Informe de Auditoría Forense Base de Datos "BD SYS SISEDUCATIVO"

**MYSQL VERSIÓN 5.0** 

1. Introducción

1.1. Objetivo del Informe

El propósito de este informe es identificar y evaluar la vulnerabilidad en la

integridad de los datos en la base de datos "BD\_SYS\_SISEDUCATIVO" MYSQL

**VERSIÓN 5.0** 

- Fecha de la Auditoría: 2024/08/05

- Auditor Líder: Ingeniero Alexis Cadrasco García

1.2. Alcance

Este informe cubre la evaluación de la base de datos

"BD SYS SISEDUCATIVO" MYSQL VERSIÓN 5.0 en términos de su integridad

de datos y cualquier vulnerabilidad identificada durante el proceso de

auditoría.

1.3. Metodología

La auditoría se ha llevado a cabo mediante una combinación de análisis

manual y herramientas automatizadas, incluyendo revisiones

configuración, análisis de logs, y pruebas de integridad de datos.

2. Descripción del Entorno

2.1. Detalles del Sistema

- Versión de MySQL: 5.0

- Sistema Operativo: Centos 7.0

- Hardware: Servidor tipo desktop

### 2.2. Configuración Actual

### - Archivos de Configuración:

### [mysqld]

```
# Configuración del servidor MySQL
```

user= root

pid-file=/var/run/mysqld/mysqld.pid

socket=/var/run/mysqld/mysqld.sock

datadir=/var/lib/mysql

port=3306

max\_connections=200

bind-address=127.0.0.1

 ${\sf sql\_mode=STRICT\_TRANS\_TABLES}, {\sf NO\_ENGINE\_SUBSTITUTION}$ 

### [client]

# Configuración de clientes MySQL

port=3306

socket=/var/run/mysqld/mysqld.sock

### [mysqldump]

# Configuración para mysqldump

Auditor líder - Ingeniero Alexis Cadrasco García

quick

quote-names

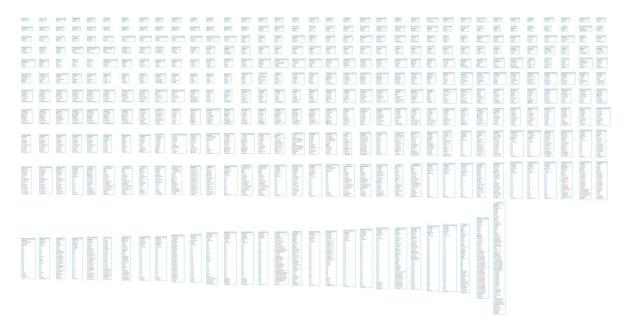
max\_allowed\_packet=16M

### [mysql]

# Configuración del cliente MySQL

prompt= $\u@\h [\d]>$ 

- Estructura de la Base de Datos:



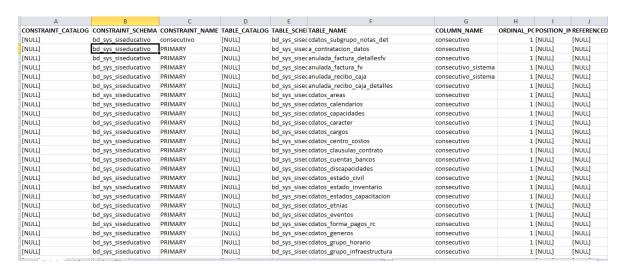
- 3. Identificación de Vulnerabilidades
- 3.1. Pruebas de Integridad
- **3.1.1 Integridad Referencial**: Al evaluar las restricciones de claves foráneas y otras restricciones de integridad, se identifica que no existe integridad

referencial a través de llaves foráneas. Por lo tanto las implicaciones que esto trae son las siguientes:

- Datos Huérfanos: Registros en tablas hijas que no tienen correspondencia en las tablas padres, lo que puede llevar a datos incompletos o erróneos.
- Inconsistencias: Inconsistencias en los datos debido a la falta de restricciones que aseguren que las relaciones entre tablas se mantengan.
- **Problemas en Consultas:** Dificultades para realizar consultas que dependen de la consistencia entre tablas, lo que puede afectar los informes y análisis de datos.
- **Dificultades en la Mantenimiento:** Mayor complejidad en el mantenimiento de datos y en la implementación de cambios en el esquema de la base de datos.

