UNMSM
Fundación
SAN MARCOS
Por el desarrollo de la Ciencia y la Cultura

DIPLOMADO DE ESPECIALIZACIÓN

GESTIÓN DE LA CIBERSEGURIDAD Y PRIVACIDAD

RESUMEN EJECUTIVO

Documento Maestro de Los Lineamientos del Modelo de Seguridad y Privacidad de la Información

JULIO – OCTUBRE 2026

CENCAEP
CAPACITA

GOBIERNO DIGITAL · SEGURIDAD DE LA INFORMACIÓN · PRIVACIDAD

RESUMEN EJECUTIVO

Lineamientos del Modelo de Seguridad y Privacidad de la Información

Documento Maestro MSPI · Versión 5.0 · MinTIC Colombia · 21 de abril de 2025

Conclusión ejecutiva El MSPI convierte la seguridad y la privacidad en una capacidad institucional permanente, gobernada por la alta dirección y gestionada con base en riesgos. Su valor no reside en acumular políticas, sino en demostrar que los controles protegen servicios públicos, datos personales, activos críticos y continuidad operativa mediante evidencia verificable y mejora continua.

Lectura estratégica

La versión 5.0 del Modelo de Seguridad y Privacidad de la Información proporciona a las entidades públicas nacionales y territoriales de Colombia una ruta para formalizar su Sistema de Gestión de Seguridad y Privacidad de la Información (SGSPI). El modelo adopta la lógica PHVA y la amplía en cinco fases: diagnóstico, planificación, operación, evaluación del desempeño y mejoramiento continuo.

El enfoque integra gobierno institucional, protección de datos personales, gestión de activos, infraestructura crítica cibernética, riesgos, incidentes, vulnerabilidades, terceros y continuidad. La seguridad deja de ser una responsabilidad exclusiva del área de tecnología y pasa a formar parte de la gestión institucional, con decisiones, recursos y rendición de cuentas en el Comité Institucional de Gestión y Desempeño.

Mensajes clave para la alta dirección

- **Gobernar antes que reaccionar.** La dirección debe aprobar el marco, asignar responsables, disponer recursos y revisar el desempeño al menos en los espacios definidos por el modelo.

Priorizar según el riesgo. Los controles se seleccionan a partir de activos, amenazas, vulnerabilidades, impacto, probabilidad y apetito de riesgo; no mediante una lista aplicada sin contexto.

Probar la eficacia. Inventarios, matrices, planes, registros, indicadores, auditorías y acciones correctivas constituyen la evidencia de que el sistema funciona.

Proteger la misión. La finalidad es sostener servicios esenciales, reducir el impacto de incidentes y preservar la confianza ciudadana.

01 | RESUMEN EJECUTIVO

Finalidad, alcance y arquitectura del modelo

Un marco institucional para gestionar seguridad, privacidad y resiliencia digital.

Objeto y audiencia

El documento está dirigido principalmente a entidades públicas colombianas del orden nacional y territorial, así como a proveedores vinculados a la Política de Gobierno Digital y a terceros que adopten el modelo. Su propósito es facilitar la implementación del MSPI, desarrollar la estrategia de seguridad digital, institucionalizar la protección de la información y apoyar la identificación y el tratamiento de riesgos.

El modelo se apoya en la Resolución 500 de 2021 y se articula con la Política de Gobierno Digital, el MIPG, la protección de datos personales, la transparencia y el acceso a la información pública. También toma como referente ISO/IEC 27001:2022 y menciona prácticas complementarias de GDPR y NIST SP 800-53 para escenarios que requieren mayor profundidad técnica.

Ciclo de implementación

Fase	Pregunta de gestión	Resultado esperado
1. Diagnóstico	¿Cuál es la situación actual?	Brechas y nivel de madurez mediante el instrumento de evaluación MSPI.
2. Planificación	¿Qué se protegerá y cómo?	Alcance, gobierno, política, activos, riesgos, tratamiento, recursos y cultura.
3. Operación	¿Cómo se ejecutan los controles?	Controles implementados, riesgos tratados y evidencias de operación.
4. Evaluación	¿Qué tan eficaz es el sistema?	Indicadores, seguimiento, auditoría interna y revisión por la dirección.
5. Mejoramiento	¿Qué debe corregirse o fortalecerse?	Acciones correctivas y plan anual de mejora.

