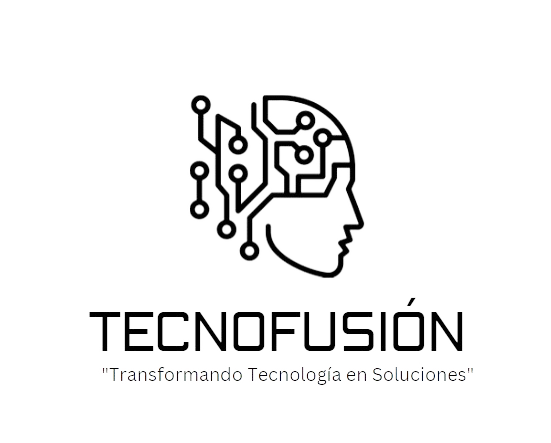
**Desarrollo de plataforma de ventas de entradas con identificación**

**“Documento de Verificación de Base de Datos”**

**Autores:**

Allain Alegre, Diego Arturo

**Administrador de Base de Datos**

**Fecha de creación del documento:**

30/09/2023

versión 1.0

**Indice**

[**1. Introducción 3**](#_heading=h.gjdgxs)

[**2. Objetivos de la verificación 3**](#_heading=h.30j0zll)

[**3. Procedimientos de Verificación 3**](#_heading=h.1fob9te)

[**4. Responsabilidades y Roles 4**](#_heading=h.3znysh7)

[**5. Calendario y Frecuencia 5**](#_heading=h.2et92p0)

[**6. Resultados y Reporte 6**](#_heading=h.tyjcwt)

[**7. Conclusiones y Recomendaciones 6**](#_heading=h.3dy6vkm)

# **Introducción**

Este documento explora la importancia de la verificación de base de datos como una herramienta crítica para la autenticación de usuarios, la gestión de perfiles, el control de accesos y la protección de datos sensibles. Además, analizaremos los objetivos y procedimientos que pueden ser implementados con éxito en este tipo de sistemas para garantizar su funcionamiento seguro y eficiente.

La verificación de la base de datos es de vital importancia por varias razones fundamentales, entre ellas la seguridad de los datos sensibles, ya que garantiza que la información se mantenga segura y confidencial, el control de acceso que garantiza que solo las personas autorizadas tengan acceso a eventos o instalaciones, la integridad de los datos, asegurando que la información almacenada sea precisa y coherente y la auditoría y rastreo, llevando un registro detallado de las actividades dentro del sistema.

# **Objetivos de la verificación**

Los objetivos de la verificación de base de datos son esenciales para garantizar la integridad, seguridad y eficiencia del sistema en su conjunto. Algunos de los objetivos clave son los siguientes:

* + **Autenticación de Usuarios:** Verificar la identidad de los usuarios que acceden al sistema, asegurando que solo las personas autorizadas puedan realizar transacciones y acceder a información sensible.
  + **Integridad de los Datos:** Garantizar que la información almacenada en la base de datos sea precisa y esté libre de errores, lo que evita problemas como la duplicación de entradas o la pérdida de datos críticos.
  + **Gestión de Perfiles de Usuarios:** Permitir la administración efectiva de los perfiles de usuarios, lo que incluye la creación, actualización y eliminación de cuentas de usuarios de manera segura y eficiente.
  + **Seguridad de Datos:** Garantizar la protección de datos sensibles, como información de pago y datos personales, para cumplir con regulaciones de privacidad y evitar posibles infracciones de seguridad.
  + **Auditoría y Registro:** Mantener un registro de todas las transacciones y actividades dentro del sistema, lo que facilita la identificación de anomalías y la revisión de auditoría.
  + **Cumplimiento Legal y Regulatorio:** Asegurarse de que el sistema cumple con las leyes y regulaciones relevantes, como la protección de datos y las regulaciones de venta de entradas.
  + **Disponibilidad y Rendimiento:** Mantener un rendimiento óptimo del sistema y la base de datos para evitar interrupciones en la venta de entradas y proporcionar una experiencia de usuario sin problemas.

# **Procedimientos de Verificación**

**Integridad de datos:**

* Verificar que los registros de los usuarios registrados tengan identificadores únicos.
* Validar que los datos personales, como nombres, apellidos y números de documento de identidad, sean correctos y únicos.
* Comprobar que no existan registros duplicados en la base de datos de usuarios.

**Precisión de datos:**

* Realizar controles de calidad de datos para asegurar que la información almacenada en la base de datos, como detalles del evento y detalles del usuario, sea precisa y sin errores.
* Implementar validaciones de datos para evitar la entrada de información incorrecta o incoherente.

**Consistencia de datos:**

* Establecer reglas y restricciones de integridad de datos para garantizar que la información en la base de datos sea coherente y cumpla con estándares predefinidos.
* Realizar pruebas periódicas para identificar y corregir inconsistencias en los datos.

**Seguridad de datos:**

* Aplicar controles de acceso basados en roles para limitar quién puede acceder y modificar la información en la base de datos.
* Encriptar datos sensibles, como información de pago y datos personales, tanto en tránsito como en reposo.

**Rendimiento:**

* Realizar pruebas de carga y optimización de consultas para garantizar que el sistema funcione de manera eficiente incluso durante períodos de alta demanda, evitando tiempos de inactividad y lentitud en el servicio.

**Respaldos y recuperación:**

* Implementar un plan de respaldo regular para garantizar la disponibilidad de datos en caso de fallos del sistema o pérdida de información.
* Establecer procedimientos de recuperación para restaurar la base de datos en su estado correcto después de un incidente.

**Optimización de consultas:**

* Analizar y ajustar las consultas de la base de datos para garantizar una recuperación de datos rápida y eficiente.
* Utilizar índices y técnicas de optimización de consultas para mejorar el rendimiento.

**Gestión de cambios:**

* Implementar un proceso de control de cambios para administrar actualizaciones de software y cambios en la estructura de la base de datos.
* Realizar pruebas exhaustivas antes de implementar cambios en producción para evitar interrupciones no planificadas.

**Auditoría:**

* Habilitar el registro de auditoría para mantener un registro de todas las actividades en la base de datos, incluidos los cambios en los datos y el acceso de usuarios.
* Realizar revisiones periódicas de los registros de auditoría para detectar actividades inusuales o sospechosas.

# **Responsabilidades y Roles**

# **Calendario y Frecuencia**

# **Resultados y Reporte**

# **Conclusiones y Recomendaciones**