PLAN DE COMUNICACIÓN Y SENSIBLIZACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (SGSI)

(Antiguo Plan de cambio y cultura del MSPI)

2026-2027

REGIÓN ADMINISTRATIVA Y DE PLANEACIÓN ESPECIAL
RAP-E REGION CENTRAL

DIRECCIÓN ADMINISTRATIVA Y FINANCIERA

Proceso Gestión TIC

2026

BOGOTÁ BOYACÁ CUNDINAMARCA META TOLIMA HUILA

REGIÓN CENTRAL
RAP-E | Estamos Construyendo Región

Contenido

INTRODUCCIÓN 3

GLOSARIO 4

OBJETIVO GENERAL 6

Objetivos específicos (ver el documento maestro MSPI 7.4.2) 6

ALCANCE 6

ROLES Y NECESIDADES 6

DISEÑO DEL PLAN DE CAPACITACIÓN Y SENSIBILIZACIÓN 9

IMPLEMENTACIÓN DEL PLAN DE CAPACITACIÓN Y SENSIBILIZACIÓN 9

CRONOGRAMA 9

MEJORA CONTINUA 11

Indicadores de seguimiento 11

CONTROL DE CAMBIOS 12

INTRODUCCIÓN

La implementación de un Sistema de Gestión de Seguridad y Privacidad de la Información - SGSI basado en Modelo de Seguridad y Privacidad de la Información – MSPI de MinTIC, en la Región Administrativa y de Planeación Especial - RAP-E Región Central, requiere no solo la adopción de políticas, procedimientos y controles técnicos, sino también la consolidación de una cultura y apropiación institucional orientada a garantizar la confidencialidad, integridad, disponibilidad, privacidad y no repudio de la información de la entidad, además de la gestión responsable de los riesgos inherentes que trae consigo la información.

Es importante mencionar que el factor humano juega un papel fundamental en la seguridad de la información, ya que, siempre se ha identificado como una variable volátil en términos de exposición de los activos de información a diversos riesgos, por lo que la falta de formación del talento humano puede dar lugar a errores y en ocasiones provocar estrés personal o profesional adicional, generando situaciones que pueden derivar en graves problemas tanto para el individuo como para la Entidad.

En este sentido, la comunicación efectiva, la capacitación, la sensibilización periódica, y la apropiación institucional como elementos fundamentales para el establecimiento del SGSI en la cultura institucional constituyen factores críticos de éxito con el propósito de garantizar la continuidad de las operaciones y el cumplimiento del modelo y la sostenibilidad del Sistema de Gestión de Seguridad de la Información - SGSI.

El presente plan de comunicación, capacitación, sensibilización, concientización y cultura establece las estrategias, actividades, responsabilidades e indicadores necesarios para promover comportamientos seguros, fortalecer las competencias de los servidores públicos, contratistas y terceros, y asegurar que los lineamientos del SGSI sean comprendidos, adoptados y aplicados de manera transversal en todos los procesos de la RAP-E.

Este plan no solo se enfoca en actividades en pro de mejorar las habilidades técnicas y profesionales de los funcionarios y contratistas de la Entidad, sino que también está orientado a fomentar una cultura organizacional sólida que valore la adaptación, la innovación y el cumplimiento de las normativas vigentes. Al proporcionar un marco estructurado para la formación continua, el plan busca fortalecer el desempeño individual y colectivo, promover la integración de nuevas estrategias y procesos, y asegurar una alineación efectiva con los objetivos estratégicos institucionales.

Este documento resalta la relevancia de potenciar la conciencia y el entendimiento de los funcionarios, contratistas y terceros de la RAP-E Región Central respecto a la Política de Seguridad y Privacidad de la Información de la Entidad. El propósito es capacitar a todo el talento humano con el fin de que adquieran capacidades que permitan enfrentar adecuadamente las amenazas, o incidentes que pongan en riesgo la seguridad de la información institucional.

Nota: A lo largo del documento se menciona indistintamente los términos, seguridad digital, seguridad de la información y seguridad, refiriéndose al mismo concepto, igualmente, continuidad del negocio y continuidad de la operación de los servicios TIC.