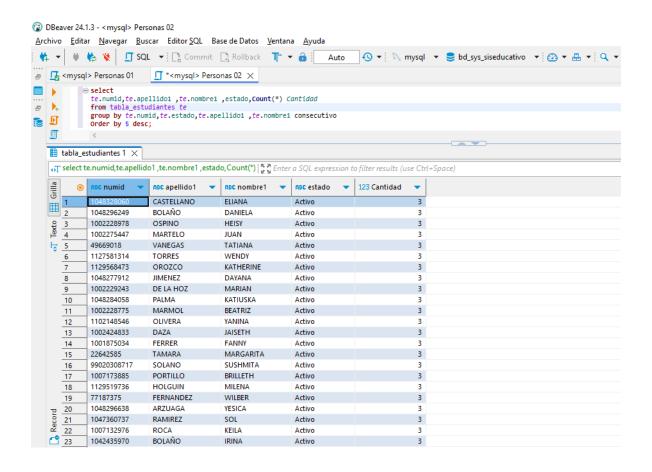
Sentencia SQL para ver la información del schema 'BD\_SYS\_SISEDUCATIVO'

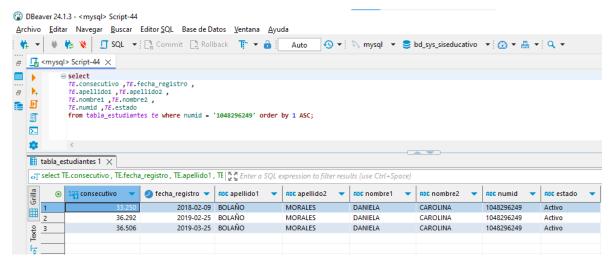
## SELECT \* FROM INFORMATION\_SCHEMA.KEY\_COLUMN\_USAGE WHERE CONSTRAINT SCHEMA ='BD SYS SISEDUCATIVO';



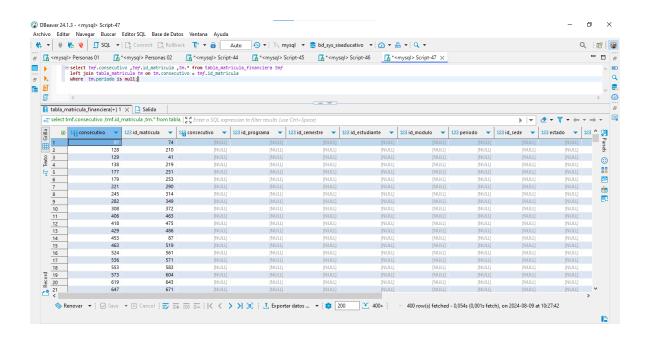
Se anexa archivo en Excel con el resultado de la consulta sql. (Constraint SisEducativo Ver2.xlsx)

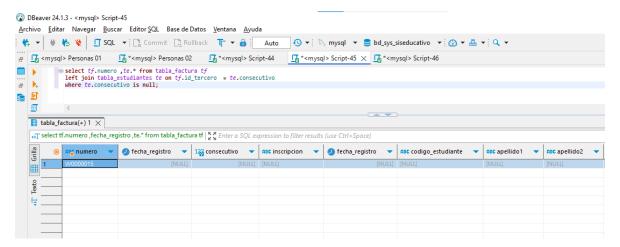
- **3.1.2 Consistencia de Datos:** Revisando la consistencia entre los datos almacenados y las reglas definidas en el esquema, se evidencia que existen discrepancias entre estos, por ejemplo:
  - Datos Duplicados: Registros redundantes en la base de datos que deberían ser únicos.



