ejecute SQL comandos como un usuario SYS.	1	Aplicado
57	DBMS_PRVTAQIM	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de la tabla DBMS_PRVTAQIM para evitar que un usuario no autorizado escale privilegios por cualquier instrucción SQL y que podría ejecutarse como usuario SYS.	1	Aplicado

58	DBMS_IJOB y DBMS_PDB_EXEC_SQL	Asegurar que el privilegio EXECUTE sea revocado de PUBLIC de las tablas DBMS_IJOB y DBMS_PDB_EXEC_SQL para evitar que un atacante cambie de identidad utilizando un nombre de usuario diferente para ejecutar un trabajo de base de datos.	1	Aplicado
59	SYS.AUD$	Asegurar que usuarios no autorizados tengan privilegios sobre la tabla SYS.AUD$ para que no permita distorsión en los registros de auditoría, escondiendo actividades no autorizadas.	1	Aplicado
60	SYS.DBA_%	Asegurar que el privilegio PUBLIC sea revocado de todas las tablas sensibles del usuario SYS que sean encontradas en la vista DBA_% para evitar que usuarios no autorizados puedan manipular los datos confidenciales.	1	Aplicado
61	CDB_LOCAL_ADMINAUTH$, DEFAULT_PWD$, ENC$, HISTGRM$, HIST_HEAD$, LINK$, PDB_SYNC$, SCHEDULER$_CREDENTIAL, USER$, USER_HISTORY$ y XS$VERIFIERS	Asegurar que el privilegio ALL sea revocado de las tablas CDB_LOCAL_ADMINAUTH$, DEFAULT_PWD$, ENC$, HISTGRM$, HIST_HEAD$, LINK$, PDB_SYNC$, SCHEDULER$_CREDENTIAL, USER$, USER_HISTORY$ y XS$VERIFIERS del usuario SYS para evitar que usuarios no autorizados puedan manipular los datos sensibles y confidenciales.	1	Aplicado
62	%ANY%	Asegurar que los privilegios tipo %ANY% sean revocados de todos los objetos no autorizados de la base de dato para evitar que usuarios no autorizados puedan manipular los datos confidenciales o dañen el catálogo de datos.	1	Aplicado
63	ADMIN_OPTION	Asegurar que de la tabla DBA_SYS_PRIVS.% se revoke los privilegios no autorizados donde el campo ADMIN_OPTION sea igual a YES para evitar que los usuarios puedan otorgar sus mismos privilegios a otros usuarios.	1	Aplicado
64	EXECUTE ANY PROCEDURE	Asegurar que el privilegio EXECUTE ANY PROCEDURE sea revocado de los esquemas OUTLN y DBSNMP para evitar que tenga más privilegios de los necesarios.	1	Aplicado
65	SELECT ANY DICTIONARY	Asegurar que este privilegio sea revocado de cuentas no administrativas para evitar que un usuario no autorizado pueda recopilar información sobre la base de datos a través del diccionario de datos objetos. La información recopilada podría utilizarse potencialmente para explotar la base de datos.	1	Aplicado

66	SELECT ANY TABLE	Asegurar que este privilegio sea revocado de cuentas no administrativas para evitar que un usuario no autorizado pueda visualizar sin autorización información sensible.	1	Aplicado
67	AUDIT SYSTEM	Asegurar que este privilegio sea revocado de cuentas no administrativas para evita que un usuario no autorizado pueda alterar las actividades de auditoria programadas, como deshabilitar la creación de pistas de auditoría.	1	Aplicado
68	EXEMPT ACCESS POLICY	Asegurar que este privilegio sea revocado de cuentas no administrativas para evitar que un usuario no autorizado pueda acceder a todas las filas de una tabla independientemente de los bloqueos de seguridad a nivel de fila.	1	Aplicado
69	BECOME USER	Asegurar que este privilegio sea revocado de cuentas no administrativas para evitar que un usuario no autorizado pueda usar privilegios otorgados a otro usuario,	1	Aplicado
70	CREATE PROCEDURE	Asegurar que este privilegio sea revocado de cuentas no administrativas para evitar que un usuario no autorizado pueda crear procedimientos no autorizados que facilitan el robo de datos o la denegación de servicio al corromper las tablas de datos.	1	Aplicado
71	ALTER SYSTEM	Asegurar que este privilegio sea revocado de cuentas no administrativas para evitar que un usuario no autorizado pueda modificar las operaciones en ejecución de la instancia.	1	Aplicado
72	CREATE ANY LIBRARY y CREATE LIBRARY	Asegurar que estos privilegios sean revocados de cuentas no administrativas para evitar que un usuario no autorizado pueda crear objetos que están asociados a las bibliotecas compartidas.	1	Aplicado
73	GRANT ANY OBJECT PRIVILEGE, GRANT ANY ROLE y GRANT ANY PRIVILEGE	Asegurar que estos privilegios sean revocados de cuentas no administrativas para evitar que un usuario no autorizado pueda acceder o cambiar datos confidenciales, o dañar el catálogo de datos debido a un potencial daño al acceso de instancia.	1	Aplicado
74	SELECT_CATALOG_ROLE	Asegurar que este rol sea revocado de cuentas no administrativas para evitar que un usuario no autorizado pueda divulgar todos los datos del diccionario.	1	Aplicado
75	EXECUTE_CATALOG_ROLE	Asegurar que este rol sea revocado de cuentas no administrativas para evitar que un usuario no autorizado pueda interrumpir las operaciones mediante la inicialización de procedimientos no autorizados.	1	Aplicado

