Título: Articulo PIA-02

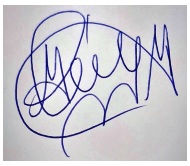
Autor: Juan Gabriel Alfaro Orias

Universidad Cenfotec

Curso: PIA-02

TRIBUNAL EXAMINADOR

Este proyecto fue aprobado por el Tribunal Examinador de la carrera: **Maestría Profesional en Ciberseguridad,** requisito para optar por el título de grado de **Maestría,** para el estudiante: **Alfaro Orias Juan Gabriel.**



Digitally signed by MIGUEL PEREZ MONTERO (FIRMA)
Date: 2024.02.27 11:13:34 -06'00'

M.Sc. Miguel Pérez Montero
Tutor

JASON ULLOA HERNANDEZ (FIRMA)

Firmado digitalmente por JASON ULLOA HERNANDEZ (FIRMA)
Fecha: 2024.02.27 07:46:12 -06'00'

M.Sc. Jason Ulloa Hernández
Lector 1

JORGE ARTURO GARNIER ROVIRA (FIRMA)

Firmado digitalmente por JORGE ARTURO GARNIER ROVIRA (FIRMA)
Fecha: 2024.02.26 19:46:45 -06'00'

MBD. Jorge Arturo Garnier Rovira
Lector 2

Firmado digitalmente por JUAN GABRIEL ALFARO ORIAS (FIRMA)
Fecha: 2024.02.27 12:44:11 -06'00'

San José, Costa Rica, 26 de febrero de 2024

Firmada digitalmente, de conformidad con la Ley de Certificados, Firmas Digitales y Documentos Electrónicos N° 8454, destacando el artículo 9°-

GUIA PARA REFORZAR LA CONFIDENCIALIDAD DE LA INFORMACION ALMACENADA EN LAS BASES DE DATOS ORACLE POR MEDIO DE CRIPTOGRAFIA.

Juan Gabriel Alfaro Orias[1]

[1]Universidad CENFOTEC, San José, Costa Rica

e-mail: jalfaroo@ucenfotec.ac.cr

ABSTRACT. Este artículo proporciona un análisis detallado sobre la falta de encriptación en las bases de datos costarricenses, subrayando la vulnerabilidad del país ante los ataques cibernéticos recientes que comprometieron la seguridad de la información. La innovación radica en la presentación de soluciones concretas y minuciosas para implementar sistemas de encriptación sólidos en bases de datos Oracle, ofreciendo respuestas prácticas a un problema urgente en el ámbito de la seguridad informática. Esta propuesta no solo es un llamado a la acción, sino que se erige como una guía integral que detalla la implementación de estrategias específicas para proteger la información sensible de ciudadanos y empresas.

El valor de este artículo reside en su enfoque práctico y detallado, proporcionando directrices claras sobre la implementación de sistemas de encriptación en un contexto donde la seguridad de los datos es crucial. Al ofrecer soluciones tangibles y estrategias específicas, este recurso se convierte en un material esencial para aquellos que buscan comprender y abordar la problemática de la seguridad de la información en un entorno digital cada vez más amenazante en términos de ciberseguridad.

PALABRAS CLAVE*:* Oracle Transparent Data Encryption (TDE), RMAN, Oracle Wallet, Data Masking, Firewall SQL.

INTRODUCCIÓN

En la actualidad digital, la seguridad de la información se ha convertido en una prioridad crucial en todos los ámbitos. Costa Rica se ha enfrentado a desafíos sustanciales en la protección de datos y la ciberseguridad, especialmente a través de su confrontación con eventos como el robo y secuestro de información perpetrado por grupos como Conti durante el año 2022. Es esencial comprender la necesidad de establecer medidas de seguridad sólidas, como la encriptación de datos en reposo, para proteger la información confidencial. Aunque algunas empresas pueden ya estar empleando esta técnica, es vital realizar revisiones periódicas de las políticas de seguridad para asegurar la aplicación efectiva de las mejores prácticas, especialmente dada la prevalencia del uso de bases de datos Oracle en nuestra región. Este enfoque garantizará una defensa adecuada contra posibles vulnerabilidades de seguridad y reducirá los riesgos relacionados con accesos no autorizados a los datos.

Los ataques cibernéticos en Costa Rica, ejecutados por grupos como Conti y Hive, han tenido graves consecuencias, incluyendo el robo y secuestro de información de gran valor. Estos grupos han empleado ransomware como método para cifrar datos y exigir rescates a cambio de su liberación. Este escenario ha provocado una significativa inquietud y ha impactado negativamente a algunas empresas e instituciones estatales.

La seguridad de la información en Costa Rica ha experimentado un impacto significativo debido a estos eventos, lo cual ha suscitado una mayor conciencia y acciones para prevenir futuros ataques. En respuesta a los desafíos de seguridad planteados por estos incidentes, el encriptamiento de datos en reposo ha surgido como una medida crucial para proteger la información almacenada en bases de datos. Esta técnica implica la aplicación de algoritmos de cifrado a los datos mientras permanecen en reposo, ya sea en dispositivos de almacenamiento físico o en otros medios digitales. El propósito es asegurar que, incluso si alguien logra acceder físicamente a los medios de almacenamiento, los datos permanezcan ilegibles sin la clave de cifrado correspondiente.

Es fundamental mantener una sólida solución de cifrado de datos en reposo en las bases de datos para mitigar eventos similares provocados por estos grupos cibercriminales. Al implementar el cifrado, se establece una barrera adicional que protege la confidencialidad e integridad de los datos almacenados.

La criptografía de datos en bases de datos ofrece diversos beneficios: no solo previene el acceso no autorizado a información sensible, sino que también asegura el cumplimiento de regulaciones como el Reglamento General de Protección de Datos (GDPR) y leyes locales de privacidad.

La criptografía, aplicada en el cifrado de datos tanto en reposo como en tránsito, desempeña un papel crítico en la salvaguarda de la integridad de la información alojada en las bases de datos Oracle. Al utilizar algoritmos criptográficos seguros, los datos se convierten en una forma ilegible para aquellos que carecen de la clave de cifrado correspondiente.

