INFORME DE VERIFICACIÓN DE CUMPLIMIENTO DE SEGURIDAD DEL SOFTWARE

Conforme a la Resolución 500 de 2021 - MinTIC

---

1. Información General

Nombre del Sistema :	Software de Control de Visitantes
Versión	21.2264.36.225
Entidad Pública	Distrito Especial de Ciencia, Tecnología e Innovación de Medellín – Secretaría de Movilidad
Proveedor	Grupo Tecnologico SATS S.A.S.
Responsable Técnico	Luis Pineda J
Ambiente Evaluado	Desarrollo , Pruebas y Producción

Nombre del Sistema :	Software de Parqueadero
Versión	10.1964.16.80
Entidad Pública	Distrito Especial de Ciencia, Tecnología e Innovación de Medellín – Secretaría de Movilidad
Proveedor	Grupo Tecnologico SATS S.A.S.
Responsable Técnico	Luis Pineda J
Ambiente Evaluado	Desarrollo , Pruebas y Producción

2. Objetivo

Verificar que el software cumple con los lineamientos de seguridad definidos en la Resolución 500 de 2021, el Modelo de Seguridad y Privacidad de la Información (MSPI), la Ley 1581 de 2012 y las mejores prácticas internacionales de desarrollo seguro.

---

3. Alcance

La evaluación comprende:

- Arquitectura : Cliente – Servidor
- Base de datos : SQL Server Anexo: Diagrama de Despliegue v2.pdf

- Aplicación Escritorio - DeskTop Visual Studio .NET
- Infraestructura : Anexo : Diagrama de arquitectura.pdf
- Autenticación : Clave de encriptación SHA256

---

4. Evaluación del Ciclo Seguro de Desarrollo

Control	Cumple	Observaciones
Se definieron requisitos de seguridad	SI	
Se realizó análisis de riesgos	SI	
Existe revisión de arquitectura	SI	
Existe revisión de código	SI	
Existen pruebas de seguridad	SI	
Existe aprobación antes de producción	SI	
Existe plan de respuesta a incidentes	SI	

---

5. Evaluación de Vulnerabilidades

Vulnerabilidad (OWASP Top 10)	Cumple	Riesgo	Evidencia / Observación
Broken Access Control	Sí	Bajo	Se implementan controles de acceso basados en roles (RBAC), validación de permisos en servidor y restricciones por perfil de usuario.
Cryptographic Failures	Sí	Bajo	La información sensible se transmite las credenciales se almacenan utilizando algoritmos de hash seguros y cifrado cuando aplica.
Injection	Sí	Bajo	Se utilizan consultas parametrizadas y validación de entradas para prevenir SQL Injection y otros tipos de inyección.
Insecure Design	Sí	Bajo	El desarrollo sigue principios de diseño seguro, validación de requisitos de seguridad y revisión de arquitectura durante el ciclo de vida del software.

Security Misconfiguration	Sí	Bajo	Los ambientes de producción mantienen configuraciones seguras, servicios innecesarios deshabilitados y acceso restringido únicamente a personal autorizado.
Vulnerable Components	Sí	Bajo	Se realiza revisión periódica de librerías, componentes y dependencias, aplicando actualizaciones de seguridad cuando se identifican vulnerabilidades conocidas.
Authentication Failures	Sí	Bajo	Se implementan políticas de contraseñas seguras, autenticación de usuarios y control de intentos fallidos.
Software Integrity Failures	Sí	Bajo	Las actualizaciones del software son controladas y verificación de integridad de los componentes publicados.
Logging & Monitoring Failures	Sí	Bajo	El sistema registra eventos de autenticación, errores, accesos y operaciones críticas, facilitando la trazabilidad y auditoría del sistema.

Resultado de la evaluación: Se realizó la revisión de los controles de seguridad del software tomando como referencia las categorías del OWASP Top 10. Como resultado de la evaluación no se identificaron vulnerabilidades críticas o altas que comprometan la confidencialidad, integridad o disponibilidad de la información.