Principios de aplicación

Proporcionalidad. El alcance y los controles deben ajustarse al contexto, la misión, el tamaño, los procesos y los recursos de cada entidad.

Trazabilidad. Las decisiones deben quedar respaldadas por documentación controlada, responsables, fechas, criterios y aprobaciones.

Transversalidad. La seguridad involucra procesos, personas, instalaciones, tecnología, proveedores y tratamiento de datos; no se limita a herramientas informáticas.

Ciclo continuo. El diagnóstico se actualiza después de evaluar el desempeño para medir avance y alimentar la mejora.

Criterio de éxito Una fase solo se considera completada cuando se cumplen todos los requisitos definidos para ella. Por tanto, el avance debe medirse por resultados y evidencias, no por actividades aisladas.

02 | RESUMEN EJECUTIVO

Gobierno, contexto y responsabilidades

La seguridad efectiva comienza con decisiones institucionales claras.

Comprensión del contexto y de las partes interesadas

La planificación parte del conocimiento de la entidad: misión, objetivos estratégicos, procesos, servicios, arquitectura empresarial, sedes, recursos, cultura y condiciones internas y externas. Sobre esta base se identifican las partes interesadas y sus requisitos legales, reglamentarios, contractuales y operativos. El resultado esperado es un análisis documentado que conecte las necesidades institucionales con el diseño del SGSPI.

El alcance debe definir con precisión procesos, activos, sistemas, personas, recursos y áreas físicas cubiertas. El documento recomienda priorizar inicialmente los procesos misionales por su impacto estratégico y exposición. Un alcance excesivamente amplio sin recursos suficientes puede producir cumplimiento aparente; uno demasiado reducido puede dejar fuera servicios o dependencias críticas.

Liderazgo y toma de decisiones

El Comité Institucional de Gestión y Desempeño, o su equivalente, debe recibir formalmente las funciones asociadas a seguridad y privacidad. Allí se aprueban la política, los objetivos, los recursos, los planes y las decisiones sobre riesgos. El responsable de seguridad participa de manera permanente para mantener el vínculo entre la estrategia institucional, el riesgo y la ejecución técnica.

Actor	Responsabilidad principal
Alta dirección / nominador	Patrocinar el modelo, aprobar decisiones de alto nivel y asegurar recursos.
Comité Institucional de Gestión y Desempeño	Aprobar políticas, planes, riesgos, aplicabilidad, prioridades y seguimiento.
Responsable de seguridad de la información	Coordinar el MSPI, monitorear su ejecución y reportar avances y desviaciones.

Actor	Responsabilidad principal
Líderes de proceso	Gestionar los riesgos de sus procesos y aprobar los tratamientos correspondientes.
Áreas ejecutoras y usuarios	Implementar los controles asignados; cumplir políticas, proteger activos y reportar eventos oportunamente.

Independencia y autoridad

El modelo indica que el responsable del MSPI debe depender de un área estratégica distinta de Tecnología, contar con un equipo de apoyo y participar con voz y voto en el comité de gestión institucional. Cuando no exista personal de planta, se admite compartir el responsable entre entidades mediante servicios contratados, siempre que se justifique la limitación de recursos.

Riesgo de gobierno Si la misma unidad que implementa los controles concentra la definición, supervisión y evaluación, se debilitan la independencia, la transparencia del reporte y la capacidad de escalar riesgos no aceptables.

03 | RESUMEN EJECUTIVO

Activos, infraestructura crítica y gestión del riesgo

La prioridad se determina por el valor de la información y el impacto sobre la misión.

Inventario y clasificación

Cada proceso debe identificar los activos de información que generan valor y requieren protección. El inventario debe incluir información, sistemas, hardware, software, soportes, instalaciones, personas y otros elementos asociados a su tratamiento. La clasificación considera confidencialidad, integridad y disponibilidad, identifica datos personales y reconoce infraestructura crítica y servicios esenciales.

