UNAM

RED·TIC

Red de Responsables TIC

U N A M

Lineamientos y recomendaciones para la administración de bases de datos

Segunda versión

Octubre de 2022

Contenido

I. OBJETIVO 4

II. ALCANCE 4

III. TÉRMINOS Y DEFINICIONES 4

IV. RESPONSABILIDADES DEL PERSONAL INVOLUCRADO 5

A. De los titulares de las entidades o dependencias universitarias 5
B. De los responsables de las Tecnologías de Información y Comunicación (TIC) 6
C. De los administradores de bases de datos 6
D. Del personal universitario que hace uso de las bases de datos 6

V. SOBRE LA INTEGRACIÓN DE TECNOLOGÍAS PARA LAS BASES DE DATOS 6

A. Unificación de las bases de datos universitarias 6
B. Consideraciones para la homologación en bases de datos 7
C. Interoperabilidad de las bases de datos 7
D. Neutralidad tecnológica 7
E. Calidad de datos 8
F. Consideraciones de servicios en la nube 9

VI. SOBRE EL DISEÑO DE LAS BASES DE DATOS 9

A. Consideraciones sobre el modelado relacional de datos 9
B. Consideraciones sobre el diccionario de datos 10

VII. SOBRE LA CREACIÓN Y CONFIGURACIÓN DE BASES DE DATOS 11

A. Consideraciones sobre la creación de bases de datos 11
B. Consideraciones sobre la configuración de bases de datos 11
1. Parámetros de configuración 11
2. Cuentas 12
3. Seguridad 12

VIII. SOBRE EL ALMACENAMIENTO DE INFORMACIÓN 13

A. Medios de almacenamiento 13
B. Protección de datos 13
C. Uso de la información 14

IX. GESTIÓN DE LAS BASES DE DATOS 14

A. Memorias técnicas sobre las bases de datos 14
B. Gestión de las solicitudes de bases de datos 14
C. Gestión del servicio de las bases de datos 14
D. Monitoreo de las bases de datos 15

X. SEGURIDAD DE LAS BASES DE DATOS 15

A. Plan de respaldos y recuperación 15
B. Consideraciones para la disponibilidad 16
C. Eliminación de la información 16
1. Datos personales 16
2. Respaldos 16

3. Medios de almacenamiento *17*
D. CONSIDERACIONES GENERALES DE SEGURIDAD 17

XI. SOBRE RECURSOS HUMANOS EN BASES DE DATOS 18

A. REFORZAMIENTO DE CAPACIDADES Y HABILIDADES DEL PERSONAL QUE ADMINISTRA LAS BASES DE DATOS 18
B. DIFUSIÓN DE BUENAS PRÁCTICAS EN LAS BASES DE DATOS 18

XII. MARCO LEGAL APLICABLE 18

1. ANEXOS 20

ANEXO I. DICCIONARIO DE DATOS 20
ANEXO II. MEMORIA DE LOS PARÁMETROS DE CONFIGURACIÓN 21
ANEXO III. SOLICITUD DE BASE DE DATOS 22

2. BIBLIOGRAFÍA Y REFERENCIAS ELECTRÓNICAS 24

3. CRÉDITOS 26

Lineamientos y recomendaciones para la administración de bases de datos. Segunda versión

I. Objetivo

Las entidades académicas y dependencias administrativas de la UNAM cuentan con diferentes bases de datos gestionadas con métodos profesionales que les permitan brindar mejores servicios a partir de datos estructurados y consistentes, a fin de dar cumplimiento a las atribuciones y funciones que tienen encomendadas de acuerdo con el plan de desarrollo institucional vigente.

Estos lineamientos se presentan como una guía para la creación, uso, operación, aseguramiento, mantenimiento y administración de las bases de datos. Su finalidad es aportar prácticas probadas que contribuyan en las actividades relacionadas con la gestión del área.

El documento fue elaborado por especialistas de la Red de Responsables TIC, la Red de Ingeniería de Software y Base de Datos, la Dirección General de Cómputo y de Tecnologías de Información y Comunicación de esta universidad, así como por estudiosos de otras áreas universitarias, con la finalidad de dar respuesta a la solicitud del Consejo Asesor de Tecnologías de Información y Comunicación (CATIC) de la UNAM para promover prácticas validadas, así como para homologar procedimientos en la materia al interior de nuestra casa de estudios.

II. Alcance

Estos lineamientos son aplicables para todas las entidades académicas y dependencias universitarias que administran bases de datos de forma interna. De manera complementaria, pueden ser de valor en caso de que esta actividad sea realizada por un proveedor de servicios.

III. Términos y definiciones

Administrador de bases de datos. El administrador de bases de datos (DBA) es el profesional de tecnologías de la información y la comunicación, responsable de los aspectos técnicos, tecnológicos, científicos, inteligencia de negocios y legales de bases de datos (Benítez, 2016:5).

Almacenamiento de datos como servicio (Data Storage as a Service, DSaaS). Categoría de servicio en la nube. La capacidad que se ofrece al cliente del servicio en la nube consiste en la provisión y el uso de almacenamiento de datos y capacidades relacionadas.

Datos sucios. Son aquellos que están incompletos, son erróneos o inexactos, o que no cumplen con cualquiera de las características de calidad que le son asignadas.

Datos unificados. Son aquellos que reúnen fuentes de datos dispares para presentar una vista única de los datos de una organización.

Encargado. La persona física o jurídica distinta a las áreas, entidades o dependencias, que realizan el tratamiento de los datos personales a nombre de la Universidad.

Esquema global. Es un modelo para la vista presentada de los datos en respuesta a una consulta.

Fuente primaria de datos autoritativa. Es el área universitaria de la cual se obtiene información confiable para otros usos, como emisión de informes o prestación de servicios. Es responsable de actualizar y validar dicha información a partir de datos que la misma área genera o que obtiene e integra a partir de fuentes de datos autónomas.

Limpieza de datos (Data cleansing). Proceso para corregir o eliminar datos incorrectos, corruptos, formateados incorrectamente, duplicados o incompletos dentro de un conjunto de datos.

Metadatos. Datos que describen o proporcionan el contexto para otros datos.

Neutralidad tecnológica y portabilidad de datos. Se refiere a "la capacidad de trasladar y reutilizar fácilmente los datos entre distintas aplicaciones y sistemas" (Comisión Europea, 2017:11).

Nivel de servicio. Definición que establece los niveles de calidad, con los que operará y estará disponible un sistema o servicio digital (Diario Oficial de la Federación, 2011).

Punto objetivo de recuperación. Define la pérdida de datos que se puede aceptar, es decir, el intervalo de tiempo entre dos copias de seguridad.

Silos de datos. Colección de datos a la que un área tiene acceso pero otras no, por lo que un sistema se mantiene aislado de los demás sistemas de la organización.

Sistema Manejador de Bases de Datos (Database Management System, DBMS). Aplicación que "sirve de interfaz entre la base de datos, el usuario y otras aplicaciones" utilizadas (NETEC, 2019), y que permite a los usuarios definir, crear y mantener la base de datos, y proporciona acceso controlado a la misma.

Tiempo objetivo de recuperación. Tiempo que puede transcurrir antes de la recuperación completa de los datos, es decir, cuánto tomará obtener una copia de seguridad.

Tratamiento. La obtención, uso, divulgación o almacenamiento de datos personales, por cualquier medio. El uso abarca cualquier acción de acceso, manejo, aprovechamiento, transferencia o disposición de datos personales (Congreso de la Unión, 2017:5).