La criptografía, aplicada en firmas digitales, garantiza la integridad de la información al detectar cualquier intento de modificar los datos firmados. Cualquier alteración en la información respaldada por una firma digital, mediante cifrado asimétrico, provoca resultados incorrectos durante el proceso de validación, indicando así una modificación no autorizada. Así mismo, la información encriptada garantiza la confidencialidad de la información, dado que esta no puede ser interpretada por un atacante, lo cual contribuye también a añadir una capa de seguridad adicional, que asegura, razonablemente, que los datos almacenados permanecen intactos y sin modificaciones no autorizadas.

Finalmente, los incidentes de robo y secuestro de información en Costa Rica subrayan la importancia de implementar medidas sólidas de seguridad, incluyendo el encriptamiento de datos en reposo y en tránsito. Esta solución proporciona una capa adicional de protección, asegurando la confidencialidad, integridad y disponibilidad

de los datos almacenados, preservando la ilegibilidad de los datos para personas no autorizadas a través de la criptografía. plataformas.

MÉTODO

El método seguido en esta investigación se centró en un análisis exhaustivo de algunos métodos criptográficos empleados en bases de datos relacionales, abordando la carencia de cifrado en datos en reposo y los sistemas operativos que albergan estos motores de bases de datos. Se empleó un enfoque combinado descriptivo y cualitativo respaldado por una profunda revisión documental y un análisis de contenido de fuentes especializadas.

El objeto de estudio se focalizó en evaluar y proponer soluciones concretas para mejorar la seguridad en bases de datos que carecían de métodos de cifrado. La revisión documental se realizó mediante fuentes altamente especializadas, principalmente el Oracle Database Security Guide y el Oracle Database Advanced Security Administrator's Guide, adquiridos de la IEEE Digital Library y Google Scholar. Estos recursos ofrecieron una visión detallada de estándares de seguridad, mejores prácticas y soluciones de encriptación aplicables a estos entornos.

Se realizó un análisis minucioso de seis artículos, tres de la IEEE y tres obtenidos de Google Scholar. Estos documentos permitieron comparaciones detalladas y evaluaciones en profundidad de soluciones criptográficas, evaluaciones de bases de datos Oracle y almacenamiento tanto de datos estructurados como no estructurados.

Para la recopilación de datos, se priorizó la revisión documental con el objetivo de respaldar las hipótesis planteadas y cumplir con los objetivos establecidos. La revisión de contenido se centró en examinar normativas, metodologías y buenas prácticas sugeridas por Oracle. Se identificaron herramientas fundamentales como Oracle Wallet, Oracle Transparent Data Encryption y Oracle Advanced Security.

El análisis de información se llevó a cabo mediante una revisión de contenido detallada y la categorización de datos, estableciendo criterios de evaluación claros y precisos. Se buscó comprender la interrelación de elementos en el desarrollo tecnológico, extrayendo conclusiones cruciales para la propuesta de solución.

En síntesis, la investigación se centró en métodos criptográficos aplicados en bases de datos relacionales, haciendo uso de fuentes de alta calidad obtenidas de la IEEE y Google Scholar. La revisión documental y el análisis de contenido permitieron identificar prácticas recomendadas y soluciones fundamentales propuestas por Oracle, todas orientadas a reforzar la seguridad de datos en reposo y prevenir ataques como el ransomware y el secuestro de información.

RESULTADOS

La presente sección es una guía exhaustiva y detallada que aborda seis objetivos fundamentales para fortalecer la seguridad en las bases de datos Oracle. Desde la creación del Oracle Wallet hasta la implementación del firewall nativo de SQL, cada objetivo se sumerge en aspectos críticos de seguridad. Se comienza explicando

meticulosamente cómo crear y gestionar el Oracle Wallet, abarcando desde la generación de la master key hasta las políticas recomendadas para su administración efectiva. Luego, se profundiza en el enmascaramiento de datos mediante Oracle Data Masking, proporcionando no solo técnicas prácticas, sino también una orientación sobre políticas específicas de encriptación y protección de información sensible.

Después, se detalla la encriptación de respaldos con RMAN, ofreciendo pautas precisas para establecer contraseñas robustas y políticas de gestión efectivas. A continuación, se adentra en la administración de accesos y roles en la base de datos, brindando directrices claras para definir roles específicos, implementar mecanismos de autenticación y realizar auditorías periódicas. Además, se explora el cifrado a nivel del sistema operativo con LUKS y GPG, asegurando la protección de archivos sensibles y scripts relevantes. Finalmente, se culmina con la implementación del firewall nativo de SQL, estableciendo un escudo de seguridad para controlar el flujo de datos y prevenir posibles amenazas. Esta guía integral es una herramienta invaluable para garantizar la seguridad, la confidencialidad de datos y el cumplimiento normativo en entornos Oracle.

Objetivo 1: Configuración Oracle Wallet

La configuración del Oracle Wallet supone un pilar fundamental en términos de ciberseguridad al ofrecer un entorno altamente protegido para almacenar contraseñas y datos confidenciales de usuarios. La creación de una clave maestra y su asociación con el Wallet aseguran un cifrado robusto de las credenciales, reduciendo significativamente las vulnerabilidades relacionadas con el acceso no autorizado a la base de datos. Este enfoque técnico proporciona un nivel adicional de seguridad al emplear métodos de cifrados avanzados, lo que no solo salvaguarda las contraseñas, sino que también minimiza las posibilidades de exposición de información sensible.

En el contexto de la protección de la base de datos, la configuración del Oracle Wallet constituye una barrera esencial frente a posibles intrusiones. Al controlar el acceso y almacenar las contraseñas de manera encriptada, se mitigan riesgos inherentes a la seguridad, como la suplantación de identidad o el acceso no autorizado. La utilización de esta tecnología fortalece la infraestructura de seguridad de la base de datos al ofrecer un método seguro y eficaz para la gestión de credenciales, lo que conlleva a una reducción significativa de potenciales amenazas cibernéticas y salvaguarda la integridad de la información crítica almacenada en la base de datos.

