
	SISTEMA INTEGRADO DE GESTIÓN	<b>Código</b>	<b>L-E-SIG-003</b>
	<b>POLITICA ESPECIFICA DE GESTION DE BASE DE DATOS</b>	<b>Versión:</b>	<b>3.0</b>
DACTA SAC	<b>DOCUMENTO CONTROLADO</b>	<b>Vigente desde:</b>	<b>22/02/2024</b>
		<b>Página:</b>	<b>1 de 5</b>

## Política Específica de Gestión de Base de Datos

### RESTRINGIDO

Este documento una vez impreso se convertirá en una copia no controlada, a menos que cuente con un sello de "Copia Controlada", antes de su aplicación, consulte su vigencia con el Comité del SIG.


	SISTEMA INTEGRADO DE GESTIÓN	Código	L-E-SIG-003
	POLITICA ESPECIFICA DE GESTION DE BASE DE DATOS	Versión:	3.0
DACTA SAC	DOCUMENTO CONTROLADO	Vigente desde:	22/02/2024
		Página:	2 de 5

## ÍNDICE

1. OBJETIVO, ALCANCE Y USUARIOS .....	3
2. DOCUMENTOS DE REFERENCIA .....	3
3. POLÍTICA ESPECÍFICA .....	3
3.1. DE LOS USUARIOS EN GENERAL .....	3
3.2. DEL ADMINISTRADOR DE BASE DE DATOS.....	4
4. AUDITORÍA.....	4
5. REGISTROS .....	5
6. CONTROL DE CAMBIOS.....	5

### RESTRINGIDO

Este documento una vez impreso se convertirá en una copia no controlada, a menos que cuente con un sello de “Copia Controlada”, antes de su aplicación, consulte su vigencia con el Comité del SIG.

	SISTEMA INTEGRADO DE GESTIÓN	Código	L-E-SIG-003
	POLITICA ESPECIFICA DE GESTION DE BASE DE DATOS	Versión:	3.0
DACTA SAC	DOCUMENTO CONTROLADO	Vigente desde:	22/02/2024
		Página:	3 de 5

## 1. OBJETIVO, ALCANCE Y USUARIOS

El objetivo del presente documento es definir reglas de acceso a las bases de datos en función a los requerimientos del negocio de DACTA y las políticas de seguridad de la información.

Este documento se aplica a todo el alcance del Sistema Integrado de Gestión (SIG).

Los usuarios de este documento son todos los colaboradores de DACTA.

## 2. DOCUMENTOS DE REFERENCIA

- NTP-ISO/IEC 27001:2022 Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de la seguridad de la información, cláusulas 5.10, 8.10, 8.11, 8.12

## 3. POLÍTICA ESPECÍFICA

### 3.1. DE LOS USUARIOS EN GENERAL

Todo el personal que interactúa con bases de datos, carpetas con información de propiedad de DACTA o de los clientes de DACTA está obligado a;


- Conocer, a cumplir y a hacer cumplir esta Política.
- Guardar la debida reserva sobre los datos a los que hayan tenido acceso en razón de su puesto de trabajo u otra circunstancia.
- Impedir el acceso de personas no autorizadas a la información, en cuya gestión, tramitación o custodia no participe.
- Acceder a las bases de datos, únicamente a través de aplicaciones autorizadas por DACTA y respetando la Política Específica de Gestión de Accesos.
- Están obligados a notificar al Oficial de Seguridad de la Información cualquier incidente o sospecha del mismo que afecte la seguridad de la información de las bases de datos.

### 3.2. DEL COORDINADOR DE TI

- Asegurar la disponibilidad, confidencialidad e integridad del sistema operativo y del sistema gestor de base de datos en todos los servidores de DACTA destinados a este fin.
- Resolver cualquier incidente o fallo relacionado con el sistema operativo y el sistema gestor de base de datos en el servidor, en el menor tiempo posible según sea el incidente.
- Deshabilitar o desinstalar cualquier software o servicio que no justifique su presencia dentro de un servidor donde esté funcionando el sistema gestor de base de datos.
- Garantizar que los servidores lógicos que contienen las bases de datos, en ambientes de producción, sean de función dedicada a este propósito. Por ello, no se permite dar otros usos a estos servidores.
- Asegurar, que los usuarios que se conecten a las aplicaciones que interactúan con las bases de datos y que contengan información de DACTA, cuenten con la licencia respectiva.
- Asegurar la separación de los ambientes en productivo de los ambientes de prueba para evitar que la base de datos de productivo se procese en ambiente de prueba.

**RESTRINGIDO**

Este documento una vez impreso se convertirá en una copia no controlada, a menos que cuente con un sello de "Copia Controlada", antes de su aplicación, consulte su vigencia con el Comité del SIG.