IV. Responsabilidades del personal involucrado

A. De los titulares de las entidades o dependencias universitarias

- Comunicar y difundir la aplicación de los presentes lineamientos, así como concientizar a su comunidad sobre la importancia de su adopción.
- Impulsar acuerdos institucionales que favorezcan el aprovechamiento de las bases de datos universitarias para generar más y mejores servicios que beneficien a la comunidad, bajo el marco legal vigente.

B. De los responsables de las Tecnologías de Información y Comunicación (TIC)

- Documentar y dar seguimiento a los procedimientos establecidos y de mejora en el marco de aplicación de los presentes lineamientos.

C. De los administradores de bases de datos

- Contribuir a la aplicación de estos lineamientos en las actividades que le sean asignadas.
- Comunicar a los responsables de las TIC las propuestas de mejora para la administración de las bases de datos y las oportunidades que se identifiquen para una mejor gestión y aprovechamiento de la información que contienen.

D. Del personal universitario que hace uso de las bases de datos

- Utilizar la información contenida en las bases de datos universitarias bajo el marco legal referido y considerando prácticas de calidad de datos en los casos que intervengan en la actualización de información.

V. Sobre la integración de tecnologías para las bases de datos

A. Unificación de las bases de datos universitarias

- Como primer paso para unificar sus bases de datos, las áreas universitarias deben buscar la integración de las mismas. Para ello es necesario identificar las fuentes de datos (sistemas heredados, bases de datos propias, bases de datos de otras áreas universitarias, sistemas locales, datos en la nube, entre otros) que poseen y requieren.
- Se deberán identificar y comprender los datos relevantes en los procesos universitarios bajo su responsabilidad, y aquellos que aporten valor o sean esenciales para apoyar la toma de decisiones, catalogando el conjunto de datos, verificando su limpieza y completitud, y documentando los mismos con metadatos.
- Es necesario definir una vista de datos unificada (esquema global), considerando las distintas fuentes de información y favoreciendo la conexión y el dominio de los conjuntos de datos, de manera que se pueda publicar datos unificados y fiables que se presenten de forma consistente para facilitar su consulta al usuario final. Para ello se deben considerar estructuras preestablecidas y un diccionario de datos que defina claramente los formatos y las especificaciones necesarias para cada tipo de dato registrado.
- Las áreas universitarias deberán privilegiar la automatización de la extracción de los datos en las diversas fuentes de información y la simplificación de los procesos de extracción de datos.
- Considerar la frecuencia con la que cambia la información, el tipo de datos, definir una estrategia de unificación, considerar la integración semántica y el tipo de tratamiento que se le dará a los datos para la entrega al usuario final.
- Se debe promover la eliminación o disminución de silos de datos con la intención de:
  - Buscar que los usuarios tengan acceso a datos de valor en menor tiempo.
  - Facilitar las tareas de conexión a los datos.
  - Entender el flujo de información y contribuir a la mejora de los procesos de consulta, intercambio y uso de datos.

- Eliminar o disminuir el doble trabajo de registro de datos en diferentes sistemas y procesos.
- Evitar la duplicidad u omisión de información.
- Ahorrar trabajo humano y de procesamiento.
- Maximizar el valor de los datos, aprovechar la variedad de datos existentes y como resultado contribuir a la mejora de la toma de decisiones.
- Permitir la compartición de información entre sistemas.

B. Consideraciones para la homologación en bases de datos

- Identificar, entender, documentar, catalogar y en su caso reclasificar los datos de interés almacenados en las bases de datos para centrar los esfuerzos en conjuntos de datos específicos. Los datos de interés son aquellos que se consideran como los más relevantes para la Universidad.
- Dar una etiqueta o categoría a cada base de datos de acuerdo con el contexto, la utilidad de la misma o la necesidad que satisfaga.
- Realizar procesos de limpieza de datos que consideren al menos un análisis exploratorio para conocer el estado actual de la información y llevar a cabo la evaluación de la calidad de los datos, de acuerdo con métricas de calidad y aplicando los criterios de decisión. Esto permitirá identificar el origen de los datos sucios y establecer mecanismos que los corrijan o excluyan.
- Fomentar que las bases de datos sigan reglas definidas de semántica y sintaxis que permitan su homologación y contribuyan a la compartición entre diferentes fuentes de datos para la gestión universitaria.

C. Interoperabilidad de las bases de datos

- Las áreas universitarias deberán homologar criterios y procedimientos que faciliten la compartición y/o el intercambio de información sin descuidar la protección de los datos, según su naturaleza y conforme a la normatividad aplicable.
- En las áreas universitarias se deberá establecer un manejo estandarizado del significado de los datos contenidos en las bases de datos, es decir, un vocabulario compartido, estandarizado y consensuado que facilite la interoperabilidad semántica.
- Se deberán establecer metadatos que permitan describir los datos contenidos en la base de datos para facilitar la interoperabilidad con los sistemas.
- En medida de lo posible se deberán unificar las tecnologías de bases de datos en el área universitaria, de manera que se privilegie la compartición e intercambio de datos con calidad.
- Es necesario verificar que los componentes tecnológicos usados en los sistemas de información del área universitaria permiten la interacción con otros (comunicación y trasmisión) y facilitan la compartición y/o el intercambio de datos.
- Se deberán establecer mecanismos para exportar datos, preferentemente en formatos abiertos (servicios web, texto plano con separadores, csv, json, xml, entre otros) y con los metadatos establecidos, o permitir la conexión a la base de datos de acuerdo con las restricciones de permisos.
- Las áreas universitarias deberán establecer prácticas de limpieza de datos almacenados en diferentes bases de datos que sean de su responsabilidad y homologarlos en caso de que dependan de fuentes primarias autoritativas de datos.

D. Neutralidad tecnológica

- Las áreas universitarias deberán privilegiar aquellas plataformas tecnológicas de bases de datos que faciliten la compartición y el almacenamiento seguro de la información.

- Fomentar la neutralidad tecnológica para favorecer el desarrollo y uso de plataformas de software libre, código abierto y/o propietario que facilite la compartición e intercambio de información y agilice los servicios universitarios. Algunas características que deberán tener los estándares abiertos seleccionados son: estar vigentes, ser referentes internacionales y contar con amplio soporte por una comunidad u organización.
- Preferir tecnologías y estándares que faciliten el intercambio y uso de los datos respetando los procesos y reglas de negocio de las áreas universitarias con el fin de mejorar su calidad, alcanzar los objetivos que tengan en común y obtener beneficios mutuos.
- Al seleccionar las tecnologías a utilizarse en los servicios universitarios, se deberá considerar su alto grado de adaptabilidad a los cambios tecnológicos y a los requerimientos cambiantes para responder a las necesidades institucionales y de los usuarios.
- Se deberán verificar los requisitos de hardware y software indicados por el proveedor para la instalación o actualización del manejador de bases de datos.
- Los titulares de las áreas universitaria asignarán a los responsables de observar y evaluar la obsolescencia tecnológica de las plataformas e infraestructura que soportan los servicios que ofrecen, buscando que las nuevas tecnologías viables consideren el uso de protocolos y estándares abiertos para faciliten la comunicación y transferencia de datos, así como su almacenamiento seguro.