Los propietarios y custodios deben revisar el inventario periódicamente y siempre que cambie un proceso, sistema o servicio. La utilidad del inventario depende de su conexión con la gestión del riesgo: un registro

desactualizado impide reconocer exposiciones, dependencias y concentraciones de impacto.

Valoración del riesgo

La entidad debe aplicar una metodología consistente, válida y comparable para identificar eventos que puedan afectar la confidencialidad, integridad, disponibilidad, privacidad y continuidad. El análisis define propietarios del riesgo, consecuencias, probabilidad, nivel resultante, apetito, criterios de aceptación y prioridad de tratamiento.

Componente	Decisión que habilita
Activo y propietario	Determina qué se protege y quién responde por la decisión.
Amenaza y vulnerabilidad	Explica cómo podría materializarse un evento adverso.
Impacto y probabilidad	Permite estimar y comparar el nivel de riesgo.
Apetito y aceptación	Define qué exposición puede asumir formalmente la entidad.
Control y riesgo residual	Muestra el efecto esperado del tratamiento y la exposición remanente.
Seguimiento	Verifica cambios, eficacia y necesidad de ajustes.

Tratamiento y declaración de aplicabilidad

El plan de tratamiento debe seleccionar controles pertinentes, asignar responsables y fechas, y permitir trazabilidad. Los dueños de los riesgos aprueban formalmente el plan; la decisión se eleva al Comité Institucional de Gestión y Desempeño. La declaración de aplicabilidad registra los controles adoptados, su estado y la justificación de exclusiones según los riesgos y las capacidades técnicas y humanas.

La versión 5.0 pide considerar amenazas avanzadas persistentes, vulnerabilidades emergentes, entornos de nube y riesgos de la cadena de suministro digital. Esto exige incorporar inteligencia de amenazas, dependencias de terceros y cambios tecnológicos dentro de la evaluación, no como anexos desconectados.

Punto crítico Aceptar un riesgo residual es una decisión de negocio e institucional. Debe estar sustentada, aprobada por la autoridad competente y sujeta a revisión cuando cambien el contexto, los activos o las amenazas.

04 | RESUMEN EJECUTIVO

Operación, resiliencia y evidencia

La operación traduce el riesgo priorizado en controles sostenibles y verificables.

Implementación operacional

La fase de operación ejecuta el Plan de Seguridad y Privacidad y el plan de tratamiento de riesgos. Cada proceso debe documentar acciones, controles, responsables, fechas y presupuesto. Los proyectos que no puedan implementarse en el corto o mediano plazo deben escalarse al comité para decidir prioridades, recursos, medidas compensatorias o aceptación formal del riesgo.

El modelo requiere actualizar el inventario de activos, la matriz de riesgos, la gestión de eventos e incidentes y la gestión de vulnerabilidades. También exige conservar evidencia de los controles implementados. Para elevar la resiliencia, recomienda reforzar el monitoreo continuo y los mecanismos de alerta temprana que permitan detectar y responder oportunamente a ciberataques.

Capacidades operativas prioritarias

- **Gestión de identidades y accesos.** Altas, cambios, bajas, privilegios, autenticación segura y revisión periódica.
- **Gestión de vulnerabilidades y configuración.** Inventario técnico, evaluación de exposición, remediación priorizada y configuraciones controladas.
- **Monitoreo y registro.** Trazas protegidas, sincronización de tiempo, correlación de eventos y análisis de actividad anómala.
- **Respuesta a incidentes.** Canales de reporte, evaluación, contención, respuesta, recuperación, aprendizaje y articulación con equipos CSIRT/CERT cuando corresponda.

Continuidad y recuperación. Copias de respaldo probadas, redundancia, preparación TIC para la continuidad y recuperación frente a interrupciones.

Terceros y cadena de suministro. Requisitos contractuales, evaluación de proveedores, seguridad de servicios en nube y gestión de cambios.

Cultura y documentación

La competencia técnica debe complementarse con comunicación, sensibilización y formación según el rol. El plan de cambio, cultura y apropiación debe incluir prácticas frente a phishing, ingeniería social, ciberhigiene y reporte de eventos, además de medir la eficacia de la capacitación. La documentación del SGSPI debe mantenerse identificada, versionada, disponible para quienes la necesiten y protegida contra alteración o divulgación indebida.

