MONOGRAFIA DE ESTUDIO SOBRE LA METODOLOGÍA DE ASEGURAMIENTO DE BASES DE DATOS COMERCIALES (ORACLE)

PEDRO JOSE CARRILLO BERMUDEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTA D.C.
2020

MONOGRAFIA DE ESTUDIO SOBRE LA METODOLOGÍA DE ASEGURAMIENTO DE BASES DE DATOS COMERCIALES (ORACLE)

PEDRO JOSE CARRILLO BERMUDEZ

Proyecto de Grado – Monografía presentado para optar por el titulo de ESPECIALISTA EN SEGURIDAD INFORMATICA

Ing. FERNANDO ZAMBRANO HERNANDEZ
Director de Proyecto

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTA D. C.
2020

NOTA DE ACEPTACIÒN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Bogotá D.C.., Fecha sustentación

DEDICATORIA

Con amor dedico este trabajo a mi familia, esposa e hijos, que con paciencia soportaron mis olvidos y ausencias, pero que también ayudaron para que yo pudiera alcanzar este nuevo escalón en mi desempeño profesional; sin ellos nunca hubiera sido posible.

AGRADECIMIENTOS

Agradezco a las directivas de la Universidad Nacional Abierta y a Distancia UNAD, quienes con su trabajo continuo nos brindan la oportunidad de estudiar y laborar, por otro lado, a cada uno de los tutores y asesores que me acompañaron en el proceso les reconozco que sin su apoyo y colaboración éste logro no lo hubiera alcanzado.

CONTENIDO

pág.

LISTA DE TABLAS

pág.

RESUMEN

La información constituye uno de los activos más valiosos de la organización y por tanto es necesario custodiarla para evitar que caiga equivocadamente en manos de terceros; conscientes de lo anterior las organizaciones han considerado que la mejor alternativa es adquirir e instalar unos gestores de bases de datos robustos y que tengan el debido soporte técnico.

Sin embargo, a pesar de que las bases de datos son sistemas con componentes tecnológicos avanzados, se hace necesario conocer y aplicar una metodología que garantice su aseguramiento, porque pueden presentarse fallas o errores debido a la falta de seguridad en la infraestructura sobre la que corre el software de la base de datos, por la incorrecta configuración de los procesos de conexión, por prácticas inadecuadas realizadas por los usuarios funcionales y por la deficiencia en el proceso de asignación de privilegios a usuarios específicos o roles, entre muchas otras.

Por lo anterior, es importante realizar la identificación, implementación y seguimiento de una metodología de aseguramiento de las bases de datos que garantice que un sistema cumpla con los pilares de confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad en el tratamiento del activo que es la información.

ABSTRACT

Information constitutes one of the most valuable assets of the organization and therefore it is necessary to guard it to avoid falling into the hands of third parties; aware of the above, organizations have considered that the best alternative is to acquire and install robust database managers that have the appropriate technical support.

However, despite the fact that the databases are systems with advanced technological components, it is necessary to know and apply a methodology that guarantees their assurance, because failures or errors can occur due to the lack of security in the infrastructure on which runs the software of the database, due to the incorrect configuration of the connection processes, due to inadequate practices carried out by the functional users and due to the deficiency in the process of assigning privileges to specific users or roles, among many others.
Therefore, it is important to identify, implement and monitor a database assurance methodology that ensures that a system complies with the pillars of confidentiality, integrity, availability, traceability and authenticity in the treatment of the asset that is the information.

Keywords: Palabras claves en inglés

- Databases
- Pillars of information
- Access Control
- Password
- User privileges and Roles
- Database backup
- Vulnerabilities
- SQL Injections
- Audit

INTRODUCCIÓN

Los avances tecnológicos se dan a pasos agigantados y ninguna persona natural o jurídica, puede estar alejada de ellos; es imposible no vincularnos al uso de la tecnología, dependemos de ella para comunicarnos, para llevar organizadas nuestras cuentas, ya sea personales o empresariales, aún nuestras reuniones sociales están mediadas o inmediatizadas por la tecnología.

Pero en ese deseo apresurado de hacer uso o disfrutar de herramientas tecnológicas, no podemos olvidarnos de los riesgos latentes que se presentan con su uso; por eso las organizaciones, especialmente aquellas que manejan grandes y valiosos volúmenes de información, tienen que estar debidamente protegidos frente al uso malintencionado de la información y de los sistemas computacionales. En ese momento se evidencia que no es solo disponer de los equipos y programas tecnológicos, sino que es necesario, o mejor obligatorio, definir las políticas y estrategias que salvaguarden los datos que nos han confiado y los que resultan de nuestra actividad comercial o profesional.

Por todo lo anterior, es que se han definido normas, reglas y metodologías que permitan asegurar los sistemas informáticos ante las amenazas internas o externas que lo rodean. En este trabajo pretendemos organizar de manera fácil una metodología que asegure técnica y procedimentalmente las bases de datos, específicamente una base de datos Oracle, quizá la más difundida a nivel mundial.

1. DEFINICIÓN DEL PROBLEMA

1.1 FORMULACIÓN DEL PROBLEMA

Implementar una solución informática integral no es solo adquirir muchos equipos y algunos programas informáticos que faciliten controlar las transacciones financieras que una empresa realiza, sino que el valor de la información, el valor de todos los activos de la organización debe ser salvaguardado y para eso se requiere la aplicación de una metodología clara, concisa y precisa que indique los aspectos a considerar para realizar el aseguramiento de un sistema de base de datos comercial.

El Aseguramiento de las Bases de datos (ABD), es el conjunto de métodos, herramientas y técnicas que permiten gestionar la seguridad de un producto de software basado en el uso de un repositorio de base de datos. Pero pese a ser un elemento fundamental a la hora desarrollar e implementar un proyecto, no todas las empresas lo aplican debido a su reducido presupuesto, falta de personal o adaptaciones de estándares más complejos; esto fue analizado en el primer estudio nacional sobre amenazas digitales que realizaron en conjunto Colombia, la OEA y el BID y que se concluye en el informe “Impacto de los incidentes de seguridad digital en Colombia 2017”[1] que indica que aunque un 96% de las empresas utilizan internet, menos de la mitad tienen en cuenta los aspectos de la seguridad en sus sistemas.

Este aseguramiento incluye desde definir los activos, categorizarlos según su importancia, analizar las vulnerabilidades, riesgos y amenazas a las que están expuestos y establecer los controles a implementar ante cada evento potencial.

[1] BID. MinTIC. [Sitio web]. Bogotá: Impacto de los incidentes de Seguridad digital en Colombia. [Consulta: 31 de marzo 2019]. Disponible en: https://publications.iadb.org/en/impact-digital-security-incidents-colombia-2017

Como consecuencia de lo mencionado, el actual enfoque en la creación y mantenimiento de aplicaciones en base de datos es lograr que aporten un alto grado de interacción pero que además sean seguras y confiables. El principal problema en este tipo de escenarios, es que no hay experiencia suficiente, ni existen metodologías necesarias para llevar a cabo las pruebas que verifiquen que dichas interfaces carecen de cualquier tipo de deficiencia.

Una gestión importante durante su montaje y después durante la operación del sistema es el análisis de las vulnerabilidades de los bases de datos, que para el caso de Oracle, no son pocas porque aunque este software está en permanente actualización, no deja de tener aspectos para mejorar en cuanto a seguridad, tal como se describe en el portal www.cvedetails.com[2] el cual analiza y expone las diversas vulnerabilidades de las diferentes bases de datos o software.

Al finalizar este proyecto, se dispondrá de una metodología de aseguramiento de las bases de datos que garantice que un sistema cumpla con los pilares de confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad en el tratamiento del activo que es la información.

[2] ORACLE. [Sitio web]. California: Vulnerabilidades de Oracle. [Consulta: 4 de marzo 2019]. Disponible en: https://www.cvedetails.com/vulnerability-list/vendor_id-93/product_id-467/cvssscoremin-5/cvssscoremax-5.99/Oracle-Database-Server.html

2 JUSTIFICACIÓN

Todas las empresas, independientemente de su objeto social, pretenden crecer en sus ventas de productos o servicios y en sus volúmenes de transacciones, así como en sus instalaciones y obviamente en los recursos tecnológicos que les permitan controlar sus negocios y sus finanzas; como lo confirmaron los resultados del Observatorio de Economía Digital[3] desarrollado por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTic) que concluye que el 96% de las empresas en Colombia utilizan internet, pero solo unas pocas (32% invierten en ciberseguridad) son conscientes que no es solo adquirir una nueva infraestructura, un nuevo gestor de base de datos o contratar a un grupo de ingenieros que le brinden mantenimiento al sistema; hay otra serie de variables tecnológicas que redundan en el éxito del mismo.

Es ahí donde se ubica la necesidad de realizar aseguramiento a las bases de datos, no solo desde aspectos de vista físicos como una buena infraestructura física representada en instalaciones locativas, servidores de bases datos y aplicativos, redes locales y de internet, personal calificado, etc., sino además de aspectos lógicos como el aseguramiento de perfiles de usuario, claves de acceso, sistemas operativos, firewalls, dmz, software para redes lan y wan, etc.

Como este aspecto es algo que generalmente no se tiene en cuenta, sino que lo hacemos como una reacción a un riesgo materializado porque no se tiene una metodología aplicable desde el momento del diseño mismo de la solución informática, entonces, con este trabajo se pretende documentar una metodología de aseguramiento de la base de datos comercial Oracle, una de las de mayor

[3] Ministerio de Tecnologías de la Información y las Comunicaciones. [Sitio web]. Colombia. Primeros resultados del observatorio de Economía digital. [Consulta:10 de abril 2019]. Disponible en https://www.mintic.gov.co/portal /inicio/Sala-de-Prensa/Noticias/61929:MinTIC-revela-los-primeros-resultados-del-Observatorio-de-Economia-Digital

utilización en el mercado, de manera que sirva como referente durante la implementación de una solución tecnológica.

Queremos mostrar cómo el concepto de aseguramiento no solo se refleja en actividades o tareas, sino también en la forma cómo trabaja el equipo, como se controla la seguridad en el gestor de base de datos y las métricas utilizadas no solo para medir los resultados obtenidos, sino también para poder mejorar los procesos internos.

3 OBJETIVOS

3.1 OBJETIVO GENERAL

Consultar y documentar una metodología para el aseguramiento de bases de datos comerciales y generar recomendaciones para una instalación de base de datos Oracle, que garantice un servicio efectivo y proteja el recurso de la información ante cualquier intromisión interna o externa.

3.2 OBJETIVOS ESPECÍFICOS

- Identificar y realizar la documentación de una metodología utilizada para el aseguramiento de Bases de Datos comerciales como Oracle desde el ámbito de la infraestructura.

- Identificar y realizar la documentación de una metodología utilizada para el aseguramiento de Bases de Datos comerciales como Oracle, a partir del software de la BD.

- Identificar y documentar la metodología utilizada para el aseguramiento de Bases de Datos comerciales como Oracle, a partir de las herramientas de administración de la BD.

- Resumir las técnicas, estrategias y herramientas para el aseguramiento de bases de datos que permitan, desde la seguridad física y lógica, hacer frente a las diversas amenazas internas y externas y que permitan reducir las vulnerabilidades que el sistema pueda tener.

- Generar recomendaciones a partir de la documentación y consultas realizadas referentes al aseguramiento de Bases de Datos comerciales como Oracle, a partir de la aplicación de metodología de análisis de riesgos.

4 MARCO REFERENCIAL

4.1 MARCO TEÓRICO

El término metodología[4] generalmente se define como el grupo de mecanismos o procedimientos racionales, empleados para el logro de un objetivo; pero a nivel del software, hace referencia al conjunto de técnicas, procedimientos y soportes documentales empleados en el diseño, construcción e implementación de sistemas de información.

Su objetivo principal es exponer una serie de técnicas de modelado de sistemas que permitan desarrollar un software de calidad, que incluyen heurísticas de construcción y criterios de comparación de modelos de sistemas, pruebas técnicas y funcionales, así como el establecimiento y aseguramiento de los sistemas y de la información que procesan y almacenan.

Como estamos inmersos en un ambiente informático, específicamente hablando de las bases de datos y de un aspecto vital como es la seguridad, tanto de la parte de infraestructura como de la información misma, entonces durante el desarrollo de este proyecto pretendemos realizar la identificación, implementación y seguimiento de una metodología de aseguramiento de las bases de datos que garantice que un sistema cumpla con los pilares[5] de confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad en el tratamiento del activo que es la información.

[4] Conceptodefinición. [Sitio web]. España. Metodología. [Consulta:13 de abril 2019]. Disponible en: https://conceptodefinicion.de/metodologia/

[5]_ Firma-e. [Sitio web]. España. Pilares de la seguridad. [Consulta:13 de abril 2019]. Disponible en: https://www.firma-e.com/blog/pilares-de-la-seguridad-de-la-informacion-confidencialidad-integridad-y-disponibilidad/ /

Desde el punto de vista informático, la base de datos[6] es un sistema formado por un conjunto de datos almacenados en discos que permiten el acceso directo a ellos y un conjunto de programas que manipulan ese conjunto de datos. Cada base de datos se compone de una o más tablas que guarda un conjunto de datos; cada tabla tiene una o más columnas y filas. Las columnas guardan una parte de la información sobre cada elemento que queramos guardar en la tabla y cada fila de la tabla conforma un registro.

Generalmente se dispone de guías para desarrollar diversas pruebas de seguridad tanto en la parte de la infraestructura (hardware) como de las bases de datos, pero no es solo realizar pruebas aisladas, sino contar con una metodología[7] precisa que nos indique como llevar a cabo el aseguramiento total.

Con las consideraciones anteriores, pretendemos enfocarnos en consultar y documentar una metodología para el aseguramiento de bases de datos comerciales y generar recomendaciones para una instalación de base de datos Oracle, tendiente a garantizar un efectivo servicio y salvaguardar el recurso de la información ante cualquier intromisión interna o externa.

Todo proceso de aseguramiento pasa por la seguridad informática[8] que sirve para garantizar la privacidad de la información y la continuidad del servicio, tratando de minimizar la vulnerabilidad de los sistemas y de la información contenida en ellos, así como de las redes privadas y sus recursos.
Además cualquier proceso o procedimiento debe estar avalado o enmarcado dentro de la normatividad vigente, es así como existen leyes o decretos que

[6] Maestros de la web. [Sitio web]. España. Qué son las bases de datos.. [Consulta:17 de abril 2019]. Disponible en: http://www.maestrosdelweb.com/que-son-las-bases-de-datos/
[7] Observatorio tecnológico. [Sitio web]. España.Introducción a la seguridad informática. [Consulta:10 de abril 2019]. Disponible en: http://recursostic. educacion.es/observatorio/web/gl/software/software-general/1040-introduccion-a-la-seguridad-informatica?start=3
[8] CANO, Jeimy J. [Sitio web]. Colombia. Paradigmas en la seguridad informática. [Consulta:10 de febrero 2019]. Disponible en: http://www.derechotecnologico.com/estrado/estrado003.html

coadyuvan al aseguramiento y tratamiento de la información; en Colombia se formuló una Ley (la 1273 de 2009)[9], que describe los delitos informáticos y las penas aplicables en cada situación, así como también se reguló el buen uso de los datos de las personas y las empresas, la ley de protección de datos personales – Ley 1581 de 2012[10] – que complementa la regulación vigente para la protección del derecho fundamental que tienen todas las personas naturales a autorizar la información personal que es almacenada en bases de datos o archivos, así como su posterior actualización.