E. Calidad de datos

- Las áreas universitarias deberán establecer controles y mecanismos que permitan abordar de manera institucional las siguientes características de los datos:
  - Portabilidad de las bases de datos. Se deberán considerar el uso de metadatos, así como las funciones y características de SQL estándar que faciliten la migración e interoperabilidad de las bases de datos, cuando sea requerido.
  - Disponibilidad de las bases de datos. El área universitaria determinará el nivel de disponibilidad de acuerdo con las necesidades de la misma, con la protección requerida de los datos y con los costos relacionados.
  - Recuperabilidad de las bases de datos. Las áreas universitarias deberán establecer sus planes de respaldo y recuperación considerando la importancia de la información, el tipo de respaldo y la frecuencia con que se realizará, seleccionando el medio de almacenamiento, haciendo la verificación de los respaldos y documentando los respaldos realizados. Para ello establecerán un Punto objetivo de recuperación y Tiempo objetivo de recuperación de la información en cada base de datos que tengan bajo su responsabilidad.
  - Accesibilidad de las bases de datos. Se determinará de acuerdo con las necesidades del área universitaria, estableciendo los mecanismos y sistemas que permitan a los usuarios adquirir fácilmente los datos almacenados.
- Deberán evitar en la medida de lo posible la libre captura por parte del usuario, ya sea con "*combobox*" que traiga los datos válidos de un catálogo, o bien, establecer validaciones en los sistemas de captura y la creación de restricciones en las bases de datos para mantener la conformidad con la normativa vigente, los estándares, formato o convenciones establecidos por el área universitaria.
- De igual forma se deberán establecer los mecanismos necesarios para garantizar la completitud, consistencia, exactitud y precisión de los datos almacenados.

F. Consideraciones de servicios en la nube

- Las áreas universitarias deberán considerar el cumplimiento normativo que debe observar la información almacenada en bases de datos con el fin de determinar si es factible utilizar un servicio en la nube pública, una nube híbrida o una nube privada.
- Previo a la contratación del servicio, las áreas universitarias deben considerar como mínimo:
  - Identificar los datos, procesos y funciones que se pretendan migrar al servicio en la nube.
  - Definir el modelo de aprovisionamiento que garantice el control sobre el tratamiento y almacenamiento de los datos.
  - Identificar las necesidades del área universitaria y en caso de elegir una solución de cómputo en la nube, por ejemplo: base de datos como servicio (BDaaS), plataforma como servicio (PaaS), infraestructura como servicio (IaaS), Almacenamiento como servicio (STaS), por mencionar algunos, se deberá:
    - Valorar si el área universitaria realizará la gestión de los servicios en la nube o estará a cargo del proveedor.
    - Evaluar las políticas de cobro de servicios en la nube, como costos por proceso, costos por transferencia de datos, etc., con base en una planeación de capacidades y procesos a largo plazo en la Universidad.
    - Evaluar los términos y condiciones del servicio de manera que cumplan con la normatividad y respondan a las necesidades del área universitaria.
- En la evaluación de los proveedores, las áreas universitarias deberán considerar al menos los siguientes criterios:
  - La reputación del proveedor tomando en cuenta el nivel de cumplimiento y la calidad del servicio que presta.
  - Si ha habido incidentes de seguridad y las medidas de mitigación que fueron aplicadas,
  - La jurisdicción o normatividad que rige al proveedor y al contrato.
  - La ubicación geográfica de los centros de tratamiento de información.
  - Notificaciones que garanticen la información oportuna sobre cualquier cambio o actualización en el servicio en la nube.
- Es recomendable seleccionar proveedores que reflejen lo siguiente, a través de cláusulas para la contratación o adhesión a sus servicios:
  - Prácticas alineadas a la normatividad mexicana, en materia de protección de datos personales.
  - Que eviten que reclamen, en cualquier momento, la propiedad de la información proporcionada por el área universitaria, ni de la información que se genere directamente relacionada con el servicio.
- Deben quedar claramente documentados los niveles de servicio a los que se compromete el proveedor y las medidas de seguridad disponibles.
- Para eliminar o destruir la información del área universitaria el proveedor deberá utilizar métodos de borrado seguro, en un periodo definido, durante y después de la prestación del servicio.

VI. Sobre el diseño de las bases de datos

A. Consideraciones sobre el modelado relacional de datos

- Las áreas universitarias deberán observar lo siguiente en el modelo de datos:
  - Utilizar una nomenclatura estándar para las bases de datos y sus objetos, aplicable a todos los proyectos y que sea constante durante su diseño.
  - Evitar las palabras reservadas para el motor de base de datos que se utilice.

- Dentro de la definición de las entidades y campos se deben mantener nombres cortos y descriptivos, sin utilizar espacios en blanco, acentos, la letra ñ (eñe) o caracteres especiales.
- Cada entidad de la base de datos se debe normalizar a la tercera forma normal por lo menos.
- Todas las entidades deben tener una llave primaria.
- Establecer una convención de nomenclatura para el nombrado de las entidades y campos, vistas y procedimientos que represente la información que tienen o manejan.
- Los nombres de las entidades deben ser únicos.
- Los nombres de los atributos deben ser únicos dentro de las áreas universitarias.
- Considerar el uso de campos de longitud variable para aquellos datos cuyos valores lo justifique, y mantener un tamaño fijo en datos como el número de cuenta, cuya longitud no cambia. Esto tiene como finalidad mejorar el rendimiento de lecturas y escrituras.
- Se deben utilizar restricciones de llave foránea cuando sean necesarias.
- Especificar en el manejador de base de datos los tipos de integridad referencial que se utilizarán: nulificación, cascada y/o restricción, considerando las reglas de negocio de cada aplicación.
- Se deben crear índices en las columnas que son diferentes a la clave principal y que se utiliza de manera recurrente para consultar la entidad (tabla), ordenando las columnas de las más a las menos utilizadas. Es importante que en la consulta se conserve el mismo orden de columnas que en el índice creado.
- También es importante considerar que entre más índices se crean, mayor tiempo de mantenimiento en disco y memoria se requiere para la actualización de los árboles generados.
- Es necesario revisar dentro de la documentación del Sistema Manejador de Bases de Datos Relacional (RDBMS por sus siglas en inglés) a emplear, la longitud máxima permitida para los nombres de tablas y campos. Se recomienda un uso máximo de 25 caracteres.
- Para bases de datos con objetos digitales, como audios, textos, videos e imágenes, se recomienda el uso de estándares internacionales de catalogación que describan con metadatos tanto el contenido como la información relacionada con la propiedad intelectual, entre otros aspectos; esto facilita el intercambio con otros sistemas y bases de datos. Se sugiere el uso de estándares como Dublin Core o Marc21.
- El modelo de datos debe estar documentado con diagramas entidad-relación y diccionario de datos, además de ser consistente con su modelo relacional.

B. Consideraciones sobre el diccionario de datos

- Las áreas universitarias deberán documentar de manera formal y completa las bases de datos que desarrollen o que estén bajo su responsabilidad (Anexo I. Diccionario de datos).
- El diccionario de datos deberá facilitar la comprensión y proveer de sentido; por tanto, debe documentar la existencia, el significado y uso de cada elemento de la base de datos.
- Las personas responsables de los datos en las áreas universitarias deben mantener actualizado el contenido del diccionario de datos, incluidas sus definiciones y valores.
- Cuando sea posible, crear la estructura de la base de datos con la descripción de los campos mediante comentarios. Esto permite que el diccionario de datos pueda ser generado de forma automática mediante herramientas o consultas a la base de datos.
- Cuando se trate de una adquisición o contrato con un tercero, se deberá solicitar al proveedor que proporcione la siguiente documentación, como mínimo: el diccionario de datos, el diagrama entidad-relación y los parámetros de configuración de la base de datos.

- Los diccionarios de datos deben revisarse periódicamente para garantizar su vigencia, al menos cada 6 meses o cuando exista un cambio en la estructura de la base de datos. Para la actualización de diccionarios de datos, se sugiere realizar una ingeniería en reversa que se encuentra disponible en herramientas de código abierto.

