Corporación Autónoma Regional de Santander

CAS

MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN - CAS

Contenido

1. Introducción 3
2. Alcance del Modelo 3
3. Marco Normativo y Estratégico 3
3.1. Normativa Nacional Aplicable 4
3.2. Normas y Estándares Internacionales 4
3.3. Lineamientos Estratégicos Institucionales 5
4. Principios Rectores del MSPI 5
4.1. Confidencialidad 6
4.2. Integridad 6
4.3. Disponibilidad 6
4.4. Legalidad 6
4.5. Responsabilidad Compartida 7
4.6. Prevención y mejora continua 7
5. Objetivos del Modelo 7
5.1. Objetivo General 7
5.2. Objetivos Específicos 7
Matriz de Vinculación entre Controles Institucionales y Procedimientos Operativos (SOPs) 8

1. Introducción

La seguridad de la información y la privacidad de los datos constituyen pilares fundamentales para la confianza digital en las entidades públicas. En un entorno tecnológico cada vez más interconectado, las amenazas cibernéticas, el tratamiento de datos personales y la gestión de riesgos digitales requieren un abordaje estratégico, normativo y organizacional.

En respuesta a esta necesidad, el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) establece el Modelo de Seguridad y Privacidad de la Información (MSPI), en el marco de la Estrategia de Gobierno Digital, como una herramienta de adopción obligatoria para todas las entidades del Estado colombiano.

La Corporación Autónoma Regional de Santander (CAS) adopta este modelo como marco rector para gestionar de forma segura sus activos de información, conforme con la Resolución 500 de 2021, actualizada por la Resolución 746 de 2022, y las buenas prácticas internacionales establecidas por la norma ISO/IEC 27001:2022.

2. Alcance del Modelo

El MSPI aplica a todos los activos de información de la CAS, independientemente de su forma, ubicación, propietario o medio de almacenamiento. Esto incluye datos físicos, digitales, personales, estratégicos, confidenciales, sistemas de información, infraestructuras, procesos y servicios institucionales, así como a los contratistas, proveedores y usuarios que interactúan con dicha información. El alcance es transversal a todas las áreas organizacionales.

3. Marco Normativo y Estratégico

La implementación del MSPI en la Corporación Autónoma Regional de Santander (CAS) se fundamenta en un sólido marco normativo y estratégico que garantiza la coherencia legal, la interoperabilidad institucional y la adopción de estándares internacionales en seguridad y privacidad de la información.

Este marco integra leyes nacionales, decretos reglamentarios, directrices ministeriales y normas internacionales, estableciendo los lineamientos para la gestión efectiva de riesgos, protección de datos personales, transparencia, uso seguro de tecnologías de la información y continuidad de la operación institucional.

3.1. Normativa Nacional Aplicable

Ley 1581 de 2012: Régimen General de Protección de Datos Personales. Establece los principios, derechos y deberes en el tratamiento de datos personales, obligando a la CAS a implementar medidas técnicas, humanas y administrativas que garanticen su seguridad.

Ley 1712 de 2014: Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional. Impulsa el acceso seguro, oportuno y veraz a la información pública que gestiona la entidad, respetando los criterios de confidencialidad.

Ley 1266 de 2008: Régimen de Habeas Data financiero, aplicable en los casos en que la entidad administre datos con fines crediticios o financieros.

Decreto 620 de 2020: Reglamenta el Modelo de Gobierno Digital, en el cual el MSPI se constituye como uno de sus componentes estratégicos. Exige a las entidades la adopción de medidas integrales para la gestión de la seguridad de la información.

Resolución 500 de 2021 y Resolución 746 de 2022 del MinTIC: Establecen los lineamientos técnicos y organizacionales que deben seguir las entidades públicas para la implementación del MSPI, con base en las buenas prácticas y normas internacionales.

3.2. Normas y Estándares Internacionales

ISO/IEC 27001:2022: Norma internacional para la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI). Define los requisitos para establecer, operar, mantener y mejorar de forma continua los controles de seguridad.