76	DBA	Asegurar que este rol sea revocado de cuentas no administrativas para evitar que un usuario no autorizado pueda generar una gran cantidad de problemas innecesarios. Este privilegio abre la puerta a violaciones de datos, violaciones de integridad y condiciones de denegación de servicio.	1	Aplicado
V.1.3 Configuración de parámetros de auditorías				
V.1.3.1 Configurar parámetros de auditoria tradicional				
77	AUDIT_OPTION = USER	Asegurar que la tabla DBA_STMT_AUDIT_OPTS contenga un registro donde el campo AUDIT_OPTION sea igual a USER va a permitir auditar todas las actividades que realicen en la base de datos.	1	Aplicado
78	AUDIT_OPTION = ROLE	Asegurar que la tabla DBA_STMT_AUDIT_OPTS contenga un registro donde el campo AUDIT_OPTION sea igual a ROLE va a permitir auditar todos los intentos, exitosos o no, de crear, descartar, modificar o establecer roles.	1	Aplicado
79	AUDIT_OPTION = SYSTEM GRANT	Asegurar que la tabla DBA_STMT_AUDIT_OPTS contenga un registro donde el campo AUDIT_OPTION sea igual a SYSTEM GRANT va a permitir auditar cualquier intento, exitoso o no, para otorgar o revocar cualquier privilegio o función del sistema, independientemente del privilegio en poder del usuario que intenta la operación.	1	Aplicado
80	AUDIT_OPTION = PROFILE	Asegurar que la tabla DBA_STMT_AUDIT_OPTS contenga un registro donde el campo AUDIT_OPTION sea igual a PROFILE va a permitir auditar todos los intentos, exitosos o no, de crear, descartar o alterar cualquier perfil.	1	Aplicado
81	AUDIT_OPTION = DATABASE LINK	Asegurar que la tabla DBA_STMT_AUDIT_OPTS contenga un registro donde el campo AUDIT_OPTION sea igual a DATABASE LINK va a permitir auditar todas las actividades en los enlaces de la base de datos.	1	Aplicado
82	AUDIT_OPTION = PUBLIC DATABASE LINK	Asegurar que la tabla DBA_STMT_AUDIT_OPTS contenga un registro donde el campo AUDIT_OPTION sea igual a PUBLIC DATABASE LINK va a permitir auditar todas las actividades del usuario que impliquen la creación, alteración o eliminación de los enlaces públicos.	1	Aplicado
83	AUDIT_OPTION = PUBLIC SYNONYM	Asegurar que la tabla DBA_STMT_AUDIT_OPTS contenga un registro donde el campo AUDIT_OPTION sea igual a PUBLIC SYNONYM va a permitir auditar todas las actividades del usuario que	1	Aplicado