GLOSARIO

Activo de información: se refiere a cualquier información o elemento relacionado con el tratamiento de seguridad de la información (sistemas, soportes, instalaciones, personas, etc.) que tenga valor para la organización.

Amenazas: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27001:2022).

Amenaza cibernética: aparición de una situación potencial o actual donde un agente tiene la capacidad de generar una agresión cibernética contra la población, el territorio y la organización política del Estado.

Análisis de Riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de dicho riesgo. (ISO/IEC 27001:2022).

Autorización: Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3).

CGDI: Comité de Gestión y Desempeño Institucional.

Confidencialidad: Propiedad de la información que pretende garantizar que la misma sólo sea accedida por personas o sistemas autorizados.

Ciberseguridad: Protección de activos de información, mediante el tratamiento de las amenazas que ponen en riesgo la información que se procesa, almacena y transporta mediante los sistemas de información que se encuentran interconectados.

Continuidad de negocio: Conjunto de actividades o procedimientos que facilitarán mantener el normal funcionamiento de la misionalidad de la entidad y la prestación de sus servicios.

Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

CSIRT Gobierno: Equipo de Respuesta a Incidentes de Seguridad en sus siglas en inglés (*Computer Security Incident & Response Team*), integrado por un grupo de personas técnicas especializadas, que implementan y desarrollan medidas tendientes a prevenir y gestionar incidentes de ciberseguridad de las entidades del estado.

Dato: Es una representación simbólica (numérica, alfabética, espacial, etc.) de un atributo o variable cuantitativa o cualitativa.

Disponibilidad: Propiedad de la información que pretende garantizar el acceso y uso de la información y los sistemas de tratamiento de esta por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

Información: Conjunto organizado de datos procesados que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje.

Integridad: Propiedad de la información que pretende mantener con exactitud la información tal cual fue generada, sin ser manipulada ni alterada por personas o procesos no autorizados.

MinTIC: Ministerio de Tecnologías de la Información y las Comunicaciones.

MSPI: Modelo de Seguridad y Privacidad de la Información.

No repudio: El emisor no puede negar que envió porque el destinatario tiene pruebas del envío. El receptor recibe una prueba infalsificable del origen del envío, lo cual evita que el emisor pueda negar tal envío.

Plan de continuidad del negocio: Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27001:2022).

RAP-E: Región Administrativa y de Planeación Especial - Región Central.

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27001:2022).

Seguridad de la información: Preservación de la confidencialidad, integridad, y disponibilidad de la información en cualquier medio: impreso o digital. (ISO/IEC 27001:2022).

SGSI: Sistema de Gestión de Seguridad de la Información.

Seguridad digital: Es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta y, especialmente, la información contenida o circulante, incluye la seguridad de la información (Políticas, Procedimientos y demás controles) y la seguridad informática (Herramientas de seguridad).

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27001:2022).

Virus informático / *malware* / software malicioso: Programa informático que está diseñado para realizar acciones maliciosas sobre un activo informático como copiarse a sí mismo, cifrar información, recolectar y filtrar información, entre otros, sin el consentimiento del propietario

OBJETIVO GENERAL

Definir la estrategia de comunicación, capacitación, sensibilización y concientización de la Seguridad y Privacidad de la información en todos los funcionarios de la RAP-E Región Central, para asegurar el conocimiento y la cultura sobre la política de seguridad y privacidad de la información, las buenas prácticas, los roles y las consecuencias derivadas de no aplicar las normas de seguridad y privacidad.

Objetivos específicos (ver el documento maestro MSPI 7.4.2)

1. Asegurar que el 100% de los funcionarios, contratista y terceros cuenten con los conocimientos, educación y formación o experiencia adecuada para la implementación y gestión del modelo de seguridad y privacidad de la información.
2. Tener un enfoque práctico en la respuesta a incidentes de seguridad, fortalecer la capacidad de respuesta ante ataques dirigidos y tomar las acciones para adquirir y/o fortalecer la competencia de los responsables del SGSI.
3. Concientizar una cultura institucional sobre la importancia de las buenas prácticas de seguridad en torno al manejo adecuado, seguro y responsable de los Activos de información y de los recursos tecnológicos disponibles.

