CURADURÍA URBANA PRIMERA DE SINCELEJO

Sucre - Colombia

PLAN DE CAPACITACIÓN Y SENSIBILIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN

VIGENCIA 2025

Creando una cultura de seguridad de la información
en cumplimiento del MSPI - MinTIC

www.curaduriaprimerasincelejo.com.co

CONTROL DE VERSIONES

VERSIÓN	FECHA	DESCRIPCIÓN	ELABORADO POR
1.0	[DD/MM/2025]	Versión inicial del Plan de Capacitación	[Responsable]

TABLA DE CONTENIDO

1. INTRODUCCIÓN Y OBJETIVOS

El factor humano es el eslabón más importante en la cadena de seguridad de la información. Este Plan de Capacitación establece las actividades necesarias para crear y fortalecer una cultura de seguridad en la Curaduría Urbana Primera de Sincelejo, en cumplimiento del MSPI del MinTIC.

1.1 Objetivos

1. Capacitar al 100% del personal en conceptos básicos de seguridad de la información.
2. Sensibilizar sobre amenazas comunes (phishing, malware, ingeniería social).
3. Dar a conocer las políticas y procedimientos de seguridad de la entidad.
4. Entrenar en la identificación y reporte de incidentes de seguridad.
5. Promover buenas prácticas en el manejo de información y uso de tecnología.

2. ALCANCE Y PÚBLICO OBJETIVO

Las capacitaciones aplican a todo el personal (funcionarios, contratistas, terceros) y se estructuran por niveles según el rol y responsabilidades:

NIVEL	PÚBLICO	ENFOQUE DE CAPACITACIÓN
NIVEL 1 - Básico	Todo el personal	Conceptos básicos, política de seguridad, amenazas comunes, buenas prácticas
NIVEL 2 - Intermedio	Personal con acceso a info. clasificada	Clasificación de información, protección de datos personales
NIVEL 3 - Avanzado	Resp. Seguridad, Líder Técnico	Gestión de incidentes, análisis de riesgos, controles técnicos
NIVEL 4 - Directivo	Curador Urbano, Coordinadores	Gobierno de seguridad, cumplimiento normativo

3. TEMÁTICAS DEL PROGRAMA

MÓD	TEMA	DURACIÓN	NIVEL	CONTENIDOS PRINCIPALES
1	Fundamentos de Seguridad de la Información	2 horas	Básico	CIA, importancia en entidades públicas, marco normativo, política de seguridad, responsabilidades
2	Amenazas y Ataques Cibernéticos	2 horas	Básico	Tipos de malware, phishing, ingeniería social, casos reales, taller identificación correos maliciosos
3	Buenas Prácticas de Seguridad	2 horas	Básico	Contraseñas seguras, uso correo electrónico, navegación segura, USB, dispositivos móviles, escritorio limpio
4	Protección de Datos Personales	2 horas	Intermedio	Ley 1581/2012, principios tratamiento, derechos ARCO, política de tratamiento, sanciones
5	Gestión de Incidentes de Seguridad	2 horas	Básico-Int	Qué es un incidente, cómo identificarlo, procedimiento de reporte, preservación de evidencia
6	Clasificación de Información	1.5 horas	Intermedio	Ley 1712/2014, clasificación (Pública, Clasificada, Reservada), manejo expedientes, destrucción segura

Total horas de formación: 11.5 horas por persona (Nivel Básico-Intermedio)

4. CRONOGRAMA DE ACTIVIDADES 2025

ACTIVIDAD	PÚBLICO	MODALIDAD	Q1	Q2	Q3	Q4	RESPONSABLE
Módulo 1: Fundamentos	Todos	Presencial	**X**				Resp. Seguridad
Módulo 2: Amenazas	Todos	Presencial	**X**				Resp. Seguridad
Módulo 3: Buenas Prácticas	Todos	Presencial		**X**			Resp. Seguridad
Módulo 4: Protección Datos	Nivel 2-3	Virtual		**X**			Resp. Seguridad
Módulo 5: Gestión Incidentes	Todos	Presencial			**X**		Resp. Seguridad
Módulo 6: Clasificación Info	Nivel 2-3	Virtual			**X**		Resp. Seguridad
Simulacro de phishing	Todos	Virtual		**X**		**X**	Líder Técnico
Campaña sensibilización (tips)	Todos	Correo	**X**	**X**	**X**	**X**	Resp. Seguridad
Evaluación de conocimientos	Todos	Virtual				**X**	Resp. Seguridad
Inducción nuevo personal	Nuevos	Presencial	→	→	→	→	Área Admin.

Leyenda: Q1=Ene-Mar, Q2=Abr-Jun, Q3=Jul-Sep, Q4=Oct-Dic, →=Según necesidad

5. METODOLOGÍA Y RECURSOS

5.1 Modalidades

MODALIDAD	DESCRIPCIÓN	HERRAMIENTAS
Presencial	Sesiones en instalaciones de la Curaduría	Presentaciones, material impreso
Virtual sincrónica	Sesiones en vivo por videoconferencia	Google Meet, Teams, Zoom
Virtual asincrónica	Cursos y contenidos para consulta	Videos, e-learning, cursos SENA/MinTIC
Simulacros	Ejercicios prácticos para medir respuesta	Simulación de phishing

5.2 Presupuesto Estimado

CONCEPTO	VALOR	FUENTE
Material didáctico (impresiones, folletos)	$200.000	Interno
Refrigerios para sesiones presenciales	$300.000	Interno
Capacitador externo especializado (opcional)	$1.500.000	Externo
TOTAL ESTIMADO	**$2.000.000**	

6. EVALUACIÓN E INDICADORES

6.1 Mecanismos de Evaluación

- Evaluación pre-capacitación: Prueba diagnóstica al inicio del programa.
- Evaluación post-capacitación: Prueba al finalizar cada módulo.
- Simulacro de phishing: Envío de correos simulados (semestral).
- Encuesta de satisfacción: Valoración después de cada sesión.

6.2 Criterios de Aprobación

- Asistencia mínima del 80% a las sesiones programadas.
- Calificación mínima de 70/100 en evaluaciones de conocimiento.

6.3 Indicadores de Gestión

INDICADOR	FÓRMULA / MEDICIÓN	META
Cobertura de capacitación	(Personal capacitado / Total personal) × 100	100%
Cumplimiento del plan	(Actividades ejecutadas / Programadas) × 100	≥ 90%
Promedio de calificaciones	Suma calificaciones / Número de evaluados	≥ 80/100
Tasa de aprobación	(Aprobados / Total evaluados) × 100	≥ 95%
Resistencia a phishing	(No cayeron en simulacro / Total) × 100	≥ 85%
Satisfacción promedio	Promedio encuestas de satisfacción	≥ 4.0/5.0

ANEXO A - FORMATO DE ASISTENCIA A CAPACITACIÓN

INFORMACIÓN DE LA CAPACITACIÓN	
Tema:	
Fecha:	Hora inicio: Hora fin:
Modalidad:	☐ Presencial ☐ Virtual
Capacitador:	

REGISTRO DE ASISTENTES				
No.	**NOMBRE COMPLETO**	**CARGO**	**CÉDULA**	**FIRMA**
1				
2				
3				
4				
5				
6				
7				
8				

URL de Publicación: https://curaduriaprimerasincelejo.com.co/transparencia/seguridad-digital/plan-capacitacion