CURADURIA URBANA PRIMERA DE SINCELEJO

Sucre - Colombia

PLAN DE IMPLEMENTACION DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

(MSPI)

VIGENCIA 2025

Basado en la Guia del Modelo de Seguridad y Privacidad de la Informacion
Ministerio de Tecnologias de la Informacion y las Comunicaciones

Resolucion MinTIC 1519 de 2020 - Seccion 15

www.curaduriaprimerasincelejo.com.co

Sincelejo, Enero 2025

CONTROL DE VERSIONES

VERSION	FECHA	DESCRIPCION	ELABORADO POR
1.0	[DD/MM/2025]	Version inicial del Plan de Implementacion MSPI	[Responsable de Seguridad]

TABLA DE CONTENIDO

1. INTRODUCCION

El presente documento establece el Plan de Implementacion del Modelo de Seguridad y Privacidad de la Informacion (MSPI) para la CURADURIA URBANA PRIMERA DE SINCELEJO, en cumplimiento de los lineamientos establecidos por el Ministerio de Tecnologias de la Informacion y las Comunicaciones (MinTIC) y la Resolucion 1519 de 2020.

El MSPI es un marco de referencia que permite a las entidades establecer, implementar, mantener y mejorar continuamente un Sistema de Gestion de Seguridad de la Informacion (SGSI), basado en la norma ISO/IEC 27001 y adaptado al contexto colombiano.

Este plan define las fases, actividades, responsables, recursos y cronograma necesarios para implementar el MSPI en la Curaduria, considerando su naturaleza como particular que ejerce funcion publica y sus obligaciones de transparencia.

2. OBJETIVO DEL PLAN

2.1 Objetivo General

Implementar el Modelo de Seguridad y Privacidad de la Informacion (MSPI) en la Curaduria Urbana Primera de Sincelejo, estableciendo los controles necesarios para proteger la confidencialidad, integridad y disponibilidad de los activos de informacion.

2.2 Objetivos Especificos

1. Realizar el diagnostico del estado actual de seguridad de la informacion.
2. Identificar y valorar los activos de informacion y sus riesgos asociados.
3. Definir e implementar los controles de seguridad apropiados.
4. Establecer los procedimientos de gestion de incidentes de seguridad.
5. Desarrollar capacidades de continuidad del negocio.
6. Crear una cultura de seguridad de la informacion en la organizacion.
7. Cumplir con los requisitos de la Resolucion MinTIC 1519 de 2020.

3. ALCANCE

El Plan de Implementacion del MSPI aplica a:

- Todos los procesos de la Curaduria relacionados con la gestion de licencias urbanisticas.
- Los sistemas de informacion utilizados: sitio web, sistema de gestion documental, correo electronico.
- La infraestructura tecnologica: servidores, equipos de computo, redes.
- Las instalaciones fisicas de la sede de la Curaduria.
- Todo el personal: funcionarios, contratistas y terceros con acceso a informacion.

4. MARCO DE REFERENCIA MSPI

El Modelo de Seguridad y Privacidad de la Informacion (MSPI) del MinTIC se estructura en cinco (5) fases basadas en el ciclo PHVA (Planear, Hacer, Verificar, Actuar):

FASE	NOMBRE	DESCRIPCION
FASE 1	**DIAGNOSTICO**	Evaluacion del estado actual de seguridad de la informacion mediante el uso de herramientas de autodiagnostico.
FASE 2	**PLANIFICACION**	Definicion del alcance, politica de seguridad, metodologia de gestion de riesgos y plan de tratamiento.
FASE 3	**IMPLEMENTACION**	Ejecucion del plan de tratamiento de riesgos, implementacion de controles y capacitacion del personal.
FASE 4	**EVALUACION DE DESEMPENO**	Monitoreo, medicion, analisis, evaluacion y auditoria interna del SGSI.
FASE 5	**MEJORA CONTINUA**	Tratamiento de no conformidades, acciones correctivas y mejora continua del sistema.