Sin embargo, como todo proceso, con el transcurso del tiempo se empiezan a generar entropías que lo afectan, haciendo necesaria una renovación periódica para lo cual debemos aplicar metodologías como el círculo de Deming (o círculo PDCA)[11] que invita a evaluar y corregir todo lo que hacemos; además de la importancia de gestionar un plan de análisis de vulnerabilidades[12] que mediante diversas herramientas de software permite identificar cómo y dónde podemos ser atacados, no solo para ser víctima de afectación por la pérdida de información, sino por la situación misma de tener indisponibilidad de nuestros servicios.

Con base en todas las anteriores consideraciones, cumplir con el aseguramiento de las bases de datos[13], no es solo restringir accesos o proteger la información

9 SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. [Sitio web]. Bogotá: Ley 1273 de 2009, Ley de delitos informáticos en Colombia. [Consulta: 31 de agosto 2019]. Disponible en: http://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

10 Departamento Administrativo de la Función Pública. [Sitio web]. Bogotá: Ley 1581 de 2012, Ley de protección de datos personales en Colombia. [Consulta: 30 de mayo 2019]. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

11 Acosta, David. [Sitio web]. España. El círculo de Deming (o círculo PDCA) y la gestión de PCI DSS. [Consulta:13 de diciembre 2019]. Disponible en: http://www.pcihispano.com/el-circulo-de-deming-o-circulo-pdca-y-la- gestion-de-pci-dss/ , fecha de publicación: 15 de octubre 2019.

12 Ministerio de Educación. [Sitio web]. España: Introducción a la seguridad informática-Vulnerabilidades de un sistema informático. [Consulta: 11 de junio 2019]. Disponible en: http://recursostic.educacion.es/observatorio/web/gl/ software/ software-general/1040-introduccion-a-la-seguridad-informatica?start=3

13 WELIVESECURITY. [Sitio web]. Buenos Aires: Consejos para bases de datos seguras. [Consulta: 28 de enero 2020]. Disponible en: https://www.welivesecurity.com/la-es/2017/09/05/consejos-bases-de-datos-seguras/

ante una manipulación fraudulenta, sino ser parte de todo un engranaje que mejore la eficiencia de los procesos, ayude a incrementar la productividad y esté siempre al servicio de las personas como fin último de todo nuestro quehacer.

4.2 MARCO CONCEPTUAL

Este es un resumen de la terminología empleada dentro de este marco de referencia y que es utilizada durante el desarrollo del proyecto:

- **AMENAZA.** Evento que posibilita la ocurrencia de un incidente que cause o no un daño a la información de la entidad, originado por factores externos a la organización.
- **AUTENTICIDAD.** Capacidad para determinar, verificar y garantizar las fuentes de la que proceden los datos, origen o el contenido de los mismos.
- **CONFIDENCIALIDAD.** Garantía de que la información no está disponible o divulgada a personas, entidades o procesos no autorizados. Igualmente identifica a los usuarios que acceden al sistema de información, a través de controles adecuados.
- **CONTROL:** Actividad o proceso encaminado a mitigar o evitar un riesgo. Incluye políticas, procedimientos, guías, estructuras organizacionales y buenas prácticas, que pueden ser de carácter administrativo, tecnológico, físico o legal.
- **DISPONIBILIDAD:** Es la garantía del acceso a nuestra información siempre que sea necesitada.

- **INFRAESTRUCTURA TI.** Zona específica acondicionada eléctrica y ambientalmente, para el procesamiento de datos, en cuyo espacio los equipos se encuentran conectados entre sí a través de una red.
- **INTEGRIDAD.** Protección y manejo provisto solamente por el personal autorizado en forma controlada, suministrando las metodologías de seguridad, para salvaguardar la información o activos informáticos, garantizando la modificación, borrado, manipulación y el almacenamiento de los archivos de forma segura.
- **RIESGO.** Acontecimiento que puede alcanzar un nivel de alto o bajo según corresponda y que sucede cuando la vulnerabilidad y la amenaza actúan juntas, generando un posible daño (material, informático, estructural o humano).
- **SEGURIDAD DE LA INFORMACIÓN.** Legado de medidas preventivas y de reacción establecidas en la entidad, entre las que se pueden mencionar políticas, normas, procedimientos, estructura organizacional, así como controles tecnológicos y físicos, permitiendo el resguardado, protección, confidencialidad, integridad y disponibilidad de la información institucional.
- **SISTEMA OPERATIVO**. El **Sistema Operativo** (SO) es el programa o software básico de un ordenador o dispositivo electrónico. Las funciones básicas del **Sistema Operativo** son administrar los recursos del ordenador, coordinar el hardware y organizar los archivos y directorios de su **sistema.** Sin el sistema operativo ningún computador, teléfono inteligente, o cualquier

dispositivo electrónico puede funcionar y proporcionar las facilidades que ofrece.

- **TRAZABILIDAD.** Capacidad de un sistema de información para marcar y determinar quién hace y en qué momento, una actividad, con el objetivo de analizar incidentes, detectar ataques y aprender a prevenirlos en el futuro. Se materializa en la integridad de los registros de actividad.
- **VULNERABILIDAD**. Factor interno generado de una clase de incapacidad para anticipar, asimilar y recuperar un evento natural o un acto humano e inherente a los activos de información que pueden ser explotados.

4.3 MARCO REFERENCIAL CONTEXTUAL

El desarrollo de los ambientes informáticos ha sido vertiginoso en los últimos años y especialmente lo relacionado con las bases de datos obliga a que se realice un exhaustivo análisis de cómo es su uso, los aportes al crecimiento de las organizaciones, así como también sus características lógicas y físicas necesarias para garantizar los pilares de la información.

Es innegable que cada día las empresas dependen en mayor medida de la información y de la tecnología, y que los sistemas de información están más soportados por la tecnología frente a la realidad de hace unas décadas.

Cuando leemos acerca de consejos de privacidad y seguridad solemos hablar de restricciones de acceso a las bases de datos, contraseñas fuertes, copias de respaldo frecuentes y programadas, soluciones de seguridad física y lógica, sistemas operativos y software actualizados evitando las configuraciones por

defecto[14], etc. En general, estos suelen ser los cuidados básicos y esenciales que cualquier administrador de infraestructura, no solo de base de datos, debe considerar. Sin embargo, según el sistema que esté queriendo proteger, hay otras cuestiones adicionales que deben tenerse en cuenta.

Además, es muy importante tener en cuenta los lineamientos legales o recomendaciones definidas por los entes de control, como por ejemplo, la “Guía para la elaboración de las políticas generales de seguridad y privacidad de la información”[15], diseñada y publicada por el Ministerio de las Tecnologías de la Información y las Comunicaciones (MinTic), la cual tuvo su segunda publicación en el año 2016 y que se consolida en el “Plan de Seguridad y Privacidad de la información”[16], publicado en el 2019.

Aunque generalmente se hable de seguridad informática, de seguridad de los sistemas de información o de seguridad de las tecnologías de la información, vamos a centrarnos en la seguridad de la información misma, en cómo definir los criterios aplicables como metodología para el aseguramiento de las bases de datos.

La seguridad de la información es el conjunto de medidas técnicas, operativas, organizativas y legales que permiten a las organizaciones resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de la misma.

---

[14] WELIVESECURITY. [Sitio web]. Buenos Aires: 7 motivos para decirle No a las configuraciones por defecto. [Consulta: 10 de enero 2020]. Disponible en: https://www.welivesecurity.com/la-es/2017/01/26/no-configuraciones-por-defecto/

[15] Ministerio de Tecnologías de la Información y las Comunicaciones. [Sitio web]. Colombia. Política de seguridad y privacidad de la información. [Consulta: 10 de abril 2019]. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G2_Politica_General.pdf

[16] Ministerio de Tecnologías de la Información y las Comunicaciones. [Sitio web]. Colombia. Plan de seguridad y privacidad de la información. [Consulta: 10 de abril 2019]. Disponible en: https://www.mintic.gov.co/portal/604/articles-100251_plan_seguridad_privacidad_informacion_2019.pdf

Otro tema es disponer de la información a tiempo pero que esta no sea correcta, e incluso que no se sepa, puede originar la toma de decisiones erróneas.

Durante el proceso de implementación del sistema de base de datos, pero especialmente después de estar en pleno funcionamiento, es necesario realizar un análisis periódico de las vulnerabilidades[17] que tiene el sistema, no solo desde el ámbito de los sistemas operativos, sino también desde el software de base de datos, los activos de información, las instalaciones físicas, el recurso humano y demás aspectos definidos en diversas metodologías.

Al considerar las vulnerabilidades de los sistemas operativos, es recomendable remitirse al Lenguaje de evaluación y vulnerabilidad abierta[18], (Open Vulnerability and Assessment Language OVAL) que es un estándar internacional de seguridad de la información y cuya comunidad promueve contenidos de seguridad abiertos y disponibles públicamente, para estandarizar la transferencia de esta información en todo el espectro de herramientas y servicios de seguridad.

Si nos centramos en el software de base de datos (Oracle, Mysql, SQL Server, Postgres, etc) también encontraremos que cada una de esas bases tienen muchas vulnerabilidades, las cuales se describen en el catálogo CVE[19] (Common Vulnerabilities and Exposures), que es una lista de vulnerabilidades de seguridad de la información públicamente conocidas.

17 Onasystems. [Sitio web]. Colombia. Vulnerabilidades que afectan la seguridad de las bases de datos. [Consulta: 22 de marzo 2019]. Disponible en: https://www.onasystems.net/vulnerabilidades-importantes-afectan-la-seguridad-bases-datos-las-empresas/

18 IT SECURITY DATABASE. [Sitio web]. España. Lenguaje de evaluación y vulnerabilidad abierta. [Consulta: 14 de octubre 2019]. Disponible en: http://itsecdb.com/oval/

19 CYBER-SECURITY. [Sitio web]. España. Ocho siglas relacionadas con vulnerabilidades. [Consulta: 11 de junio 2019]. Disponible en: https://www.3djuegos.com/comunidad-foros/tema/48444082/0/articulo-que-es-cve-ocho-siglas-relacionadas-con-las-vulnerabilidades/

El detalle[20] de las vulnerabilidades para las diversas bases de datos puede consultarse en https://www.cvedetails.com/ y puede verse dinámicamente su evolución a través de los años.

En la tabla 1. Vulnerabilidades en los Sistemas Operativos y en la Tabla 2. Vulnerabilidades en las Bases de Datos, que se incluyen como anexos, se muestran algunas de las vulnerabilidades más comunes.

Otro aspecto importante a tener en cuenta es el análisis de riesgos a los que puede estar expuesta la base de datos, como uno de los activos de una empresa, riesgos no solo asociados a una falla informática, sino otros eventos inherentes a las labores conexas, que parten desde el mismo momento en que se diseña la planta física, el talento humano, los recursos técnicos y económicos.

Para ello se han desarrollado diversas metodologías[21] cada una con un enfoque particular, pero que pueden resumirse en dos tipos fundamentales: cuantitativos y cualitativos. Todas tienen varios objetivos, primero, sistematizar el análisis de los riesgos a los que se podrían enfrentar los S.I, segundo, identificar los activos de una empresa y conocer los riesgos a los que están expuestos para generar estrategias de protección, tercero, tener bajo control posibles fallas de los S.I identificando que podría suceder, y cuarto, saber cómo actuar ante la materialización de un riesgo o la ocurrencia de alguna falla, con el fin de recuperar rápidamente la actividad empresarial.

Y como los sistemas informáticos crecen, evolucionan y se liberan nuevas versiones, también aparecen nuevos riesgos y debe pensarse en un nuevo

20 CVEDETAILS. [Sitio web]. España. Puntuación de las vulnerabilidades. [Consulta: 11 de junio 2019]. Disponible en: https://www.cvedetails.com/
21 UNAD. [Sitio web]. Colombia. Metodologías de análisis de riesgos en un SGSI. [Consulta: 11 de mayo 2019]. Disponible en: https://hemeroteca.unad.edu.co/index.php/publicaciones-e-investigacion/article /view/1435/1874

elemento, la seguridad digital (Ciberseguridad). Las diversas modalidades de fraude, robo de información, suplantación y demás formas delictivas, son ahora analizadas permanentemente, tanto que muchas compañías de especializan en prevenirlos y realizan conferencias donde analizan este tema y entregan conclusiones, como el reporte anual de ciberseguridad[22] de Cisco.

22 CISCO. [Sitio web]. España. Reporte de Ciberseguridad. [Consulta: 13 de abril 2019]. Disponible en: https://www.cisco.com/c/dam/global/es_mx/solutions/pdf/reporte-anual-cisco-2018-espan.pdf

5 DISEÑO METODOLÓGICO

INTRODUCCION

Balestrini[23] (2001) señala que el marco metodológico “es el conjunto de procedimientos a seguir con la finalidad de lograr los objetivos de la información de forma válida y con una alta precisión” (p.44). En otras palabras, es la estructura sistemática para la recolección, ordenamiento y análisis de la información, que permite la interpretación de los resultados en función del problema propuesto.

DISEÑO DE LA INVESTIGACIÓN

Dado que el objetivo del estudio fue recopilar las mejores prácticas para el aseguramiento de una base de datos comercial (Oracle), se recurrió a un diseño no experimental que se aplica de manera transversal; considerando que el tema de investigación tiene un sustento teórico suficiente, se procedió a realizar una investigación de tipo descriptivo para conocer a detalle la forma como se aseguran las bases de datos, no solo desde el punto de vista estrictamente técnico, sino procedimental y funcional.

De acuerdo con Hernández, Fernández y Baptista[24] (2006) la investigación no experimental “es la que se realiza sin manipular deliberadamente las variables; lo que se hace es observar fenómenos tal y como se dan en un contexto natural para después analizarlos” (p270). Estos mismos autores señalan que los diseños de

[23] BALESTRINI, Mirian. Cómo se elabora el Proyecto de Investigación. 2001. Editorial BL Consultores Asociados. Caracas. Venezuela.

[24] Hernández-Sampieri, C. Fernández y P. Baptista. Metodología de la investigación. (2006). México, DF, México: McGraw-Hill Interamericana Editores.

investigación transversales “recolectan datos en un solo momento, en un tiempo único. Su propósito es describir variables y analizar su incidencia e interrelación en un momento dado” (p.289).

ENFOQUE DE LA INVESTIGACION

El enfoque de la investigación será cualitativo porque lo que se realiza es una recopilación de recomendaciones y buenas prácticas, mas no análisis estadístico de información.

6 DESARROLLO DE LA METODOLOGÍA

Como se expuso en la introducción, implementar una solución informática integral no es solo adquirir muchos equipos y algunos programas informáticos que faciliten controlar las transacciones financieras que una empresa realiza, sino que el valor de la información, el valor de todos los activos de la organización debe ser salvaguardado y para eso se requiere la aplicación de una metodología clara, concisa y precisa que indique como realizar el aseguramiento de un sistema de base de datos comercial.