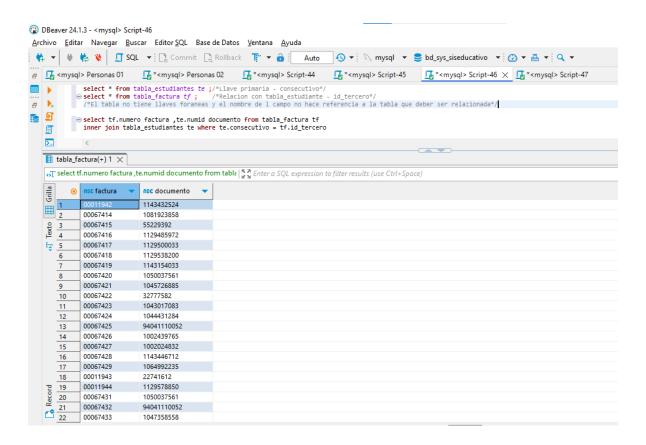


 Datos Huérfanos: Registros en tablas hijas que no tienen correspondencia en las tablas padres, violando la integridad referencial.

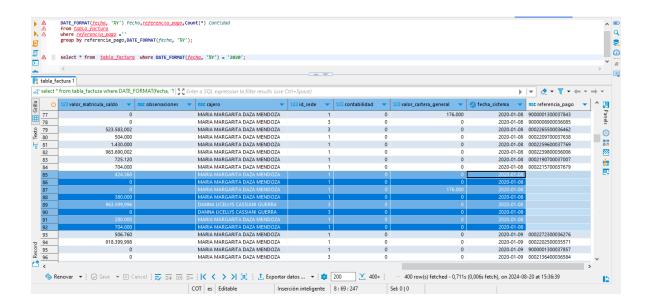




 Datos Inexactos: Datos que no corresponden a la realidad o que son incorrectos debido a errores humanos o fallos en la captura de datos.



 Datos Incompletos: Registros con campos obligatorios vacíos o incompletos que deberían estar llenos.



### Cantidad de datos incompletos por año

В	С
referencia_pago	Cantidad
	8.814
	8.988
	8.243
	10.331
	13.832
	14.647
	6.610
	2.009
	1.806
	1.310
	1.011
	244

Sentencia Sql

**SELECT** 

DATE\_FORMAT(FECHA, '%Y') FECHA,REFERENCIA\_PAGO,COUNT(\*)
CANTIDAD
FROM TABLA\_FACTURA

WHERE REFERENCIA\_PAGO ="
GROUP BY REFERENCIA\_PAGO,DATE\_FORMAT(FECHA, '%Y');

• **Datos Incompatibles:** Datos que no cumplen con las reglas de negocio o las restricciones definidas en el esquema de la base de datos.

Formato de consecutivo diferente, se anexa evidencia.

### Sentencia Sql

**SELECT** 

**TF.NUMERO** 

FACTURA,TF.FECHA,TF.HORA,TF.VALOR\_TOTAL,TE.NUMID

DOCUMENTO,CONCAT(TE.NOMBRE1,'',TE.APELLIDO1) NOMBRE

FROM TABLA\_FACTURA TF

INNER JOIN TABLA\_ESTUDIANTES TE ON TE.CONSECUTIVO =

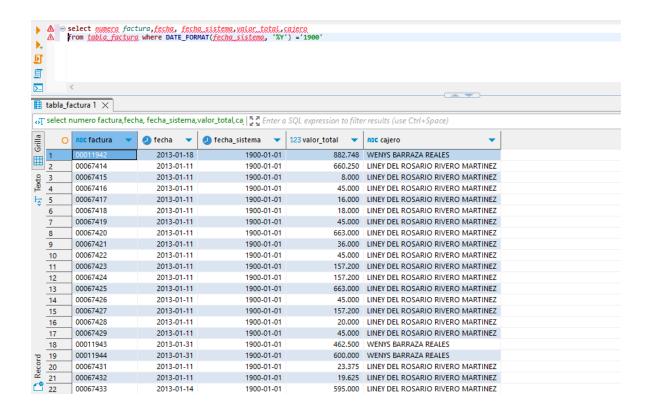
TF.ID\_TERCERO

WHERE TF.NUMERO LIKE '%W%';