VII. Sobre la creación y configuración de bases de datos

A. Consideraciones sobre la creación de bases de datos

- Las áreas universitarias deben considerar las siguientes buenas prácticas en la creación de una base de datos: organizarla y estructurarla según las necesidades del área, considerar la limpieza de los datos que almacenará, su optimización, así como la estandarización y/o la homogeneización de los datos, según los criterios definidos por el área.
- Las áreas universitarias como parte del proceso de creación de la base de datos y sus objetos, deberán realizar un análisis del volumen y crecimiento de los datos, para obtener un dimensionamiento adecuado de la infraestructura, configuración y tamaño de la base de datos a crear.
- Identificar el número de transacciones esperadas, niveles de concurrencia, número de usuarios potenciales, entre otros aspectos, para dimensionar de forma correcta e informada la creación de una base de datos.
- Al generar una base de datos, se debe definir un responsable técnico o administrador de la misma y un responsable o propietario de la información contenida.

B. Consideraciones sobre la configuración de bases de datos

1. Parámetros de configuración

- Para establecer los parámetros de configuración en el Sistema Manejador de Bases de Datos las áreas universitarias deben considerar aspectos como:
  - Modelo de arquitectura a aplicar para las bases de datos.
  - Establecer diferentes arquitecturas en términos de capacidades, permisos, procesamiento, y según el ambiente; si es de producción, pruebas o para el desarrollo de aplicaciones.
  - Capacidad actual de almacenamiento que ocupan las bases de datos.
  - Tipo de datos que se almacena.
  - Volumen de transacciones diarias de las bases de datos.
  - Volumen de consultas a las bases de datos.
  - Puerto de acceso que tiene por defecto el servidor de bases de datos y cuál se utilizará por seguridad.
  - Número de aplicaciones y/o clientes que se conectan a las bases de datos de forma simultánea.
  - Parámetros a nivel de sistema operativo y de red para el soporte de número de usuarios esperados, o número de objetos abiertos en la base de datos, por ejemplo "file descriptors", tiempos de no actividad antes de cerrar una conexión, entre otros.
  - Número de aplicaciones y de clientes que se conectan a las bases de datos.
  - Ancho de banda utilizado para la transferencia de información.
  - Hora pico que demanda un mayor uso de recursos del servidor de base de datos.
  - Nivel de disponibilidad requerida, de acuerdo con la base de datos más crítica que se alojará en el servidor de bases de datos.

- Identificar qué objetos son más utilizados para ponerlos residentes en memoria principal y mejorar el rendimiento de las aplicaciones.
- Revisar si se requiere procesamiento paralelo para las consultas de las bases de datos.
- Evaluar si es necesario el particionamiento de objetos de base de datos para permitir el acceso paralelo.
- Políticas de usuario y contraseña que se aplicarán.
- Permisos y accesos requeridos para las bases de datos.
- Manejo de cifrado para las bases de datos.
- Monitoreo y auditoría para las bases de datos.
- En diferentes servidores de bases de datos, tener disponibles las soluciones analíticas OLAP y las operacionales OLTP para evitar problemas con la compatibilidad de recursos y de desempeño.

2. Cuentas

- Los nombres de usuario deben ser genéricos, orientados a la función o rol, no al nombre de la persona; deben tener los permisos estrictamente necesarios (mínimos).
- No se deben compartir cuentas, pues esto elimina la responsabilidad, aumentan el riesgo y dificultan la auditoría de la actividad del usuario.
- Es necesario separar las funciones de administración, seguridad y operaciones, entre otras.
- Las cuentas de tareas administrativas deben ser individuales; no deben ser compartidas por un grupo.

3. Seguridad

- Revisar y analizar las listas de verificación de seguridad de la base de datos y las recomendaciones emitidas por el proveedor y entidades reconocidas de seguridad (NIST, WASP, CSV Database, entre otros) para su aplicación y configuración.
- Debe considerarse la habilitación de los registros de auditoría necesarios para la presentación de informes de cumplimiento y para los análisis forenses, en caso de incumplimiento u otro evento adverso.
- En el caso de las bases de datos grandes y/o sensibles, o para sistemas de misión crítica, deben identificarse, evaluarse e implantarse los servicios de recuperación de desastres y servicios de seguridad necesarios, como pueden ser: el *failover clustering*, respaldos automáticos, replicación, entre otros.
- Fortalecer la seguridad de la base de datos mediante la configuración:
  - Inhabilitar los servicios innecesarios.
  - Eliminar las cuentas innecesarias, incluidas las cuentas por defecto del manejador de bases de datos.
  - Bloquear los usuarios de administración por defecto y cambiarlos por usuarios creados con fines administrativos, cuando el Sistema Manejador de Bases de Datos lo permita.
  - Utilizar contraseñas seguras para las cuentas y otorgarles el mínimo de privilegios.
  - Configurar las direcciones IP y los usuarios con acceso a cada base de datos, considerando los permisos mínimos que necesitan para realizar sus actividades.
  - Instalar regularmente las actualizaciones del software del Sistema Manejador de Bases de Datos, después de haber sido probadas.
  - Utilizar puertos diferentes a los que indica por defecto el Sistema Manejador de Bases de Datos.
  - El puerto de acceso a la base de datos debe estar restringido por firewalls o sistemas de prevención de intrusiones (IPS); el acceso sólo debe permitirse a los equipos que lo requieran.

VIII. Sobre el almacenamiento de información

A. Medios de almacenamiento

- Las áreas universitarias seleccionarán el tipo de almacenamiento, la infraestructura y las soluciones que permitan fortalecer el uso y protección de la información almacenada de acuerdo con sus necesidades y en cumplimiento de la normatividad universitaria.
- Los medios de almacenamiento seleccionados deben garantizar la accesibilidad, asegurando la disponibilidad inmediata de los datos para optimizar las tareas y necesidades de los usuarios.
- Las áreas universitarias deben establecer los tiempos de conservación de los medios de almacenamiento de las bases de datos y de sus respaldos de acuerdo con la naturaleza, utilidad y clasificación de la información.
- Se deben establecer procedimientos para asegurar el acceso a los datos en los medios de almacenamiento, tanto al medio como a la lectura de los formatos en sí, a través de todo el período de conservación que marque la normatividad universitaria.

B. Protección de datos

- Toda base de datos que se genere con recursos o información de la universidad, debe ser considerada propiedad de la UNAM, a menos que sea construida en colaboración con instituciones externas y que se tenga copropiedad, o que en los instrumentos legales de colaboración quede especificado lo contrario.
- La información deberá ser clasificada en función de su valor, requisitos legales, confidencialidad, sensibilidad y criticidad para la organización. Esta clasificación está a cargo del responsable de la información, quien debe indicar la necesidad, prioridad y grado de protección que requiere la información.
- Las áreas universitarias deben cumplir con la legislación en protección de datos personales y sus principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad por parte de todos los involucrados en el tratamiento.
- Cualquier base de datos que se cree y contenga datos personales debe observar los criterios que establecen el ***Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México***, los **Lineamientos para la Protección de Datos Personales en posesión de la Universidad Nacional Autónoma de México**, las **Normas Complementarias sobre Medidas de Seguridad Técnicas, Administrativas y Físicas para la Protección de Datos Personales en Posesión de la Universidad**, así como la ***Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados***.
- Para cualquier persona u organización ajena a las áreas universitarias que requiera acceso a las bases de datos estará condicionado a:
    - Realizar una solicitud por escrito para su autorización por el titular de la entidad académica o dependencia administrativa de la UNAM. Únicamente se otorgará el acceso, si ya se cuenta con evidencia positiva de la petición.
    - Que no sea información considerada reservada o confidencial.
    - Cuando exista una orden judicial o del Ministerio Público.
    - Al cumplimiento de lo establecido por el ***Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México***, la ***Ley General de Transparencia y Acceso a la Información Pública***, así como la ***Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados***.