	SISTEMA INTEGRADO DE GESTIÓN	Código	L-E-SIG-003
	POLITICA ESPECIFICA DE GESTION DE BASE DE DATOS	Versión:	3.0
DACTA SAC	DOCUMENTO CONTROLADO	Vigente desde:	22/02/2024
		Página:	4 de 5

### 3.3. DEL ADMINISTRADOR DE BASES DE DATOS

- Monitorear el desempeño de la base de datos y la correcta ejecución de las transacciones del sistema gestor de base de datos.
- Debe asegurar que todas las bases de datos de DACTA sean almacenadas en servidores, y en ningún caso deben mantenerse en computadores personales.
- Gestionar la solución a cualquier incidente o fallo relacionado con el funcionamiento de los objetos de base de datos, en cualquiera de los servidores de base de datos y el menor tiempo posible según sea el incidente.
- Depurar o eliminar objetos obsoletos dentro de la base de datos o que no cumplan con los estándares de desarrollo.
- Asegurarse, que los usuarios matriculados en cada base de datos se encuentren como usuarios activos. Los usuarios huérfanos deben ser eliminados.

### 3.4. DEL USO DE LAS BASES DE DATOS PARA PRUEBAS DE CALIDAD DEL SOFTWARE

- Para acceder a la base de datos de un cliente, los responsables de Desarrollo y de Aseguramiento de la calidad de software deben solicitar la publicación de la base de datos respectiva especificando:
  - Código y nombre del proyecto
  - Ambiente donde debe ser publicado (Desarrollo, Pruebas, Beta), según le corresponda.
  - Fecha en la que debe ser publicada la base de datos.
  - Tiempo preciso, en horas, que estará publicada la base de datos
  - Personal que accederá a esa base de datos y sus cuentas de usuario
- Las solicitudes de publicación de las respectivas bases de datos deben hacerse con 48 o 24 horas de anticipación previas al momento del uso. Eso dependerá del tamaño de la Base de datos.
- El tiempo de publicación, que se solicite, ya sea para el desarrollo o para las pruebas debe ser concordante con los tiempos estipulados para el desarrollo o para las pruebas dentro del plan de actividades.
- El Coordinador de TI ofuscará la información de clientes que contenga la base de datos a publicar, en cualquiera de los ambientes. Esto no aplicará en los casos que el cliente solicite explícitamente el análisis de la información de un cliente en específico. El responsable del proyecto debe sustentar la no ofuscación de los datos.

En caso de no cumplir con la presente Política Específica de Gestión de Base de Datos, los lineamientos de seguridad de la información u otros directivas o procedimientos de seguridad de la información, se reportará el evento al Oficial de Seguridad de la Información para que tome conocimiento y disponga las acciones correspondientes, de considerarlo necesario. De esta forma, tomará las medidas disciplinarias necesarias, las cuales están sujetas al Código de ética y conducta de DACTA.

## 4. AUDITORÍA

- El Oficial de Seguridad de la Información deberá comprobar periódicamente que esta política se cumpla.






**RESTRINGIDO**

<b>DACTA</b>	SISTEMA INTEGRADO DE GESTIÓN	Código	L-E-SIG-003
	POLITICA ESPECIFICA DE GESTION DE BASE DE DATOS	Versión:	3.0
DACTA SAC	DOCUMENTO CONTROLADO	Vigente desde:	22/02/2024
		Página:	5 de 5

## 5. REGISTROS

Código	Nombre de Registro	Responsable del Control	Tiempo de Conservación
N/A	N/A	N/A	N/A

## 6. CONTROL DE CAMBIOS

Versión	Fecha	Descripción	Elaborado por	Revisado por	Aprobado por
1	30/06/2021	Emisión	OSI	Comité SIG	Gerente General
2	20/09/2021	Modificación	OSI	Comité SIG	Gerente General
3	22/02/2023	Modificación	OSI	Comité SIG	Gerente General
3	22/02/2024	Revisión	OSI	Comité SIG	Gerente General
<b>Firmas de la versión vigente</b>					
			S. Rafaile	S. Rafaile	
					
			A. Morales	A. Morales	
<b>Identificación de las modificaciones</b>					
Versión	Descripción de cambios				
2	Se insertó el capítulo 3.4 DEL USO DE LAS BASES DE DATOS PARA PRUEBAS DE CALIDAD DEL SOFTWARE				
3	Se actualizó el documento con el nuevo logo de DACTA. Se actualiza el requisito normativo según nueva versión ISO 27001:2022. Se modifica cláusula 2. DOCUMENTOS DE REFERENCIA Se agrega el control 5.10				

### RESTRINGIDO

Este documento una vez impreso se convertirá en una copia no controlada, a menos que cuente con un sello de "Copia Controlada", antes de su aplicación, consulte su vigencia con el Comité del SIG.