ALCANCE

El presente plan de sensibilización y comunicación de seguridad de la información está dirigido y aplica para todos los funcionarios, contratistas, colaboradores y terceros de la Región Administrativa y de Planeación Especial - Región Central. Este plan cubre todos los procesos, activos de información y servicios tecnológicos institucionales.

ROLES Y NECESIDADES

La seguridad y privacidad de la información de la RAP-E Región Central es una responsabilidad compartida, entre todos, donde cada dependencia, desde su rol, contribuye activamente a la apropiación del SGSI a través del presente Plan de comunicaciones y sensibilización; para estos efectos se establecieron los roles de usuarios en la Entidad y por cada uno de ellos las responsabilidades respectivas, las cuales se presentan en la tabla 1:

Tabla 1. Roles y responsabilidades institucionales

Roles	*Responsabilidades*
Alta dirección: Junta directiva, Gerente y jefes de áreas.	*Debe conocer, entender y aplicar la reglamentación del orden nacional y territorial, que fundamenten el SGSI de la RAP-E, así mismo debe comprometerse y apoyar el cumplimiento de las políticas de seguridad y*

	privacidad de la información y sus anexos, guías, planes o complementos. Además, es crucial que comprendan la importancia de su rol en liderazgo, ya que su ejemplo guiará las acciones del personal a su cargo.
Comité de Gestión y Desempeño Institucional	*Debe conocer y evaluar los informes de ejecución del Plan de Comunicaciones y Sensibilización con el fin de formular recomendaciones para mejorar la estrategia de apropiación. así mismo debe asegurar la articulación del plan con el MIPG y el Plan de Acción institucional.*
Encargado de la infraestructura tecnológica y seguridad de la información o Líder de SGSI (Equipo de seguridad de la información)	*Deben estar informados y ser conscientes de las leyes, lineamientos, políticas y procedimientos vinculados al SGSI. También deben diseñar, actualizar y coordinar la ejecución del Plan de Comunicaciones y Sensibilización, definir los mensajes clave, públicos objetivo y contenidos técnicos, debe coordinar con Comunicaciones, TIC y Talento Humano las actividades del plan para ejecutar y liderar campañas de cultura de seguridad y privacidad; consolidar evidencias, indicadores y reportes de ejecución, así como, debe socializar lecciones aprendidas derivadas de incidentes de seguridad.*
Gestión TIC (sistemas y soporte)	*El grupo de Gestión TIC debe conocer todo el SGSI para apoyar la divulgación de buenas prácticas de uso seguro de sistemas y plataformas digitales, debe participar en jornadas de capacitación y sensibilización técnica, debe apoyar campañas sobre contraseñas seguras, correo electrónico, dispositivos personales, teletrabajo y seguridad digital, también debe aportar insumos técnicos como material pedagógico y reportar incidentes o comportamientos recurrentes que evidencien brechas culturales.*
Oficina asesora de comunicaciones	*Esta Oficina debe elaborar y diseñar piezas comunicativas alineadas con el Plan de Comunicaciones del SGSI, también debe apoyar la divulgación y difusión de mensajes clave de seguridad a través de los canales institucionales.* *Asegurar lenguaje claro, accesible y coherente con la identidad institucional y acompañar y*

	apoyar campañas periódicas de capacitación y sensibilización.
Oficina asesora de planeación institucional	*Esta Oficina debe articular el presente Plan con el Plan de Acción institucional, apoyar la definición de indicadores y metas de este plan, incorporar los resultados del plan en ejercicios de seguimiento, evaluación y mejora y asegurar la alineación con MIPG y Gobierno Digital.*
Talento Humano	*Este proceso debe incorporar contenidos de seguridad y privacidad de la información en los procesos de inducción y reinducción, apoyar la programación y registro de capacitaciones del presente plan, promover la participación de todo el personal en las actividades de capacitación y sensibilización, integrar los compromisos de seguridad con carácter obligatorio en los procesos de vinculación y desvinculación y apoyar la medición de cobertura y asistencia del plan.*
Líderes de Procesos misionales y de apoyo	*Estos líderes deben socializar las políticas y mensajes del SGSI dentro de sus equipos, deben fomentar el cumplimiento de buenas prácticas de seguridad en los procesos a su cargo, identificar necesidades de sensibilización específicas de su proceso, facilitar la participación del personal en las actividades del plan y reportar comportamientos de riesgo o brechas de conocimiento.*
Servidores públicos	*Los servidores deben participar activamente en las actividades de comunicación y sensibilización, aplicar lo aprendido y las buenas prácticas en su labor diaria, consultar y conocer las políticas y lineamientos del SGSI, reportar incidentes, dudas o situaciones de riesgo para la información y contribuir a la construcción de la cultura de autocuidado digital.*
Contratistas, proveedores y terceros	*Estos grupos de personas deben estar informados sobre todos los lineamientos del SGSI, esto incluye conocer y cumplir los lineamientos y actualizaciones del SGSI, así como Atender las comunicaciones institucionales relacionadas con seguridad y privacidad, también participar en las actividades de sensibilización cuando aplique y*