А	В	С	D	Е	F
factura	fecha	hora	valor_total	documento	nombre
W000001	3/05/2019	11:59:35 a. m.	168.000	1001931111	WENDY SANJUANELO
W0000002	3/05/2019	5:40:20 p. m.	210.000	1001993810	DIONISIO BERTEL
W0000003	3/05/2019	7:43:57 p. m.	210.000	250364	TATIANA BUELVAS
W0000004	6/05/2019	5:55:08 p. m.	168.000	1001940651	JOSE SALAS
W0000005	6/05/2019	6:56:59 p. m.	98.000	1001940651	JOSE SALAS
W000006	9/05/2019	2:02:52 p. m.	20.000	1002155723	VICTOR MENDEZ
W0000007	13/05/2019	11:45:24 a. m.	123.750	1193050536	DULCE PACHECO
W0000008	14/05/2019	5:00:50 p. m.	80.000	1002154530	RUBEN HERNANDEZ
W0000009	16/05/2019	10:57:24 a. m.	84.000	1001939113	LIZETH SERGE
W0000010	16/05/2019	4:36:51 p. m.	24.000	1001931111	WENDY SANJUANELO
W0000011	20/05/2019	7:14:47 p. m.	36.000	1001939113	LIZETH SERGE
W0000012	21/05/2019	11:52:58 a. m.	48.000	1002025562	KELLY ZUÑIGA
W0000013	21/05/2019	11:57:06 a. m.	168.000	1002025562	KELLY ZUÑIGA
W0000014	22/05/2019	10:18:03 a. m.	70.000	1001939525	ANA GALLOR
W0000016	5/06/2019	12:49:11 p. m.	10.000	1002024832	KATIA PEREZ
W0000017	7/06/2019	10:05:57 a. m.	509.250	1001875092	JANINE MOLINA
W0000018	8/06/2019	9:23:01 a. m.	200.000	1002035138	YULEY RODRIGUEZ
W0000019	8/06/2019	9:23:01 a. m.	200.000	1002035138	YULEY RODRIGUEZ
W0000020	17/06/2019	1:57:38 p. m.	2.800	1001994148	LISBIK CABRERA
W0000021	16/07/2020	4:02:25 p. m.	120.000	1045672256	LUZ PALACIOS
W0000022	14/12/2020	9:47:20 a. m.	131.000	1001789049	MERILY MADERA
W0000023	16/12/2020	3:34:38 p. m.	12.500	1143160917	KANELVY RUIZ
W0000024	17/12/2020	9:59:39 a. m.	12.500	1001825143	KAYLEN OROZCO
W0000025	19/12/2020	11:42:32 a. m.	12.500	1048330163	YERLEYDIS CAMARGO

#### Formato de fecha no acorde

SELECT NUMERO FACTURA, FECHA, FECHA\_SISTEMA, VALOR\_TOTAL, CAJERO FROM TABLA\_FACTURA WHERE DATE\_FORMAT(FECHA\_SISTEMA, '%Y') = '1900'

