

Palermo Huila, 15 de marzo de 2026

**Señores**

**E.S.E. Hospital San Francisco de Asís**

Asunto: Certificación Cumplimiento Criterios de Seguridad

Mediante la presente, se certifica que el portal web de la E.S.E. Hospital San Francisco de Asís cual se encuentra publicado en el dominio:

<https://www.esehospitalsanfranciscocodeasis.gov.co/>.

Cumple con los siguientes criterios de seguridad de acuerdo con el Anexo 3, puntos 3.2 y 3.3 de la Resolución MinTIC 1519 del 2020, en lo concerniente al sitio web y alojamiento web.

<b>Criterio</b>	<b>Cumple</b>
Implementar o exigir controles de seguridad relacionados con el control de la autenticación, definición de roles y privilegios y separación de funciones	Si
Exigir medidas de seguridad al proveedor del hosting (políticas de seguridad robustas y un nivel de madurez en seguridad optimizado).	Si
Aplicar mecanismos de hardening para eliminar configuraciones y credenciales por defecto, además de deshabilitar métodos HTTP peligrosos como put, delete, trace y restringir en lo posible la administración remota.	Si
Proteger la integridad del código, mediante: (i) la validación exhaustiva de: inputs, variables post y get (no enviar parámetros sensibles a través del método get), Cookies (habilitar atributos de seguridad como Secure y HttpOnly), y, cabeceras HTTP; (ii) la sanitización de los parámetros de entrada: es decir, que cuando se reciba la información de dichas variables se eliminen etiquetas, saltos de línea, espacios en blanco y otros caracteres especiales que comúnmente conforman un script, además de la restricción de formatos y tamaños de subidas de archivos; (iii) la sanitización y escape de variables en el código; (iv) verificación estándar de las Políticas de Origen de las cabeceras; y (v) la verificación y comprobación del token de CSRF (cuando aplique).	Si
Ejecutar monitoreos de seguridad sobre las páginas web que contemple, entre otras, las siguientes acciones: escaneo de archivos infectados, escaneo de vulnerabilidades, análisis de patrones para detectar acciones sospechosas, verificación contra listas negras, monitoreo del tráfico para detectar ataques de denegación de servicios	Si

Exigir mecanismos de autenticación dentro de los sitios web a través de la creación de contraseñas fuertes y solicitar renovaciones periódicas de las mismas garantizando la accesibilidad de persona con discapacidad.	Si
Mantener actualizado el software, frameworks y plugins de los sitios web.	Si
Restringir el uso de login contra ataques de fuerza bruta, implementando, entre otros: mecanismos de captcha accesibles o auto detectable, y/o limitar la tasa de intentos de login.	Si
Ocultar y restringir páginas de acceso administrativo.	Si
Restringir la escritura de archivos desde la web a través de la asignación de permisos de solo lectura.	Si
Crear copias de respaldo.	Si
Almacenar trazas o logs de auditoría de los eventos de seguridad, logins, entre otros.	Si
Garantizar conexiones seguras a través de uso de certificados, SSL (HTTPS para la confianza de usuarios) y cifrado en la estructura de las peticiones para portales transaccionales, para evitar la manipulación de parámetros en las peticiones.	Si
Implementar mensajes genéricos de error, que no revelen información acerca de la tecnología usada, excepciones o parámetros que dispararon el error específico, los cuales deberán ser comprensibles por parte de las personas, incluyendo la accesibilidad para las personas con discapacidad.	Si
Proteger el binario de la aplicación, a través de métodos de ofuscación que impidan realizar procedimientos de ingeniería inversa (reversing) para analizar la lógica de la aplicación.	No Aplica
Sanitización de parámetros de entrada mediante la eliminación de etiquetas, saltos de línea, espacios en blanco y otros caracteres especiales que comúnmente conforman un «script», además de la restricción de formatos y tamaños para subida de archivos.	Si
Sanitización de caracteres especiales (secuencia de Escape de variables en el código de Programación)	Si
Revisar las recomendaciones de seguridad en la guía de desarrollo seguro de aplicaciones y Servicios Web Seguros de la Open Web Application Security Project (OWASP).	No Aplica
Implementar en los servidores los controles necesarios (hardware o software) de protección de acceso y de ataques como Cross-site scripting, SQL injection o Denial-of-service, entre otros.	Si
Incorporar validación de formularios tanto del lado del cliente como del lado del servidor.	Si
Implementar monitoreos de seguridad sobre la plataforma tecnológica que hace parte del sitio web (escaneo de vulnerabilidades, escaneo de archivos infectados, análisis de patrones para detectar acciones sospechosas, verificación contra listas negras, monitoreo del tráfico para detectar ataques de denegación de servicios) y realizar las acciones de mitigación correspondientes	Si

Establecer los planes de contingencia, DRP y BCP, que permita garantizar la continuidad de la sede electrónica o del sitio web 7/24 los 365 días del año.	No, se debe ampliar la plataforma y estructurar dichos planes.
Restringir la escritura de archivos en el servidor web a través de la asignación de permisos de roles y los privilegios asociados.	Si
Implementar sistemas antivirus en el servidor web, para garantizar medidas contra infecciones de malware a los archivos del mismo.	Si
Controlar el escalamiento de privilegios en los Sistemas Operativos, servidor web y Bases de datos que hacen parte de la infraestructura del portal web.	No aplica
Realizar análisis estático del código con el objetivo de identificar vulnerabilidades que se encuentra en la programación de las aplicaciones	No aplica
Cumplir con la estandarización de código fuente para portales web, siguiendo las buenas prácticas del W3C (World Web Wide Consortium), de forma que permita la correcta visualización de la información a los usuarios	Si
Adoptar validadores HTML y CCS para la continua revisión del sitio web y su mejora continua, a través de las buenas prácticas del W3C (World Web Wide Consortium).	Si
Cumplir con los estándares definidos para la integración al Portal Único del Estado Colombiano GOV.CO, incluyendo la validación de la codificación, en caso de que les aplique.	No, se deben estudiar dichos estándares
Incluir lenguaje común de intercambio para la generación y divulgación de la información y datos estructurados y no estructurados dispuestos en medios electrónicos, como los sitios web de los sujetos obligados y el Portal Único del Estado Colombiano GOV.CO, en caso de que les aplique.	No, se debe revisar si para la ESE Aplica.
Implementar un sistema de control de versiones (Git), que permitan planear y controlar la vida de la aplicación, y en una fase a mediano plazo poder implementar un sistema de integración, cambio y despliegue continuo.	No aplica

Cordialmente,

*John Fenner B.*

---

**JOHN FENNER BERMUDEZ CABRERA**  
**M.P. 161122-0613014 TLM**  
**INGENIERO DE SISTEMAS**