

**LA GERENTE DE LA
E.S.E. HOSPITAL MANUEL URIBE ÁNGEL
NIT. 890.906.347-9**

CERTIFICA

Conforme a la verificación realizada y la constancia expedida el 24 de julio 2024, por la empresa 1Cero1 Software, con la cual, se tiene contratada la implementación de la página web y el soporte de esta, para el cumplimiento de la Resolución 1519 de 2020 en materia de la información a publicar según lo señalado en la Ley 1712 del 2014 y los requisitos en materia de acceso a la información al portal web <https://www.hospitalmua.gov.co>, la ESE Hospital Manuel Uribe Ángel de Envigado (Ant), cumple con los **estándares de calidad y las condiciones técnicas y de seguridad digital** definidas en el Anexo Técnico Nro. 3 de la resolución en mención, dado los controles de seguridad que permiten garantizar la protección de la información.

De acuerdo con la información remitida por el proveedor, 1Cero1 Software, quienes anexaron el diagnóstico de seguridad del portal web de la entidad, a la fecha, se puede certificar que: Dado que el portal web de la ESE, está desarrollado en la plataforma de Microsoft SharePoint, este cuenta con el sistema de seguridad que ofrece esta tecnología y adopta los mecanismos de autenticación, autorización y seguridad, tales como:

- Token de seguridad (STS) para la autenticación del servidor.
- Sistema de autenticación de identidades basado en formularios de ASP.NET.
- Medidas de seguridad en autenticación, roles y privilegios.
- Administración del software a través de granjas de desarrollo en .NET.
- Entornos de Ejecución para desarrollo.
- Control de acceso por medio de sistema FBA.

Niveles de seguridad enfocados en la estructura web:

- Control de versionamiento.
- Sanitización de código y pruebas de testing.
- Respaldos de seguridad en la nube.
- Implementación de certificado de seguridad SSL
- Aplicación de antivirus y firewall en servidor.
- Habilitación de cabeceras de seguridad (CSP, X-Content-Type-Options, etc.).
- Actualización de librerías de desarrollo.
- Controles de protección de acceso y de ataques como Cross-site scripting, SQL injection o Denial-of-service, entre otros.

Adicional a los anteriores se cumple con otras medidas de seguridad desde la E.S.E. como:

- Política de seguridad y privacidad de la información y seguridad digital
- Reporte y monitoreo de incidentes cibernéticos graves o muy graves al CSIRT-Gobierno o CoCERT. Sin eventos presentados en la vigencia 2023.
- Modelo de Seguridad y Privacidad de la Información (MSPI)

El presente se emite a los 29 días del mes de julio de 2024.

MARTHA LUCÍA VÉLEZ ARANGO
Gerente