Las vulnerabilidades de riesgo bajo identificadas fueron mitigadas mediante los controles implementados y forman parte del proceso continuo de mantenimiento y actualización del software

Control implementado	Estado
Consultas parametrizadas en SQL Server	✓ Implementado
Validación de entradas del usuario	✓ Implementado
Control de acceso por perfiles y roles	✓ Implementado
Cifrado SHA 256	✓ Implementado
Registro de auditoría (Logs)	✓ Implementado
Actualización periódica de componentes	✓ Implementado
Control de errores sin revelar información sensible	✓ Implementado

6. Evaluación de Autenticación

Control	Cumple	Riesgo	Evidencia / Observación
Contraseñas robustas	Sí	Bajo	El sistema exige contraseñas con longitud mínima, combinación de letras mayúsculas, minúsculas, números y caracteres especiales.
Bloqueo por intentos	Sí	Bajo	Se bloquea temporalmente la cuenta o se restringe el acceso después de varios intentos fallidos consecutivos de autenticación, mitigando ataques de fuerza bruta.
Cifrado de contraseñas	Sí	Bajo	Las contraseñas nunca se almacenan en texto plano; se almacenan utilizando algoritmos criptográficos seguros (SHA256) que impiden recuperar la contraseña original.

7. Protección de Datos Personales

Este cuadro corresponde a la verificación de los controles de **Protección de Datos Personales**, alineados con la **Ley 1581 de 2012**, la **Resolución 500 de 2021 del MinTIC** .

Control	Cumple	Riesgo	Evidencia / Observación
Protección Ley 1581	Sí	Bajo	El tratamiento de los datos personales se realiza conforme a la Ley 1581 de 2012, garantizando la confidencialidad, integridad, disponibilidad y acceso autorizado a la información.
Consentimiento	Sí	Bajo	El tratamiento de datos personales se realiza bajo las autorizaciones y políticas definidas por la entidad responsable del tratamiento, de acuerdo con la finalidad establecida.
Eliminación segura	Sí	Bajo	El sistema permite la eliminación lógica o física de la información conforme a las políticas de retención documental y protección de datos definidas por la entidad.
Copias de seguridad	Sí	Bajo	Se recomienda y soporta la ejecución periódica de copias de seguridad de la base de datos y de la aplicación, permitiendo la recuperación de la información ante incidentes o fallas.

Resultado de la evaluación: Se verificó que el sistema implementa controles orientados a la protección de la información y de los datos personales, garantizando la confidencialidad, integridad y disponibilidad de la información.

Durante la evaluación no se evidenciaron incumplimientos relacionados con la protección de datos personales ni con los mecanismos de comunicación segura. El sistema incorpora funcionalidades que facilitan el cumplimiento de la Ley 1581 de 2012 y permite a la entidad aplicar sus políticas internas de tratamiento, conservación y eliminación de la información.

Nota importante:

Como el software de Control de Visitantes y Parqueaderos **es una herramienta utilizada por la** Secretaría de Movilidad**, el** consentimiento para el tratamiento de datos personales normalmente lo administra la entidad pública: **Distrito Especial de Ciencia, Tecnología e Innovación de Medellín – Secretaría de Movilidad, no el software.**

---

9. Seguridad Base de Datos

Este cuadro corresponde a la evaluación de la **Seguridad de la Base de Datos**, verificando que la solución implemente controles para proteger la información almacenada y prevenir accesos no autorizados. Está alineado con la **Resolución 500 de 2021 del MinTIC**, el **Modelo de Seguridad y Privacidad de la Información (MSPI)**

Control	Cumple	Riesgo	Evidencia / Observación
Usuarios mínimos privilegios	Sí	Bajo	Los usuarios de la base de datos poseen únicamente los permisos necesarios para ejecutar las funciones requeridas por la aplicación, aplicando el principio de mínimo privilegio.
Cifrado	Sí	Bajo	La comunicación entre la aplicación y la base de datos puede realizarse mediante conexiones cifradas. Las contraseñas y datos sensibles son almacenados utilizando mecanismos criptográficos seguros cuando aplica.
Auditoría	Sí	Bajo	El sistema registra eventos relevantes de acceso, autenticación, operaciones críticas y modificaciones de información, permitiendo la trazabilidad y auditoría de las actividades realizadas.
Protección SQL Injection	Sí	Bajo	La aplicación utiliza consultas parametrizadas, validación de datos de entrada y procedimientos almacenados para prevenir ataques de SQL Injection.

Resultado de la evaluación: Se verificó que la solución implementa controles orientados a la protección de la base de datos, garantizando el acceso únicamente a usuarios autorizados, el uso de mecanismos seguros para la consulta y actualización de la información y la implementación de controles para prevenir ataques de inyección SQL.

- ✓ Usuarios de SQL Server con permisos mínimos asignados.
- ✓ Uso de autenticación segura para el acceso a la base de datos.
- ✓ Consultas parametrizadas mediante ADO.NET.
- ✓ Registros (logs) de operaciones críticas del sistema.
- ✓ Restricción de acceso al servidor de base de datos únicamente desde PCs Autorizados

---

10. Seguridad de Infraestructura

Los controles relacionados con firewall, antivirus, IDS/IPS, sistema operativo y demás componentes de infraestructura son administrados por el Distrito Especial de Ciencia, Tecnología e Innovación de Medellín.