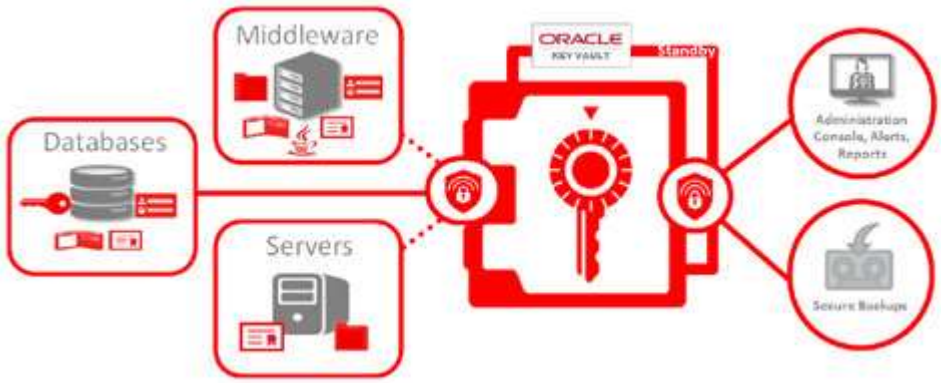


Imagen 1. Oracle Wallet

Guía de configuración:

https://zenodo.org/records/10184434?token=eyJhbGciOiJIUzUxMiJ9.eyJpZCI6IjcyMTNlOTI0LThlNWYtNDIzOC1hMTgzLWI2NTFjY2M3ODZmNSIsImRhdGEiOnt9LCJyYW5kb20iOiJmZDdlNmUwZDhlYmUxOWJiN2RkYjY1YmZlZDY5OTIwNCJ9.ZDGVGEj3bxh4VtZy8aMAdNpLtL0pjYqC2_OeWPzluLpM0pbUvAdZ7xtYGocre-fwYye7Cw60-zRI6AgTcIqy0A

Objetivo 2: Oracle Data Masking y Oracle Transparent Data Encryption (TDE)

La confección de una guía para encriptar datos en reposo con Oracle Data Masking supone un aporte significativo en términos de protección de datos sensibles. Esta herramienta permite aplicar técnicas avanzadas de enmascaramiento, como sustitución, generación aleatoria y sustitución mediante lookup, para salvaguardar información confidencial como números de seguridad social o datos financieros. Al documentar la utilización de Oracle Data Masking, se establecen políticas y procedimientos detallados para identificar y enmascarar datos sensibles, añadiendo una capa adicional de seguridad a la base de datos y asegurando que la información solo sea accesible por usuarios autorizados.

En el análisis de contenido, se profundiza en la instalación, configuración y definición de perfiles de enmascaramiento, destacando la relevancia de identificar exhaustivamente los datos sensibles presentes en la base de datos. Además, se establecen políticas claras de enmascaramiento, categorizando los datos sensibles y definiendo reglas específicas para cada categoría, lo que permite un control preciso sobre el acceso y modificación de las políticas de enmascaramiento. Asimismo, se aborda la implementación del encriptado de datos en reposo mediante métodos como Transparent Data Encryption (TDE), detallando los requisitos de configuración, la gestión de claves y la importancia de la supervisión y auditoría continua para garantizar la integridad y seguridad de los datos en todo momento. Esta guía técnica ofrece un procedimiento para fortalecer la protección de datos sensibles y minimizar riesgos de acceso no autorizado a la información almacenada en la base de datos.

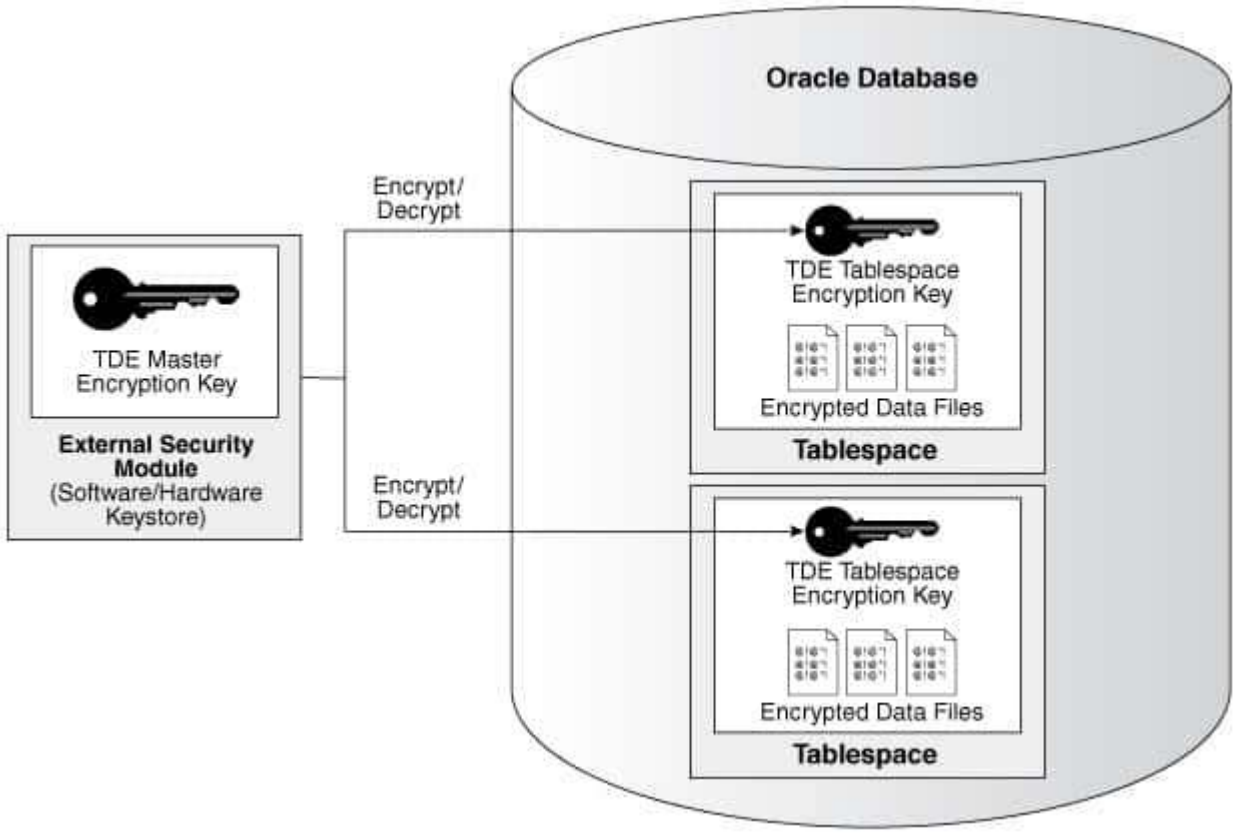


Imagen 3. Transparent Data Encryption (TDE)