		impliquen la creación, alteración o eliminación de los sinónimos públicos.		
84	AUDIT_OPTION = SYNONYM	Asegurar que la tabla DBA_STMT_AUDIT_OPTS contenga un registro donde el campo AUDIT_OPTION sea igual a SYNONYM va a permitir auditar todas las actividades del usuario que impliquen la creación, alteración o eliminación de los sinónimos públicos.	1	Aplicado
85	AUDIT_OPTION = DIRECTORY	Asegurar que la tabla DBA_STMT_AUDIT_OPTS contenga un registro donde el campo AUDIT_OPTION sea igual a DIRECTORY va a permitir auditar todas las actividades del usuario que impliquen la creación, alteración o eliminación de un directorio.	1	Aplicado
86	AUDIT_OPTION = SELECT ANY DICTIONARY	Asegurar que la tabla DBA_STMT_AUDIT_OPTS contenga un registro donde el campo AUDIT_OPTION sea igual a SELECT ANY DICTIONARY va a permitir auditar todas las actividades del usuario relacionadas con esta capacidad.	1	Aplicado
87	AUDIT_OPTION = GRANT ANY OBJECT PRIVILEGE	Asegurar que la tabla DBA_STMT_AUDIT_OPTS contenga un registro donde el campo AUDIT_OPTION sea igual a GRANT ANY OBJECT PRIVILEGE va a permitir para auditar todas las actividades del usuario relacionadas con otorgar o revocar cualquier privilegio de objeto, que incluye privilegios sobre tablas, directorios, modelos de minería.	1	Aplicado
88	AUDIT_OPTION = GRANT ANY PRIVILEGE	Asegurar que la tabla DBA_STMT_AUDIT_OPTS contenga un registro donde el campo AUDIT_OPTION sea igual a GRANT ANY PRIVILEGE va a permitir auditar todas las actividades del usuario administrador relacionadas con cambiar la seguridad infraestructura, para eliminar, agregar, modificar usuarios y más.	1	Aplicado
89	AUDIT_OPTION = DROP ANY PROCEDURE	Asegurar que la tabla DBA_STMT_AUDIT_OPTS contenga un registro donde el campo AUDIT_OPTION sea igual a DROP ANY PROCEDURE va a permitir auditar todas las actividades del usuario que impliquen la eliminación de procedimientos.	1	Aplicado
90	SYS.AUD$	Asegurar que el privilegio ALL este habilitado en la tabla SYS.AUD$ va proporcionar pruebas forenses desde el inicio de actividades no autorizadas.	1	Aplicado
91	AUDIT_OPTION = PROCEDURE	Asegurar que la tabla DBA_STMT_AUDIT_OPTS contenga un registro donde el campo AUDIT_OPTION sea igual a PROCEDURE va a permitir auditar todas las actividades del usuario que impliquen la creación, alteración o eliminación de un procedimiento.	1	Aplicado

92	AUDIT_OPTION = ALTER SYSTEM	Asegurar que la tabla DBA_STMT_AUDIT_OPTS contenga un registro donde el campo AUDIT_OPTION sea igual a ALTER SYSTEM va permitir auditar cualquier intento no autorizado de alterar el sistema, estos registros pueden ser muy útiles.	1	Aplicado
93	AUDIT_OPTION = TRIGGER	Asegurar que la tabla DBA_STMT_AUDIT_OPTS contenga un registro donde el campo AUDIT_OPTION sea igual a TRIGGER va a permitir auditar todas las actividades del usuario que impliquen la creación, alteración o eliminación de un trigger.	1	Aplicado
94	AUDIT_OPTION = CREATE SESSION	Asegurar que la tabla DBA_STMT_AUDIT_OPTS contenga un registro donde el campo AUDIT_OPTION sea igual a CREATE SESSION va a permitir auditar todos los intentos de conexión a la base de datos, ya sea con éxito o no, así como las desconexiones/cierres de sesión de auditoría.	1	Aplicado
V.1.3.2 Configurar parámetros de auditoría unificada				
95	CREATE USER	Asegurar habilitar la auditoría de la instrucción CREATE USER va permitir el registro de todas las creaciones de cuentas ya sean exitosas o no, emitidas por los usuarios independientemente de los privilegios que tienen los usuarios.	1	Aplicado
96	ALTER USER	Asegurar habilitar la auditoría de la instrucción ALTER USER va permitir el registro de todos los cambios de contraseña, bloqueo de cuentas. También va registrar los cambios de propiedades de los usuarios, Profiles, tablespaces por defecto o temporales y las cuotas de espacio en los tablespaces ya sean exitosas o no, emitidas por los usuarios independientemente de los privilegios que tienen los usuarios.	1	Aplicado
97	DROP USER	Asegurar habilitar la auditoría de la instrucción DROP USER va permitir el registro de todas las eliminaciones de cuentas o esquemas de la base de datos ya sean exitosas o no, emitidas por los usuarios independientemente de los privilegios que tienen los usuarios.	1	Aplicado
98	CREATE ROLE	Asegurar habilitar la auditoría de la instrucción CREATE ROLE va permitir el registro de todas las creaciones de colecciones de privilegios de sistema, privilegios de objetos que se otorgan a los usuarios o a otros roles ya sean exitosas o no, emitidas por los usuarios independientemente de los privilegios que tienen los usuarios.	1	Aplicado