ISO/IEC 27002:2022: Código de buenas prácticas para la gestión de controles de seguridad, que complementa los controles definidos en la 27001.

ISO/IEC 27005:2018: Norma especializada en la gestión de riesgos de seguridad de la información. Proporciona un enfoque sistemático para la identificación, análisis, evaluación, tratamiento y monitoreo de riesgos.

ISO 31000:2018: Norma de gestión de riesgos a nivel organizacional, transversal a todos los procesos institucionales.

ITIL v4 (Information Technology Infrastructure Library): Buenas prácticas para la gestión de servicios de TI, útiles para estructurar los procesos operativos asociados a la seguridad y continuidad del servicio.

3.3. Lineamientos Estratégicos Institucionales

Política de Seguridad de la Información de la CAS: Documento institucional que define el compromiso de la alta dirección frente a la protección de los activos de información y la adopción de mecanismos de seguridad.

Plan Estratégico de Tecnologías de la Información (PETI): Marco institucional que orienta la inversión, modernización y alineación tecnológica, incluyendo componentes de seguridad.

Modelo Integrado de Planeación y Gestión (MIPG): Establece el enfoque de articulación de los planes, políticas, procesos y resultados institucionales, integrando la gestión del riesgo y el control interno.

Sistema Integrado de Gestión (SIG): Incluye los procesos de calidad, ambiental, seguridad y salud, articulados con la seguridad de la información como un componente transversal.

4. Principios Rectores del MSPI

El Modelo de Seguridad y Privacidad de la Información (MSPI) de la CAS se sustenta en un conjunto de principios que orientan la toma de decisiones, la

definición de **controles** y la cultura organizacional en torno a la gestión de riesgos digitales y protección de los activos de información.

Estos principios rectores están alineados con las buenas prácticas internacionales y buscan garantizar un entorno confiable, transparente, resiliente y conforme con la legislación vigente:

4.1. Confidencialidad

Garantizar que la información institucional solo sea accesible por personas, sistemas o procesos autorizados. Este principio implica el uso de controles de acceso, cifrado, mecanismos de autenticación y segmentación de responsabilidades, evitando la exposición no deseada de datos sensibles.

4.2. Integridad

Preservar la exactitud, consistencia y completitud de la información durante su ciclo de vida. Se previenen modificaciones no autorizadas, errores de procesamiento, pérdida o corrupción de datos mediante controles como registros de auditoría, validaciones lógicas, copias de seguridad y trazabilidad.

4.3. Disponibilidad

Asegurar que la información y los servicios estén accesibles de forma oportuna, confiable y continua para quienes lo requieren. Esto contempla la implementación de planes de continuidad, redundancia de infraestructura, tolerancia a fallos y monitoreo permanente.

4.4. Legalidad

Cumplir con las disposiciones legales y normativas vigentes en materia de protección de datos, acceso a la información pública, gobierno digital y seguridad informática. La legalidad se traduce en el diseño de políticas, procedimientos y controles que respeten los derechos de los titulares y las obligaciones institucionales.

4.5. Responsabilidad Compartida

Fomentar una cultura organizacional donde todos los actores —directivos, funcionarios, contratistas y usuarios— comprendan y asuman su papel en la protección de la información. La seguridad no es una función exclusiva del área TIC, sino un compromiso transversal en toda la entidad.

4.6. Prevención y mejora continua

Priorizar la identificación oportuna de riesgos, la gestión proactiva de vulnerabilidades y la retroalimentación institucional como base para mejorar los controles. Se promueve la revisión periódica de políticas, la actualización tecnológica y la formación continua.

5. Objetivos del Modelo

El Modelo de Seguridad y Privacidad de la Información (MSPI) de la CAS tiene como finalidad estructurar un enfoque sistémico, preventivo y adaptable para proteger la información institucional, reducir los riesgos digitales y garantizar el cumplimiento normativo. Su implementación permite fortalecer la confianza institucional y asegurar la resiliencia operativa ante incidentes de seguridad o fallas tecnológicas.

Los objetivos se dividen en generales y específicos, permitiendo su integración con la planeación estratégica, la gestión de riesgos, el control interno y el gobierno digital.