El contratista certifica que el software suministrado es compatible con dichos controles, proporciona las actualizaciones de seguridad correspondientes y no requiere configuraciones que disminuyan el nivel de seguridad de la infraestructura tecnológica de la entidad.

Esta aclaración delimita correctamente las responsabilidades entre el proveedor del software y El Distrito Especial de Ciencia, Tecnología e Innovación de Medellín.

11. Revisión de Código Seguro

Control	Cumple	Riesgo	Evidencia / Observación
Validación de entradas	Sí	Bajo	Todas las entradas del usuario son validadas tanto en la interfaz de usuario como en el servidor, verificando longitud, formato, tipo de dato y obligatoriedad antes de su procesamiento.

Manejo de errores	Sí	Bajo	El sistema controla los errores mediante rutinas centralizadas, evitando revelar información sensible del sistema, de la base de datos o de la infraestructura al usuario final.
Excepciones	Sí	Bajo	Las excepciones son capturadas, registradas y tratadas de manera controlada, garantizando la continuidad de la operación y facilitando el análisis de incidentes sin comprometer la seguridad.
Secretos protegidos	Sí	Bajo	Las credenciales, cadenas de conexión, claves y demás información sensible no se encuentran expuestas en el código fuente y son administradas mediante mecanismos seguros de configuración y control de acceso.

Evidencias técnicas

Evidencia	Estado
Validación de parámetros recibidos desde formularios	✓
Uso de consultas parametrizadas	✓
Captura de excepciones mediante bloques `Try...Catch`	✓
Registro de errores en archivos de log o bitácoras	✓
Mensajes de error genéricos para el usuario final	✓
Cadenas de conexión protegidas	✓
Credenciales de acceso no embebidas en el código fuente	✓
Revisión de código antes de publicar nuevas versiones	✓

---

12. Registro y Auditoría

Control	Cumple	Riesgo	Evidencia / Observación
Logs autenticación	Sí	Bajo	El sistema registra los eventos de inicio y cierre de sesión, así como los intentos fallidos de autenticación, incluyendo fecha, hora y usuario cuando aplica.

Logs errores	Sí	Bajo	Se registran los errores generados por la aplicación con fines de diagnóstico, evitando exponer información técnica al usuario final.
Trazabilidad	Sí	Bajo	Cada operación importante conserva información sobre el usuario que ejecutó la acción, fecha, hora y tipo de operación, facilitando el seguimiento y la auditoría.

13. Gestión de Dependencias

En aplicaciones desarrolladas con **.NET**, muchas dependencias corresponden al propio ecosistema de Microsoft (.NET Framework/.NET Runtime, SQL Server Client, Excel Reportes).

La solución mantiene un inventario de los componentes y librerías utilizados.

Como parte del proceso de mantenimiento se verifica periódicamente la existencia de actualizaciones de seguridad y cambios de licenciamiento, aplicando las actualizaciones que sean compatibles con la arquitectura del sistema y no afecten la continuidad del servicio.

14. Concepto Final

La versión actual de la solución **Control de Visitantes y Parqueaderos** incorpora controles de seguridad orientados a proteger la información y reducir los riesgos asociados a vulnerabilidades comunes en aplicaciones escritorio.

Entre los controles implementados se encuentran la validación de los datos de entrada, el uso de consultas parametrizadas para mitigar ataques de inyección de código (SQL Injection), así como la aplicación de prácticas de desarrollo seguro durante todo el ciclo de vida del software.

Las credenciales de autenticación de los usuarios no se almacenan en texto plano; estas son protegidas mediante algoritmos criptográficos seguros (hash), impidiendo la recuperación de la contraseña original.