  - Que el tercero garantice la protección de la información indicando por escrito los métodos y recursos tecnológicos que utilizará.
- Los datos personales contenidos en bases de datos sólo pueden ser requeridos por el titular de los mismos o salvo las excepciones contenidas en el ***Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México***, así como en la ***Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados***.

C. Uso de la información

- Las áreas universitarias serán responsables de registrar en un formato cualquier información relacionada con el uso y operación de las bases de datos a nivel de la entidad o dependencia.
- El responsable técnico o administrador de las bases de datos debe mantener y actualizar la documentación técnica y administrativa formalmente, a más tardar cinco días después de cualquier cambio en los RDBMS o en la base de datos.

IX. Gestión de las bases de datos

A. Memorias técnicas sobre las bases de datos

- El responsable técnico o administrador de bases de datos deberán crear y mantener actualizadas las memorias técnicas de las bases de datos, que permitan identificar:
  - Qué actividades se han realizado, cuándo, cómo y quién las realizó.
  - Los detalles técnicos de la base de datos.
  - Las especificaciones a tomar en cuenta en caso de una restauración.
- Se recomienda el uso de herramientas que permitan la ingeniería en inversa para el mantenimiento de estas memorias técnicas. (Anexo II. Memoria de los parámetros de configuración).

B. Gestión de las solicitudes de bases de datos

- Para la gestión de las bases de datos se deben elaborar solicitudes de creación de bases de datos que permitan tener un control y seguimiento de las mismas. Esto permite a los administradores de bases de datos identificar fácilmente las peticiones recibidas y las características solicitadas, así como su mantenimiento (Anexo III. Solicitud de bases de datos).
- Se deben registrar las modificaciones a las bases de datos para garantizar la trazabilidad de los cambios aprobados. Cualquier ajuste debe ser gestionado para disminuir riesgos, esto implica evaluar y planear el proceso de cambio para favorecer la continuidad del servicio.

C. Gestión del servicio de las bases de datos

- El área universitaria debe poseer la documentación e inventario de la infraestructura, así como copias de respaldo de los entornos donde se ejecutan sus distintos motores de los Sistemas Manejadores de Bases de Datos utilizados.
- Cuando sea posible, mantener al servidor de bases de datos como dedicado y en otros ambientes tener los otros servicios, tales como el servidor de aplicaciones, entre otros.
- Considerar un proceso de gestión de proveedores, el cual “se ocupa de gestionar la relación con los suministradores de servicios de los que depende la organización de TI. Su principal objetivo es alcanzar la mayor calidad a un precio adecuado” (OSIATIS, s.f.), principalmente cuando se adquiera un servicio de bases de datos en la nube como *Software as a Service* (SaaS) o un contenedor que incluye una base de datos administrada de forma tradicional,

considerando la selección del proveedor y la administración de los contratos (negociación, cumplimiento, renovación o terminación).

- Realizar la gestión de la continuidad de los servicios de bases de datos, en caso de que una base de datos sea crítica para las actividades sustantivas de la entidad o dependencia universitaria. El administrador de bases de datos, en conjunto con el responsable del servicio o sistema, deben definir un plan de continuidad para recuperar y restaurar la funcionalidad parcial o total de la misma en caso de algún incidente.
- El responsable técnico o administrador de bases de datos debe generar un catálogo de servicios de bases de datos vigentes del área universitaria. El catálogo debe incluir, al menos, el nombre del servicio, proceso para solicitarlo, costo (si lo tuviera) y los datos del contacto de quien atiende el servicio. El responsable del catálogo de servicios debe mantenerlo actualizado para que su información sea precisa.
- Se debe realizar el seguimiento a las actualizaciones del software base (sistema operativo) y verificar si estas actualizaciones son compatibles con el software del Sistema Manejador de Bases de Datos.
- Se debe actualizar un inventario de los activos de la base de datos para gestionarlos e identificar riesgos críticos que permitan establecer salvaguardas y responsables de su ejecución.
- La liberación e implementación de los activos de las bases de datos y sus servicios debe ser administrada, es necesario planear, ejecutar y verificar que se encuentren en funcionamiento de acuerdo con las características definidas en el tiempo y calidad esperada.
- Es necesario mantener un registro formal, completo y suficiente de los incidentes, problemas y eventos relacionados con las bases de datos para su gestión. Debe incluir la descripción del incidente, su impacto, la forma en que se resolvió y la fecha del suceso.

D. Monitoreo de las bases de datos

- El administrador debe monitorear y verificar el correcto funcionamiento de las bases de datos, además de revisar los archivos de bitácora (logs), para comprobar que no existan eventos por atender o riesgos potenciales que afecten la operación y seguridad de las bases de datos.

X. Seguridad de las bases de datos

A. Plan de respaldos y recuperación

- Los propietarios de información determinarán los requerimientos para resguardar los datos en función de su criticidad. Con base en ello, se define y documenta con el administrador de la base de datos, un esquema de resguardo de la información adecuado.
- Se deben realizar respaldos periódicamente para protección de la información. La frecuencia de los respaldos se realiza de acuerdo con las necesidades de la entidad académica o dependencia universitaria. Por ejemplo, bases de datos que tienen un nivel elevado de transacciones y que contienen información importante, necesitan respaldos más frecuentes que aquéllas que tienen pocos cambios.
- Se deben establecer los medios de almacenamiento, el proceso, el formato para guardar los respaldos de seguridad de las bases de datos, los tipos de respaldos a realizar y la periodicidad de acuerdo con las características de la base de datos y el servicio solicitado por el responsable de la información.
- Se deberá efectuar un registro que sirva de control de los respaldos realizados a las bases de datos que tenga como datos mínimos: el nombre de la base de datos, tipo de respaldo realizado, medio de almacenamiento y fecha.

- Para contar con mecanismos confiables sobre el proceso de respaldo y recuperación, éstos se deben probar periódicamente para validar que se realizaron correctamente y se encuentran en buen estado.
- Los responsables de la información y/o el administrador de bases de datos deben definir el tiempo de almacenamiento de los respaldos y documentar el método de destrucción de aquellos que no son útiles.
- Se debe generar una política interna para resguardar los respaldos de manera segura, sin que exista dependencia de una persona para recuperar y, en su caso, restaurar la información.
- Es necesario depositar los respaldos de las bases de datos en una ubicación diferente a la de los servidores de la dependencia administrativa o entidad académica. También se requiere definir un procedimiento que detalle, de manera completa, la forma en que serán recuperados los respaldos.
- Una vez definidas las políticas de respaldo, restauración y recuperación, se deben establecer procedimientos documentados y automatizarlos a nivel sistema operativo.

B. Consideraciones para la disponibilidad

- Antes que una base de datos entre a producción, es necesario realizar pruebas de carga y estrés para determinar si soportará la operación (el volumen de datos y peticiones) que requiere la aplicación o si es necesario hacer ajustes. Por ejemplo: se debe comprobar el tiempo de ejecución de las sentencias o consultas a las bases de datos para añadir índices, modificar parámetros de configuración o el procesamiento de los datos.
- Las áreas universitarias definirán el nivel de disponibilidad necesario de sus bases de datos, de acuerdo con su criticidad y en cumplimiento de la normatividad. También determinarán los mecanismos y procedimientos necesarios para su cumplimiento, como pueden ser la utilización de un tipo de RAID en discos, implementación de un clúster, la replicación, espejeo a nivel de base de datos (Database Mirroring) o distribución de las bases de datos, entre otros.
- De acuerdo con los recursos e infraestructura disponibles, se deben documentar los niveles de servicio que se pueden cumplir por cada aplicación que establezca conexiones con las bases de datos.
- Si se requiere un nivel de servicio mayor que la capacidad disponible, debe informarse al respecto para definir la autorización de recursos distintos, la adquisición de algún equipo o si se comparte o traslada el alojamiento dentro de la UNAM o con un tercero.