5.1. Objetivo General

Establecer un marco técnico, organizacional y normativo que permita a la CAS implementar, mantener y mejorar de forma continua las capacidades institucionales necesarias para proteger la seguridad y privacidad de la información, garantizando su confidencialidad, integridad, disponibilidad y cumplimiento legal.

5.2. Objetivos Específicos

- Implementar controles organizacionales, físicos, técnicos y jurídicos para salvaguardar los activos de información institucional.

- Fortalecer la cultura organizacional en materia de seguridad y privacidad mediante procesos de sensibilización, formación y apropiación digital.
- Identificar, valorar y tratar los riesgos que afecten la continuidad, integridad o legalidad de los procesos que dependen de la información.
- Establecer procedimientos normalizados (SOPs) para la gestión de incidentes, accesos, respaldos, clasificación de la información y tratamiento de datos personales.
- Promover el cumplimiento de los lineamientos del MinTIC y las normas ISO/IEC 27001, 27002 y 27005, como marco de referencia del modelo.
- Integrar la gestión de seguridad con el Sistema Integrado de Gestión (SIG), el MIPG y el Plan Estratégico de Tecnologías de la Información (PETI).

Matriz de Vinculación entre Controles Institucionales y Procedimientos Operativos (SOPs)

Objetivo del Anexo

Establecer la relación entre los **controles institucionales definidos en el Modelo de Seguridad y Privacidad de la Información (MSPI)** y los **Procedimientos Operativos Estandarizados (SOPs)** que garantizan su aplicación práctica dentro de la Corporación Autónoma Regional de Santander – CAS.
Esta vinculación permite demostrar la trazabilidad entre las políticas, los riesgos identificados y las acciones operativas que soportan la gestión de seguridad de la información.

Alcance

La matriz aplica a todos los procesos, áreas y dependencias que intervienen en la implementación del MSPI, abarcando tanto los controles técnicos como los organizacionales y legales.
Cada control se asocia con uno o varios SOPs que describen las actividades operativas, los responsables, las evidencias requeridas y la frecuencia de ejecución o revisión.

Lineamientos Normativos

La matriz se fundamenta en los siguientes referentes:

- **Norma ISO/IEC 27001:2022** – Controles aplicables al Sistema de Gestión de Seguridad de la Información (SGSI).
- **Estrategia de Gobierno Digital del MinTIC** – Lineamientos para la implementación del MSPI en entidades públicas.
- **Política Institucional de Seguridad de la Información de la CAS.**

Responsabilidades

El **Responsable de Seguridad de la Información (RSI)** y el **Comité de Seguridad de la Información** deberán garantizar:

- La actualización anual de la matriz.
- La verificación de cumplimiento de los SOPs asociados.
- La conservación de las evidencias que respalden la aplicación de los controles.
- La integración de los resultados en los informes de gestión del MSPI.

Componente MSPI	Actividad MSPI	SOP Primario	Tarea Operativa	Responsable	Evidencia Esperada	Frecuencia
Actividades de Gobierno y Planeación del MSPI	**Definir y actualizar el alcance del MSPI.**					
	Aprobar y socializar la política de seguridad y privacidad de la información.					
	Asignar roles y responsabilidades del MSPI.					
	Realizar revisión periódica del modelo.					
	Asegurar alineación con lineamientos MinTIC e ISO/IEC 27001.					
Gestión de Activos de Información	**Identificar y actualizar el inventario de activos de información.**	**SOP-07 Clasificación de Información**	Actualizar el inventario de activos de la información	TIC	Invetario de activos publicado	
Gestión de Riesgos de Seguridad de la Información	**Elaborar y mantener la matriz de riesgos.**	**SOP-11 Gestión de Riesgos**	Actualziar la Matriz de Riesgos de Seguridad de la Información	TIC	Matriz de riesgos actualizada	
Implementación de Controles de Seguridad	**Implementar controles organizacionales, técnicos y físicos.**					
	Gestionar controles de acceso a la información.	**SOP-01 Control de Accesos**	Crear usuario	TIC	Registro de usuarios	Permanente
			Modificar permisos	TIC	Bitácora de cambios	Permanente
			Revocar accesos	TIC	Registro de bajas	Permanente
	Aplicar controles de seguridad en sistemas de información.		Implementar Controladora de Dominio	TIC	Aplicación con seguridad	Anual
	Asegurar respaldo y recuperación de la información.	**SOP-02 Respaldos**	Ejecutar backup	TIC	Logs de backup	Mensual