99	ALTER ROLE	Asegurar habilitar la auditoría de la instrucción ALTER ROLE va permitir el registro de todos los movimientos que se realizan en la colección de privilegios de sistema, privilegios de objetos que se otorgan a los usuarios o a otros roles ya sean exitosas o no, emitidas por los usuarios independientemente de los privilegios que tienen los usuarios.	1	Aplicado
100	DROP ROLE	Asegurar habilitar la auditoría de la instrucción DROP ROLE va permitir el registro de todas las eliminaciones de colecciones de privilegios de sistema, privilegios de objetos que se otorgan a los usuarios o a otros roles ya sean exitosas o no, emitidas por los usuarios independientemente de los privilegios que tienen los usuarios.	1	Aplicado
101	GRANT	Asegurar habilitar la auditoría de la instrucción GRANT va permitir el registro de todas las otorgaciones de privilegios a los usuarios o a otros roles ya sean exitosas o no, emitidas por los usuarios independientemente de los privilegios que tienen los usuarios	1	Aplicado
102	REVOKE	Asegurar habilitar la auditoría de la instrucción REVOKE va permitir el registro de todas las revocatorias de privilegios a los usuarios o a otros roles ya sean exitosas o no, emitidas por los usuarios independientemente de los privilegios que tienen los usuarios	1	Aplicado
103	CREATE PROFILE	Asegurar habilitar la auditoría de la instrucción CREATE PROFILE va permitir el registro de todas las creaciones de políticas de contraseñas, como reglas de complejidad de contraseñas, restricciones de reutilización y límites de uso de recursos ya sean exitosas o no, emitidas por los usuarios independientemente de los privilegios que tienen los usuarios.	1	Aplicado
104	ALTER PROFILE	Asegurar habilitar la auditoría de la instrucción ALTER PROFILE va permitir el registro de todas las modificaciones de políticas de contraseñas, como reglas de complejidad de contraseñas, restricciones de reutilización y límites de uso de recursos ya sean exitosas o no, emitidas por los usuarios independientemente de los privilegios que tienen los usuarios.	1	Aplicado
105	DROP PROFILE	Asegurar habilitar la auditoría de la instrucción DROP PROFILE va permitir el registro de todas las modificaciones de políticas de contraseñas, como reglas de complejidad de contraseñas, restricciones de reutilización y límites de uso de recursos ya sean	1	Aplicado

		exitosas o no, emitidas por los usuarios independientemente de los privilegios que tienen los usuarios		
106	CREATE DATABASE LINK	Asegurar habilitar la auditoría de la instrucción CREATE DATABASE LINK va permitir el registro de todas las creaciones de los enlaces para establecer conexiones de base de datos a base de datos, estas conexiones están disponibles sin autenticación ya sean exitosas o no, emitidas por los usuarios independientemente de los privilegios que tienen los usuarios.	1	Aplicado
107	ALTER DATABASE LINK	Asegurar habilitar la auditoría de la instrucción ALTER DATABASE LINK va permitir el registro de todas las modificaciones de los enlaces para establecer conexiones de base de datos a base de datos, estas conexiones están disponibles sin autenticación ya sean exitosas o no, emitidas por los usuarios independientemente de los privilegios que tienen los usuarios	1	Aplicado
108	DROP DATABASE LINK	Asegurar habilitar la auditoría de la instrucción ALTER DATABASE LINK va permitir el registro de todas las eliminaciones de los enlaces para establecer conexiones de base de datos a base de datos, estas conexiones están disponibles sin autenticación ya sean exitosas o no, emitidas por los usuarios independientemente de los privilegios que tienen los usuarios	1	Aplicado
109	CREATE SYNONYM	Asegurar habilitar la auditoría de la instrucción CREATE SYNONYM va permitir el registro de todas las creaciones de un nombre alternativo para un objeto de base de datos como tabla, vista, procedimiento, objeto java o incluso otro sinónimo ya sean exitosas o no, emitidas por los usuarios independientemente de los privilegios que tienen los usuarios.	1	Aplicado
110	ALTER SYNONYM	Asegurar habilitar la auditoría de la instrucción ALTER SYNONYM va permitir el registro de todas las modificaciones de un nombre alternativo para un objeto de base de datos como tabla, vista, procedimiento, objeto java o incluso otro sinónimo ya sean exitosas o no, emitidas por los usuarios independientemente de los privilegios que tienen los usuarios	1	Aplicado
111	DROP SYNONYM	Asegurar habilitar la auditoría de la instrucción DROP SYNONYM va permitir el registro de todas las eliminaciones de un nombre alternativo para un objeto de base de datos como tabla, vista, procedimiento, objeto java o incluso otro sinónimo ya sean exitosas o no, emitidas por	1	Aplicado