C. Eliminación de la información

1. Datos personales

- Para el retiro y conservación de la información contenida en la base de datos, deberá considerarse lo establecido en la normatividad aplicable.

2. Respaldos

- Los respaldos periódicos de una base de datos, que no sea necesario conservar de acuerdo con la normatividad vigente y los criterios aprobados por el área universitaria, se pueden destruir según los procesos especificados y aprobados en el área universitaria.
- Cuando una base de datos vaya a ser dada de baja (retirada) por obsolescencia o cambio de un sistema, el responsable deberá avisar al administrador de base de datos para establecer la fecha de retiro y la realización de un respaldo total.

3. Medios de almacenamiento

- La información confidencial que no sea necesario conservar, se debe proteger y/o destruir de acuerdo con los mecanismos determinados por la normatividad vigente y por los criterios avalados por escrito de los responsables de los datos.
- Para la eliminación de información sensible o confidencial de los medios de almacenamiento de las bases de datos se deberán usar métodos de borrado seguro en los medios electrónicos (soportes) que la contengan, y que a su vez consideren la escritura de valores aleatorios y al menos 7 sobre-escrituras, para evitar su recuperación por personas no autorizadas.
- En el caso de desecho de equipos de cómputo que contengan bases datos y medios de almacenamiento que contengan respaldo o archivos de las bases de datos por obsolescencia o daño se debe considerar la destrucción física de soportes no robustos como CD o DVD; en este caso se puede utilizar una destructora de soportes magnéticos. Cuando se trate de los discos duros o cintas se puede optar por el borrado seguro, la desmagnetización o la destrucción física. De igual forma se puede recurrir a empresas especializadas en la destrucción certificada de información, gestionando evidencia del proceso.
- Para el procedimiento de borrado seguro de la información en los equipos de cómputo que vayan a ser transferidos o dados de baja se observará lo estipulado en la Circular DGTIC/003/2017 - Procedimiento para el borrado de información.

D. Consideraciones generales de seguridad

- Los mecanismos de seguridad aplicables serán definidos por el responsable o propietario de la información, junto con el responsable técnico o administrador de bases de datos, cumpliendo con lo establecido en la normatividad universitaria y prácticas probadas de seguridad.
- Se deberán usar estos mecanismos para complementar las políticas de seguridad del área universitaria. También se podría partir del análisis específico que algún experto haya realizado sobre las necesidades de seguridad para la base de datos, de acuerdo con sus características.
- Deben definirse y documentarse, bajo criterios específicos y claros, los niveles de autorización (control de acceso) de las bases de datos de las entidades académicas o dependencias administrativas de la UNAM. Se debe partir del siguiente principio: otorgar al usuario únicamente los permisos requeridos (justificados) para sus fines.
- En bitácoras se debe llevar un control de los nuevos permisos de acceso que se generen, así como de la modificación del nivel de permisos de un usuario. Se recomienda generar un formato específico de control para el registro de esta información en la entidad.
- Se deberán utilizar procedimientos almacenados y vistas para la obtención de datos siempre que sea posible, ya que aportan seguridad, encapsulamiento, facilidad de mantenimiento y rapidez.
- Los equipos de cómputo físicos que contengan base de datos deberán encontrarse en un lugar seguro, con cerradura y, de ser posible, en un ambiente monitoreado, para prevenir el acceso no autorizado, la pérdida de datos o el robo. Este espacio debe mantener una temperatura adecuada para los servidores.
- No se debe iniciar sesión en los servidores de manera remota con la cuenta de administración de la base de datos, es necesario utilizar cuentas individuales desde la consola. En caso de realizar una conexión remota, es necesario utilizar canales seguros.
- Se deben establecer auditorías sobre datos críticos siempre que las características del RDBMS lo permitan. Una auditoría es el proceso que permite revisar, medir y dar seguimiento al uso de la base de datos.

XI. Sobre recursos humanos en bases de datos

A. Reforzamiento de capacidades y habilidades del personal que administra las bases de datos

- En sus planes de capacitación anual, las áreas universitarias deben contemplar el fortalecimiento de las competencias técnicas de los administradores de bases de datos. Se requiere capacitación formal en sistemas operativos, gestión de servicios, seguridad, diseño de bases de datos, tendencias, nuevas tecnologías, entre otros.
- El área universitaria también debe considerar la capacitación de desarrolladores y diseñadores de software, científicos de datos y administradores de servidores, entre otros, de acuerdo con las necesidades específicas.

B. Difusión de buenas prácticas en las bases de datos

- El área universitaria debe fomentar el intercambio de experiencias y buenas prácticas que el equipo de trabajo haya adquirido para implementar bases de datos. Se pueden aprovechar los espacios que la universidad ofrece, como el Repositorio Institucional de la UNAM, Toda la UNAM en Línea, la Red de Responsables TIC, la Red de Ingeniería y Bases de Datos, entre otros.
- El responsable TIC debe fomentar la difusión de prácticas que favorezcan la homogeneización y unificación de tecnología y procesos en los servicios de bases de datos.

XII. Marco legal aplicable

Existe un marco legal aplicable en México y la UNAM sobre el tratamiento de la información, el cual contempla reglamentos, normas y leyes que deben considerarse para que las actividades del personal involucrado con las bases de datos, se lleven a cabo dentro de un marco de legalidad.

Durante el ciclo de vida de la información, se debe observar la normatividad aplicable a cada etapa. Por ejemplo, en el manejo de la información de datos personales es preciso observar su protección y establecer los mecanismos necesarios para garantizar el cumplimiento de lo establecido en la ***Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados*** a nivel federal y en el ***Acuerdo por el que se establecen los lineamientos para la Protección de Datos Personales en Posesión de la Universidad Nacional Autónoma de México***, por mencionar algunos.

A continuación, se indican las normas que es necesario contemplar.

- Leyes, reglamentos y normas federales
  - Código Penal Federal.
  - Ley Federal del Derecho de Autor.
  - Ley Federal de Protección a la Propiedad Industrial.
  - Ley General de Archivos.
  - Ley General de los Derechos de Niñas, Niños y Adolescentes.
  - Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
  - Ley General de Transparencia y Acceso a la Información Pública.
  - Lineamientos Generales de Protección de Datos Personales para el Sector Público.
  - Acuerdo mediante el cual se aprueba la Adición del Título Décimo a los Lineamientos Generales de Protección de Datos Personales para el Sector Público.
  - Criterios mínimos sugeridos para la contratación de servicios de cómputo en la nube que impliquen el tratamiento de Datos Personales.

- Acuerdo por el que se emiten las políticas y disposiciones para impulsar el uso y aprovechamiento de la informática, el gobierno digital, las tecnologías de la información y comunicación, y la seguridad de la información en la Administración Pública Federal.