El Aseguramiento de las Bases de datos (ABD), es el conjunto de métodos, herramientas y técnicas que permiten gestionar la seguridad de un producto de software basado en el uso de un repositorio de base de datos. Pero pese a ser un elemento fundamental a la hora de desarrollar e implementar un proyecto, no todas las empresas lo aplican debido a presupuesto, falta de personal o adaptaciones de estándares más complejos.

Como se describe en el art. 5 de la ley 1314 del 2009, el sistema de aseguramiento de la información se compone además por principios, conceptos, técnicas, interpretaciones y guías, que regulan las calidades personales, el comportamiento, la ejecución del trabajo y los informes de aseguramiento.

Este aseguramiento incluye desde definir los activos, categorizarlos según su importancia, analizar las vulnerabilidades, riesgos y amenazas a las que están expuestos y establecer los controles a implementar ante cada evento potencial.

La identificación, implementación y seguimiento de una metodología de aseguramiento de las bases de datos que garantice que un sistema cumpla con los pilares de confidencialidad, integridad, disponibilidad, trazabilidad y

autenticidad en el tratamiento de la información, que disminuya la incertidumbre y la complejidad, debe verse desde diversos aspectos, estos son los analizados a continuación.

6.1 ASEGURAMIENTO DE LA INFRAESTRUCTURA TECNOLOGICA

Todo sistema tecnológico está apoyado en una serie de herramientas físicas, comúnmente llamada infraestructura tecnológica, la cual se compone de los equipos (computadores, redes, servidores, routers, arreglos de discos, etc), así como del sistema operativo de cada equipo y del software o los programas ofimáticos y específicos que utiliza cada empresa.

La primera barrera que debe facilitar el aseguramiento de la infraestructura tecnológica es la instalación de sistemas operativos robustos, que deben permanecer actualizados a las últimas versiones liberadas por los fabricantes, con parches debidamente catalogados, así mismo con todos los demás programas computacionales.

Es importante que la empresa disponga y aplique un exhaustivo plan de reposición y actualización de hardware, de actualización de equipos, o que establezca los contratos adecuados para proveerse de infraestructura cloud que se contrata con grandes proveedores y que garantizan un adecuado control y un respaldo a la información, mejor que cualquiera de nuestras mejores máquinas o herramientas.

Dentro del Plan de Continuidad del Negocio (PCN[25]) se deben establecer los cronogramas de sustitución o reposición de infraestructura, así como la adecuación de unas instalaciones físicas debidamente aseguradas, con

[25] Riesgo Cero. [Sitio web]. Bogotá: Guía para gestionar un plan de continuidad de negocios. [Consulta: 23 de octubre 2019]. Disponible en: https://www.riesgoscero.com/academia/especiales/guia-para-gestionar-un-plan-de-continuidad-de-negocio-segun-la-iso-22301

condiciones adecuadas en cuanto se refiere a climatización, prevención del riesgo de inundaciones, incendios o cualquier otro fenómeno natural asociado.

Las redes y sus componentes deben estar debidamente protegidos con elementos como firewall (físicos y lógicos), los sistemas operativos[26] y los programas informáticos con sistemas de usuarios y claves de acceso, sistemas de auditoría y respaldos permanentes (diarios, semanales, totales e incrementales).

Todo lo anterior hace referencia a la instalación principal o centro de cómputo donde se hace el procesamiento y salvaguardia de la información; sinembargo se aconseja disponer de centros de cómputo alternos y con replicación de datos en línea, de manera que la “caída” de uno se ve soportada por el sistema espejo que se haya configurado, siendo “transparente” para el usuario final.

El usuario final no necesita saber o definir aspectos como el sistema operativo de la máquina sobre la cual trabajará, pero si es importante programar una capacitación en caso de que sea un cambio drástico frente a los sistemas operativos a los cuales está acostumbrado a utilizar.

Pero, aunque puede concluirse que es muy importante tener un buen centro de cómputo con todas las especificaciones técnicas, el objetivo de esta monografía es otro y como tal, solo incluiré unos manuales de instalación de centros de cómputo como referencia.

Como en los manuales de instalación de bases de datos no se suele hablar del proceso previo, es muy importante que se dedique tiempo a esta decisión, porque

[26] Tecnología Informática. [Sitio web]. España. El sistema operativo. [Consulta:17 de abril 2019]. Disponible en: https://www.tecnologia-informatica.com/el-sistema-operativo/

una vez elegido el SGBD[27], es más difícil cambiarlo luego, ya que todo implica costos de inversión y tiempo.

Entre los aspectos a considerar para seleccionar el SGBD están:

- El tamaño de la base de datos, porque un gran tamaño de base de datos requiere utilizar software muy potente para la gestión de la misma, además podría necesitarse organizar los datos en distintas unidades de disco o incluso requerir clústeres o sistemas distribuidos.
- Conectividad: en la actualidad necesitamos que la base de datos sea accesible desde Internet, por lo cual debemos estimar las formas de conexión y la seguridad sobre la información transmitida.
- Según el número de usuarios que acceden la información almacenada, se requiere controles avanzados de seguridad para diferenciar los roles y permisos para cada uno.
- Si el número de conexiones simultáneas va a ser alto, se hace necesario disponer de un SGBD con grandes capacidades de trabajo concurrente y entonces pocos sistemas son capaces de brindarlo.
- El uso del hardware propio de la empresa puede predeterminar la selección del SGBD al estar limitados por el mismo. Debe elegirse un software que funcione rápidamente en el hardware dispuesto.
- Además, algunas políticas de las empresas, asociadas al uso de software libre o por acuerdos con empresas de software también pueden influir en la selección del SGBD.

Después de definido el SGBD es importante asegurar que cumpla con otros requisitos, por ejemplo:

[27] INESEM. [Sitio web]. España. Los gestores de bases de datos más utilizados. [Consulta: 2 de agosto 2019]. Disponible en: https://revistadigital.inesem.es/ informatica-y-tics/los-gestores-de-bases-de-datos-mas-usados/

- Sistemas operativos (SGBD que sea multiplataforma).
- Paquetes o aplicaciones preinstaladas. Por ejemplo en SO Linux se requieren paquetes como el compilador de C; en Windows (los Service Pack) o software de terceros (como máquina Java, el Framework .Net o un servidor web especifico).
- En cuanto a memoria RAM y procesador, todos requieren un valor mínimo de memoria a disposición y un modelo de procesador con una velocidad mínima en el mismo.
- Se requiere un espacio mínimo de disco duro y con buena velocidad de lectura y escritura.
- En cuanto a conexiones de red, puede ser importante que tenga una conectividad particular (como una dirección IP fija) o que pueda cumplir con una función concreta como servidor de dominio.

6.2 INSTALACIÓN DEL SOFTWARE DE BASE DE DATOS (ORACLE)

Oracle ha simplificado notablemente el proceso de instalación de la base de datos en las últimas versiones[28], reduciendo el tiempo requerido para realizar el proceso y mostrando las opciones por default o los valores mínimos requeridos para que tenga un funcionamiento adecuado.

La decisión de instalar uno u otro de los sabores (versiones) de Oracle deberá ser de acuerdo a las proyecciones y metas de la empresa o negocio, siempre guardando equilibrio entre necesidades, expectativas, recursos disponibles, etc.

[28] ORACLE. [Sitio web]. California: Gestor de clusters. [Consulta:11 junio 2019]. Disponible en: https://docs.oracle.com/cd/E87217_01/DVCMI/c2_installation. htm#DVCMI112

El Oracle Universal Installer (OUI[29]) se utiliza para instalar el software Oracle Database. OUI es una utilidad de interfaz gráfica de usuario que le permite ver el software de Oracle que está instalado en su máquina o si lo instala desde cero.

Antes de instalar el software, OUI realiza varias verificaciones automatizadas para asegurarse de que su computadora cumpla con los requisitos básicos de hardware y software para una instalación de Oracle Database. Si su computadora no cumple con los requisitos, se muestra un mensaje de error. Algunos de los requisitos para instalar el software son un mínimo de memoria física, memoria virtual suficiente (intercambio) y un mínimo de espacio libre en disco.

Después de realizada la instalación es importante realizar la verificación de conexión a la base de datos, utilizando la utilidad SQL*Plus[30].

Sin embargo, tener instalada la última versión de Oracle no garantiza el éxito de nuestra instalación informática, después de eso viene el diseño y construcción de los diferentes artefactos (tablas, índices, funciones, procedimientos, paquetes, usuarios, logs, etc) de la base de datos, armonizados de manera que se apliquen los criterios de normalización, indización, encadenamiento lógico, etc. La construcción de un aplicativo basado en una base de datos Oracle es una intrincada pero organizada telaraña que debe ser ejecutada por expertos; del buen levantamiento de requerimientos, análisis, desarrollo, pruebas y ajustes dependerá finalmente el éxito del proyecto.

Otro aspecto muy importante es la parametrización y afinamiento de la base de datos, porque aunque el diseño y construcción del aplicativo sea muy bueno, la

[29] ORACLE. [Sitio web]. California: Instalando Oracle 12C. [Consulta: 4 marzo 2019]. Disponible en: https://www.oracle.com/webfolder/technetwork/ tutorials/obe/db/12c /r1/Windows_DB_Install_OBE/Installing_Oracle_Db12c_ Windows.html
[30] UDIMA. [Sitio web]. Madrid: SQL. [Consulta: 20 de agosto 2019]. Disponible en: https://www.mundoracle.com/entorno-sql-plus.html?Pg=sql_plsql_10.htm

base se va degradando y requiere ajustes periódicos, incluso las labores del administrador de la base de datos (DBA[31]) incluyen la realización de respaldos (diarios, semanales, mensuales, etc) de la información, la administración de datos históricos, la depuración de aquellos datos obsoletos, la definición de perfiles y roles, la segregación de funciones, la definición de aspectos críticos de seguridad, los RTO[32] y RPO permitidos por la organización y, muchos, muchos etcéteras adicionales.

Durante la instalación de la herramienta Oracle están disponibles innumerables ayudas en línea que facilitan el proceso, pero además posteriormente se puede ajustar cualquiera de los parámetros básicos, haciendo que el crecimiento no sea un problema. En la bibliografía se incluyen algunas fuentes consultadas.

6.3 ASEGURAMIENTO DURANTE LA ADMINISTRACION DE LA BASE DE DATOS

Toda organización que maneja grandes volúmenes de datos requiere un sistema de gestión de base de datos (DBMS[33] - Database Management System); es allí donde surge la figura del Administrador de la Base de datos (DBA).

El DBA es la persona o grupo de personas encargadas de administrar, supervisar y asegurar el adecuado uso de los datos dentro de un DBMS.

Cuando se habla de Administración de la Base de datos, deben distinguirse dos roles separados: Administración de datos y administración de bases de datos.

[31] CESSI. [Sitio web]. Argentina. Administrador de Base de Datos. [Consulta: 10 de febrero 2019]. Disponible en: https://www.cessi.org.ar/perfilesit/detalle-de-administrador-de-base-de-datos-dba-12
[32] Software Greenhouse. [Sitio web]. España. RPO y RTO. [Consulta: 30 de marzo 2019]. Disponible en: https://www.swgreenhouse.com/conceptos-de-continuidad-de-negocio/rto-rpo
[33] TECHTARGET. [Sitio web]. Londres: Searchdatacenter. [Consulta: 12 de septiembre 2019]. Disponible en: https://searchdatacenter.techtarget.com/es/ definicion/ Sistema-de-gestion-de-bases-de-datos-o-DBMS

La función del administrador de datos es decidir inicialmente cuáles datos deben almacenarse en la base de datos, y luego establecer las políticas y estrategias para garantizar los pilares de la información después de tener los datos almacenados. El administrador de datos es por lo general, un gerente, no un técnico. El técnico responsable de poner en práctica las decisiones del administrador de datos es el administrador de bases de datos (DBA, database administrator).

Pero en general, ¿cuáles son las funciones que realiza un DBA?

Pueden definirse múltiples tareas, pero vamos a enunciar las más generales: Gestión General de Base de Datos, Modelado de Datos y Diseño de Base de Datos, Auditoría, Integración con aplicaciones, Respaldo y recuperación de datos, Inteligencia de negocios y almacenamiento de datos, Planificación y administración de capacidad, Administración de cambios y opcionalmente Desarrollo de aplicaciones.

Un plan de aseguramiento de cualquier base de datos, aunque esta monografía se orienta hacia Oracle, debe incluir al menos las siguientes labores:

1. Un plan de respaldo de la información almacenada en la base de datos: este debe ser diario, semanal o mensual considerando además que dicho respaldo puede ser total o incremental según se considere.

2. Un plan de pruebas de restauración del respaldo realizado, que garantice que los procesos de backup están siendo correctamente realizados y que corresponden a lo esperado. Un aspecto importante es que los backups deben ser cifrados[34], de manera que sean de imposible manipulación en caso de una

[34] GDAE. [Sitio web]. España. Backup cifrado. [Consulta:10 de abril 2020]. Disponible en: https://www.gadae.com/blog/haz-un-backup-cifrado-si-quieres-protegerte-del-robo-de-datos/

intrusión de extraños.

3. Administración de los usuarios (administrativos, funcionales y genéricos) que hacen uso de la base, porque aunque los usuarios funcionales deben estar considerados dentro del diseño y construcción de la base de datos, los usuarios administradores de la base de datos, que tienen conocimientos especializados, deben ser monitoreados y auditados de manera que cualquier acción sobre la base pueda ser revisada.

4. Como toda plataforma de base de datos necesita de un usuario especial que ejecuta conjuntamente tareas administrativas y funcionales específicas, por ejemplo procesos de cierres, transmisión de archivos o estructuras específicas, se debe tener un monitoreo especial y además garantizar que se tengan triggers de repudiación para todas aquellas conexiones que tengan un origen extraño o de direcciones desconocidas o que accedan por puertos no autorizados.

5. En las bases de datos de mayor tamaño, el administrador de la base (DBA) debe estar atento a la administración de los logs, tamaños de filesystems, tablespaces, porque eso garantiza que el rendimiento del aplicativo asociado a la base de datos, sea el mejor.

6. Un aspecto importante es determinar el momento adecuado para la extracción de información a archivos o bases históricas, que reduzcan los tamaños de la base de datos, lo que redunda en procesos de respaldo y rendimiento. Un aspecto paralelo es el particionamiento de tablas con gran volumen de datos, ya sea por periodos de información o por criterios asociados al tipo de información que se maneja.

7. Además, se debe realizar permanente seguimiento al rendimiento de la base de datos, es decir a la velocidad de respuesta al usuario, determinando aquellos procesos frecuentes, periódicos u ocasionales, que “consumen” mayormente los recursos físicos de la base (memoria o disco) y que se convierten en cuellos

de botella. Es deber del DBA reportar aquellos que deben ser objeto de análisis de cargas, realizando las recomendaciones respectivas acerca del uso de índices o reconstrucción de sentencias de búsqueda o actualización.

8. El DBA debe garantizar que haya ambientes separados de desarrollo, pruebas, implementación y producción, teniendo especial cuidado en que, las bases de pruebas, aunque utilicen datos tomados de producción hayan sufrido la anonimización o trastocamiento de datos.

9. El DBA debe asegurar que, a partir de la estricta separación de ambientes, cualquier control de cambios al software de la base de datos se hará desde el ambiente de pruebas finales, después que los controles de cambio hayan sido autorizados por los usuarios funcionales y aprobados por el respectivo comité.