5. DIAGNOSTICO INICIAL

5.1 Estado Actual

Segun el resultado de la Auditoria ITA 0998 de la Procuraduria General de la Nacion, la Curaduria obtuvo en la seccion de Seguridad Digital (Anexo 3, Seccion 15):

CRITERIO	ESTADO	OBSERVACION
15.1.a - Politica de Seguridad Digital publicada	**NO CUMPLE**	No existe documento publicado
15.1.b - Evidencia de implementacion MSPI	**NO CUMPLE**	No hay evidencia de implementacion
Puntaje Seccion Seguridad Digital	**33.3/100**	Nivel: ALTO (requiere accion)

5.2 Brechas Identificadas

- No existe una Politica de Seguridad de la Informacion formalizada y publicada.
- No se ha realizado inventario y clasificacion de activos de informacion.
- No existe analisis de riesgos de seguridad de la informacion.
- No hay procedimientos documentados de gestion de incidentes.
- No se ha implementado un plan de continuidad del negocio.
- No se realizan capacitaciones en seguridad de la informacion.
- No hay auditorias internas de seguridad.

6. FASES DEL PLAN DE IMPLEMENTACION

6.1 FASE 1: DIAGNOSTICO

Duracion estimada: 4 semanas

#	ACTIVIDAD	ENTREGABLE	RESPONSABLE
1.1	Aplicar herramienta de autodiagnostico MSPI del MinTIC	Informe de autodiagnostico	Resp. Seguridad
1.2	Identificar y documentar los activos de informacion	Inventario de activos	Todas las areas
1.3	Clasificar los activos segun su criticidad	Matriz de clasificacion	Resp. Seguridad
1.4	Identificar vulnerabilidades y amenazas	Informe de vulnerabilidades	Resp. Seguridad
1.5	Elaborar informe de diagnostico consolidado	Informe de diagnostico	Resp. Seguridad

6.2 FASE 2: PLANIFICACION

Duracion estimada: 6 semanas

#	ACTIVIDAD	ENTREGABLE	RESPONSABLE
2.1	Definir el alcance del SGSI	Documento de alcance	Curador Urbano
2.2	Elaborar y aprobar la Politica de Seguridad	Politica de Seguridad	Curador Urbano
2.3	Definir metodologia de gestion de riesgos	Metodologia de riesgos	Resp. Seguridad
2.4	Realizar analisis y valoracion de riesgos	Matriz de riesgos	Resp. Seguridad
2.5	Elaborar plan de tratamiento de riesgos	Plan de tratamiento	Resp. Seguridad
2.6	Elaborar Declaracion de Aplicabilidad (SOA)	SOA	Resp. Seguridad

6.3 FASE 3: IMPLEMENTACION

Duracion estimada: 12 semanas

#	ACTIVIDAD	ENTREGABLE	RESPONSABLE
3.1	Implementar controles de acceso logico	Procedimiento de control de acceso	Area Administrativa
3.2	Implementar controles de seguridad fisica	Procedimiento de seguridad fisica	Area Administrativa
3.3	Implementar politica de respaldo de informacion	Procedimiento de backup	Resp. Seguridad
3.4	Implementar controles de seguridad en el sitio web	Informe de hardening web	Webmaster
3.5	Elaborar procedimiento de gestion de incidentes	Procedimiento de incidentes	Resp. Seguridad
3.6	Elaborar Plan de Continuidad del Negocio	Plan de Continuidad (BCP)	Curador Urbano
3.7	Realizar capacitacion al personal	Registros de capacitacion	Resp. Seguridad
3.8	Publicar documentos en el sitio web	URLs de publicacion	Webmaster

6.4 FASE 4: EVALUACION DE DESEMPENO

Duracion estimada: 4 semanas

#	ACTIVIDAD	ENTREGABLE	RESPONSABLE
4.1	Definir indicadores de gestion de seguridad	Tablero de indicadores	Resp. Seguridad
4.2	Realizar monitoreo de controles implementados	Informe de monitoreo	Resp. Seguridad
4.3	Realizar auditoria interna del SGSI	Informe de auditoria	Auditor interno
4.4	Revision por la direccion	Acta de revision	Curador Urbano

6.5 FASE 5: MEJORA CONTINUA

Duracion: Permanente

#	ACTIVIDAD	ENTREGABLE	RESPONSABLE
5.1	Gestionar no conformidades identificadas	Registro de no conformidades	Resp. Seguridad
5.2	Implementar acciones correctivas	Plan de acciones correctivas	Todas las areas
5.3	Actualizar documentacion del SGSI	Documentos actualizados	Resp. Seguridad
5.4	Aplicar nuevamente autodiagnostico MSPI	Informe de autodiagnostico	Resp. Seguridad