- Normatividad universitaria, lineamientos y recomendaciones
  - Acuerdo por el que se establecen los lineamientos para la Protección de Datos Personales en Posesión de la Universidad Nacional Autónoma de México.
  - Lineamientos Generales para la Organización, Administración y Conservación de los Archivos de la Universidad Nacional Autónoma de México.
  - Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.
  - Normas complementarias sobre medidas de seguridad técnicas, administrativas y físicas para la protección de datos personales en posesión de la Universidad.

1. Anexos

Anexo I. Diccionario de Datos

El diccionario de datos contribuye al mantenimiento de la base de datos y de las aplicaciones que hacen uso de la información almacenada, debido a que describe de forma ordenada los datos. MySQL Workbench, entre otras herramientas CASE, permiten generar un diccionario de datos de manera automática. La información también se puede obtener a través de consultas a las tablas del sistema del RDBMS o mediante captura manual en un archivo de Word o Excel. A continuación, se propone un formato con los datos mínimos que debe tener cada tabla.

Nombre de la tabla	
Descripción	

- **Nombre de la tabla:** Nombre de la tabla.
- **Descripción:** Descripción de los datos que almacenará la tabla, por ejemplo: La tabla almacenará los datos personales de los alumnos.

Nombre del campo	Tipo de dato	Restricción de nulidad (Sí/No)	PK (Sí/No)	FK (Sí/No)	Default	Descripción

- **Nombre del campo:** Nombre del campo o atributo en la base de datos.
- **Tipo de dato:** Clasificación del tipo de dato del campo y su longitud. Por ejemplo: varchar(20), integer, char(5).
- **Restricción de nulidad (Not Null Constraint):** Indica por medio de los valores Sí o No, si el atributo es obligatorio o puede almacenar valores nulos.
- **Llave primaria (PK):** Indica si el campo forma parte de la llave primaria o primary key.
- **Llave secundaria (FK):** Indica si el campo forma parte de la llave foránea o foreign key.
- **Default:** Indica el valor por defecto del campo cuando no se asigna un valor en una operación de INSERT.
- **Descripción:** Señala brevemente los datos que contiene el campo. Por ejemplo: Almacena el nombre del alumno.

Los datos propuestos para el diccionario de datos no son restrictivos, pueden aumentar de acuerdo con las necesidades del proyecto. Esto permite reunir toda la información que se requiera para facilitar el trabajo de los desarrolladores, analistas, probadores de software, administradores de la base de datos y otros involucrados.

Además de los datos básicos mencionados, la documentación se puede completar con lo siguiente:

Ejemplo del dato: Se refiere a una indicación sobre los valores que se pueden almacenar en el campo para facilitar su comprensión. Si se trata de un atributo respecto al estado civil, “soltero” sería un ejemplo.

Nombres de los índices a los que pertenece el campo: Nombre del índice o índices que se hayan creado en la tabla y de los cuales forma parte el campo, por ejemplo: IDX_NOMBRE. Se sugiere que se especifique el tipo de índice requerido, así como el orden de los campos líderes que forman el índice.

Otro tipo de constraints o restricciones: Indica si el atributo tiene otro tipo de limitante, además de Not Null; por ejemplo, de tipo CHECK, utilizado para controlar los valores que se pueden almacenar en el campo. En el caso de un atributo sobre el género, los posibles valores se pueden restringir con “M” o “F” solamente. También se pueden agregar otras restricciones, como la de tipo UNIQUE, para indicar que el valor almacenado en el campo es único.

Por último, se debe indicar el tipo de integridad referencial implementada: nulificación, cascada o restrictivo.

Observaciones o notas adicionales: Se puede registrar información importante sobre las tareas relacionadas con el uso, mantenimiento o desarrollo de la base de datos. Por ejemplo: ingresar registros considerando una secuencia, un *trigger* (disparador en cumplimiento de un evento específico) que afecte los datos almacenados o alguna política de respaldo y borrado de los datos almacenados en la tabla, entre otros.

Triggers, procedimientos almacenados, funciones definidas por el usuario y funciones: Se deben documentar en aspectos tales como su objetivo, descripción breve de los mismos, entre otros.

Anexo II. Memoria de los parámetros de configuración

En el mantenimiento de bases de datos de producción, la migración a un nuevo servidor o la resolución de problemas de producción es recomendable identificar los valores que se modificaron en los parámetros de configuración de la base de datos. Para ello es necesario un listado con el nombre del parámetro y el nuevo valor asignado; si el cambio requiere de autorización, se puede agregar la fecha de aprobación y el nombre de quien autoriza.

Parámetro de la base de datos	Valor anterior	Nuevo valor	Fecha de cambio y persona que lo realiza

Parámetro de la base de datos: Nombre del parámetro de la base de datos.
Valor anterior: Valor asignado al parámetro antes del cambio.
Nuevo valor: Valor del parámetro después de ser modificado.
Fecha del cambio y persona que lo realiza: Fecha de la actualización del valor del parámetro y nombre de quien lo modificó.

Anexo III. Solicitud de base de datos

Se recomienda que la solicitud incluya los datos de:

- **Sistema Manejador de Base de Datos (RDBMS): Se debe especificar el sistema y la versión que se requiere**, por ejemplo: MySQL 8.0, PostgreSQL 14.3, MongoDB 5.0, entre otros.
- **Nombre de la base de datos:** Sugerencia de nombre para la base de datos. Se asignará si está disponible.
- **Valores solicitados de los parámetros de configuración diferentes a la instalación por defecto:** Nombre de los parámetros de configuración de la base de datos y los valores que se solicita se les asigne. La siguiente tabla muestra el ejemplo de una solicitud de parámetros de **shared_buffers** y **work_mem,** superiores a los valores por defecto de PostgreSQL:

Parámetro	Valor
shared_buffers	**200MB**
work_mem	**5MB**

- **Conjunto de caracteres e idioma:** Nombre del conjunto de caracteres (character set) e idioma que se solicita. Por ejemplo: UTF8 Spanish Mexico.
- **Nombre(s) de la(s) cuenta(s) de usuario de la base de datos:** Propuesta de nombres para las cuentas de usuario de la bases de datos solicitada. Se podrán asignar siempre y cuando estén disponibles y cumplan con las restricciones de nombrado de objetos, las cuales pueden variar de un manejador de base de dato a otro. Por ejemplo: que los nombres de usuario no sean palabras reservadas o no inicien con caracteres numéricos.
- **Perfil y/o permisos de la cuenta solicitada:** Perfil que se requiere para el usuario de la base de datos y/o permisos específicos. Por ejemplo:

Cuenta: usu_administrador
Dueño de la base de datos
Cuenta: usu_informe
Permisos de lectura de las tablas y vistas

- **Nombre del host o direcciones IP de los equipos con acceso a la base de datos:** Listado de direcciones IP desde las cuales se puede acceder directamente a la base de datos, debe incluir la IP del servidor de aplicaciones o equipo de cómputo con herramientas que usará la información de la base de datos. Se recomienda que esta lista contemple sólo las direcciones IP de los equipos que sea indispensable se conecten a la base de datos. Los equipos de usuarios que van a consultar la base de datos a través de una aplicación web, no deben incluirse en esta lista.
- **Fecha de inicio:** Fecha estimada en la que comenzará a utilizarse la base de datos.

- **Fecha de término:** En caso de tener el dato, especificar la fecha en que la base de datos dejará de operar. Al finalizar su tiempo de vida, la base de datos será respaldada y se eliminará del servidor.
- **Tipo de respaldo y periodicidad solicitada:** Indicar el tipo de respaldo a realizar. Los tipos de respaldo, las herramientas para generarlo y el formato varían, según el RDBMS utilizado. El siguiente ejemplo se puede aplicar para una base de datos de PostgreSQL:

Realizar respaldo diario con la herramienta pg_dump usando los parámetros -Fc -O -x para que genere un archivo binario sin la información del dueño de la base de datos.