Evidencia mínima No basta con declarar que existe un control. La entidad debe poder mostrar su diseño, aprobación, operación, resultados, excepciones, responsables, revisiones y acciones de mejora.

05 | RESUMEN EJECUTIVO

Medición, auditoría y mejoramiento continuo

La eficacia se demuestra mediante resultados comparables y decisiones documentadas.

Seguimiento e indicadores

La entidad debe definir indicadores que midan la evolución de la madurez y la eficacia del MSPI. Los métodos de medición deben ser reproducibles y comparables, con tiempos, responsables y recursos para el monitoreo. Los resultados deben integrarse al tablero de control del plan de acción y reportarse al Comité Institucional de Gestión y Desempeño.

Dimensión	Ejemplo de evidencia de gestión
Cobertura	Procesos y activos incluidos frente al alcance aprobado.
Riesgo	Riesgos altos tratados, vencidos y aceptados; evolución del riesgo residual.
Control	Controles implementados y probados; excepciones y medidas compensatorias.
Incidentes	Tiempos de detección, contención y recuperación; recurrencia y causas.
Vulnerabilidades	Exposición por criticidad, antigüedad y cumplimiento de plazos de remediación.
Cultura	Cobertura y eficacia de formación; reportes de phishing y eventos por usuarios.
Continuidad	Pruebas de respaldo, restauración y ejercicios de continuidad completados.

Auditoría interna y revisión por la dirección

El MSPI establece al menos una auditoría interna anual para evaluar cumplimiento, no conformidades y oportunidades de mejora. El plan de auditoría debe estar aprobado por el Comité de Coordinación de Control Interno y considerar documentación de fases anteriores, incidentes, compromisos institucionales, indicadores y cambios del contexto, incluidos factores políticos, económicos, sociales, tecnológicos, ambientales y legales.

La alta dirección revisa periódicamente la conveniencia, adecuación y eficacia del sistema. Esta revisión debe producir un acta, decisiones y compromisos verificables, además de actualizar la política y el manual cuando cambien las necesidades, riesgos o requisitos aplicables.

Corrección y aprendizaje

Las no conformidades deben corregirse, mitigar sus efectos y analizarse para evitar recurrencia. Los hallazgos, auditorías, incidentes y resultados de desempeño alimentan un plan anual de mejora con acciones,

responsables, plazos y recursos. La mejora continua cierra el ciclo y vuelve a alimentar el diagnóstico de madurez.

Indicador de madurez real Una organización madura no es la que reporta cero incidentes, sino la que detecta, registra, contiene, aprende y reduce de manera demostrable la exposición y el impacto.

06 | RESUMEN EJECUTIVO

Arquitectura de controles ISO/IEC 27001:2022

El anexo organiza 93 controles en cuatro dominios complementarios.

El MSPI incorpora los controles del Anexo A de ISO/IEC 27001:2022 como catálogo de referencia para el tratamiento. Su adopción no es automática: cada control debe relacionarse con riesgos identificados, justificarse en la declaración de aplicabilidad y evaluarse de acuerdo con el contexto institucional.

Dominio	Controles	Cobertura ejecutiva
A.5 Organizacionales	37	Políticas, roles, amenazas, activos, acceso, proveedores, nube, incidentes, continuidad, cumplimiento y privacidad.
A.6 Personas	8	Antecedentes, obligaciones laborales, formación, disciplina, confidencialidad, trabajo remoto y reporte.
A.7 Físicos	14	Perímetros, accesos, instalaciones, ambiente, áreas seguras, equipos, medios, servicios y eliminación segura.

Dominio	Controles	Cobertura ejecutiva
A.8 Tecnológicos	34	Endpoints, privilegios, autenticación, malware, vulnerabilidades, configuración, DLP, respaldo, registros, redes, criptografía y desarrollo seguro.

Controles con mayor efecto transversal

Inteligencia de amenazas y vulnerabilidades. Mejora la anticipación y permite priorizar remediaciones según exposición real.