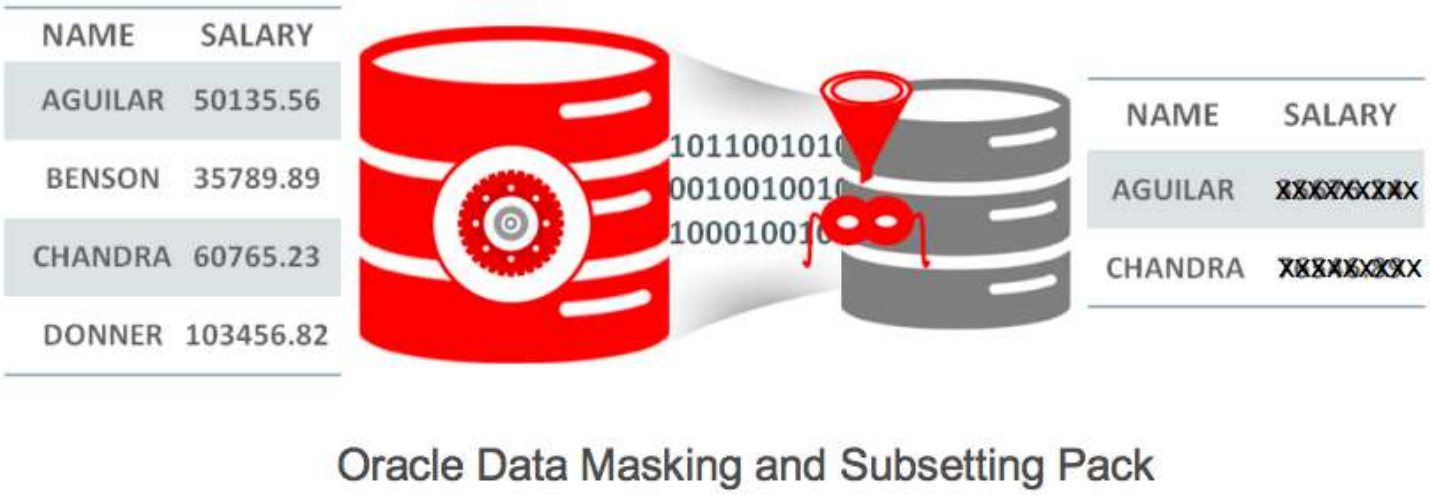


Imagen 2. Oracle Data Masking

Guía de configuración:

https://zenodo.org/records/10205696?token=eyJhbGciOiJIUzUxMiJ9.eyJpZCI6Ijg0NzNlMWNkLWRjYmMtNDQ1My1hNzU4LWQyZmQxNzIxODk1NiIsImRhdGEiOnt9LenctyCJyYW5kb20iOiIyZmE1N2Q5MDcwNzk4ZTUzMmEwY2RiZTFkM2E0NWNhMCJ9.2og6_eFJUtjaiO7ZgPvbwhoOtdUPmCp91J7jlQvelYW8zMCrCqWOeThungP8jEAevh8gnWuEQuNWj6IaINwt5Q

Objetivo 3: RMAN Backups Encrypted

Se enfoca en la construcción de una guía detallada para encriptar respaldos de bases de datos utilizando RMAN (Recovery Manager) con contraseñas. Esta guía busca establecer contraseñas sólidas para cifrar los respaldos de la base de datos, asegurando un acceso restringido y exclusivo para usuarios autorizados. Al emplear RMAN para realizar respaldos y configurar contraseñas seguras para encriptarlos, se prioriza la seguridad de la información respaldada, reduciendo el riesgo de accesos no autorizados.

Este instructivo técnico abarca la configuración y el uso de RMAN, verificando su instalación y familiarizándose con sus comandos y opciones. Se centra en la selección de algoritmos de encriptación adecuados y establece políticas para definir contraseñas robustas, además de indicar procedimientos para el cambio periódico de contraseñas. Además, se hace hincapié en la importancia de políticas de acceso y autorización, así como en la implementación de auditorías y controles de seguridad para proteger las contraseñas de encriptación y detectar posibles brechas de seguridad. Estos pasos de configuración tecnica se convierten en un recurso esencial para salvaguardar los respaldos de la base de datos y garantizar la integridad y confidencialidad de la información almacenada.