			Verificar integridad	TIC	Informe verificación	Mensual
			Prueba de restauración	TIC	Informe prueba	Trimestral
	Gestionar cambios en los sistemas.	**SOP-05 Control de Cambios**	Impllmentar Formato *F-PGT-008 Control de cambios al software*	TIC	Implementación en producción y actualización de la documentación.	Ocurrencia
Gestión de Incidentes de Seguridad	**Detectar y reportar incidentes de seguridad.**	**SOP-03 Incidentes**	Identificación y registro de eventos anómalos o incidentes	Usuarios	Tickets de mesa de ayuda	Ocurrencia
			Notificación formal al canal definido (mesa de ayuda, correo, formato)	Usuarios		Ocurrencia
	Clasificar y analizar incidentes.	**SOP-03 Incidentes**	Clasificar el incidente (confidencialidad, integridad, disponibilidad)	TIC	Registro de clasificación del incidente	Ocurrencia
			Evaluar impacto y criticidad	TIC	Informe de análisis	Ocurrencia
			Analizar causa raíz	TIC	Matriz o tabla de severidad	Ocurrencia
	Atender y mitigar incidentes.	**SOP-03 Incidentes**	Ejecutar acciones de contención	TIC	Registro de acciones de mitigación	Ocurrencia
			Aplicar medidas correctivas	TIC		Ocurrencia
			Restaurar servicios afectados	TIC	Bitácoras técnicas	Ocurrencia

			Escalar si aplica	TIC	Reportes de recuperación del servicio	Ocurrencia
	Documentar incidentes y lecciones aprendidas.	**SOP-03 Incidentes**	Documentar el cierre del incidente	TIC	Acta o formato de cierre	Ocurrencia
			Proponer acciones de mejora	TIC	Plan de mejora asociado	Ocurrencia
	Generar reportes de incidentes.	**SOP-03 Incidentes**	Consolidación y análisis periódico de incidentes	TIC	Informes de incidentes	Ocurrencia
Continuidad del Negocio y Respaldo	**Definir planes de continuidad y recuperación.**	**SOP-08 Continuidad**	Actualizar Plan de Contingencia	TIC	documento publicado en intranet y socializado	
	Realizar pruebas de continuidad.	**SOP-08 Continuidad**	Realizar purebas de recuoperacion de backups	TIC	documentacion de pruebas realizadas	
	Mantener respaldos de información.	**SOP-02 Respaldos**	Ejecutar backup	TIC	Logs de backup	Mensual
			Verificar integridad	TIC	Informe verificación	Mensual
			Prueba de restauración	TIC	Informe prueba	Trimestral
Concienciación y Capacitación	**Diseñar el plan de sensibilización.**	**SOP-10 Capacitación**	Formular cronograma de capacitacion es seguridad de la informacion	TIC	Listado de asistencia	
Cumplimiento y Mejora Continua	**Realizar auditorías internas del MSPI.**	**SOP-09 Auditoría**	Realizar auditoría interna	Control Interno y/o SGI	Informe auditoría	Anual
	Gestionar acciones correctivas y preventivas.		Proponer acciones de mejora	TIC	Plan de mejora asociado	
	Actualizar los instrumentos de planeación del Modelo de		Revisión de políticas,	TIC	Manual de Políticas de	

Actualización de los instrumentos de planeación del MSPI	**Seguridad y Privacidad de la Información (MSPI)**		lineamientos y procedimientos vigentes		Seguridad de la Información actualizado	
			Identificación de brechas entre el MSPI y los SOP implementados	TIC	Instrumentos de planeación del MSPI ajustados	
			Actualizacion del MSPI	TIC		