Neiva, 15 de mayo de 2026

CERTIFICACIÓN

La empresa CLICK MASIVO S.A.S. identificada con NIT 901.147.222-9 certifica que la página web de la ESE CARMEN EMILIA OSPINA, cumple con aspectos a tener en cuenta de conformidad con la ley 1712 de 2014.

El portal se encuentra publicado en el dominio https://esecarmenemiliaospina.gov.co/ y cumple con la normatividad implementada por la estrategia GEL, con los criterios de accesibilidad web del Anexo 1 y 3 de la Resolución MinTIC 1519 del 2020 y de Usabilidad Web, tanto a nivel de la estructura web, como en los trámites implementados de manera parcial y total en línea.

Sitio responsive adaptable a dispositivos móviles.

Calificación Validación de Accesibilidad: AA. CMS - Wordpress con motores de Bases de Datos MYSQL.

Esta aplicación es escalable y modular, permite ser adaptable y permite la comunicación entre diferentes sistemas, aportando al cumplimiento de los Ítems “seguridad y privacidad de la información” y “TIC para Gestión”.

1. ACCESIBILIDAD WEB.

Directrices de Accesibilidad Web.

a. Los elementos no textuales (p. ej. imágenes, diagramas, mapas, sonidos, vibraciones, etc.) que aparecen en el sitio web tienen texto alternativo.
b. Los videos o elementos multimedia tienen subtítulos y audio descripción (cuando no tiene audio original), como también su respectivo guion en texto. (en los siguientes casos también deben tener lenguaje de señas: para las alocuciones presidenciales, información sobre desastres y emergencias, información sobre seguridad ciudadana, rendición de cuentas anual de los entes centrales de cada sector del Gobierno Nacional).
c. El texto usado en el sitio web es de mínimo 12 puntos, con contraste de color que permita su visualización, y con posibilidad de ampliación hasta el 200% sin desconfiguración del contenido.
d. El código de programación y el contenido del sitio web está ordenado, con lenguaje de marcado bien utilizado y comprensible sin tener en cuenta el aspecto visual del sitio web, con una estructura organizada, identificación coherente y

unificada de los enlaces (vínculos/botones), y con la posibilidad de una navegación lineal y continua con esos enlaces, incluyendo un buscador.

e. Los formularios o casillas de información tienen advertencias e instrucciones claras con varios canales sensoriales (p. ej. Campos con asterisco obligatorio, colores, ayuda sonora, mayúscula sostenida).
f. Al navegar el sitio web con tabulación se hace en orden adecuada y resaltando la información seleccionada.
g. Se permite control de contenidos con movimientos y parpadeo y de eventos temporizados.
h. El lenguaje de los títulos, páginas, sección, enlaces, mensajes de error, campos de formularios, es en español claro y comprensible (siguiendo la guía de lenguaje claro del DAFP, en el caso de las entidades públicas, disponible en: https://www.portaltributariodecolombia.com/wp-content/uploads/2015/07/portaltributariodecolombia_guia-de-lenguaje-claro-para-servidores-publicos.pdf).
i. Los documentos (Word, Excel, PDF, Power Point, etc.) cumplen con los criterios de accesibilidad establecidos en el Anexo 1 de la Resolución 1519 de 2020 para ser consultados fácilmente por cualquier persona.

2 CONDICIONES DE SEGURIDAD DIGITAL

- Implementar o exigir controles de seguridad relacionados con el control de la autenticación, definición de roles y privilegios y separación de funciones.
- Exigir medidas de seguridad al proveedor del hosting (políticas de seguridad robustas y un nivel de madurez en seguridad optimizado).
- 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.
- 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).
- 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.

- 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.
- Mantener actualizado el software, frameworks y plugins de los sitios web.
- 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.
- Ocultar y restringir páginas de acceso administrativo.
- Restringir la escritura de archivos desde la web a través de la asignación de permisos de solo lectura.
- Crear copias de respaldo.
- Almacenar trazas o logs de auditoría de los eventos de seguridad, logins, entre otros.
- 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. (adicional al cifrado SSL), También deben habilitar las cabeceras de seguridad, entre otras las siguientes: Content-Security-Policy (CSP), X-Content-Type-Options, X-Frame-Options, X-XSS-Protection, StrictTransport-Security (HSTS), Public-Key-Pins (HPKP) Referrer-Policy, FeaturePolicy.
- 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.
- 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.
- 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.
- Sanitización de caracteres especiales (secuencia de Escape de variables en el código de Programación).

- 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.
- Incorporar validación de formularios tanto del lado del cliente como del lado del servidor.
- 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.
- Restringir la escritura de archivos en el servidor web a través de la asignación de permisos de roles y los privilegios asociados.
- Implementar sistemas antivirus en el servidor web, para garantizar medidas contra infecciones de malware a los archivos de este.
- Controlar el escalamiento de privilegios en los Sistemas Operativos, servidor web y Bases de datos que hacen parte de la infraestructura del portal web.

3. PROGRAMACIÓN DEL CÓDIGO FUENTE:

- Realizar análisis estático del código con el objetivo de identificar vulnerabilidades que se encuentra en la programación de las aplicaciones.
- 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.
- 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).

Agradecemos su atención, Cordialmente,

Cordialmente,

OSCAR EMILIO ANTOLINEZ COLLAZOS
Webmaster Click Masivo SAS