	reportar incidentes o vulnerabilidades identificadas.

Fuente: elaboración propia

DISEÑO DEL PLAN DE CAPACITACIÓN Y SENSIBILIZACIÓN

Los temas para la socialización, cursos, charlas o capacitaciones, que se abordarán mediante la divulgación de información, la creación de piezas audiovisuales enviadas a los correos institucionales, fondos de pantalla y otros canales establecidos, se detallan a continuación:

- Uso adecuado del correo electrónico Institucional.
- Tips de Seguridad de la información.
- Canales de comunicación.
- Seguridad en el puesto de trabajo.
- Boletines COLCERT.

IMPLEMENTACIÓN DEL PLAN DE CAPACITACIÓN Y SENSIBILIZACIÓN

Este plan busca crear capacidades a todos los funcionarios, contratistas y terceros de la RAP-E en seguridad y la privacidad de la Información, así mismo, busca contribuir a la gestión del riesgo creando capacidades institucionales y personales de seguridad digital y ciberseguridad.

Este cronograma de capacitaciones responde a la implementación del SGSI a través de su política de Seguridad y Privacidad de la Información y sus anexos.

¿Qué problema institucional ayuda a resolver?

Por lo tanto, la implementación de este cronograma está orientado y ataca las debilidades en seguridad de la información que se presentan en la Entidad, abordando el fortalecimiento de las capacidades humanas como factor de riesgo importante dentro del ecosistema de seguridad institucional dando seguimiento en búsqueda de la mejora continua.

CRONOGRAMA

La Tabla 2 muestra la programación de las actividades relacionadas con el SGSI 2026-2027 institucional durante el segundo trimestre de 2026 y el 2027.

Tabla 2. Cronograma Plan de comunicaciones SGSI 2026-2027

Cronograma de actividades del plan de Comunicación de SGSI RAP- E 2026-2027								
2026	**Ítem**	**Actividad de capacitación o sensibilización**	**Jul**	**Ago**	**Sep**	**Oct**	**Nov**	**Dic**
	1	Lanzamiento del SGSI institucional						

Segundo Semestre 2026	2	Principios de la seguridad de la información						
	3	Roles y responsabilidades del nuevo SGSI						
	4	Capacitación de seguridad para teletrabajadores						
	5	Sensibilización vía correo electrónico institucional: Responsabilidades individuales y reporte de incidentes.						
	6	Taller: Gestión y clasificación de activos de información						
	7	Capacitación: Control de accesos, usuarios y contraseñas						
	8	Sensibilización vía correo institucional: Uso adecuado del correo electrónico e internet						
	9	Capacitación: Uso seguro de plataformas en línea						
	10	Sensibilización vía correo institucional: Escritorio y pantalla limpia						
2027	**Ítem**	**Actividad de capacitación o sensibilización**	**Ene**	**Feb**	**Mar**	**Abr**	**May**	**Jun**
Primer Semestre 2027	11	Capacitación: Identificación y reporte de incidentes de seguridad						
	12	Taller práctico: Gestión de incidentes y lecciones aprendidas						
	13	Capacitación: Continuidad del negocio (BIA, DRP, respaldo)						
	14	Sensibilización vía correo electrónico: Código malicioso y phishing						

	15	Capacitación: Gestión de cambios y RFC						
2027	**Ítem**	**Actividad de capacitación o sensibilización**	**Jul**	**Ago**	**Sep**	**Oct**	**Nov**	**Dic**
Segundo Semestre 2027	16	Reinducción general en SGSI						
	17	Evaluación de conocimientos SGSI						
	18	Taller de refuerzo para líderes						
	19	Socialización presencial de resultados SGSI 2027						
	20	Elaboración del plan de capacitación 2027						