10. El DBA debe ejecutar herramientas estadísticas y de perfilado de datos que escanean los valores, las columnas y las relaciones en y entre los conjuntos de datos, utilizando frecuencia y análisis de asociación para evaluar los valores de datos, formatos y completitud, e identificar los valores atípicos que pueden indicar errores.

11. El DBA debe participar en la construcción del Plan de Continuidad del Negocio (PCN), asegurando que lo propuesto esté acorde a la infraestructura y la construcción física y lógica de la base de datos.

    El PCN es la respuesta prevista por una empresa ante aquellas situaciones de riesgo que le pueden afectar de forma crítica, es decir, que impiden la operación tecnológica normal que soporta sus procesos de negocio. No importa el tamaño de la empresa o el coste de las medidas de seguridad implantadas, toda organización necesita un Plan de continuidad de negocio o de recuperación de desastres, ya que en cualquier momento se encontrará con una incidencia de seguridad o algún evento que detenga súbitamente la operación de la empresa.

12. Otro aspecto a tener en cuenta es realizar periódicamente un análisis de riesgos, donde se analicen los diferentes activos de información, su interrelación y su valor, en el sentido de qué perjuicio (coste) supondría su degradación, a que amenazas están expuestos esos activos, que salvaguardas están dispuestas y su eficacia, el impacto si se materializa una amenaza y el nivel de riesgo ponderado según la tasa de ocurrencia de la amenaza.

6.4 ASEGURAMIENTO DURANTE EL DISEÑO DEL PRODUCTO (SW) O SERVICIO DE BD

A veces nos preguntamos, si el sistema o aplicativo que funciona sobre la base de datos hace lo que espera el usuario, ¿qué más debemos hacer?

Para hallar la respuesta a esa pregunta, desde la óptica del aseguramiento de la base de datos hay muchas otras preguntas, entre las cuales es importante mencionar:

1. ¿Cualquier usuario tiene a su disposición toda la información almacenada en la base de datos, o ésta debe ser segmentada según los perfiles definidos para cada usuario o actividad?

   La respuesta es que, aunque un sistema funcione “bien”, no todos los usuarios deben disponer de las opciones para consultar toda la información de la base de datos, entre mejor sea la segmentación mediante perfiles, mejor será la administración de roles y perfiles y más fácil será determinar el responsable de cualquier cambio de la información. Esto va en línea con la confidencialidad y disponibilidad de la información.

2. ¿La base dispone de logs de auditoría que permiten determinar quién, cómo y cuándo un usuario ha realizado inserciones, actualizaciones o borrado de la información?

   Toda base de datos, en especial las bases construidas sobre Oracle, tienen logs de auditoría, pero los rastros de auditoría deben definirse desde el momento mismo de la construcción, habrá algunos propios de la base de datos, pero muchos otros a partir de la codificación o parametrización sobre los objetos de la base, tampoco es aconsejable que a todo objeto se le realice auditoría, pero sí a

aquellas tablas transaccionales sobre las que gira el núcleo del negocio. Esto va en línea con la integridad de la información.

Un aspecto adicional que se controla en las bases de datos es el ingreso autorizado, porque puede determinarse que determinados usuarios funcionales sólo puedan ingresar y realizar transacciones sobre la base de datos, cuando se conectan desde determinados equipos (especificados por IP) y que además lo hagan en horarios específicos; esto permite tener mejor control y reducir brechas de seguridad.

3. ¿La base o el sistema de base de datos tiene una base de contingencia o replicación[35] en caso de alguna falla del servidor principal, que permita que se vuelva a tener el sistema disponible en el menor tiempo posible?

   Los sistemas de base de datos, especialmente aquellos que tienen alta transaccionalidad, deben tener un sistema de respaldo o de recuperación que garantice la menor pérdida de información, esto es importante antes de poner en funcionamiento el sistema, debe hacer parte de los costos del proyecto y de la administración del mismo, incluso contemplando que ese sistema esté en una instalación física alejada del servidor principal. Esto va en línea con la disponibilidad de la información.

4. ¿Se tienen definidos los RTO[36] y RPO? En los dos casos la respuesta dependerá de la criticidad de cada aplicación.

[35] Powerdata. [Sitio web]. España. Replicación de bases de datos. [Consulta: 30 de marzo 2019]. Disponible en: https://blog.powerdata.es/el-valor-de-la-gestion-de-datos/beneficios-de-la-replicacion-de-base-de-datos#:~:text=Una%20replicaci%C3%B3n%20de%20base%20de,de%20la%20base%20de%20datos.&text=Actualmente%20existen%20en%20la%20red,sigue%20el%20modelo%20cliente%2Dservidor.

[36] Software Greenhouse. [Sitio web]. España. RPO y RTO. [Consulta: 30 de marzo 2019]. Disponible en: https://www.swgreenhouse.com/conceptos-de-continuidad-de-negocio/rto-rpo

Según la transaccionalidad en la base, los responsables de los sistemas, de la información y de la operatividad normal, deben definir con los dueños de la empresa o los stakeholders, cuáles serán los tiempos máximos de pérdida de información permisible (RPO) y el tiempo de recuperación (RTO) o reinicio del sistema. Las grandes instalaciones procuran que en los dos casos sea cero, en ellos los niveles de integridad, confidencialidad y disponibilidad deben ser los mejores.

5. ¿El diseño de la base está debidamente construido sobre los criterios de integridad de la información, teniendo tablas paramétricas o referenciales que coadyuven en una mejor calidad de los datos?

   Aunque actualmente se habla de bases de datos NoSQL[37] (a veces llamado "no solo SQL"), las empresas comerciales que manejan grandes volúmenes de datos utilizan el modelo clásico de SGBDR (Sistema de Gestión **de Bases de Datos Relacionales**) que están construidos a partir de mantener integridad referencial entre las diferentes tablas que constituyen los sistemas, el manejo de índices, triggers, etc y que garantizan una mejor calidad de datos y que facilitan la generación de estadísticas y reportes para los usuarios. Esto va en línea con la integridad de la información.

6. ¿La base almacena históricamente los eventos sucedidos en ella, de manera que se tenga trazabilidad de cada uno y pueda hacerse una reconstrucción en caso de cualquier falla?

   Toda base de datos, en especial las bases construidas sobre Oracle, tienen logs de auditoría[38], pero los rastros de auditoría deben definirse desde el momento

[37] UNIR. [Sitio web]. España. Bases de datos NoSql. [Consulta:17 de abril 2019]. Disponible en: https://www.unir.net/ingenieria/revista/noticias/bases-de-datos-nosql/549204809132/
[38] ORACLE. [Sitio web]. California: Configurando Logs de auditoría. [Consulta: 4 marzo 2019]. Disponible en: https://docs.oracle.com/cd/E56339_01/html/E53973/audittask-14.html#scrolltoc

mismo de la construcción, habrá algunos propios de la base de datos, pero muchos otros a partir de la codificación o parametrización sobre los objetos de la base, tampoco es aconsejable que a todo objeto se le realice auditoría, pero sí a aquellas tablas transaccionales sobre las que gira el núcleo del negocio Generalmente todo operación de conexión, inserción, actualización o borrado sobre objetos de la base de datos debe dejar rastros de auditoría los cuales se configuran como disparadores (triggers[39]). Esto va en línea con la integridad de la información.

7. ¿Se controla correctamente los procesos de control de cambios[40] (de la información y del software) y se guarda bitácora o control de versiones de los mismos?

   Aunque un sistema de base de datos esté cumpliendo el objetivo para el cual fue creado y se piense que no es necesario realizar cambios al mismo, también es cierto que la entropía va generando la necesidad de hacer algunos ajustes, los cuales deben ser debidamente revisados y controlados para su correcta implementación. Cualquier cambio o ajuste debe estar documentado y tener la debida aprobación de los usuarios funcionales y los respectivos encargados de las pruebas y la parte tecnológica involucrada, cuidando de causar la menor incidencia durante las ventanas de mantenimiento programadas. Esto va en línea con la integridad de la información.

8. ¿Cómo parte del diseño y construcción se consideró el uso de token de seguridad, hash y firmas digitales?

[39] ORACLE. [Sitio web]. California: Creando triggers en Oracle. [Consulta: 4 marzo 2019]. Disponible en: https://docs.oracle.com/cd/B19306_01/server.102/b14200/ statements_7004.htm
[40] Superintendencia de Sociedades. [Sitio web]. Colombia. Modelo de gestión de cambios. [Consulta: 14 de mayo 2019]. Disponible en: https://www.supersociedades.gov.co/superintendencia/oficina-asesora-de-planeacion/polinemanu/sgi/Documents/Documentos%20Infraestructura%20 Tecnologica/Documentos/GINT-PR-006%20Cambios%20al%20Ambiente%20Productivo.pdf

La seguridad es otro de los aspectos importantes en el diseño y construcción de un sistema de base de datos, porque además de la definición de usuarios y contraseñas, pueden configurarse medios de seguridad como los token o firmas digitales. Este dispositivo, unido a la programación en el software, genera una protección porque mientras no se tenga ese token, no podrá ejecutarse el módulo o la opción definida. Las firmas digitales además pueden garantizar el cifrado de la información y las restricciones de acceso.

9. ¿Cuál es la calidad de los datos o información y cuáles los criterios de evaluación de la calidad?

   La calidad de la información siempre debe ser otro criterio fundamental dentro del aseguramiento de un sistema de base de datos, independiente del software de base de datos que se utilice, por ello es oportuno conocer algunas metodologías que existen para la estandarización de datos:

   a. Metodología TQdM[41] (Total Quality data Management[42]), tiene como enfoque la mejora continua de dos diferentes categorías de procesos: en primera instancia, los procesos enfocados a la información, y a la definición de la misma, con el desarrollo de sistemas de información y modelos de bases de datos que permitan la administración de los datos que sirvan para suministrar dicha información; en segunda instancia, se encuentran procesos de negocios que entregan la información anterior, a los tomadores de decisiones y a los trabajadores de la información.

      Para lograr que esta metodología se lleve a cabo, se deben seguir una serie de procesos de calidad que inician con la identificación de los dominios o

[41] Caballero, Ismael, et al. Calidad de datos. Madrid. Ed Ra-ma, 2018. p.90.
[42] O'REILLY. [Sitio web]. California: Gestión de datos de calidad total (TQdM). [Consulta: 4 marzo 2019]. Disponible en: https://www.oreilly.com/library/view/improving-data-arehouse/9780471253839/12_chapter04.html

grupos de información a revisar, valorando la calidad de la base de datos, la experiencia y satisfacción de los usuarios con la calidad de datos e identificando las medidas para determinar la calidad de los datos.

El primer proceso, es la valoración de la calidad al momento de definir los datos y la arquitectura de la información; el segundo proceso, es la valoración de la calidad de la información, que va de la mano con los procesos de negocio de la compañía, y en donde se identifican los flujos de datos que típicamente maneja la empresa; el tercer proceso es la medición del costo que tendría la información que no ofrece los estándares de calidad de los datos; el cuarto proceso, trata sobre el proceso de limpieza de los datos, en donde se mejoran los datos y los productos de la empresa; el quinto es la mejora de la calidad de los procesos de información y el sexto trata sobre establecer un entorno de la calidad de la información.

b. Metodología TDQM[43]: El objetivo de esta metodología es considerar la información como un proceso de producción. (Tecnology, 2002); se basa en cuatro etapas cíclicas (Planear, Hacer, Verificar y Actuar) y centrando el esfuerzo en la definición de productos de información y medición de la calidad de datos.

c. Metodología AIMQ[44] (Assessment and Improved Methodology for Quality). Esta metodología consta de 3 elementos para la valoración de la calidad:
   - Fase subjetiva: Realización de encuestas. Fase objetiva: Medir la calidad de los datos.

[43] GALARZA ROSALES, Julio Alberto y URIONA HERRERA, Cristhian Fabián. Modelos de Madurez en los Datos de una Organización: Caso de Estudio Universidad Católica Boliviana "San Pablo" Cochabamba. *RevActaNova.* [online]. 2012, vol.5, n.4 [Consultado 09 de diciembre 2019], pp. 462-476 . Disponible en: http://www.scielo.org.bo/scielo.php?script=sci_arttext&pid=S1683-07892012000200004

[44] Lee, Y.W., Strong, D.M., Kahn, B.K. & Wang, R.Y. [Sitio web]. Estados Unidos. AIMQ: a methodology for information quality assessment. Information & management. [Consulta: 17 de abril 2019]. Disponible en: http://web.cba.neu. edu/~ywlee/publication/aimq.pdf

- Comparar los resultados de las valoraciones subjetivas y objetivas.
- Tomar acciones para la mejora de la calidad de datos.

Como parte del aseguramiento, es bueno concluir que, aunque se disponga del mejor software de base de datos y las mejores herramientas a disposición de los usuarios, mientras no se tenga una correcta y válida información, no podemos decir que nuestra base está asegurada o es segura para su utilización y cumplimiento de los objetivos para los cuales se creó.

6.5 IMPLEMENTACIÓN DE SEGURIDAD FÍSICA Y LÓGICA

La seguridad de los sistemas de bases de datos es un aspecto muy importante, no solo se consideran como básicos la definición de roles, perfiles y usuarios, sino que deben tenerse en cuenta algunos otros ítems como:

1. Uso de barreras de seguridad (firewall[45]) tanto físicos como lógicos. Aunque esto es un costo adicional en la instalación, es muy importante que se considere porque siempre será menor al costo que representa perder la información o no estar seguro de la calidad de la misma.

   Los firewalls pueden ser hardware, software o ambos y durante los últimos 25 años constituyen la primera línea de defensa en la seguridad de una red. Establecen una barrera entre las redes internas seguras, controladas y fiables y las redes externas poco fiables como Internet.

2. Establecer en las redes de computadores lo que se conoce como áreas desmilitarizadas (DMZ[46]) que aíslen los equipos críticos y reduzcan las

[45] CISCO. [Sitio web]. España. Qué es firewall. [Consulta:13 de abril 2019]. Disponible en https://www.cisco.com/c/es_es/products/ security/firewalls/what-is-a-firewall.html
[46] INCIBE. [Sitio web]. España. Qué es una DMZ. [Consulta: 2 de agosto 2019]. Disponible en: https://www.incibe.es/protege-tu-empresa/blog/dmz-y-te-puede-ayudar-proteger-tu-empresa

intromisiones externas. En esa zona desmilitarizada se ubican los recursos que son accesibles desde internet, como son el servidor de correo o el servidor web.

3. Según el sistema operativo sobre el que funcionan los equipos y software de aplicación y ofimáticos, debe realizar protección sobre los directorios o filesystem[47] de cada instalación de cómputo, porque ninguna protección se debe considerar como suficiente en este mundo cibernético.

   El file system de un sistema operativo determina la manera en que los archivos son nombrados y cómo y dónde son colocados y almacenados en los dispositivos. Sistemas operativos como Windows, MacOS, UNIX o Linux emplean un file system que usa una estructura jerárquica organizada como un árbol de directorios a los cuales se les asignan permisos para ser leídos, actualizados, ejecutados o borrados de acuerdo al perfil de quien se conectó a una computadora.

