

DOCUMENTO SOPORTE DE ALINEACIÓN MSPI V5.0

Requerimientos y Lineamientos de Seguridad y Privacidad de la Información para el Portal Web Oficial

Entidad: Institución Educativa Cárdenas Centro

Marco Normativo: Modelo MSPI v5.0 (MinTIC) / Ley 1581 / Ley 1712

Sitio Web: <https://cardenascentro.edu.co/>

Fecha de Emisión: Julio de 2026

PROPÓSITO INSTITUCIONAL DEL DOCUMENTO

El presente documento establece formalmente el marco de implementación, requerimientos técnicos, legales y organizacionales del **Modelo de Seguridad y Privacidad de la Información (MSPI v5.0)** emitido por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), aplicado específicamente al activo digital misional correspondiente al portal web institucional de la **Institución Educativa Cárdenas Centro** (<https://cardenascentro.edu.co/>).

1. MARCO LEGAL Y ALCANCE OPERATIVO

El portal web de la Institución Educativa Cárdenas Centro actúa como la plataforma pública de interacción, transparencia y prestación de servicios digitales para la comunidad educativa (estudiantes, acudientes, docentes, directivos y ciudadanía general). En cumplimiento de la normativa colombiana vigente, este activo digital debe ceñirse a:

- **Constitución Política de Colombia:** Artículos 15 (Habeas Data e Intimidad), 209 y 269.
- **Ley 1581 de 2012 y Decreto 1377 de 2013:** Protección de Datos Personales y tratamiento de Información Identificable Personal (PII).
- **Ley 1712 de 2014:** Transparencia y del Derecho de Acceso a la Información Pública Nacional.
- **Decreto 1078 de 2015 y Decreto 767 de 2022:** Decreto Único Reglamentario del Sector TIC y Política de Gobierno Digital.
- **Decreto 338 de 2022:** Gobernanza de la Seguridad Digital y gestión de incidentes.
- **Resolución MinTIC 500 de 2021 & Documento Maestro MSPI v5.0 (2025/2026):** Estándares de seguridad digital para entidades públicas.

2. FASES DEL CICLO PHVA APLICADAS AL PORTAL WEB

La implementación del MSPI en la plataforma web de la institución se estructura operacionalmente bajo las cinco (5) fases del ciclo continuo definido por el MinTIC:

Fase 0: Diagnóstico (Análisis GAP)

Evaluación inicial de brechas de la infraestructura del portal web respecto a las exigencias del MSPI. Medición del nivel de madurez en controles de alojamiento web (hosting), bases de datos de formularios, certificados SSL/TLS y mecanismos de protección de datos de menores de edad procesados a través del portal.

Fase 1: Planificación (Planear)

- **Alcance del MSPI Web:** Inclusión formal del servidor, CMS, base de datos, formularios web, certificados y registros de la página web institucional.
- **Liderazgo y Política:** Aprobación de la Política de Seguridad e Intimidad Digital en el Portal Web por el Comité Institucional de Gestión y Desempeño.
- **Inventario y Clasificación:** Identificación de activos digitales (Dominio, Hosting, Bases de Datos de Contacto/Matrículas, Gestor de Contenidos).
- **Valoración de Riesgos Web:** Análisis de vulnerabilidades frente a inyección SQL, XSS, desfiguración de página (Defacement), ataques DDoS e ingeniería social/Phishing.

Fase 2: Operación (Hacer)

Despliegue e implementación efectiva de las políticas, salvaguardas y controles técnicos definidos en la Declaración de Aplicabilidad (SOA). Incluye la configuración de Firewalls de Aplicaciones Web (WAF), gestión de parches de seguridad del CMS y habilitación de protocolos seguros HTTPS/TLS 1.3.

Fase 3: Evaluación de Desempeño (Verificar)

Monitoreo mediante indicadores de disponibilidad del portal, análisis de registros de accesos (logs), auditorías internas semestrales de seguridad web y revisiones periódicas de cumplimiento normativo por parte de la alta dirección institucional.

Fase 4: Mejoramiento Continuo (Actuar)

Implementación de acciones correctivas ante alertas de seguridad reportadas por el CSIRT Gobierno/ COLCERT, remediación de hallazgos de auditoría y actualización del Plan de Tratamiento de Riesgos en cada vigencia.