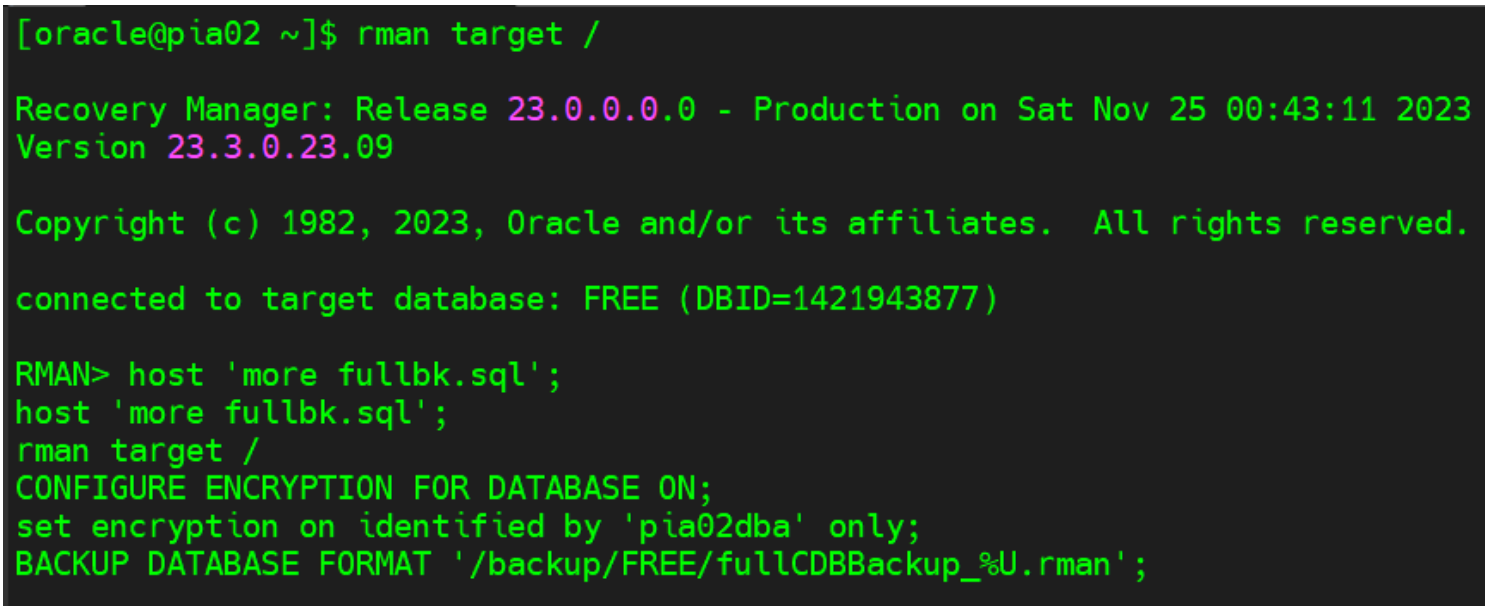


Imagen 4. RMAN Full Backup Cifrado

Guía de configuración:
https://zenodo.org/records/10205714?token=eyJhbGciOiJIUzUxMiJ9.eyJpZCI6IjFjMzI2NjJiLWMyNjQtNGQ3Yy1iOWMzLTk4YjJkOGE4MzNmZiIsImRhdGEiOnt9LCJyYW5kb20iOiI2NmVlZjFmZjVkYjcxZjk1ZGE1ZjJiOGNkYzA0YWU2OSJ9.rCtUTC4Dl1-0s17TrfaTd2Y-R135ar1B8iqLeJ6kSHJXp0r1rUK4kYdV1S-mBHnJl7pW9ww2SARCJfIv6DgUnQ

Objetivo 4: Auditoria de Base de datos (accesos, roles, privilegios, política de contraseñas seguras)

Las instrucciones tienen la función de establecer y gestionar el acceso a la información en reposo a través de roles, privilegios y mecanismos de autenticación en la base de datos. Al definir roles específicos y asignar permisos de manera adecuada, se busca controlar y limitar el acceso a la información, asegurando que los usuarios solo dispongan de los datos necesarios para sus tareas. Además, se prioriza la implementación de políticas robustas de autenticación y autorización para prevenir accesos no autorizados y garantizar la seguridad de la información almacenada.

La guía aborda la identificación de roles y privilegios necesarios, considerando requisitos normativos y de seguridad de la organización. Se enfoca en asignar permisos a usuarios y roles, alineados con sus responsabilidades y necesidades de acceso. Asimismo, establece políticas de contraseñas seguras y configura la autorización en la base de datos para definir reglas de acceso específicas.

Además, se hace énfasis en la implementación de auditorías y monitoreo constante para registrar actividades de acceso y detectar comportamientos sospechosos. Este enfoque proactivo se completa con la revisión periódica de accesos, roles y privilegios para mantener la adecuación con las necesidades de seguridad, desactivando cuentas innecesarias y manteniendo un ambiente seguro y controlado en la gestión de la información en reposo.

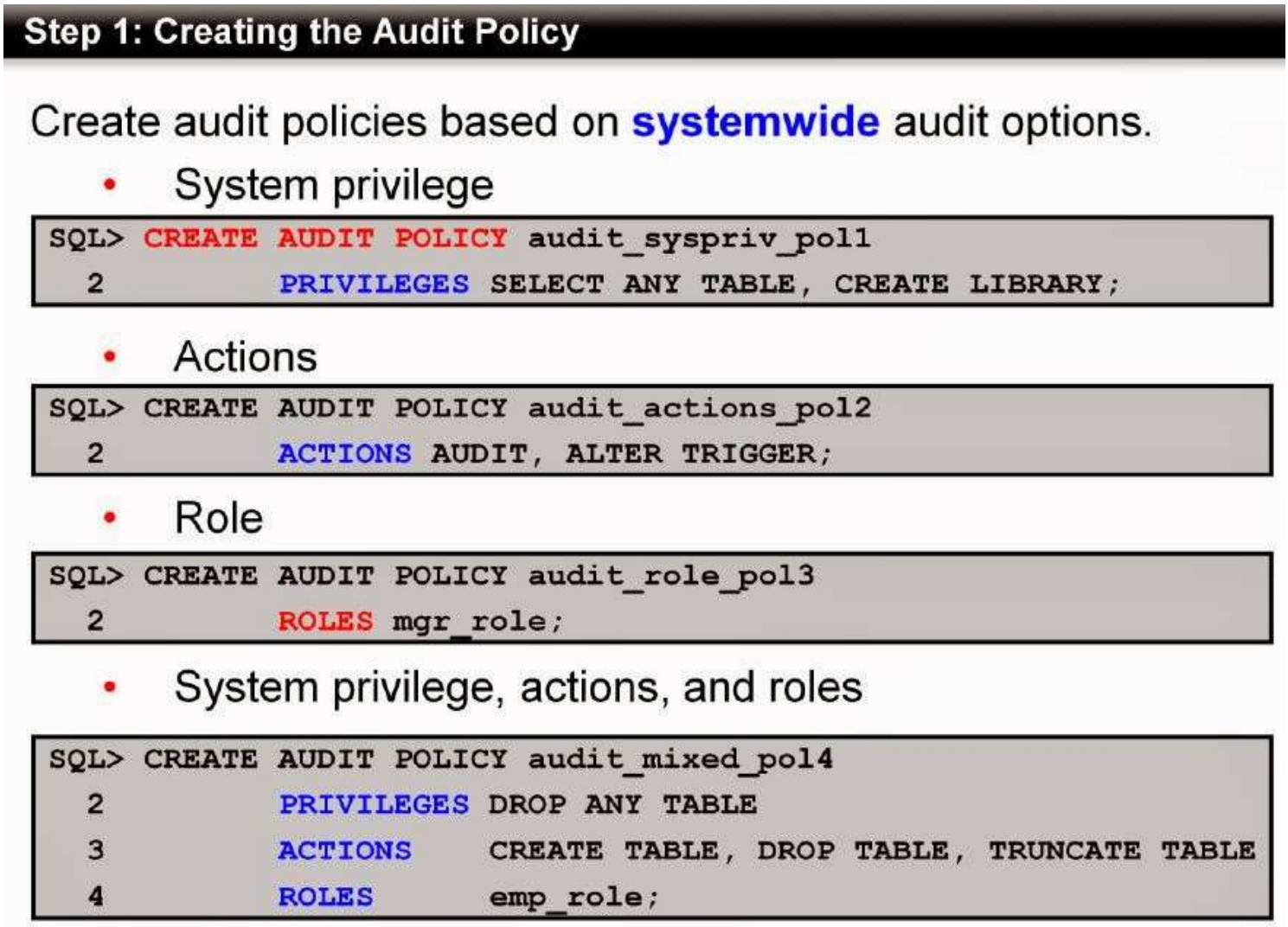


Imagen 5. Política de auditoria

Guía de configuración:

https://zenodo.org/records/10205721?token=eyJhbGciOiJIUzUxMiJ9.eyJpZCI6IjgwZjI4NGJhLThlMTgtNGQ5NS1iZmQ0LTVhYTQ0MzBiZGU2NSIsImRhdGEiOnt9LCJyYW5kb20iOiIzOWE0ODNkNGE1MTRhODU1ZThlOGM2YTcyNzNmMzkyNCJ9.RFWrzfn-1rOMTpivFYA29enY4KJc6Pawr8XqgBSWNlFTV69owjjvKjgWaWjpwiQhk95PSivvEFSlKY5dX9P-zw

Objetivo 5: LUKS y GPG para encriptamiento de sistemas de archivos, particiones de discos y scripts a nivel de OS.

Se enfoca en la implementación de LUKS y GPG para cifrar sistemas de archivos, particiones, discos y scripts a nivel del sistema operativo. Al emplear LUKS para el cifrado de sistemas y GPG para proteger datos sensibles en scripts y archivos, se asegura la confidencialidad de la información, fortaleciendo así la seguridad. Ofrece una visión integral, desde la verificación de compatibilidad y la identificación de elementos a cifrar hasta la generación

de contenedores seguros con LUKS, estableciendo contraseñas y configuraciones óptimas para el desbloqueo automático durante el inicio del sistema.

Además, detalla procesos para GPG, como la creación de pares de claves para el cifrado y descifrado de datos relevantes. Proporciona instrucciones claras sobre la gestión segura de claves privadas, cifrado de datos sensibles y configuración del sistema para un cifrado y descifrado efectivos. Destaca la importancia de políticas de mantenimiento y gestión, incluyendo el cambio regular de contraseñas y la implementación de medidas de respaldo para garantizar la recuperación en situaciones adversas. Finalmente, hace hincapié en pruebas exhaustivas y auditorías para verificar la correcta implementación del cifrado y detectar posibles intentos de acceso no autorizado o violaciones de seguridad relacionadas con este.

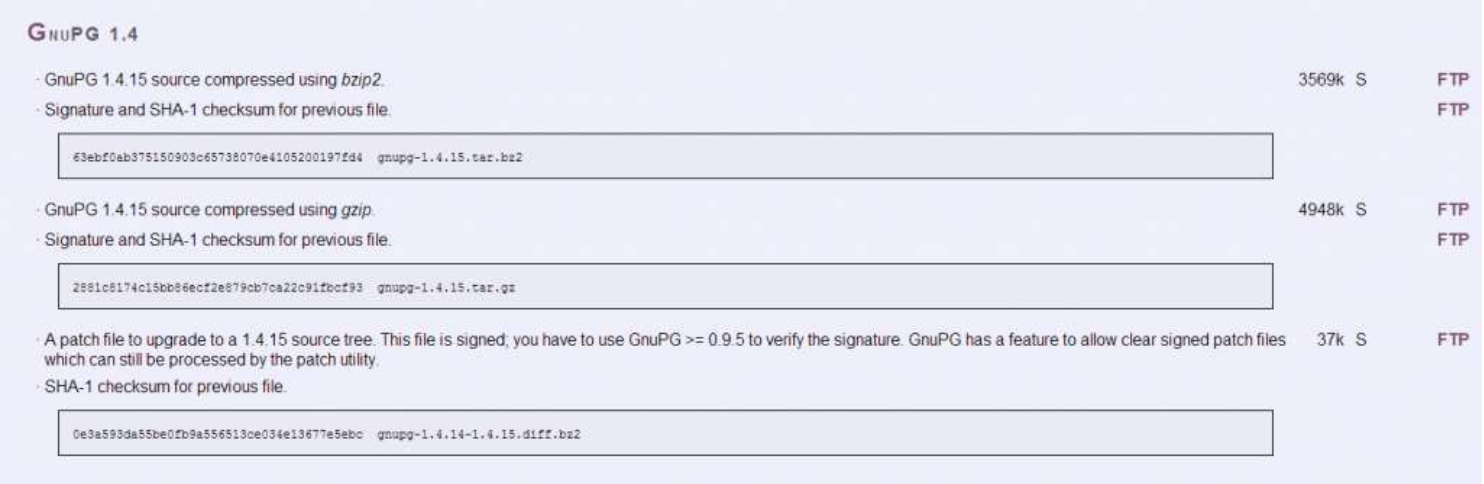


Imagen 6. Cifrado con GPG

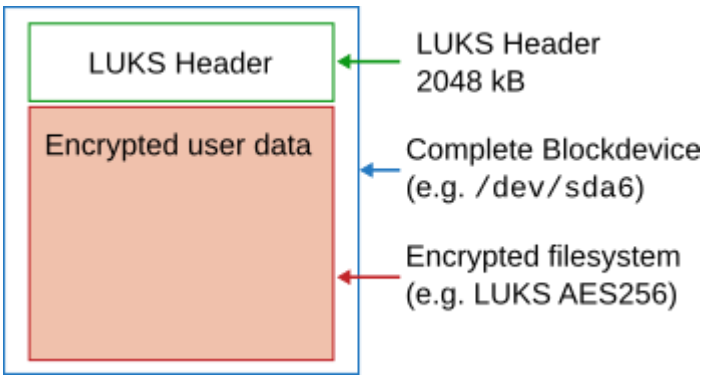


Imagen 7. Cifrado de sistema de archivo

Guía de configuración:
https://zenodo.org/records/10205734?token=eyJhbGciOiJIUzUxMiJ9.eyJpZCI6ImM0OTg2N2M1LWE2YzctNDZjYi05NGJhLTc1NWFmYTEyZjJlYiIsImRhdGEiOnt9LCJyYW5kb20iOiIxOTY3ZTg1NDhjODljMDkzNDdjMTh

iZTQ3OTllYjViOCJ9.-seBpVT958uSzUjh4yTI6aZRuzyfHu9lffwBadaLN0IjGqNEE8x5e4Ah5I0KHuB4DBrW3cGDpcJrP7wGUNfSkA