7. CRONOGRAMA DE IMPLEMENTACION

El siguiente cronograma presenta la distribucion de las fases a lo largo del ano 2025:

FASE	E	F	M	A	M	J	J	A	S	O	N	D
1. Diagnostico	X											
2. Planificacion		X	X									
3. Implementacion				X	X	X	X	X	X			
4. Evaluacion										X	X	
5. Mejora Continua												X

8. RECURSOS REQUERIDOS

8.1 Recursos Humanos

ROL	DEDICACION	RESPONSABILIDADES
Responsable de Seguridad	Parcial (50%)	Coordinacion general del proyecto
Curador Urbano	Segun requerimiento	Aprobacion de politicas y recursos
Webmaster / Soporte TI	Parcial (30%)	Implementacion de controles tecnicos
Personal de todas las areas	Segun capacitaciones	Participacion en capacitaciones

8.2 Recursos Tecnologicos

- Software antivirus/antimalware con licencia vigente.
- Sistema de backup (local y en la nube).
- Certificado SSL/TLS para el sitio web.
- UPS para equipos criticos.
- Herramientas de analisis de vulnerabilidades.

8.3 Presupuesto Estimado

CONCEPTO	VALOR	OBSERVACION
Capacitacion del personal (horas)	$2.000.000	Interno/Externo
Licencias de software de seguridad	$1.500.000	Anual
Certificado SSL/TLS	$300.000	Anual
Servicio de backup en la nube	$600.000	Anual
Auditoria externa (opcional)	$3.000.000	Una vez
TOTAL ESTIMADO	**$7.400.000**	

9. INDICADORES DE SEGUIMIENTO

INDICADOR	FORMULA	META	FRECUENCIA
Avance del plan de implementacion	(Actividades ejecutadas / Total actividades) x 100	>= 90%	Mensual
Cobertura de capacitacion	(Personal capacitado / Total personal) x 100	100%	Semestral
Incidentes de seguridad	Numero de incidentes en el periodo	<= 2	Trimestral
Tiempo respuesta a incidentes	Promedio de horas para contener incidentes	<= 4 horas	Por evento
Cumplimiento de backups	(Backups exitosos / Backups programados) x 100	100%	Mensual
Puntaje autodiagnostico MSPI	Resultado herramienta MinTIC	>= 80%	Anual
Hallazgos de auditoria cerrados	(Hallazgos cerrados / Total hallazgos) x 100	>= 90%	Semestral

10. RIESGOS DEL PROYECTO

RIESGO	PROBABILIDAD	MITIGACION
Falta de compromiso de la direccion	Media	Presentar beneficios y obligaciones legales. Incluir en objetivos institucionales.
Recursos insuficientes	Media	Priorizar actividades criticas. Buscar alternativas de bajo costo.
Resistencia al cambio del personal	Alta	Capacitacion continua. Comunicacion de beneficios. Apoyo de la direccion.
Falta de personal especializado	Media	Capacitar personal interno. Contratar asesoria externa puntual.
Cambios en la normatividad	Baja	Monitoreo constante de actualizaciones normativas. Flexibilidad en el plan.
Incidentes de seguridad durante implementacion	Media	Implementar controles basicos desde el inicio. Tener plan de respuesta.

11. APROBACION Y COMPROMISO

El suscrito, en mi calidad de Curador Urbano Primero de Sincelejo, APRUEBO el presente Plan de Implementacion del Modelo de Seguridad y Privacidad de la Informacion (MSPI) y me comprometo a:

8. Asignar los recursos humanos, tecnicos y financieros necesarios para su ejecucion.
9. Liderar la implementacion del MSPI como prioridad institucional.
10. Realizar seguimiento periodico al avance del plan.
11. Promover una cultura de seguridad de la informacion en la organizacion.
12. Aprobar las politicas y procedimientos de seguridad que se desarrollen.
13. Participar en la revision por la direccion del SGSI.

Para constancia se firma en la ciudad de Sincelejo, a los _____ dias del mes de _____ de 2025.

[NOMBRE DEL CURADOR URBANO]	**[NOMBRE RESPONSABLE SEGURIDAD]**
Curador Urbano Primero de Sincelejo	Responsable de Seguridad de la Informacion
APROBO	**ELABORO**

URL de Publicacion: https://curaduriaprimerasincelejo.com.co/transparencia/seguridad-digital/mspi