4. Se debe definir la manera en que se realizan las conexiones remotas a la base de datos, estableciendo conexiones tipo SSL/VPN que tendrán restricciones y validaciones frente a directorio activo, puertos de conexión, esquemas de datos, etc, aplicando el principio de mínimo privilegio[48].

   El principio de mínimo privilegio consiste en reducir los privilegios de las cuentas de usuario al nivel mínimo necesario para el desempeño de las tareas autorizadas buscando minimizar el impacto de cualquier fallo o vulnerabilidad del sistema.

[47] Angelfire. [Sitio web]. California. Qué es un filesystem. [Consulta: 21 de agosto 2019]. Disponible en: http://www.angelfire.com/mac2/so/file.htm

[48] WELIVESECURITY. [Sitio web]. Buenos Aires: Principio del mínimo privilegio. [Consulta: 14 de enero 2020]. Disponible en: https://www.welivesecurity.com/la-es/2018/06/08/principio-menor-privilegio-limitar-acceso-imprescindible/

5. Se debe implementar cifrado en los equipos, servidores y herramientas transaccionales con el fin de mantener la protección de la información.

   En el mundo criptográfico, cifrar una información significa ocultar el contenido de un mensaje a simple vista, mediante un procedimiento que utiliza un algoritmo matemático. Estos algoritmos modifican el texto, de manera que sólo sabiendo el mismo algoritmo se puede descifrar para saber qué es lo que se dice.
   Para proteger archivos de datos, Oracle proporciona cifrado transparente de datos (TDE[49]). TDE cifra los datos confidenciales almacenados en los archivos de datos y para evitar descifrados no autorizados, almacena las claves de cifrado en un módulo de seguridad externo a la base de datos.

6. Utilizar múltiples factores de autenticación al realizar transacciones financieras, incluyendo los hash[50] y/o firmas digitales.

   En los últimos años se ha puesto muy de moda el uso de herramientas de seguridad como son los hash y la implementación de firmas digitales que hacen válidos los documentos expedidos por medios electrónicos y sirven como medida de protección o certificación de una información.

   Una función criptográfica hash - usualmente llamada “hash”- está formada por un algoritmo matemático que transforma cualquier bloque arbitrario de datos en una nueva serie de caracteres con una longitud fija, generalmente de 40 caracteres.

---

[49] ARCGIS. [Sitio web]. Estados Unidos. Cifrado Transparente de datos TDE. [Consulta: 23 de octubre 2019]. Disponible en: https://desktop.arcgis.com/es/ arcmap/10.4/extensions/data-reviewer/transparent-data-encryption-tde-for-the-reviewer-workspace-in-oracle.htm

[50] Karspesky. [Sitio web]. Estados Unidos. HASH. [Consulta: 27 de junio 2019]. Disponible en https://latam.kaspersky.com/blog/que-es-un-hash-y-como-funciona/2806/

7. Realizar backups de la información en las plataformas dispuestas por la empresa, los cuales debe ser cifrados preferiblemente.

   Todo sistema informático, aún un computador personal por más simple que parezca, debe tener respaldo de la información almacenada, de manera que en caso de daño o adulteración fraudulenta, ésta pueda ser restaurada.

   Para la mayoría de instalaciones informáticas, se considera adecuado cifrar los backups de manera que en caso de pérdida o extravío no quede al descubierto información confidencial.

En conclusión, no es solo poner unos servicios a disposición de los usuarios o ciudadanos, sino brindarles la tranquilidad de que son seguros, generar confianza digital y garantizar que las estadísticas o valores contabilizados corresponden a la realidad del negocio.

6.6 ASEGURAMIENTO MEDIANTE ANÁLISIS DE RIESGOS DE UN DBMS

Otro ítem muy importante dentro de los sistemas de gestión de base de datos (DBMS) es el aspecto de la gestión de los riesgos.

Cuando se habla de gestionar la seguridad de la información, en lo que generalmente se piensa es en la serie de normas ISO 27000. Si bien ISO 27005 e ISO 31000 son los estándares más conocidos para la gestión de riesgos, hay otras alternativas que pueden ayudar a la empresa dentro de la gestión de la seguridad de la información y que permiten conocer y controlar los riesgos a los cuales está expuesta la información de la compañía.

Dentro de cada aplicación informática es necesario analizar y gestionar los riesgos a los que están expuestos los Sistemas de Información, presentando a la

administración, usuarios y todo individuo vinculado a la organización, los riesgos no solo asociados a una falla informática, sino otros eventos inherentes a las labores colaterales o tangenciales, que parten desde el mismo momento en que se diseña la planta física, el talento humano, los recursos técnicos y económicos.

Para ello se han desarrollado diversas metodologías cada una con un enfoque particular, pero que pueden resumirse en dos tipos fundamentales: cuantitativos y cualitativos. Todas tienen como objetivos:

- Sistematizar el análisis de los riesgos a los que se podrían enfrentar los S.I
- Identificar los activos de una empresa y conocer los riesgos a los que están expuestos para generar estrategias de protección.
- Tener bajo control posibles fallas de los S.I identificando que podría suceder con mucha, bastante o poca probabilidad
- Saber cómo actuar ante la materialización de un riesgo o la ocurrencia de alguna falla, con el fin de recuperar rápidamente la actividad empresarial.

Entre las metodologías más difundidas y aplicadas están: Octave, Magerit, Estándar ISO/IEC 27005 y Mehari.

Generalmente cuando se habla de los activos de una empresa, se piensa en las instalaciones locativas, los vehículos, los sistemas computacionales, los recursos financieros, la propiedad intelectual, pero se olvidan algunos otros aspectos que son importantes.

Por eso durante la aplicación de estas metodologías deben considerarse los siguientes activos, sugeridos, por ejemplo, en la metodología Magerit:

1.- **[D]** Datos o información.
2.- **[K]** Claves Criptográficas.
3.- **[S]** Servicios.

4.- **[SW]** Software – Aplicaciones informáticas.
5.- **[HW]** Equipamiento informático (Hardware).
6.- **[COM]** Redes de Comunicaciones.
7.- **[Media]** Soportes de Información.
8.- **[AUX]** Equipamiento Auxiliar.
9.- **[L]** Instalaciones.
10.- **[P]** Personal.

Pero es oportuno indicar que el análisis de los riesgos no es una labor solo para cuando se inician o ponen en marcha los sistemas de información, sino que la evaluación de los riesgos debe hacerse periódicamente, porque la entropía va afectando los sistemas, el cambio mismo que tienen las personas y las organizaciones, su dinámica de crecimiento, etc, son elementos que adquieren criticidad en cualquier momento.

Al realizar periódicamente un análisis de riesgos, se analizan los diferentes activos de información, su interrelación y su valor, en el sentido de qué perjuicio (coste) supondría su degradación, a que amenazas están expuestos esos activos, que salvaguardas están dispuestas y su eficacia frente al riesgo, el impacto (daño) si se materializa una amenaza y el nivel de riesgo ponderado según la tasa de ocurrencia de la amenaza.

La metodología Magerit[51] se fundamenta en analizar el impacto que puede tener para la empresa la violación de la seguridad, buscando identificar las amenazas que pueden llegar a afectar la compañía y las vulnerabilidades que pueden ser utilizadas por estas amenazas, logrando así tener una identificación clara de las medidas preventivas y correctivas más apropiadas.

[51] Portal administración electrónica. [Sitio web]. Madrid: MAGERIT v3: Metodología de Análisis y Gestión de Riesgos de los sistemas de información. [Consulta: 22 de marzo 2019]. Disponible en: http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.VCmVZhZRVJQ.

Esta metodología presenta en tres libros una guía completa y paso a paso de cómo llevar a cabo el análisis de riesgos. El primer libro hace referencia al Método, describe la estructura que debe tener el modelo de gestión de riesgos muy ajustado al modelo ISO. El segundo es un Catálogo de Elementos que puede utilizar la empresa para enfocar el análisis de riesgo y el tercero es una Guía de Técnicas frecuentemente utilizadas en el análisis de riesgos.

7 CONCLUSIONES

El mundo informático es quizá el que avanza más rápidamente en su desarrollo o el que mas dinámica de cambio se ve a nivel global, tan es así, que los equipos tecnológicos llegan a su nivel de obsolescencia en muy pocos meses o años.

Además, esa misma dinámica hace que nuevas amenazas o vulnerabilidades no sean analizadas en el mismo momento de lanzar una nuevo producto, ya sea de hardware o de software, porque el deseo de brindar nuevas herramientas o facilidades a cualquier usuario del común hace que nuevas brechas de seguridad estén a la orden del día, unido al insospechado auge de aquellos que buscan hallar el camino para sacar provecho de cualquiera de ellas.

Por ello, esta metodología no se centró en detallar o sugerir una herramienta de software o hardware como la que va a solucionar todos los problemas, sino en recomendar una serie de pasos o estrategias que sumadas van a reducir o minimizar los problemas de seguridad asociados a cualquier sistema informático, no solo lo relacionado con las bases de datos, sino con la cotidianidad, porque ya es común que nuestro teléfono celular sea equivalente al computador que teníamos hace algunos años, con la facilidad de llevarlo a todas partes y no requerir de instalaciones especiales para establecer una conexión remota.

Un aspecto que se escapa a cualquier metodología o cualquier herramienta de software es el factor humano, ese puede ser la mayor debilidad o fortaleza dependiendo de la integridad y honestidad de las personas, por ello merecería un capítulo especial, pero como no es un estudio psicológico o social de las personas, no se incluye aquí, pero es oportuno recordar la importancia de contar con talento humano permanentemente capacitado y con garantías laborales que generen crecimiento personal y pertenencia institucional.

Es responsabilidad de cualquier administrador de base de datos, mantener actualizados o sugerir la renovación permanente de equipos de cómputo, accesorios o dispositivos, software ofimático o software especializado, además de realizar periódicamente la aplicación de metodologías de análisis de riesgo y vulnerabilidades que afectan el sistema que administra y sugerir las recomendaciones sin importar que estas no obedezcan a temas estrictamente técnicos, sino funcionales u operativos, pero que puedan reflejarse en el correcto funcionamiento de un sistema.

BIBLIOGRAFÍA

Acosta, David. [Sitio web]. España. El círculo de Deming (o círculo PDCA) y la gestión de PCI DSS. [Consulta:13 de diciembre 2019]. Disponible en: http://www.pcihispano.com/el-circulo-de-deming-o-circulo-pdca-y-la- gestion-de-pci-dss/ , fecha de publicación: 15 de octubre 2019.

Agrawal, A. [Sitio web]. España. eXploit protocol blog. [Consulta:13 de abril 2019]. Disponible en: http://exploitprotocol.blogspot.com/2013/10/pentester-academy-web-application_30.html

Amber, S.W. [Sitio web]. Canadá. Agile database techniques. [Consulta: 2 de octubre 2019]. Disponible en: http://www.agiledata.org/essays/ mappingObjects.html.

ARCGIS. [Sitio web]. Estados Unidos. Cifrado Transparente de datos TDE. [Consulta: 23 de octubre 2019]. Disponible en: https://desktop.arcgis.com/es/ arcmap/10.4/extensions/data-reviewer/transparent-data-encryption-tde-for-the-reviewer-workspace-in-oracle.htm

AREITIO BERTOLÍN, J. [Sitio web]. España. Test de penetración y gestión de vulnerabilidades, estrategia clave para evaluar la seguridad de red. [Consulta:13 de septiembre 2019]. Disponible en: http://www.redeweb.com/_txt/ 653/36.pdf

ARIAS, Fidias. El Proyecto de Investigación. Guía para su elaboración. 3ra Edición. 1999. Editorial Episteme. Caracas. Venezuela.

B. Guhanik. [Sitio web]. Estados Unidos. Service accounts vulnerabilities. Information Security Reading Room. [Consulta:23 de enero 2020]. Disponible en: http://goo.gl/dIUIRY

BALESTRINI, Mirian. Cómo se elabora el Proyecto de Investigación. 2001 Editorial BL Consultores Asociados. Caracas. Venezuela.

Berkeley Security, University of California. [Sitio web]. Estados Unidos. Database Hardening Guidelines. [Consulta: 10 de marzo 2020]. Disponible en: https://security.berkeley.edu/node/138.

BID. MinTIC. [Sitio web]. Bogotá: Impacto de los incidentes de Seguridad digital en Colombia. [Consulta: 31 de marzo 2019]. Disponible en: https://publications.iadb.org/en/impact-digital-security-incidents-colombia-2017

Caballero, Ismael, et al. Calidad de datos. Madrid. Ed Ra-ma, 2018. p.90.

CANO, Jeimy J. [Sitio web]. Colombia: Auditoría de Seguridad, Evaluación de Seguridad y Pruebas de Penetración: tres paradigmas en la Seguridad Informática. 1996. P. 71. [Consulta: 10 de febrero 2019]. Disponible en: http://www.derechotecnologico.com/ estrado/estrado003.html

CESSI. [Sitio web]. Argentina. Administrador de Base de Datos. [Consulta: 10 de febrero 2019]. Disponible en: https://www.cessi.org.ar/perfilesit/detalle-de-administrador-de-base-de-datos-dba-12

CVEDETAILS. [Sitio web]. España. Puntuación de las vulnerabilidades. [Consulta: 11 de junio 2019]. Disponible en: https://www.cvedetails.com/

CYBER-SECURITY. [Sitio web]. España. Ocho siglas relacionadas con vulnerabilidades. [Consulta: 11 de junio 2019]. Disponible en: https://www.3djuegos.com/comunidad-foros/tema/48444082/0/articulo-que-es-cve-ocho-siglas-relacionadas-con-las-vulnerabilidades/

CISCO. [Sitio web]. España. Reporte de Ciberseguridad. [Consulta:13 de abril 2019]. Disponible en: https://www.cisco.com/c/dam/global/es_mx/solutions /pdf/reporte-anual-cisco-2018-espan.pdf

CISCO. [Sitio web]. España. Qué es firewall. [Consulta:13 de abril 2019]. Disponible en https://www.cisco.com/c/es_es/products/ security/firewalls/what-is-a-firewall.html

Departamento Administrativo de la Función Pública. [Sitio web]. Bogotá: Ley 1581 de 2012, Ley de protección de datos personales en Colombia. [Consulta: 30 de mayo 2019]. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

FASTLANE. [Sitio web]. Panamá: Simple Nomad,The Unofficial NT Hack FAQ, Section 05. [Consulta: 20 de agosto 2019]. Disponible en: http://www.fastlane.net/homepages/thegnome/faqs/nt/

Firma-e. [Sitio web]. España. Pilares de la seguridad. [Consulta:13 de abril 2019]. Disponible en: https://www.firma-e.com/blog/pilares-de-la-seguridad-de-la-informacion-confidencialidad-integridad-y-disponibilidad/

FRANCO, David A; PEREA, Jorge L y TOVAR, Luis C. Herramienta de detección de vulnerabilidades mediante Banner Grabbing. [en línea]. Cartagena (Colombia). Universidad de Cartagena. 2013, vol.24, n.5 [Consultado 04 Diciembre de 2019]. ISSN 0718-0764. Disponible en: http://dx.doi.org/10.4067/S0718-07642013000500003

GALARZA ROSALES, Julio Alberto, URIONA HERRERA, Cristhian Fabián. Modelos de Madurez en los Datos de una Organización: Caso de Estudio Universidad Católica Boliviana “San Pablo”. Cochabamba (Bolivia). Revista Acta Nova, 5(4), 462-476. [Consultado 28 de abril de 2020]. ISSN 1683-0789. Disponible en: http://www.scielo.org.bo/scielo.php?script=sci_arttext&pid=S1683-07892012000200004&lng=es&tlng=es.