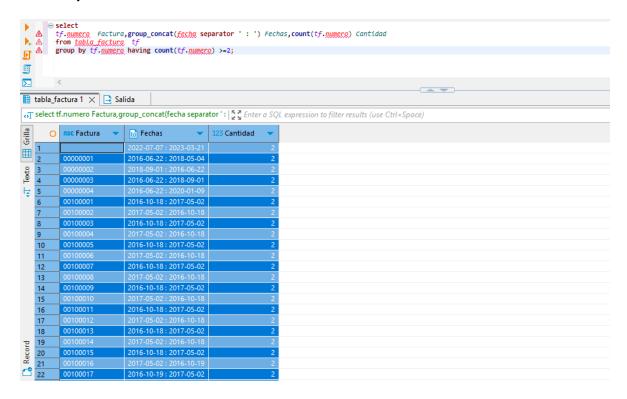


А	В	С	D	Е
factura	fecha	fecha_sistema	valor_total	cajero
91990	4/12/2015	1/01/1900	230.000	LINEY DEL ROSARIO RIVERO MARTINEZ
91991	4/12/2015	1/01/1900	30.000	LINEY DEL ROSARIO RIVERO MARTINEZ
91992	4/12/2015	1/01/1900	436.160	LINEY DEL ROSARIO RIVERO MARTINEZ
91994	4/12/2015	1/01/1900	580.000	LINEY DEL ROSARIO RIVERO MARTINEZ
91995	4/12/2015	1/01/1900	45.000	LINEY DEL ROSARIO RIVERO MARTINEZ
91996	4/12/2015	1/01/1900	30.000	LINEY DEL ROSARIO RIVERO MARTINEZ
91997	4/12/2015	1/01/1900	20.000	LINEY DEL ROSARIO RIVERO MARTINEZ
91998	4/12/2015	1/01/1900	50.000	FRANCISCO JAVIER DIAZ MENDOZA
91999	5/12/2015	1/01/1900	40.000	LINEY DEL ROSARIO RIVERO MARTINEZ
92000	5/12/2015	1/01/1900	130.000	LINEY DEL ROSARIO RIVERO MARTINEZ
92001	5/12/2015	1/01/1900	202.000	LINEY DEL ROSARIO RIVERO MARTINEZ
92002	5/12/2015	1/01/1900	173.000	LINEY DEL ROSARIO RIVERO MARTINEZ
92003	5/12/2015	1/01/1900	50.000	LINEY DEL ROSARIO RIVERO MARTINEZ
92004	5/12/2015	1/01/1900	410.000	LINEY DEL ROSARIO RIVERO MARTINEZ
92005	5/12/2015	1/01/1900	30.000	LINEY DEL ROSARIO RIVERO MARTINEZ
92006	5/12/2015	1/01/1900	255.000	LINEY DEL ROSARIO RIVERO MARTINEZ
92007	5/12/2015	1/01/1900	30.000	LINEY DEL ROSARIO RIVERO MARTINEZ
92008	5/12/2015	1/01/1900	310.000	LINEY DEL ROSARIO RIVERO MARTINEZ
92009	5/12/2015	1/01/1900	30.000	LINEY DEL ROSARIO RIVERO MARTINEZ
92010	5/12/2015	1/01/1900	100.000	LINEY DEL ROSARIO RIVERO MARTINEZ
92011	5/12/2015	1/01/1900	80.000	LINEY DEL ROSARIO RIVERO MARTINEZ
92012	5/12/2015	1/01/1900	151.000	LINEY DEL ROSARIO RIVERO MARTINEZ
92013	5/12/2015	1/01/1900	277.200	LINEY DEL ROSARIO RIVERO MARTINEZ
92014	5/12/2015	1/01/1900	170.000	LINEY DEL ROSARIO RIVERO MARTINEZ

- **3.1.3 Verificación de Datos Corruptos:** se logra Identificar posibles corrupciones o anomalías en los datos. Dentro de estas se encuentran:
- **3.1.3.1** Recaudos vía PSE que no están asociados en la pasarela de pagos. (Se anexa archivo Matriculas Financiera.xlsx)



# **3.1.3.2** Recaudos repetidos para la cartera de otros estudiantes. (Se anexa archivo)



#### Sentencia Sql

SELECT TF.NUMERO FACTURA, GROUP\_CONCAT (FECHA SEPARATOR ' : ')
FECHAS, COUNT (TF.NUMERO) CANTIDAD FROM TABLA\_FACTURA TF
GROUP BY TF.NUMERO HAVING COUNT (TF.NUMERO) >= 2;

Α	В	С
Factura	Fechas	Cantidad
	2022-07-07:2023-03-21	2
1	2016-06-22:2018-05-04	2
2	2018-09-01:2016-06-22	2
3	2016-06-22:2018-09-01	2
4	2016-06-22:2020-01-09	2
100001	2016-10-18:2017-05-02	2
100002	2017-05-02:2016-10-18	2
100003	2016-10-18 : 2017-05-02	2
100004	2017-05-02 : 2016-10-18	2
100005	2016-10-18 : 2017-05-02	2
100006	2017-05-02 : 2016-10-18	2
100007	2016-10-18 : 2017-05-02	2
100008	2017-05-02 : 2016-10-18	2
100009	2016-10-18 : 2017-05-02	2
100010	2017-05-02 : 2016-10-18	2
100011	2016-10-18 : 2017-05-02	2
100012	2017-05-02 : 2016-10-18	2
100013	2016-10-18 : 2017-05-02	2
100014	2017-05-02 : 2016-10-18	2
100015	2016-10-18 : 2017-05-02	2
100016	2017-05-02 : 2016-10-19	2
100017	2016-10-19 : 2017-05-02	2
100018	2017-05-02 : 2016-10-19	2
100019	2016-10-19 : 2017-05-02	2
4 h hi 11-i-4	/11-2-2 /11-2-2 /8-7 /	