Objetivo 6: Oracle SQL Firewall

El enfoque del sexto objetivo se centra en la implementación del firewall nativo de SQL en bases de datos Oracle para reforzar la seguridad y salvaguardar la integridad de la información almacenada. Este firewall actúa como una barrera protectora, resguardando contra amenazas como ataques de inyección SQL y asegurando un control preciso del flujo de datos hacia y desde la base de datos. Comienza con una evaluación exhaustiva de la infraestructura existente, verificando la versión y licencia de Oracle Database para asegurar la disponibilidad y licenciamiento adecuado del firewall nativo de SQL.

Posteriormente, se detalla el diseño e implementación del firewall, definiendo reglas de seguridad específicas para salvaguardar contra amenazas conocidas. Configura el firewall para inspeccionar y bloquear tráfico malicioso o no autorizado, sin interferir con operaciones legítimas. Luego, se enfoca en pruebas de funcionamiento, ajustes y refinamientos basados en escenarios de ataque simulados para optimizar la eficacia del firewall.

Además, incluye la capacitación del personal sobre su funcionamiento y procedimientos de monitoreo y gestión de reglas de seguridad, junto con la documentación detallada de configuraciones y ajustes realizados para referencias futuras. Finalmente, se establece un programa de evaluación continua para revisar el desempeño del firewall, realizar análisis de riesgos periódicos y actualizar las reglas de seguridad según nuevas amenazas o

cambios en la infraestructura de la base de dat

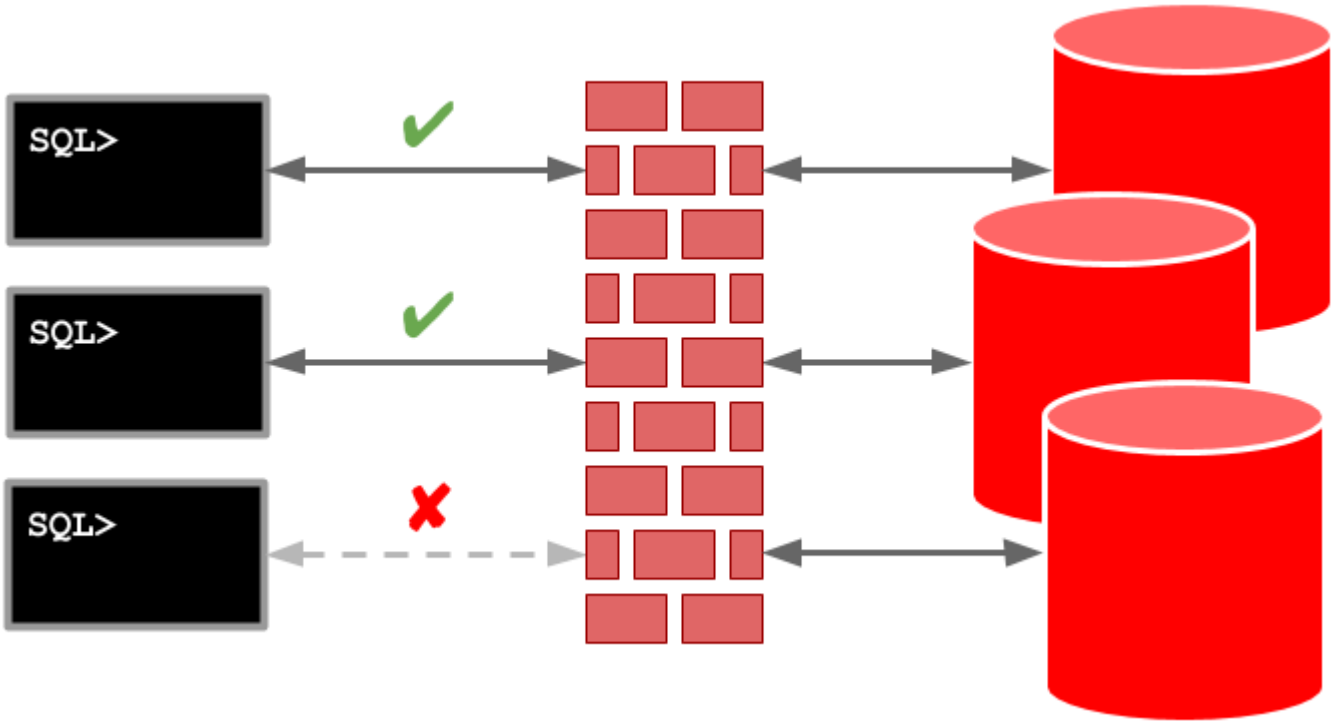


Imagen 8. Oracle SQL Firewall

Guía de configuración:
https://zenodo.org/records/10205738?token=eyJhbGciOiJIUzUxMiJ9.eyJpZCI6Ijk2YmIzMzdjLThlNDYtNDU2My1hNWRkLTA4ZTI3ODI3OTU2ZSIsImRhdGEiOnt9LCJyYW5kb20iOiJhMzE3YTU0NGI0YWQ4NmQzNTFlNWM1YWNhMzdiYmMzNyJ9.1_lDUZSwoLv86ibfdCV4ZQ1WvSYlYk3MsadQD2bY_rmd87xqztalxUuIdMc3_kLUAOGcBiGwubvaWPpacy7v1g

DISCUSIÓN

En el análisis de todos los objetivos propuestos, se evidencia una estrategia integral y exhaustiva para fortalecer la seguridad en entornos de bases de datos Oracle. Cada objetivo aborda distintos aspectos de protección de la información, desde la creación y gestión de Oracle Wallet para salvaguardar contraseñas hasta la implementación de firewalls nativos de SQL y cifrado de datos sensibles a nivel de sistema operativo con LUKS y GPG.