GDAE. [Sitio web]. España. Backup cifrado. [Consulta:10 de abril 2020]. Disponible en: https://www.gadae.com/blog/haz-un-backup-cifrado-si-quieres-protegerte-del-robo-de-datos/

Gobierno digital. [Sitio web]. Colombia: Modelo de seguridad y privacidad de la información. [Consulta:10 de abril 2020]. Disponible en: //www.facebook.com/GobDigitalCO/videos/hablemosdegobiernodigital-modelo-de-seguridad-y-privacidad-de-la-informaci%C3%B3n/1343779946009784/?__so__=permalink&__rv__=related_videos

HERNANDEZ SAMPIERI, Roberto y otros; Metodología de la Investigación. 2003. Mc Graw-Hill, México D.F., México.

IIT SECURITY DATABASE. [Sitio web]. España. Lenguaje de evaluación y vulnerabilidad abierta. [Consulta: 14 de octubre 2019]. Disponible en: http://itsecdb.com/oval/

INCIBE. [Sitio web]. España. Qué es una DMZ. [Consulta: 2 de agosto 2019]. Disponible en: https://www.incibe.es/protege-tu-empresa/blog/dmz-y-te-puede-ayudar-proteger-tu-empresa

INESEM. [Sitio web]. España. Los gestores de bases de datos más utilizados. [Consulta: 2 de agosto 2019]. Disponible en: https://revistadigital.inesem.es/informatica-y-tics/los-gestores-de-bases-de-datos-mas-usados/

ISO: [Sitio web]. Estados Unidos. ISO/IEC 27001:2013 - Information technology -- Security techniques. [Consulta: 22 de julio 2019]. Disponible en: https://www.iso.org/standard/54534.html

Karspesky. [Sitio web]. Estados Unidos. HASH. [Consulta: 27 de junio 2019]. Disponible en https://latam.kaspersky.com/blog/que-es-un-hash-y-como-funciona/2806/

Lee, Y.W., Strong, D.M., Kahn, B.K. & Wang, R.Y. [Sitio web]. Estados Unidos. AIMQ: a methodology for information quality assessment. Information & management. [Consulta: 17 de abril 2019]. Disponible en: http://web.cba.neu.edu/~ywlee/publication/aimq.pdf

Microsoft. [Sitio web]. Estados Unidos: Transparent Data Encryption. [Consulta: 13 de octubre 2019]. Disponible en: http://goo.gl/aH2IQI

Microsoft SQL Server Security. [Sitio web]. Estados Unidos: Security in SQL. [Consulta: 13 de octubre 2019]. Disponible en: www.microsoft.com/sql/ technologies/security/default.mspx

Microsoft Download Center. [Sitio web]. Estados Unidos: Microsoft SQL Server 2012 Best Practices Analyzer. [Consulta: 13 de octubre 2019]. Disponible en: https://www.microsoft.com/en-us/download/ details.aspx?id=29302.

Ministerio de Educación. [Sitio web]. España: Introducción a la seguridad informática-Vulnerabilidades de un sistema informático. [Consulta: 11 de junio 2019]. Disponible en: http://recursostic.educacion.es/observatorio/web/gl/ software/ software-general/1040-introduccion-a-la-seguridad-informatica?start=3

Ministerio de Tecnologías de la Información y las Comunicaciones. [Sitio web]. Colombia. Primeros resultados del observatorio de Economía digital. [Consulta:10 de abril 2019]. Disponible en https://www.mintic.gov.co/portal /inicio/Sala-de-Prensa/Noticias/61929:MinTIC-revela-los-primeros-resultados-del-Observatorio-de-Economia-Digital

Ministerio de Tecnologías de la Información y las Comunicaciones. [Sitio web]. Colombia. Política de seguridad y privacidad de la información. [Consulta:10 de abril 2019]. Disponible en https://www.mintic.gov.co/gestionti/615/articles-5482_G2_Politica_General.pdf

Ministerio de Tecnologías de la Información y las Comunicaciones. [Sitio web]. Colombia: Plan de Seguridad y Privacidad de la Información MINTIC. [Consulta:10 de abril 2020]. Disponible en:https://www.mintic.gov.co/portal/604/ articles-100251_plan_seguridad_ privacidad_informacion_2019.pdf

MONOGRAFIAS. [Sitio web]. España: Instalación de centros de cómputo. [Consulta:10 de octubre 2018]. Disponible en: https://www.monografias.com/ trabajos81/instalacion-centro-computo/instalacion-centro-computo2.shtml

Microsoft MSDN. [Sitio web]. Estados Unidos: Inyección de código SQL. [Consulta:11 de octubre 2018]. Disponible en: http://msdn.microsoft.com/es-es/library/ms161953.aspx

National Security Agency. [Sitio web]. Estados Unidos: Minimize the Effectiveness of SQL Injection Attacks. [Consulta:11 de octubre 2018]. Disponible en: https://www.nsa.gov/ia/_files/factsheets/ SqlInjectionFactSheet.pdf.

Onasystems. [Sitio web]. Colombia. Vulnerabilidades que afectan la seguridad de las bases de datos. [Consulta: 22 de marzo 2019]. Disponible en: https://www.onasystems.net/vulnerabilidades-importantes-afectan-la-seguridad-bases-datos-las-empresas/

ORACLE. [Sitio web]. California: Instalación de Oracle. [Consulta:11 de junio 2019]. Disponible en: https://www.oracle.com/ technetwork/es/articles/ database-performance/instal-oracle19c-window-5592361-esa.html

ORACLE. [Sitio web]. California: Gestor de clusters. [Consulta:11 junio 2019]. Disponible en: https://docs.oracle.com/cd/E87217_01/DVCMI/c2_installation.htm#DVCMI112

ORACLE. [Sitio web]. California: Vulnerabilidades de Oracle. [Consulta: 4 de marzo 2019]. Disponible en: https://www.cvedetails.com/vulnerability-list/vendor_id-93/product_id-467/cvssscoremin-5/cvssscoremax-5.99/Oracle-Database-Server.html

ORACLE. [Sitio web]. California: Instalando Oracle 12C. [Consulta: 4 marzo 2019]. Disponible en: https://www.oracle.com/webfolder/technetwork/ tutorials/obe/db/12c /r1/Windows_DB_Install_OBE/Installing_Oracle_Db12c_Windows.html

OREILLY. [Sitio web]. California: Gestión de datos de calidad total. [Consulta: 4 marzo 2019]. Disponible en: https://www.oreilly.com/library/view/improving-data-warehouse/ 9780471253839/12_chapter04.html

PCI Security Standards Council. [Sitio web]. Madrid: Requisitos y procedimientos de evaluación de seguridad Versión 3.0. [Consulta: 22 de noviembre 2019]. Disponible en: https://www.pcisecuritystandards.org/ documents/PCI_DSS_v3_05Nov13_Final_ES-LA.pdf , fecha de publicación: noviembre 2013.

Portal administración electrónica. [Sitio web]. Madrid: MAGERIT v3: Metodología de Análisis y Gestión de Riesgos de los sistemas de información. [Consulta: 22 de marzo 2019]. Disponible en: http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.VCmVZhZRVJQ.

Riesgo Cero. [Sitio web]. Bogotá: Guía para gestionar un plan de continuidad de negocios. [Consulta: 23 de octubre 2019]. Disponible en: https://www.riesgoscero.com/academia/especiales/guia-para-gestionar-un-plan-de-continuidad-de-negocio-segun-la-iso-22301

Robert Malmgren, [Sitio web]. Londres: NT Security Frequently Asked Questions Version 0.41, 2.1.9. [Consulta: 12 de septiembre 2019]. Disponible en: http://www.oocities.org/dharan6/library/hack99/ntsec.htm

SANS Institute, Brian Suddeth. [Sitio web]. Madrid: Database, the final firewall. Information Security Reading Room. [Consulta: 12 de septiembre 2019]. Disponible en: http://goo.gl/sveqYR.

Software Greenhouse. [Sitio web]. España. RPO y RTO. [Consulta: 30 de marzo 2019]. Disponible en: https://www.swgreenhouse.com/conceptos-de-continuidad-de-negocio/rto-rpo

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. [Sitio web]. Bogotá: Ley 1273 de 2009, Ley de delitos informáticos en Colombia. [Consulta: 31 de agosto 2019]. Disponible en: http://www.sic.gov.co/ recursos_user/documentos/normatividad/ Ley_1273_2009.pdf

TECHTARGET. [Sitio web]. Londres: Searchdatacenter. [Consulta: 12 de septiembre 2019]. Disponible en: https://searchdatacenter.techtarget.com/es/ definicion/ Sistema-de-gestion-de-bases-de-datos-o-DBMS

UDIMA. [Sitio web]. Madrid: SQL. [Consulta: 20 de agosto 2019]. Disponible en: https://www.mundoracle.com/entorno-sql-plus.html?Pg=sql_plsql_10.htm

UNAD. [Sitio web]. Colombia. Metodologías de análisis de riesgos en un SGSI. [Consulta: 11 de mayo 2019]. Disponible en: https://hemeroteca.unad.edu.co /index.php /publicaciones-e-investigacion/article /view/1435/1874

UNIR. [Sitio web]. España. Bases de datos NoSql. [Consulta:17 de abril 2019]. Disponible en: https://www.unir.net/ingenieria/revista/noticias/bases-de-datos-nosql/549204809132/

Vergara, César. [Sitio web]. Argentina: Malware - Ataque a la Base de Datos. [Consulta: 13 de marzo 2020]. Disponible en http://ataquebd.blogspot.mx/

WELIVESECURITY. [Sitio web]. Buenos Aires: Consejos para bases de datos seguras. [Consulta: 28 de enero 2020]. Disponible en: https://www.welivesecurity.com/la-es/2017/09/05/consejos-bases-de-datos-seguras/

WELIVESECURITY. [Sitio web]. Buenos Aires: Principio del mínimo privilegio. [Consulta: 14 de enero 2020]. Disponible en: https://www.welivesecurity.com/la-es/2018/06/08/principio-menor-privilegio-limitar-acceso-imprescindible/

WELIVESECURITY. [Sitio web]. Buenos Aires: 7 motivos para decirle No a las configuraciones por defecto. [Consulta: 10 de enero 2020]. Disponible en: https://www.welivesecurity.com/la-es/2017/01/26/no-configuraciones-por-defecto/

WELIVESECURITY. [Sitio web]. Buenos Aires: MAGERIT, metodología práctica para gestionar riesgos. [Consulta: 10 de enero 2020]. Disponible en https://www.welivesecurity.com/ la-es/2013/05/14/magerit-metodologia-practica-para-gestionar-riesgos/

Winner, Duane. [Sitio web]. Australia. Making your network safer for databases. [Consulta: 20 de agosto 2019]. Disponible en: http://goo.gl/SOZvC7

ANEXOS

Tabla 1. Vulnerabilidades de sistemas operativos

VULNERABILIDADES EN SISTEMAS OPERATIVOS

Sistema	DESCRIPCION VULNERABILIDAD	ID de definición
unix	Adobe Acrobat Reader Plugin antes de 8.0.0 para los navegadores web Firefox, Internet Explorer y Opera permite un ataque remoto ...	oval: def: 10042
unix	Un cierto parche de Red Hat para SquirrelMail 1.4.8 establece el mismo valor de cookie SQMSESSID para todas las sesiones, lo que permite ...	oval: def: 10366
unix	Adobe Flash Player 9.x hasta 9.0.48.0, 8.x hasta 8.0.35.0 y 7.x hasta 7.0.70.0, cuando se ejecuta en Linux, utiliza inseguridad.	oval: def: 10519
unix	Un cierto parche de Red Hat para acpid 1.0.4 activa efectivamente una llamada a la función abierta con argumentos insuficientes, que ...	oval: def: 10555
unix	Un error de regresión en Firefox 1.0.3 y Mozilla 1.7.7 permite a los atacantes remotos inyectar Javascript arbitrario desde un pa	oval: def: 10633
unix	Un cierto script de compilación de Red Hat para nfs-utils antes de 1.0.9-35z.el5_2 en Red Hat Enterprise Linux (RHEL) 5 omite el ajuste TCP ...	oval: def: 10638
unix	Un error tipográfico en el kernel de Linux 2.6 antes de 2.6.21-rc6 y 2.4 antes de 2.4.35 hace que RTA_MAX se use como un tamaño de matriz en lugar de ...	oval: def: 10764

unix	Adobe Flash Player 9.x hasta 9.0.48.0, 8.x hasta 8.0.35.0 y 7.x hasta 7.0.70.0 no restringe suficientemente el int ...	oval: def: 11069
Windows	Vulnerabilidad de ejecución remota de código de propiedades de archivo .lnk (Windows XP)	oval: def: 1116
unix	Un parche de Red Hat para net / ipv4 / route.c en el kernel de Linux 2.6.18 en Red Hat Enterprise Linux (RHEL) 5 permite la remoción ...	oval: def: 11167
unix	Una corrección de regresión en Mozilla Firefox 1.0.7 permite a los atacantes remotos causar una denegación de servicio (bloqueo) y posiblemente ejecutar ...	oval: def: 11202
unix	Una vulnerabilidad de "sobrescritura de pila" en GnuPG (gpg) 1.x antes de 1.4.6, 2.x antes de 2.0.2 y 1.9.0 a 1.9.95 permite att	oval: def: 11245
unix	Un error de "falta de serialización" en la función unix_dgram_recvmsg en Linux 2.4.27 y anteriores, y 2.6.x hasta 2.6.9, un ...	oval: def: 11384
unix	Un error de regresión en la ruta de código restore_all del soporte dividido de 4 / 4GB para kernels Linux que no son enormes en Red Hat Linu ...	oval: def: 11410
unix	** DISPUTADO ** Vulnerabilidad de inclusión remota de archivos PHP en funciones / plugin.php en SquirrelMail 1.4.6 y anteriores, si se re ...	oval: def: 11670
unix	Adobe Reader y Acrobat 7.0.8 y versiones anteriores permiten a los atacantes remotos asistidos por el usuario ejecutar código a través de un archivo PDF diseñado ...	oval: def: 11698
Windows	Vulnerabilidad de variable no inicializada ACCWIZ.dll	oval: def: 11756
unix	ActionScript 3 (AS3) en Adobe Flash Player 9.0.47.0, y otras versiones y otras 9.0.124.0 y versiones anteriores, permite ...	oval: def: 11874

