Sistema Administrativo de la Información Hora de eficientar al bosque por medio de tecnología	**Sistema de Administración de la Información** Reporte de seguridad	**ID reporte:** RS-001

Periodo Del 25 de abril, 2023 al 02 de mayo, 2023	**Fecha de revisión:** 02 de mayo, 2023

Integrantes:
Miguel Sosa Guardado, Owen Jesús Enríquez Ascencio, Jonathan Guillermo Díaz Magallanes, Juan Pablo Cruz Martínez

Certificado SSL/TLS

Contamos con un certificado versión 3, proveído por la empresa Let's Encrypt, generado mediante el algoritmo PKCS #1 SHA-256 con cifrado RSA, con la finalidad de que todas la peticiones realizadas al servidor (sai-colomos.dev) sean de manera segura mediante el protocolo HTTPS

Cloud Edge de ngrok

El servicio proveído por ngrok para el enlace entre el servidor de manera local con el internet utiliza el servicio Cloud Edge de ngrok, el cual se encarga de encriptar y redirigir de manera segura el tráfico desde el dominio de Google Domains hasta la red local donde se encuentra el servidor, siendo cada petición manejada por el Agente de ngrok, mismo que está instalado de manera aislada dentro del proyecto.

JWT

Para la autenticación de las peticiones entrantes al servidor utilizamos JSON Web Tokens, el cual se trata de un tokens únicos los cuales permiten la transmisión de datos de manera cifrada. Cada token se encripta utilizando el algoritmo HS256, tienen un lapso de vida de tres días para un token general, y de noventa días para un token longevo, y la palabra secreta para la firma de cada uno de ellos es una frase única hasheada mediante el algoritmo SHA-256

Passport y Passport-JWT

Para controlar la autenticación al servidor utilizamos la librería Passport, haciendo uso de su estrategia denominada Passport-JWT. Esta librería funciona a manera de middleware el cual se encarga de aceptar o rechazar las sesiones en función de la validación de los tokens

Docker

Para proteger la información almacenada en la base de datos, implementamos la utilización de contenedores de Docker. Un contenedor ejecuta la imagen más reciente de Node.js y es el encargado de ejecutar la API, así como el único que tiene un puerto a la escucha y que puede conectarse con el exterior, mientras que otro contenedor ejecuta la imagen de MongoDB en su versión 4.4.6. Ambos contenedores se comunican mediante una red interna aislada del equipo que envuelve a ambos contenedores, asegurándonos que nadie del exterior pueda manipular el contenedor que ejecuta la base de datos.

Acceso mediante sensor biométrico

Para proteger la privacidad del usuario, se habilitó la opción de acceder mediante el sensor biométrico del dispositivo, en caso de que este cuente con el hardware necesario, el cual puede ser huella dactilar para dispositivos Android y FaceID o TouchID para dispositivos iOS. De esta manera, se añade una

capa más de privacidad a la hora de acceder a la aplicación, y así, evitar que alguien ajeno tenga acceso sin el consentimiento del usuario.

Patrones para la validación de contraseñas

Al momento de que un usuario cree una contraseña nueva, esta será sometida a diferentes validaciones, esto con el fin de que sea lo más segura posible y así evitar sea vulnerada. Dichos patrones son: longitud mínima de ocho caracteres, contener al menos una letra en mayúscula, contener al menos una letra en minúscula, contener al menos un dígito y contener al menos un carácter especial determinado por la expresión regular \/W/

Aviso de confidencialidad

A continuación, se detalla el alcance y el tratamiento de la información que el usuario vuelque en la aplicación. Entiéndase por usuario toda aquella persona registrada o no, que haga uso directo o indirecto de la aplicación

Para el caso de personas registradas, toda la información que aparece en esta aplicación es manejada solo para fines informativos y para relacionar la cuenta con la persona física, además de que recopilar de manera temporal ciertos datos de los sensores (como puede ser la ubicación), los cuales son trabajados de manera local para que ciertas funciones puedan funcionar, todo esto siempre y cuando la persona otorgue los permisos necesario en la aplicación

Para usuarios no registrados, toda la información que sea volcada será manejada solamente para fines estadísticos, y de manera anónima, con el fin de no recopilar información personal más allá de la necesaria (como puede ser el nombre del individuo). Todos los datos estadísticos resultantes serán empleados de manera interna solo para fines de mejoramiento y calidad referente a eventos, actividades o todo aquello en lo que sea necesario

Toda la información de todos los usuarios es y será salvaguardada de manera tal, que siempre sea privada y bajo ninguna circunstancia serán vendida o compartida con alguna empresa sin antes hacer mención al usuario y siempre y cuando el usuario esté de acuerdo y nos exprese su aprobación de manera explícita

Notas de la revisión

Miguel Sosa Guardado Product Manager	Guadalupe Ortega Tirado Revisó