		los usuarios independientemente de los privilegios que tienen los usuarios		
112	SELECT ANY DICTIONARY	Asegurar habilitar la auditoría de la instrucción SELECT ANY DICTIONARY va permitir el registro de todas las acciones que realizan los usuarios cuando vean la definición de los objetos de esquemas, de los objetos del diccionario de datos, incluido en vistas DBA_, vistas V$, vistas X$ y tablas SYS subyacentes como TAB$ y OBJ	1	Aplicado
113	AUDSYS.AUD$UNIFIED	Asegurar habilitar la auditoría de la instrucción AUDSYS.AUD$UNIFIED va permitir el registro de todos los intentos de acceso a AUDSYS.AUD$UNIFIED, ya sea con éxito o sin éxito, independientemente de los privilegios que tengan los usuarios para emitir dichas declaraciones	1	Aplicado
114	CREATE PROCEDURE /FUNCTION / PACKAGE / PACKAGE BODY	Asegurar habilitar la auditoría de las instrucciones CREATE PROCEDURE / FUNCTION / PACKAGE / PACKAGE BODY va permitir el registro de todas las creaciones de estas instrucciones comerciales que se encuentran definido por código PL/SQL y sentencias SQL contenidas dentro de estos objetos, ya sean instrucciones satisfactorias o no satisfactorias emitidos por los usuarios independientemente de los privilegios que tengan los usuarios para emitir tales declaraciones	1	Aplicado
115	ALTER PROCEDURE / FUNCTION / PACKAGE / PACKAGE BODY	Asegurar habilitar la auditoría de las instrucciones ALTER PROCEDURE / FUNCTION / PACKAGE / PACKAGE BODY va permitir el registro de todas las modificaciones de estas instrucciones comerciales que se encuentran definido por código PL/SQL y sentencias SQL contenidas dentro de estos objetos, ya sean instrucciones satisfactorias o no satisfactorias emitidos por los usuarios independientemente de los privilegios que tengan los usuarios para emitir tales declaraciones	1	Aplicado
116	DROP PROCEDURE / FUNCTION / PACKAGE / PACKAGE BODY	Asegurar habilitar la auditoría de las instrucciones DROP PROCEDURE / FUNCTION / PACKAGE / PACKAGE BODY va permitir el registro de todas las eliminaciones de estas instrucciones comerciales que se encuentran definido por código PL/SQL y sentencias SQL contenidas dentro de estos objetos, ya sean instrucciones satisfactorias o no satisfactorias emitidos por los usuarios independientemente de los privilegios que tengan los usuarios para emitir tales declaraciones	1	Aplicado

117	ALTER SYSTEM	Asegurar habilitar la auditoría de la instrucción ALTER SYSTEM va permitir el registro de todas las modificaciones al cambiar la configuración de la instancia que podría afectar la postura de seguridad, rendimiento o funcionamiento normal de la base de datos. Además, se registrarán la ejecución de los comandos de sistema operativo, ya sean exitosas o no, realizadas por los usuarios independientemente de sus privilegios.	1	Aplicado
118	CREATE TRIGGER	Asegurar habilitar la auditoría de la instrucción CREATE TRIGGER va permitir el registro de todas las creaciones de los disparadores que contienen código para realizar validaciones o hacer cumplir restricciones críticas sobre los datos ya sean exitosas o no, ejecutadas por los usuarios independientemente de los privilegios que tienen los usuarios.	1	Aplicado
119	ALTER TRIGGER	Asegurar habilitar la auditoría de la instrucción ALTER TRIGGER va permitir el registro de todas las modificaciones de los disparadores que contienen código para realizar validaciones o hacer cumplir restricciones críticas sobre los datos ya sean exitosas o no, ejecutadas por los usuarios independientemente de los privilegios que tienen los usuarios	1	Aplicado
120	DROP TRIGGER	Asegurar habilitar la auditoría de la instrucción DROP TRIGGER va permitir el registro de todas las eliminaciones de los disparadores que contienen código para realizar validaciones o hacer cumplir restricciones críticas sobre los datos ya sean exitosas o no, ejecutadas por los usuarios independientemente de los privilegios que tienen los usuarios	1	Aplicado
121	LOGON / LOGOFF	Asegurar habilitar la auditoría de la instrucción LOGON / LOGOFF va permitir el registro de todas los inicios o cierres de sesión que realicen los usuarios independientemente de sus privilegios	1	Aplicado