Windows	Vulnerabilidad de control de ActiveX de acceso	oval: def: 11907
Windows	Vulnerabilidad de ejecución remota de código de propiedades de archivo .lnk (Windows 2000)	oval: def: 1192
Windows	Una denegación de servicio causada a través de una imagen PNG animada en Opera antes de 10.61.	oval: def: 11933
Windows	Vulnerabilidad de compensación de matriz de .NET Framework	oval: def: 12105
Windows	Infracción de acceso en el manejo de errores de URL	oval: def: 12315
Windows	Vulnerabilidad de daños en la pila de .NET Framework	oval: def: 12406
Windows	Vulnerabilidad de memoria de registro de ADO	oval: def: 12411
Windows	Vulnerabilidad de validación de Active Directory SPN	oval: def: 12485
unix	Una vulnerabilidad de seguridad en el manejo de Solaris 10 ICMP puede permitir un SystemPanic y provocar una denegación de servicio (DoS)	oval: def: 1249
Windows	Vulnerabilidad de optimización JIT de .NET Framework	oval: def: 12686
Windows	Vulnerabilidad de servicios de certificados de Active Directory	oval: def: 12749
Windows	Acceso a la vulnerabilidad de DoS de memoria no asignada	oval: def: 12915
Windows	Vulnerabilidad de herencia de clase de .NET Framework	oval: def: 13069
Windows	Accesibilidad activa Vulnerabilidad insegura en la carga de bibliotecas	oval: def: 13116
Windows	Vulnerabilidad de ejecución remota de código de archivo abierto .lnk (XP, SP1)	oval: def: 1329
Windows	** DISPUTADO ** Vulnerabilidad de ruta de búsqueda no confiable en Mozilla Network Security Services (NSS), como se usa en Google Chrome ...	oval: def: 13414

unix	Una vulnerabilidad de seguridad en el sistema de archivos de bucle invertido (LOFS) de Solaris 10 puede permitir que los archivos en una zona no global ...	oval: def: 1372
Windows	Vulnerabilidad de objetos no administrados de .NET Framework	oval: def: 13972
Windows	Vulnerabilidad de desbordamiento del búfer en Active Directory	oval: def: 14037
Windows	Vulnerabilidad de daños en el montón de .NET Framework	oval: def: 14513
Windows	Vulnerabilidad de asignación de búfer en .NET Framework	oval: def: 14655
Windows	Vulnerabilidad de suplantación de barra de direcciones (WinS03)	oval: def: 1478
Windows	Vulnerabilidad de RCE de desbordamiento del montón en caché de ADO (MS12-045)	oval: def: 14783
Windows	Vulnerabilidad de ejecución remota de código de archivo abierto .lnk (Windows 2000, SP4)	oval: def: 1488
Windows	Vulnerabilidad de serialización de .NET Framework (CVE-2012-0161)	oval: def: 14951
Windows	Vulnerabilidad de ejecución remota de código de archivo abierto .lnk (XP, SP2)	oval: def: 1517
Windows	.lnk Vulnerabilidad de ejecución remota de código en el archivo abierto (Server 2003)	oval: def: 1537
Windows	Vulnerabilidad de validación de parámetros de .NET Framework	oval: def: 15495
Windows	Vulnerabilidad de ejecución remota de código de archivo abierto .lnk (Server 2003, SP1)	oval: def: 1551
Windows	Vulnerabilidad de carga de bibliotecas inseguras en .NET Framework (MS12-074)	oval: def: 15520
Windows	Vulnerabilidad de serialización de .NET Framework (CVE-2012-0160)	oval: def: 15554
Windows	Vulnerabilidad de comparación del índice de .NET Framework	oval: def: 15580
Windows	Vulnerabilidad de suplantación de barra de direcciones (Win2K)	oval: def: 1567

unix	Una vulnerabilidad de seguridad en el kernel de Solaris puede permitir que ocurra una condición de denegación de servicio (DoS)	oval: def: 1626
Windows	Vulnerabilidad de suplantación de barra de direcciones (XP de 64 bits)	oval: def: 1646
Windows	Vulnerabilidad de desbordamiento del búfer en Active Directory (MS13-032)	oval: def: 16463
Windows	Vulnerabilidad de suplantación de barra de direcciones (XP, SP2)	oval: def: 1686
Windows	Una API de JavaScript en Adobe Reader y Acrobat 9.x antes de 9.5.5, 10.x antes de 10.1.7 y 11.x antes de 11.0.03 permite el ataque ...	oval: def: 16864
unix	/ usr / lib / print / conv_fix Vulnerabilidad de escalada de privilegios	oval: def: 1732
Windows	Vulnerabilidad de suplantación de barra de direcciones (2K / XP)	oval: def: 1775
Windows	Vulnerabilidad de suplantación de barra de direcciones (S03, SP1)	oval: def: 1788
Windows	Vulnerabilidad de daños en la memoria en el control ActiveX (S03, SP1)	oval: def: 1821
unix	Una vulnerabilidad de seguridad en la forma en que xscreensaver (1) interactúa con la tecnología de asistencia de GNOME puede permitir el comando arbitrario Ex ...	oval: def: 1832
Windows	Vulnerabilidad de daños en la memoria relacionada con el formato de archivo de acceso (CVE-2013-3156) - MS13-074	oval: def: 18442
Windows	Vulnerabilidad de daños en la memoria de acceso (CVE-2013-3155) - MS13-074	oval: def: 18624
Windows	Vulnerabilidad de daños en la memoria de acceso (CVE-2013-3157) - MS13-074	oval: def: 18664
Windows	Vulnerabilidad del compilador JIT de .NET	oval: def: 1873
Windows	Vulnerabilidad de daños en la dirección en Hyper-V (CVE-2013-3898) - MS13-092	oval: def: 18851

Windows	Vulnerabilidad de daños en la memoria en el control ActiveX (XP, SP2)	oval: def: 1891
Windows	Inscripción de certificados ActiveX Eliminación remota de certificados no autorizada	oval: def: 190
Windows	Vulnerabilidad de daños en la memoria en el control ActiveX (Win2K)	oval: def: 1924
Windows	Vulnerabilidad de daños en la memoria en el control ActiveX (2K / XP)	oval: def: 1944
Windows	Vulnerabilidad de daños en la memoria en el control ActiveX (WinS03)	oval: def: 1949
unix	Una vulnerabilidad de seguridad en el servicio in.iked (1M) puede conducir a una denegación de servicio (DoS)	oval: def: 1966
Windows	Vulnerabilidad de daños en la memoria en el control ActiveX (XP de 64 bits)	oval: def: 2009
unix	Una vulnerabilidad de seguridad en el servicio inetd (1M) de Solaris 10 puede provocar una condición de denegación de servicio (DoS)	oval: def: 2032
unix	Vulnerabilidad de "registro de defunción"	oval: def: 20741
unix	Vulnerabilidad de "registro de defunción"	oval: def: 20886
Windows	Vulnerabilidad del cargador de .NET PE	oval: def: 2093
unix	Vulnerabilidad de "registro de defunción"	oval: def: 20930
Windows	Vulnerabilidad de objetos ActiveX	oval: def: 2109
unix	Una vulnerabilidad de seguridad en la implementación de TCP de los sistemas Solaris 10 puede provocar un pánico del sistema bajo TCP / IP alto ...	oval: def: 2120
Windows	Vulnerabilidad de suplantación de barra de direcciones	oval: def: 2162
unix	Una vulnerabilidad de seguridad con la función strfreectty () del Sistema de archivos especiales (SPECFS) puede permitir un uso local sin privilegios ...	oval: def: 2173

Tabla 2. Vulnerabilidades en bases de datos

ID de CVE	Tipo de vulnerab	Fecha de actualización	Puntuación	Nivel de acceso obtenido	Complejidad	Autenticación	Confidenc.	Integridad	DETALLE
CVE-2019-2776		26/07/2019	**5.5**	Ninguna	Bajo (no existen condiciones de acceso especializadas o circunstancias atenuantes. Se requiere muy poco conocimiento o habilidad para explotar)	Sistema único (la vulnerabilidad requiere que un atacante inicie sesión en el sistema (como en una línea de comando o mediante una sesión de escritorio o una interfaz web)).	Parcial (hay una divulgación informativa considerable).	Parcial (es posible modificar algunos archivos o información del sistema, pero el atacante no tiene control sobre lo que puede modificarse o el alcance de lo que puede afectar el atacante es limitado).	Vulnerabilidad en el componente Core RDBMS de Oracle Database Server. Las versiones compatibles afectadas son 12.1.0.2, 12.2.0.1, 18c y 19c. La vulnerabilidad fácilmente explotable permite que el atacante con privilegios elevados tenga el privilegio Crear cualquier índice con acceso a la red a través de OracleNet para comprometer el RDBMS principal. Si bien la vulnerabilidad se encuentra en Core RDBMS, los ataques pueden afectar significativamente a productos adicionales. Los ataques exitosos de esta vulnerabilidad pueden resultar en acceso no autorizado a datos críticos o acceso completo a todos los datos accesibles de Core RDBMS, así como también actualización, inserción o eliminación no autorizadas de acceso a algunos de los datos accesibles de Core RDBMS. CVSS 3.0 Base Score 7.6 (Impactos de confidencialidad e integridad). Vector CVSS: (CVSS: 3.0 / AV: N / AC: L / PR: H / UI: N / S: C / C: H / I: L / A: N).
CVE-2019-2582	+ Info	25/04/2019	5.0	Ninguna	Bajo (no existen condiciones de acceso especializadas o circunstancias atenuantes. Se requiere muy poco conocimiento o habilidad para explotar).	No requerido (no se requiere autenticación para aprovechar la vulnerabilidad).	Parcial (hay una divulgación informativa considerable).	Ninguna (no hay impacto en la integridad del sistema)	Vulnerabilidad en el componente Core RDBMS de Oracle Database Server. Las versiones compatibles que se ven afectadas son 12.2.0.1 y 18c. La vulnerabilidad fácilmente explotable permite que un atacante no autenticado con acceso a la red a través de Oracle Net ponga en peligro Core RDBMS. Los ataques exitosos de esta vulnerabilidad pueden resultar en acceso de lectura no autorizado a un subconjunto de datos accesibles de Core RDBMS. CVSS 3.0 Puntaje base 5.3 (Impactos de confidencialidad). Vector CVSS: (CVSS: 3.0 / AV: N / AC: L / PR: N / UI: N / S: U / C: L / I: N / A: N).

CVE-2018-2680		2/10/2019	5.1	Ninguna	Alto (existen condiciones de acceso especializadas. Es difícil de explotar y se deben cumplir varias condiciones especiales para explotar)	No requerido (no se requiere autenticación para aprovechar la vulnerabilidad).	Parcial (hay una divulgación informativa considerable).	Parcial (es posible modificar algunos archivos o información del sistema, pero el atacante no tiene control sobre lo que puede modificarse o el alcance de lo que puede afectar el atacante es limitado).	Vulnerabilidad en el componente Java VM de Oracle Database Server. Las versiones compatibles que se ven afectadas son 11.2.0.4, 12.1.0.2 y 12.2.0.1. La vulnerabilidad difícil de explotar permite que un atacante no autenticado con acceso a la red a través de múltiples protocolos comprometa Java VM. Los ataques exitosos requieren la interacción humana de una persona que no sea el atacante y, aunque la vulnerabilidad se encuentra en Java VM, los ataques pueden afectar significativamente a productos adicionales. Los ataques exitosos de esta vulnerabilidad pueden resultar en la adquisición de Java VM. Puntuación básica de CVSS 3.0 8.3 (impactos de confidencialidad, integridad y disponibilidad). Vector CVSS: (CVSS: 3.0 / AV: N / AC: H / PR: N / UI: R / S: C / C: H / I: H / A: H).
CVE-2016-0472		7/12/2016	5.5	Ninguna	Bajo	Sistema único	Parcial	Ninguna	La vulnerabilidad no especificada en el componente XDB - Base de datos XML en Oracle Database Server 11.2.0.4, 12.1.0.1 y 12.1.0.2 permite a los usuarios autenticados remotos afectar la confidencialidad y la disponibilidad a través de vectores desconocidos.
CVE-2015-4857		23/12/2016	5.5	Ninguna	Bajo	Sistema único	Parcial	Parcial	La vulnerabilidad no especificada en el componente RDBMS en Oracle Database Server 12.1.0.1 y 12.1.0.2 permite a los usuarios autenticados remotos afectar la confidencialidad y la integridad a través de vectores desconocidos.
CVE-2015-4755		21/09/2017	5.0	Ninguna	Bajo	No requerido	Parcial	Ninguna	La vulnerabilidad no especificada en el componente de seguridad RDBMS en Oracle Database Server 12.1.0.2 permite a los atacantes remotos afectar la confidencialidad a través de vectores desconocidos.
CVE-2015-2655		21/09/2017	5.5	Ninguna	Bajo	Sistema único	Parcial	Parcial	La vulnerabilidad no especificada en el componente Application Express en Oracle Database Server anterior a 4.2.3.00.08 permite a los usuarios autenticados remotos afectar la confidencialidad y la integridad a través de vectores desconocidos.
CVE-2013-5853		5/03/2014	5.0	Ninguna	Bajo	No requerido	Ninguna	Ninguna	La vulnerabilidad no especificada en el componente Core RDBMS en Oracle Database Server 11.1.0.7, 11.2.0.3 y 12.1.0.1 permite a los atacantes remotos afectar la disponibilidad a través de vectores desconocidos.

CVE-2013-3826		18/09/2017	5.0	Ninguna	Bajo	No requerido	Parcial	Ninguna	La vulnerabilidad no especificada en el componente Core RDBMS en Oracle Database Server 11.1.0.7, 11.2.0.2, 11.2.0.3 y 12.1.0.1 permite a los atacantes remotos afectar la confidencialidad a través de vectores desconocidos.
CVE-2013-1554		10/10/2013	5.0	Ninguna	Bajo	No requerido	Ninguna	Ninguna	La vulnerabilidad no especificada en el componente Network Layer en Oracle Database Server 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.2 y 11.2.0.3 permite a los atacantes remotos afectar la disponibilidad a través de vectores desconocidos.
CVE-2013-1538		10/10/2013	5.0	Ninguna	Bajo	No requerido	Ninguna	Ninguna	La vulnerabilidad no especificada en el componente Network Layer en Oracle Database Server 11.2.0.2 y 11.2.0.3 permite a los atacantes remotos afectar la disponibilidad a través de vectores desconocidos.
CVE-2013-1519		10/10/2013	5.0	Ninguna	Bajo	No requerido	Ninguna	Parcial	La vulnerabilidad no especificada en el componente Application Express en Oracle Database Server anterior a 4.2.1 permite a los atacantes remotos afectar la integridad a través de vectores desconocidos.
CVE-2012-1747		10/10/2013	5.0	Ninguna	Bajo	No requerido	Ninguna	Ninguna	La vulnerabilidad no especificada en el componente Network Layer en Oracle Database Server 10.2.0.3, 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.2 y 11.2.0.3, cuando se ejecuta en Windows, permite que los atacantes remotos afecten la disponibilidad a través de vectores desconocidos , una vulnerabilidad diferente a CVE-2012-1746.
CVE-2012-1746		10/10/2013	5.0	Ninguna	Bajo	No requerido	Ninguna	Ninguna	La vulnerabilidad no especificada en el componente Network Layer en Oracle Database Server 10.2.0.3, 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.2 y 11.2.0.3, cuando se ejecuta en Windows, permite que los atacantes remotos afecten la disponibilidad a través de vectores desconocidos , una vulnerabilidad diferente a CVE-2012-1747.
CVE-2012-1745		10/10/2013	5.0	Ninguna	Bajo	No requerido	Ninguna	Ninguna	La vulnerabilidad no especificada en el componente Network Layer en Oracle Database Server 10.2.0.3, 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.2 y 11.2.0.3 permite a los atacantes remotos afectar la disponibilidad a través de vectores desconocidos.