Seguridad en el uso de nube y proveedores. Extiende obligaciones y monitoreo fuera del perímetro institucional.

Preparación TIC para continuidad. Conecta disponibilidad tecnológica, respaldos, redundancia y recuperación con servicios esenciales.

Prevención de fuga y enmascaramiento. Reduce el riesgo de exposición de información confidencial y datos personales.

Registro y monitoreo. Sostiene la detección, la investigación, la atribución de acciones y la mejora basada en evidencia.

Desarrollo seguro. Integra seguridad desde requisitos, arquitectura, codificación, pruebas, cambios y separación de ambientes.

Privacidad por diseño

El catálogo vincula privacidad con clasificación de información, control de acceso, cifrado, enmascaramiento, anonimización, prevención de fuga, conservación y eliminación segura. La protección de datos personales debe incorporarse desde el diseño de procesos y sistemas, no añadirse después de su puesta en producción.

Ciberseguridad y continuidad

Los controles combinan prevención, detección, respuesta y recuperación. La protección contra malware, la gestión de vulnerabilidades, la segmentación de redes y la autenticación reducen la probabilidad; los registros, alertas y reporte temprano favorecen la detección; la gestión de incidentes, los respaldos y la redundancia limitan el impacto y aceleran la recuperación.

Regla de selección Cada control debe responder a un riesgo concreto, tener un propietario, contar con recursos, producir evidencia y disponer de una prueba de eficacia. Un control sin estas condiciones es difícil de gobernar y auditar.

07 | RESUMEN EJECUTIVO

Prioridades de implementación y conclusión

Ruta ejecutiva para convertir el lineamiento en capacidad institucional.

Prioridades recomendadas

Horizonte	Prioridades
0-90 días	Formalizar gobierno y responsable; ejecutar autodiagnóstico; validar alcance; identificar servicios esenciales y activos críticos; revisar riesgos urgentes e incidentes recientes.
3-6 meses	Actualizar inventarios y matriz de riesgos; aprobar política, metodología, declaración de aplicabilidad y plan de tratamiento; asegurar recursos; fortalecer vulnerabilidades, accesos, respaldo y monitoreo.
6-12 meses	Completar controles priorizados; probar respuesta a incidentes, restauración y continuidad; evaluar terceros; medir cultura; ejecutar auditoría interna y revisión por la dirección.
Ciclo anual	Actualizar diagnóstico, contexto, amenazas y riesgos; cerrar no conformidades; revisar aceptación de riesgos; ajustar indicadores, presupuesto y plan de mejora.

Factores críticos de éxito

- **Patrocinio visible.** La alta dirección debe resolver prioridades, riesgos y recursos, no limitarse a aprobar documentos.
- **Responsabilidad distribuida.** Los líderes de proceso son dueños de los riesgos; Seguridad coordina y Tecnología ejecuta parte de los controles.

Datos y pruebas confiables. Inventarios, riesgos e indicadores deben mantenerse actualizados; respaldos, respuesta a incidentes, continuidad y controles técnicos deben probarse en condiciones realistas.

Mejora financiada. Las brechas requieren responsables, fechas y presupuesto; de otro modo se convierten en riesgos aceptados de forma implícita.

Conclusión

El MSPI versión 5.0 ofrece una estructura coherente para gestionar seguridad y privacidad como parte del gobierno institucional. Su implementación efectiva exige pasar del cumplimiento documental a la capacidad demostrable: conocer qué es crítico, decidir qué riesgos se aceptan, operar controles sostenibles, responder a incidentes, recuperar servicios y aprender de los resultados. Integrado a la planeación y al presupuesto, el modelo fortalece la continuidad de los servicios públicos, la protección de los datos y la confianza digital.

Fuente

Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia. Documento Maestro de los Lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI), versión 5.0, 21 de abril de 2025. Documento fuente de 52 páginas.

Nota metodológica: *síntesis ejecutiva elaborada a partir del contenido íntegro del documento. Las prioridades temporales de la sección final constituyen una recomendación de implementación y no sustituyen los plazos o actos formales aplicables a cada entidad.*