### 3.2. Evaluación de Impacto

**3.2.1 Impacto en la Integridad de Datos**: La integridad de datos se refiere a la precisión, consistencia y confiabilidad de los datos a lo largo de su ciclo de vida. La falta de integridad de datos puede tener impactos significativos en

diversos aspectos de una organización, afectando tanto sus operaciones diarias como su toma de decisiones estratégica.

#### 3.2.1.1 Inexactitudes y Errores en los Datos

- Decisiones Erróneas: Datos inexactos o inconsistentes pueden llevar a decisiones incorrectas, afectando la estrategia y la operación general de la organización.
- Errores Operacionales: Las operaciones diarias pueden verse afectadas por errores en los datos, como información incorrecta en órdenes de recaudo, facturación y notas, lo que puede resultar en mala calidad del servicio.

#### 3.2.1.2 Problemas de Confianza y Reputación

- **Pérdida de Confianza:** La falta de integridad de los datos puede erosionar la confianza de los clientes y socios comerciales. Los errores en los datos pueden afectar la percepción de la calidad y la fiabilidad de los servicios que se prestan por parte de la institución.
- Impacto en la Reputación: La divulgación de datos incorrectos o la exposición de información errónea puede dañar la reputación de la empresa, afectando su imagen pública y su relación con los clientes.

### 3.2.1.3 Problemas en la Integridad de las Operaciones

- Errores en la Base de Datos: Los datos inconsistentes pueden afectar la ejecución de procesos críticos, como transacciones financieras y atención al cliente, resultando en operaciones ineficientes o fallidas.
- Dificultades en la Integración de Sistemas: La integración de datos entre sistemas diferentes puede ser problemática si los datos no son consistentes, dificultando la interoperabilidad y la integración efectiva de sistemas.

#### 3.2.1.4 Riesgos en la Seguridad de Datos

- Exposición a Vulnerabilidades: La falta de integridad puede ser un indicador de problemas de seguridad más amplios, como la falta de controles adecuados, que pueden exponer a la organización a ataques y brechas de datos.
- Manipulación Maliciosa: Datos incorrectos o manipulables pueden ser explotados por actores maliciosos para comprometer la seguridad y realizar actividades fraudulentas.

#### 3.2.1.5 Impacto en la Eficiencia y Productividad

- Costos Operacionales: La corrección de errores y la gestión de datos inconsistentes pueden ser costosas en términos de tiempo y recursos, afectando la eficiencia operativa y la productividad.
- Retrasos en la Toma de Decisiones: Los problemas de integridad pueden llevar a retrasos en la toma de decisiones y en la ejecución de estrategias, afectando la capacidad de la organización para responder rápidamente a cambios en el mercado.

#### 3.3. Próximos Pasos

#### 3.3.1 Acciones Inmediatas:

### 3.3.1.1 Medidas para Mantener la Integridad de Datos

- Implementar Restricciones de Integridad: Usar claves primarias, foráneas y restricciones únicas para asegurar la consistencia y precisión de los datos.
- Automatizar Procesos: Utilizar herramientas y sistemas para automatizar la entrada y el procesamiento de datos, reduciendo la probabilidad de errores humanos.
- Realizar Auditorías y Validaciones: Implementar procesos de auditoría y validación para identificar y corregir problemas de integridad de datos de manera proactiva.

- Capacitar al Personal: Proporcionar formación regular sobre las mejores prácticas en la gestión de datos y la seguridad para reducir errores y mejorar la calidad de los datos.
- Actualizar y Revisar Sistemas: Mantener los sistemas actualizados y revisar periódicamente los procesos y controles para adaptarse a las nuevas amenazas y requisitos.