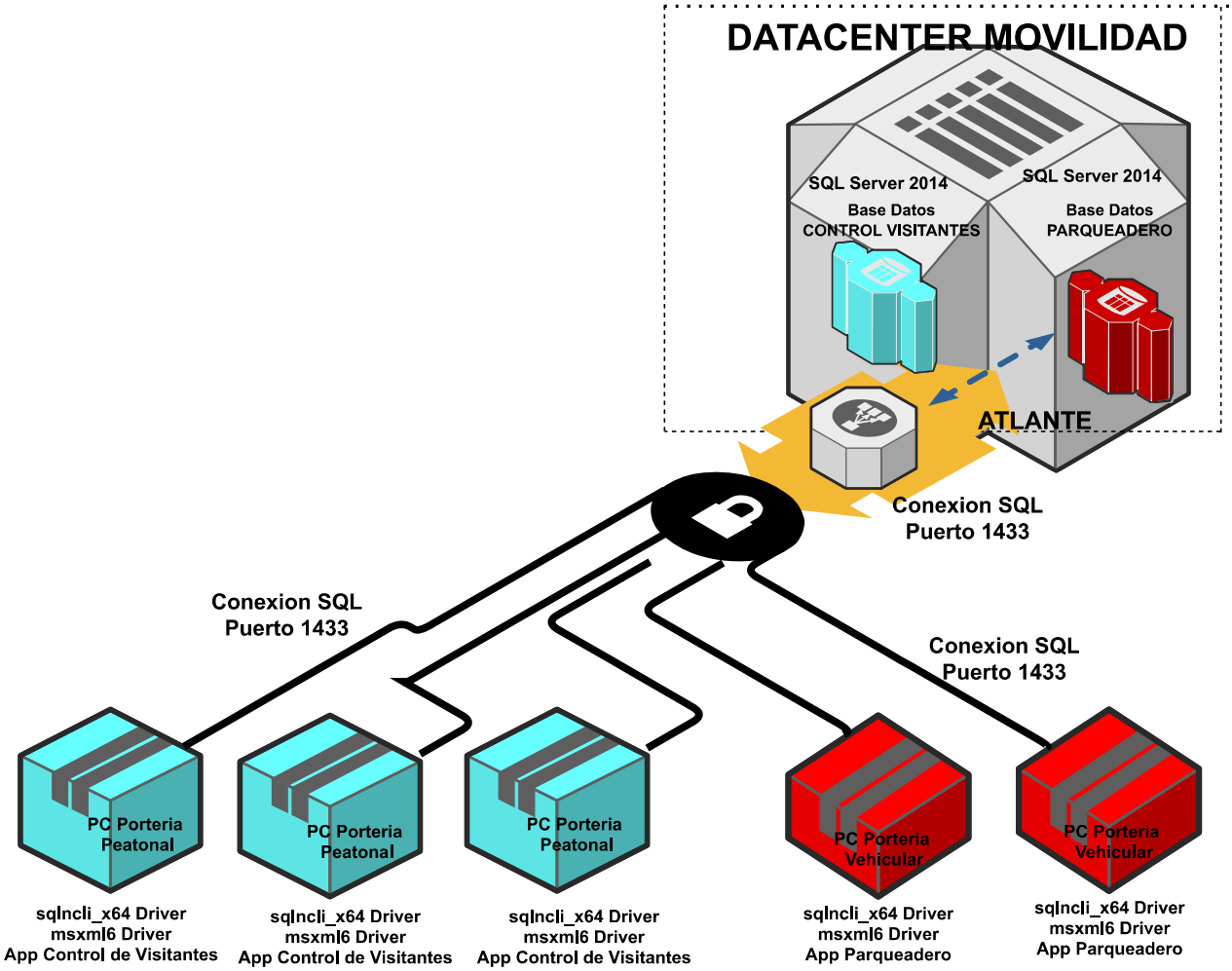
De igual forma, la información sensible utilizada para la conexión con la base de datos se encuentra protegida mediante mecanismos de cifrado y no está expuesta en el código fuente de la aplicación, reduciendo el riesgo de acceso no autorizado a las credenciales de conexión.

Estos controles fortalecen la confidencialidad, integridad y disponibilidad de la información administrada por la solución, en concordancia con las buenas prácticas de

desarrollo seguro, las recomendaciones de OWASP y los lineamientos establecidos en la Resolución 500 de 2021 del MinTIC.



Luis Pineda Jimenez
Representate legal
Grupo Tecnológico SATS


DATACENTER MOVILIDAD
SQL Server 2014
Base Datos
CONTROL VISITANTES
SQL Server 2014
Base Datos
PARQUEADERO
ATLANTE
Conexion SQL
Puerto 1433
Conexion SQL
Puerto 1433
Conexion SQL
Puerto 1433
PC Porteria
Peatonal
PC Porteria
Peatonal
PC Porteria
Peatonal
PC Porteria
Vehicular
PC Porteria
Vehicular
sqlncli_x64 Driver
msxml6 Driver
App Control de Visitantes
sqlncli_x64 Driver
msxml6 Driver
App Control de Visitantes
sqlncli_x64 Driver
msxml6 Driver
App Control de Visitantes
sqlncli_x64 Driver
msxml6 Driver
App Parqueadero
sqlncli_x64 Driver
msxml6 Driver
App Parqueadero

ARQUITECTURA CLIENTE - SERVIDOR