CVE-2012-0528		10/10/2013	**5.8**	Ninguna	Medio	No requerido	Parcial	Parcial	La vulnerabilidad no especificada en el componente Enterprise Platform Base Platform en Oracle Database Server 10.2.0.3, 10.2.0.4, 10.2.0.5 y 11.1.0.7, y Oracle Enterprise Manager Grid Control, permite a los atacantes remotos afectar la confidencialidad e integridad a través de vectores desconocidos relacionados con Marco de seguridad.
CVE-2012-0512		10/10/2013	5.5	Ninguna	Bajo	Sistema único	Parcial	Parcial	La vulnerabilidad no especificada en el componente Enterprise Platform Base Platform en Oracle Database Server 11.1.0.7 y 11.2.0.2 y Oracle Enterprise Manager Grid Control permite a los usuarios autenticados remotos afectar la confidencialidad e integridad a través de vectores desconocidos relacionados con Enterprise Config Management.
CVE-2012-0082		28/08/2017	5.5	Ninguna	Bajo	Sistema único	Ninguna	Parcial	La vulnerabilidad no especificada en el componente Core RDBMS en Oracle Database Server 10.1.0.5, 10.2.0.3, 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.2 y 11.2.0.3 permite a los usuarios autenticados remotos afectar la integridad y la disponibilidad a través de desconocidos vectores
CVE-2012-0072		28/08/2017	5.0	Ninguna	Bajo	No requerido	Ninguna	Ninguna	La vulnerabilidad no especificada en el componente Listener en Oracle Database Server 10.1.0.5, 10.2.0.3, 10.2.0.4, 10.2.0.5, 11.1.0.7 y 11.2.0.2 permite que los atacantes remotos afecten la disponibilidad a través de vectores desconocidos.
CVE-2011-2230		4/10/2011	5.0	Ninguna	Bajo	No requerido	Ninguna	Ninguna	La vulnerabilidad no especificada en el componente Core RDBMS en Oracle Database Server 10.1.0.5, 10.2.0.3, 10.2.0.4, 10.2.0.5, 11.1.0.7 y 11.2.0.1 permite que los atacantes remotos afecten la disponibilidad a través de vectores desconocidos.
CVE-2011-0875		8/09/2017	5.5	Ninguna	Bajo	Sistema único	Parcial	Parcial	La vulnerabilidad no especificada en el componente EMCTL en Oracle Database Server 11.1.0.7 y Oracle Enterprise Manager Grid Control 10.1.0.6, 10.2.0.5 y 11.1.0.1 permite a los usuarios autenticados remotos afectar la confidencialidad y la integridad a través de vectores desconocidos.

CVE-2011-0831		4/10/2011	5.5	Ninguna	Bajo	Sistema único	Parcial	Parcial	Vulnerabilidad no especificada en el componente Enterprise Config Management en Oracle Database Server 10.1.0.5, 10.2.0.3, 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.1 y 11.2.0.2; y Oracle Enterprise Manager Grid Control 10.1.0.6 y 10.2.0.5; permite a los usuarios autenticados remotos afectar la confidencialidad e integridad a través de vectores desconocidos.
CVE-2011-0816		4/10/2011	5.5	Ninguna	Bajo	Sistema único	Parcial	Parcial	Vulnerabilidad no especificada en el componente CMDB Metadata & Instance APIs en Oracle Database Server 10.1.0.5, 10.2.0.3, 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.1 y 11.2.0.2; y Oracle Enterprise Manager Grid Control 10.1.0.6 y 10.2.0.5; permite a los usuarios autenticados remotos afectar la confidencialidad e integridad a través de vectores desconocidos.
CVE-2011-0806		20/04/2011	5.0	Ninguna	Bajo	No requerido	Ninguna	Ninguna	La vulnerabilidad no especificada en el componente Network Foundation en Oracle Database Server 10.1.0.5, 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.1 y 11.2.0.2, cuando se ejecuta en Windows, permite que los atacantes remotos afecten la disponibilidad a través de vectores desconocidos .
CVE-2011-0787		20/04/2011	5.5	Ninguna	Bajo	Sistema único	Parcial	Parcial	La vulnerabilidad no especificada en el componente Application Service Level Management en Oracle Database Server 11.1.0.7 y Enterprise Manager Grid Control permite a los usuarios autenticados remotos afectar la confidencialidad y la integridad a través de vectores desconocidos relacionados con los acuerdos de nivel de servicio.
CVE-2010-2412		11/11/2010	5.5	Ninguna	Bajo	Sistema único	Parcial	Parcial	La vulnerabilidad no especificada en el componente OLAP en Oracle Database Server 11.1.0.7 permite a los usuarios autenticados remotos afectar la confidencialidad y la integridad a través de vectores desconocidos.
CVE-2010-0852		22/10/2012	5.5	Ninguna	Bajo	Sistema único	Parcial	Parcial	La vulnerabilidad no especificada en el componente XML DB en Oracle Database 9.2.0.8, 9.2.0.8DV, 10.1.0.5 y 10.2.0.3 permite a los usuarios autenticados remotos afectar la confidencialidad y la integridad a través de vectores desconocidos.
CVE-2009-2000		22/10/2012	5.0	Ninguna	Bajo	No requerido	Parcial	Ninguna	La vulnerabilidad no especificada en el componente de autenticación en Oracle Database 11.1.0.7 permite a los atacantes remotos afectar la confidencialidad a través de vectores desconocidos.

CVE-2009-1997		22/10/2012	5.0	Ninguna	Bajo	No requerido	Parcial	Ninguna	La vulnerabilidad no especificada en el componente de autenticación en Oracle Database 10.2.0.3 y 11.1.0.7 permite a los atacantes remotos afectar la confidencialidad a través de vectores desconocidos.
CVE-2009-1993		22/10/2012	5.5	Ninguna	Bajo	Sistema único	Parcial	Parcial	La vulnerabilidad no especificada en el componente Application Express en Oracle Database 3.0.1 permite a los usuarios autenticados remotos afectar la confidencialidad e integridad, relacionada con FLOWS_030000.WWV_EXECUTE_IMMEDIATE.
CVE-2009-1973		16/08/2017	5.5	Ninguna	Bajo	Sistema único	Parcial	Parcial	La vulnerabilidad no especificada en el componente Virtual Private Database en Oracle Database 10.1.0.5, 10.2.0.4 y 11.1.0.7 permite a los usuarios autenticados remotos afectar la confidencialidad y la integridad, relacionadas con las políticas de VPD.
CVE-2009-1970		16/08/2017	5.0	Ninguna	Bajo	No requerido	Ninguna	Ninguna	La vulnerabilidad no especificada en el componente Listener en Oracle Database 9.2.0.8, 9.2.0.8DV, 10.1.0.5, 10.2.0.4 y 11.1.0.7 permite que los atacantes remotos afecten la disponibilidad a través de vectores desconocidos, una vulnerabilidad diferente a CVE-2009-0991.
CVE-2009-1967		16/08/2017	5.5	Ninguna	Bajo	Sistema único	Parcial	Parcial	La vulnerabilidad no especificada en el componente de administración de configuración en (1) Oracle Database 11.1.0.7 y (2) Oracle Enterprise Manager 10.2.0.4 permite a los usuarios autenticados remotos afectar la confidencialidad y la integridad a través de vectores desconocidos, una vulnerabilidad diferente a CVE-2009-1966.
CVE-2009-1966		16/08/2017	5.5	Ninguna	Bajo	Sistema único	Parcial	Parcial	La vulnerabilidad no especificada en el componente Config Management en (1) Oracle Database 11.1.0.7 y (2) Oracle Enterprise Manager 10.2.0.4 permite a los usuarios autenticados remotos afectar la confidencialidad y la integridad a través de vectores desconocidos, una vulnerabilidad diferente a la de CVE-2009-1967.
CVE-2009-1965		22/10/2012	5.4	Ninguna	Medio	No requerido	Parcial	Parcial	La vulnerabilidad no especificada en el componente Net Foundation Layer en Oracle Database 9.2.0.8 y 10.1.0.5 permite a los atacantes remotos afectar la confidencialidad, integridad y disponibilidad a través de vectores desconocidos.

CVE-2009-1964		22/10/2012	5.5	Ninguna	Bajo	Sistema único	Parcial	Parcial	La vulnerabilidad no especificada en el componente Workspace Manager en Oracle Database 10.2.0.4 permite a los usuarios autenticados remotos afectar la confidencialidad y la integridad a través de vectores desconocidos.
CVE-2009-1021		16/08/2017	5.5	Ninguna	Bajo	Sistema único	Parcial	Parcial	La vulnerabilidad no especificada en el componente de Replicación avanzada en Oracle Database 9.2.0.8, 9.2.0.8DV, 10.1.0.5 y 10.2.0.3 permite a los usuarios autenticados remotos afectar la confidencialidad y la integridad a través de vectores desconocidos.
CVE-2009-1018		22/10/2012	5.5	Ninguna	Bajo	Sistema único	Parcial	Parcial	La vulnerabilidad no especificada en el componente Workspace Manager en Oracle Database 10.2.0.4 permite a los usuarios autenticados remotos afectar la confidencialidad y la integridad, relacionada con SYS.LTRIC (WMSYS.LTRIC).
CVE-2009-0987		16/08/2017	5.5	Ninguna	Bajo	Sistema único	Parcial	Parcial	La vulnerabilidad no especificada en el componente Upgrade en Oracle Database 9.2.0.8, 9.2.0.8DV, 10.1.0.5 y 10.2.0.3 permite a los usuarios autenticados remotos afectar la confidencialidad y la integridad a través de vectores desconocidos.
CVE-2008-6065	+ Priv	30/10/2018	5.1	Usuario	Alto	No requerido	Parcial	Parcial	Oracle Database Server 10.1, 10.2 y 11g otorga permisos de ESCRITURA de directorio para nombres de ruta arbitrarios con alias en una instrucción CREATE OR REPLACE DIRECTORIO, que permite a los usuarios autenticados remotos con privilegios CREAR CUALQUIER DIRECTORIO obtener privilegios SYSDBA aliasing el nombre de ruta del directorio de contraseña, y luego sobrescribiendo el archivo de contraseña a través de las operaciones UTL_FILE, un problema relacionado con CVE-2006-7141.
CVE-2008-2592	SQL	11/10/2018	5.5	Ninguna	Bajo	Sistema único	Parcial	Parcial	La vulnerabilidad no especificada en el componente de Replicación avanzada en Oracle Database 9.0.1.5 FIPS +, 9.2.0.8, 9.2.0.8DV, 10.1.0.5, 10.2.0.4 y 11.1.0.6 tiene un impacto desconocido y vectores de ataque autenticado remoto relacionados con SYS.DBMS_DEFER_SYS. NOTA: la información anterior se obtuvo de la CPU Oracle de julio de 2008. Oracle no ha comentado sobre las afirmaciones confiables de los investigadores de que se trata de una vulnerabilidad de inyección SQL en el procedimiento DELETE_TRAN.

CVE-2008-1816	SQL	11/10/2018	5.5	Ninguna	Bajo	Sistema único	Parcial	Parcial	Múltiples vulnerabilidades no especificadas en Oracle Database 10.1.0.5 y 10.2.0.3 tienen un impacto desconocido y vectores de ataque autenticado remoto relacionados con (1) SDO_UTIL en el componente Oracle Spatial, también conocido como DB05; o (2) auditoría fina en el componente Auditoría, también conocido como DB14. NOTA: la información previa se obtuvo de la CPU de Oracle. Oracle no ha comentado sobre las afirmaciones confiables de los investigadores de que DB05 es inyección SQL.
CVE-2007-5513		15/10/2018	5.0	Ninguna	Bajo	No requerido	Ninguna	Parcial	El componente XML DB (XMLDB) en Oracle Database 9.2.0.8, 9.2.0.8DV y 10.1.0.5 genera entradas de auditoría incorrectas en la columna USERID en la que (1) nombres de usuario largos se recortan a 5 caracteres, o (2) entradas cortas contener caracteres adicionales de nombres de usuario en entradas anteriores, también conocido como DB23.
CVE-2007-3854	SQL de desbordamiento	28/07/2017	5.5	Ninguna	Bajo	Sistema único	Parcial	Parcial	Múltiples vulnerabilidades no especificadas en Oracle Database 9.0.1.5+, 9.2.0.7 y 10.1.0.5 permiten que los usuarios autenticados remotos tengan un impacto desconocido a través de (1) SYS.DBMS_PRVTAQIS en el componente Advanced Queuing (DB02) y (2) MDSYS.MD en El componente espacial (DB12). NOTA: Oracle no ha cuestionado las afirmaciones confiables de los investigadores de que DB02 es para inyección SQL y DB12 para desbordamiento de búfer.
CVE-2007-0269		28/07/2017	5.5	Ninguna	Bajo	Sistema único	Parcial	Parcial	La vulnerabilidad no especificada en Oracle Database 9.2.0.8, 10.1.0.5 y 10.2.0.3 tiene vectores de impacto y ataque desconocidos relacionados con los privilegios Change Data Capture y sys.dbms_cdc_subscribe, también conocido como DB02.
CVE-2005-3206	DoS	10/07/2017	5.0	Ninguna	Bajo	No requerido	Ninguna	Ninguna	iSQL * Plus (isqlplus) para Oracle9i Database Server Release 2 9.0.2.4 permite a los atacantes remotos causar una denegación de servicio (parada de escucha TNS) a través de una solicitud HTTP con un parámetro sid que contiene un comando STOP.
CVE-2005-0701	Dir. Trav.	17/10/2016	5.0	Ninguna	Bajo	No requerido	Parcial	Ninguna	La vulnerabilidad transversal del directorio en Oracle Database Server 8i y 9i permite a los atacantes remotos leer o cambiar el nombre de archivos arbitrarios a través de secuencias "\\. \\ .." (barra invertida de puntos y puntos modificados) a funciones UTL_FILE como (1) UTL_FILE.FOPEN o (2) UTL_FILE.frename.

CVE-2005-0298	+ Info	10/07/2017	5.0	Ninguna	Bajo	No requerido	Parcial	Ninguna	Los objetos de DIRECTORIO en Oracle 8i a través de Oracle 10g contienen la ubicación de un directorio específico del sistema operativo, lo que permite a los usuarios con privilegios de lectura a un objeto de DIRECTORIO obtener información confidencial.
CVE-2002-0856	DoS	10/09/2008	5.0	Ninguna	Bajo	No requerido	Ninguna	Ninguna	El oyente SQL * NET para Oracle Net Oracle9i 9.0.xy 9.2 permite a los atacantes remotos causar una denegación de servicio (bloqueo) a través de ciertas solicitudes de depuración que la función de depuración no maneja correctamente.
CVE-2001-0515	DoS	10/09/2008	5.0	Ninguna	Bajo	No requerido	Ninguna	Ninguna	Oracle Listener en Oracle 7.3 y 8i permite a los atacantes remotos causar una denegación de servicio a través de un paquete de conexión mal formado con un gran valor de offset_to_data.
CVE-1999-0784	DoS	5/09/2008	5.0	Ninguna	Bajo	No requerido	Ninguna	Ninguna	Denegación de servicio en Oracle TNSLSNR SQL * Net Listener a través de una cadena con formato incorrecto al puerto de escucha, también conocido como NERP.