- **Datos del solicitante:** Nombre completo, número telefónico, correo electrónico, área universitaria y cargo. Es necesario que los datos de contacto se mantengan actualizados para aclarar dudas o dar avisos importantes, tales como una baja programada del servicio por mantenimiento, entre otros.

2. Bibliografía y referencias electrónicas

- Comisión Europea (2017). Marco Europeo de Interoperabilidad - Estrategia de aplicación. Recuperado: 9 de septiembre de 2021. https://eur-lex.europa.eu/resource.html?uri=cellar:2c2f2554-0faf-11e7-8a35-01aa75ed71a1.0010.02/DOC_3&format=PDF#:~:text=El%20Marco%20Europeo%20de%20Interoperabilidad,principios%2C%20modelos%20y%20recomendaciones%20comunes
- Congreso de la Unión (2017). Ley general de protección de datos personales en posesión de sujetos obligados. Recuperado: 17 de mayo del 2022, URL: https://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf
- Diario Oficial de la Federación (2011). Acuerdo por el que se establece el Esquema de Interoperabilidad y de Datos Abiertos de la Administración Pública Federal. Recuperado: 17 de mayo del 2022, URL: http://dof.gob.mx/nota_detalle.php?codigo=5208001&fecha=06/09/2011
- Benítez, Miguel (2016). Manual de Supervivencia del Administrador de Bases de Datos: 2ª Edición. IT Campus Academy.
- González, Alberto. et. al. (2021). Glosario de términos de TIC. Recuperado: 03 de mayo del 2022, de la Red-TIC, URL: https://www.red-tic.unam.mx/recursos/2021/2021_Glosario_RedResponsablesTIC_01.pdf
- González, Miguel. et. al. (2013). Aplicación del estándar ISO/IEC 9126-3 en el modelo de datos conceptual entidad-relación. Revista Facultad de Ingeniería, UPTC, julio - diciembre de 2013, Vol. 22, No. 35. Recuperado el 7 de octubre de 2021. URL: http://www.scielo.org.co/pdf/rfing/v22n35/v22n35a10.pdf
- Hibernate (2004). Hibernate Community Documentation. Recuperado: 06 de mayo del 2022, URL: https://docs.jboss.org/hibernate/orm/3.5/reference/es-ES/html/portability.html
- IBM (2021). ¿Qué es una base de datos en la nube? Recuperado: 03 de mayo del 2022, URL: https://www.ibm.com/mx-es/cloud/learn/what-is-cloud-database
- Agencia Digital de Innovación Pública de la Ciudad de México (2020). Guía práctica para la elaboración de diccionarios de datos. Recuperado el 06 de junio del 2022, URL: https://politicadedatos.cdmx.gob.mx/assets/ppts/guia_dicc.pdf
- Talburt, John et Zhou, Yinle (2015). ISO Data Quality Standards for Master Data. Research Gate. Recuperado el 06 de junio del 2022, URL: https://www.researchgate.net/publication/300714597_ISO_Data_Quality_Standards_for_Master_Data
- IBM (2021b) Alta disponibilidad para bases de datos. Recuperado: 6 de mayo del 2022, URL: https://www.ibm.com/docs/es/control-desk/7.6.1?topic=configuration-high-availability-databases
- Mannino, Michael (2007). Administración de bases de datos: diseño y desarrollo de aplicaciones, México, Mc Graw-Hill Interamericana, 3ra Edición, 737 pp.
- MINTIC (2016). Modelo de Seguridad y Privacidad de la Información. Recuperado: 17 de mayo del 2022, URL: https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf
- NETEC (2019). ¿Qué es un gestor de base de datos y cuáles son los más usados? Recuperado: 17 de mayo del 2022, URL: https://www.netec.com/post/que-es-un-gestor-de-base-de-datos-y-cuales-son-los-mas-usados
- Oracle (2022). Documentación de Oracle Infrastructure. Configuraciones. Recuperado: 7 de mayo del 2022, URL: https://docs.oracle.com/es-ww/iaas/mysql-database/doc/configuring-db-system.html

- OSIATIS (s.f.), Gestión de proveedores. Recuperado: 7 de mayo del 2022, URL: https://segenuino.com/itil/diseno_servicios_TI/gestion_proveedores.html
- UNAM (2021). Glosario de términos de TIC. Red-TIC, UNAM. Recuperado: 05 de abril de 2022. URL: https://www.red- tic.unam.mx/content/glosario-de-terminos-de-tic
- UNAM (2016). Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México. Recuperado: 2 de septiembre de 2022. URL: http://www.transparencia.unam.mx/documentos_transparencia/manual-de-normas_2021.pdf
- UNAM (2021). Lineamientos generales y políticas sobre almacenamiento e información compartida entre los sistemas existentes de Datos. Recuperado: 31 de agosto de 2022. URL: https://www.red-tic.unam.mx/recursos/2021/2021_Lineamiento_RedResponsablesTIC_01.pdf
- UNAM (2018). Lineamientos Generales para la Organización, Administración y Conservación de los Archivos de la Universidad Nacional Autónoma de México. Recuperado: 31 de agosto de 2022. URL: https://www.red-tic.unam.mx/recursos/LineamientosArchivosUNAM.pdf
- UNAM (2020). Normas complementarias sobre medidas de seguridad técnicas, administrativas y físicas para la protección de datos personales en posesión de la Universidad. Recuperado: 28 de junio de 2021. URL: https://www.gaceta.unam.mx/wp-content/uploads/2020/01/200130-convocatorias.pdf
- UNAM (2022). Catálogo de disposición documental. Recuperado: 31 de agosto de 2022. URL: https://www.repositoriotransparencia.unam.mx/DocumentosDigitales/descargar/JOHE_1650676046

3. Créditos

Elaboración

Dirección General de Cómputo y de Tecnologías de Información y Comunicación

Hugo Alonso Reyes Herrera (Coordinación), Alberto González Guízar, Susana Laura Corona Correa.

Dirección General de Administración Escolar

Armando Vega Alvarado

Instituto de Investigaciones en Matemáticas Aplicadas y en Sistemas

María del Pilar Angeles

Revisión

Ana Pérez Arteaga (IIMAS), Fernando Israel González Trejo (FES Acatlán), Miguel Ángel Jiménez Bernal (DGBSDI), Fernando Zaragoza Hernández (DGAE), Leonard Pulido Cauzard (DGAE), Ana Yuri Ramírez Molina (DGTIC), Leticia Martínez Calixto (DGTIC), José Othoniel Chamú Arias (DGTIC), José Luis Chávez Sánchez (DGTIC), Eprin Varas Gabrelian (DGTIC), José Luis Olín Martínez (DGTIC)

Validación

Consejo Asesor en Tecnologías de Información y Comunicación

Créditos históricos (versión 2017)

Elaboración

Dirección General de Cómputo y de Tecnologías de Información y Comunicación

Hugo Alonso Reyes Herrera (Coordinación), Alberto González Guízar, Susana Laura Corona Correa, José Luis Chávez Sánchez.

Revisión

Red Universitaria de Ingeniería de *Software* y Bases de Datos

Beatriz Peralta Cortés (Instituto de Investigaciones sobre la Universidad y la Educación), Carlos Cruz Santos (Dirección General de Administración Escolar), Dante Ortiz Ancona (Dirección General de Bibliotecas), José Antonio Salazar Carmona (Instituto de Investigaciones Bibliográficas), Ana Yuri Ramírez Molina (Instituto de Investigaciones Bibliográficas).