#### 3.3.2 Plan a Largo Plazo:

#### 3.3.2.1. Implementación de Controles de Seguridad

#### 3.3.2.1.1 Controles de Acceso:

- Autenticación y Autorización: Implementar autenticación multifactor y gestionar los permisos de acceso con el principio de menor privilegio.
- Revisión Regular de Cuentas: Revisar y ajustar las cuentas de usuario y roles periódicamente para asegurarse de que los accesos sean adecuados y necesarios.

#### 3.3.2.1.2 Cifrado de Datos:

- **Datos en Reposo:** Asegurar de que todos los datos sensibles estén cifrados en el almacenamiento.
- **Datos en Tránsito:** Usar protocolos seguros (como TLS/SSL) para cifrar datos mientras se transmiten entre el cliente y el servidor.

## **3.3.2.1.3** Seguridad Física y Ambiental:

- Control de Acceso Físico: Proteger el acceso físico a los servidores y sistemas que almacenan la base de datos.
- **Protección contra Desastres:** Implementar medidas para proteger la base de datos contra desastres naturales y otros eventos catastróficos.

#### 3.3.2.1.4 Monitoreo y Detección de Amenazas

- Monitoreo Continuo: Implementar herramientas para monitorear la actividad de la base de datos en tiempo real, buscando accesos no autorizados y comportamientos sospechosos.
- Alertas y Notificaciones: Configurar alertas para notificar al equipo de seguridad sobre eventos críticos o anomalías detectadas.
- **Registro de Eventos:** Mantener registros detallados de todas las actividades relacionadas con la base de datos.
- **Revisión de Logs:** Revisar los registros regularmente para identificar patrones sospechosos o posibles incidentes de seguridad.

#### 3.3.2.1.5. Respuesta y Recuperación ante Incidentes

- Procedimientos Documentados: Desarrollar procedimientos detallados para la respuesta a incidentes, incluyendo la identificación, contención, erradicación y recuperación.
- Equipo de Respuesta: Designar un equipo de respuesta a incidentes y asegura que esté capacitado y preparado para manejar eventos de seguridad.
- **Ejercicios de Simulación:** Realizar simulacros regulares para probar la efectividad del plan de respuesta y la capacidad del equipo para manejar incidentes reales.

### 3.3.2.1.6. Capacitación y Concienciación

- Entrenamiento Regular: Proporcionar capacitación periódica sobre seguridad de datos y prácticas recomendadas para el personal que maneja la base de datos.
- Conciencia de Amenazas: Educar al personal sobre las amenazas emergentes y cómo pueden afectar la seguridad de los datos.

• Revisión de Políticas: Actualiza las políticas de seguridad y procedimientos en función de los cambios en el entorno de amenazas y las mejores prácticas.

#### 3.3.2.1.7 Evaluación y Mejora Continua

- Auditorías Regulares: Realizar auditorías periódicas de seguridad para evaluar la efectividad de las medidas implementadas y detectar áreas de mejora.
- **Revisión de Controles:** Revisar y actualizar los controles de seguridad y procedimientos basados en los resultados de las auditorías y los cambios en el entorno de amenazas.
- Investigación de Amenazas: Manténgase al tanto de las nuevas amenazas y vulnerabilidades emergentes y ajustar el plan de seguridad en consecuencia.
- Adaptación de Estrategias: Adaptar las estrategias de seguridad para abordar las nuevas amenazas y aprovechar las nuevas tecnologías y métodos de protección.

### 3.3.2.18 Documentación y Reportes

- **Plan de Seguridad:** Mantenga un documento detallado del plan de seguridad, incluyendo políticas, procedimientos, y controles implementados.
- Informes de Incidentes: Documentar los incidentes de seguridad y las respuestas dadas para aprendizaje futuro y cumplimiento.
- Informes Periódicos: Proporcionar informes regulares a la alta dirección sobre el estado de la seguridad de la base de datos, incluyendo métricas de rendimiento y análisis de riesgos.