3. MATRIZ DE CONTROLES ESENCIALES ISO/IEC 27001:2022 PARA LA PÁGINA WEB

A continuación se establecen los controles prioritarios del Anexo A del MSPI v5.0 requeridos para garantizar la confidencialidad, integridad y disponibilidad del sitio web institucional:

Código	Nombre del Control	Dominio	Lineamiento y Especificación Técnica para cardenascentro.edu.co
A.5.9	Inventario de Activos	ORGANIZACIONAL	Registrar formalmente el dominio .edu.co, servidores de hosting, bases de datos de formularios de contacto/peticiones y cuentas administrativas del sitio web.

Código	Nombre del Control	Dominio	Lineamiento y Especificación Técnica para cardenascentro.edu.co
A.5.12	Clasificación de Información	ORGANIZACIONAL	Clasificar el contenido web en Información Pública (noticias, circulares), Clasificada (datos de estudiantes/docentes) y Reservada (credenciales administrativas).
A.5.15	Control de Acceso	ORGANIZACIONAL	Restringir la administración del CMS a usuarios autorizados mediante autenticación multifactor (MFA) y principio de menor privilegio.
A.5.23	Seguridad en Servicios en Nube	ORGANIZACIONAL	Establecer requisitos contractuales de seguridad y Acuerdos de Nivel de Servicio (SLA) con el proveedor de Hosting web y DNS.
A.5.34	Privacidad y Protección de PII	ORGANIZACIONAL	Publicar la Política de Tratamiento de Datos Personales en el portal, incluyendo aviso de privacidad en formularios web de recolección de datos.
A.7.7	Escritorio y Pantalla Despejada	FÍSICO	Garantizar el cierre automático de sesión administrativa en la consola de gestión del portal web por inactividad.
A.8.5	Autenticación Segura	TECNOLÓGICO	Exigir contraseñas robustas (mínimo 12 caracteres, complejidad alta) y renovaciones periódicas para editores y administradores web.
A.8.7	Protección contra Malware	TECNOLÓGICO	Implementar escaneo automatizado contra software malicioso e inyecciones de código en el servidor web.
A.8.8	Gestión de Vulnerabilidades	TECNOLÓGICO	Mantener actualizado el núcleo del CMS, plugins y complementos del portal web a sus versiones estables de seguridad más recientes.
A.8.13	Copia de Seguridad (Backup)	TECNOLÓGICO	Programar respaldos automatizados diarios de la base de datos y semanales del código fuente/archivos del sitio web con almacenamiento fuera de sitio.
A.8.20	Seguridad en Redes	TECNOLÓGICO	Implementar certificados SSL/TLS vigentes para forzar conexiones cifradas mediante el protocolo HTTPS.
A.8.23	Filtrado Web y WAF	TECNOLÓGICO	Desplegar un Web Application Firewall (WAF) para bloquear ataques como SQL Injection, Cross-Site Scripting (XSS) y Denegación de Servicio (DDoS).
A.8.28	Codificación Segura	TECNOLÓGICO	Asegurar la validación y sanitización de todas las entradas de datos en formularios públicos del portal institucional.

4. PROTOCOLO DE RESPUESTA A CIBERINCIDENTES WEB

En concordancia con los lineamientos de COLCERT y el MSPI v5.0, ante cualquier evento de seguridad digital en el portal web (tales como la alteración no autorizada del sitio - Defacement, indisponibilidad por ataque DDoS o filtración de datos), la institución ejecutará el siguiente procedimiento:

- Detección y Notificación:** Identificación del evento mediante alertas del WAF o monitoreo de disponibilidad, notificando inmediatamente al Oficial/Responsable de Seguridad de la Información de la entidad.
- Contención Inmediata:** Aislamiento del portal o paso temporal a modo de mantenimiento/contingencia para prevenir propagación o mayor afectación.

3. **Análisis y Erradicación:** Identificación del vector de ataque, eliminación del código malicioso e implementación de parches de corrección.
4. **Reporte Obligatorio:** Notificación formal del ciberincidente al CSIRT Gobierno / COLCERT en el menor tiempo posible conforme a los protocolos nacionales.
5. **Restauración y Lecciones Aprendidas:** Recuperación del sitio desde la copia de respaldo limpia verificada y actualización de la matriz de riesgos.

5. APROBACIÓN E INSTITUCIONALIZACIÓN

El presente documento constituye el soporte formal de alineación técnica y reglamentaria del sitio web <https://cardenascentro.edu.co/> con el Modelo de Seguridad y Privacidad de la Información (MSPI) del MinTIC, y deberá ser revisado semestralmente por el Comité Institucional de Gestión y Desempeño.

Rectoría / Dirección Institucional
IE Cárdenas Centro

Líder / Responsable de Seguridad Digital
IE Cárdenas Centro