Fuente: elaboración propia

Nota: para mayor detalle por favor revisar el archivo anexo llamado: *"Cronograma Plan de comunicación SGSI"*

MEJORA CONTINUA

La RAP-E Región Central establece un enfoque de mejora continua para el fortalecimiento del SGSI, fundamentado en el ciclo Planear-Hacer-Verificar-Actuar (PHVA). Este enfoque permite evaluar de manera periódica la eficacia de las actividades de capacitación, sensibilización y apropiación del SGSI, así como adoptar acciones de mejora orientadas a la reducción de riesgos asociados al factor humano.

Con el fin de medir el nivel de avance y efectividad del Plan de Comunicaciones, Sensibilización y Capacitación, la entidad define un conjunto de indicadores de desempeño, los cuales se encuentran directamente asociados al cronograma anual de actividades y permiten realizar seguimiento sistemático por trimestre.

Indicadores de seguimiento

Los indicadores definidos para la mejora continua son los siguientes:

1. **Porcentaje de personal capacitado en SGSI:** Permite medir la cobertura del plan de capacitación respecto del total de funcionarios y contratistas de la RAP-E.
2. **Porcentaje de asistencia a jornadas de capacitación y sensibilización:** Permite evaluar el nivel de participación efectiva del personal convocado a las actividades programadas en el cronograma.

3. **Porcentaje de resultados de evaluaciones de conocimiento:** Permite medir el grado de comprensión y apropiación de los contenidos del SGSI, a través de evaluaciones, encuestas o ejercicios de verificación aplicados posterior a las jornadas de capacitación.
4. **Reducción de incidentes de seguridad asociados a error humano:** Permite evaluar el impacto del plan en la disminución de incidentes relacionados con desconocimiento, malas prácticas o incumplimiento de políticas de seguridad de la información.

Asociación de los indicadores con el cronograma

Los indicadores definidos se encuentran alineados directamente con las actividades programadas en el cronograma trimestral de capacitación y sensibilización, de manera que cada actividad ejecutada genera insumos cuantificables para al menos uno de los indicadores establecidos. Esta relación garantiza trazabilidad entre: la planificación de las actividades, su ejecución periódica, la medición de resultados, y la toma de decisiones para la mejora continua del SGSI.

Seguimiento y análisis

El seguimiento de los indicadores se realizará de forma trimestral, coincidiendo con el cierre de cada período del cronograma, y estará a cargo del Oficial de Seguridad y Privacidad de la Información o quien haga sus veces, con el apoyo de la Gestión TIC, Talento Humano y Planeación. Los resultados consolidados serán presentados en el Informe semestral de Seguimiento del SGSI, y puestos en conocimiento del Comité Institucional de Gestión y Desempeño, como insumo para: La evaluación del avance del SGSI, la identificación de brechas de conocimiento o cultura, la priorización de acciones de refuerzo o ajuste, y la formulación de planes de mejora.

Acciones de mejora

Cuando los resultados de los indicadores evidencien desviaciones frente a las metas establecidas, la RAP-E definirá e implementará acciones correctivas y preventivas, tales como: Refuerzo de campañas de sensibilización, ajustes al contenido o modalidad de las capacitaciones, reinducciones focalizadas por dependencia o rol, y fortalecimiento del acompañamiento a líderes de proceso.

Este esquema garantiza que el Plan de Capacitación y Sensibilización del SGSI no sea un ejercicio aislado, sino un mecanismo permanente de mejora, alineado con los objetivos institucionales, la gestión del riesgo y la sostenibilidad del sistema de gestión de seguridad de la información.

CONTROL DE CAMBIOS

¿El Comité de Gestión y Desempeño Institucional o quien haga sus veces aprueba el presente Plan?

SI: ___ NO____

VERSIÓN	FECHA	DESCRIPCIÓN	LÍDER DEL PROCESO
Vr.1.0	11/05/2026	Elaboración del Plan	Leydi Támara

Vr.2.0	04/09/2026	Ajuste del cronograma	Leydi Támara