La creación de Oracle Wallets, su configuración y administración demuestran una preocupación por la seguridad en el acceso a las contraseñas de los usuarios, promoviendo el uso de master keys sólidas y políticas de actualización periódica. Esto, junto con la aplicación de Oracle Data Masking, proporciona una capa adicional de protección al enmascarar datos sensibles, siguiendo una estrategia de identificación, clasificación y enmascaramiento de datos confidenciales.

La guía para encriptar respaldos con contraseñas mediante RMAN refuerza la importancia de contraseñas sólidas, la gestión adecuada de accesos y la implementación de auditorías para detectar actividades sospechosas. A su vez, el establecimiento de roles, privilegios y políticas de acceso en la base de datos Oracle subraya la necesidad de controlar y limitar el acceso a la información en reposo, cumpliendo con estándares de seguridad y regulaciones.

El cifrado a nivel de sistema operativo con LUKS y GPG amplía la protección más allá de la base de datos, mostrando una estrategia holística para asegurar datos sensibles, tanto en la infraestructura de la base de datos como en archivos y scripts relevantes. Por último, la implementación del firewall nativo de SQL en bases de datos Oracle destaca la importancia de una defensa proactiva contra amenazas conocidas, como los ataques de inyección SQL, proporcionando una barrera efectiva entre la red privada y posibles ataques externos.

En conjunto, estos objetivos muestran un enfoque multifacético para garantizar la seguridad de los datos en reposo y en tránsito, considerando aspectos de cifrado, control de accesos, gestión de contraseñas, auditorías y monitoreo continuo. La estrategia propuesta ofrece una sólida defensa en profundidad para salvaguardar la integridad y confidencialidad de la información en entornos Oracle.

CONCLUSIONES

Concluyendo, en la actualidad digital, la seguridad de la información es primordial y Costa Rica no ha escapado a los desafíos de proteger datos y afrontar amenazas cibernéticas. Incidentes recientes, como los perpetrados por grupos como Conti y Hive en 2022, han subrayado la importancia de implementar medidas sólidas de seguridad, especialmente en bases de datos Oracle, ampliamente utilizadas en el país.

El cifrado de datos en reposo ha emergido como una medida crucial para proteger la información almacenada. Al aplicar algoritmos de cifrado a estos datos, se garantiza su ininteligibilidad sin la clave correspondiente, incluso si se accede físicamente a los medios de almacenamiento. Esto asegura la confidencialidad, integridad y disponibilidad de la información sensible.

Los objetivos específicos planteados para proteger la información, desde resguardar contraseñas con Oracle Wallet hasta cifrar archivos y scripts a nivel de sistema operativo con LUKS y GPG, ofrecen guías detalladas para implementar las mejores prácticas de seguridad.

En resumen, en la era digital, salvaguardar la información es esencial. El cifrado de datos en reposo desempeña un papel crucial en este contexto. Al seguir estas directrices, las organizaciones no solo se protegen de amenazas cibernéticas, sino que también cumplen con los estándares de seguridad requeridos..

BIBLIOGRAFÍA

Oracle (2015). "Creating and Managing Oracle Wallet." Disponible en: https://docs.oracle.com/middleware/1213/wls/JDBCA/oraclewallet.htm#JDBCA600

Oracle (2023). "Introduction to Oracle Advanced Security." Disponible en: https://docs.oracle.com/en/database/oracle/oracle-database/21/asoag/introduction-to-oracle-advanced-security.html#GUID-5D7343A0-4934-444F-97A1-5F189385A5DE

Oracle (2023). "Introduction to Oracle Data Masking and Subsetting." Disponible en: https://docs.oracle.com/en/database/oracle/oracle-database/12.2/dmksb/intro.html#GUID-24B241AF-F77F-46ED-BEAE-3919BF1BBD80

Oracle-Base (2019). "Create Self-Signed SSL Certificates." Disponible en: https://oracle-base.com/articles/linux/create-self-signed-ssl-certificates

Oracle-Base (2019). "Multitenant: Running Scripts Against Container Databases (CDBs) and Pluggable Databases (PDBs) in Oracle Database 12c Release 1 (12.1)." Disponible en: https://oracle-base.com/articles/12c/multitenant-running-scripts-cdb-and-pdb-12cr1

Oracle-Base (2019). "Secure External Password Store." Disponible en: https://oracle-base.com/articles/10g/secure-external-password-store-10gr2

Oracle-Base (2023). "SQL Firewall in Oracle Database 23c." Disponible en: https://oracle-base.com/articles/23c/sql-firewall-23c

Oracle Support (2022). "How to use encryption in RMAN backups. (Doc ID 316886.1)." Disponible en: https://support.oracle.com/knowledge/Oracle%20Database%20Products/316886_1.html

Nacion (2022). "CCSS habría sido ‘hackeada’ por un brazo de Conti llamado Hive." Disponible en: https://www.nacion.com/el-pais/salud/ccss-habria-sido-atacada-por-un-brazo-de-conti/63LQ5EQXGJF2TNIQP3A6SKTMCQ/story/

Wikipedia (2022). "Ciberataque al Gobierno de Costa Rica." Disponible en: https://es.wikipedia.org/wiki/Ciberataque_al_Gobierno_de_Costa_Rica

Imagen 1, Oracle Wallet, Disponible en:

Oracle introduces vault for encryption keys, wallet files - Help Net Security

Imagen 2. Oracle Data Masking, Disponible en:

https://www.linkedin.com/pulse/oracle-data-masking-subsetting-pack-building-kavindra-singh/

Imagen 3. Transparent Data Encryption, Disponible en:

https://easyteam.fr/oracle-tde-12c-concepts-and-implementation/

Imagen 5. Política de auditoria, Disponible en:

Oracle: Auditing - Oracle 12c Security Feature - What is New? (oracleelogs.blogspot.com)

Imagen 6. Cifrado con GPG, Disponible en:

GPG, Strong Encryption And Digital Signing Made Easy | Kaspersky official blog

Imagen 7. Cifrado de sistema de archivo, Disponible en:

LUKS In-Place Conversion Tool (johannes-bauer.com)

Imagen 8. Oracle SQL Firewall, Disponible en:

ORACLE-BASE - Service-Level Access Control Lists (ACLs) - Database Service Firewall in Oracle Database 12c Release 2 (12.2)