PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DEL SISTEMA ESTRATÉGICO DE TRANSPORTE PÚBLICO SETP TRANSFEDERAL S.A.S

Tabla de contenido

INTRODUCCIÓN

En el mundo actual, donde la información es uno de los activos más valiosos, protegerla se ha convertido en una prioridad para las organizaciones. El Sistema Estratégico de Transporte Público SETP TRANSFEDERAL S.A.S., como entidad pública descentralizada, reconoce que la seguridad y privacidad de la información no solo son requisitos legales, sino también un compromiso ético con sus beneficiarios, empleados y socios. La correcta gestión de la información es vital para garantizar la eficiencia y calidad en los servicios de transporte público, cumpliendo así con las expectativas de la ciudadanía.

La creciente digitalización y el uso de tecnologías emergentes presentan oportunidades, pero también generan riesgos significativos como el cibercrimen, las fugas de información o técnicas maliciosas (phishing, ingeniería social), así como incumplimientos normativos. Este Plan de Seguridad y Privacidad de la Información se diseña como una guía integral para afrontar dichos desafíos, asegurando la protección de los datos que maneja la organización y garantizando su uso responsable.

Este documento refleja el compromiso del SETP TRANSFEDERAL S.A.S. con el cumplimiento de las leyes vigentes, los principios del Ministerio TIC y la Política de Gobierno Digital, enmarcando una estrategia que prioriza la confidencialidad, integridad y disponibilidad de la información. Asimismo, el plan busca promover una cultura organizacional donde todos los miembros entiendan su rol en la seguridad de los datos y participen activamente en su protección, mitigando riesgos que podrían afectar la eficiencia operativa o la continuidad de los servicios.

El enfoque adoptado es proactivo y adaptativo, permitiendo responder a amenazas actuales y futuras, con una implementación gradual acorde al presupuesto institucional y alineada a los planes de desarrollo nacionales, departamentales y municipales para 2025. La adopción del Modelo de Seguridad y Privacidad de la Información (MSPI) será clave para gestionar riesgos, proteger los recursos tecnológicos y fortalecer la confianza de los actores involucrados en la gestión del SETP.

1. OBJETIVOS

Establecer las actividades contempladas en el Modelo de Seguridad y Privacidad de la Información (MSPI) de la política de Gobierno Digital del MinTIC, alineadas con la norma NTC/IEC ISO 27001, la Política Pública de Seguridad Digital, y los criterios de continuidad operativa de los servicios, con el propósito de garantizar la seguridad y privacidad de la información manejada en los procesos del Sistema Estratégico de Transporte Público de Neiva - SETP TRANSFEDERAL S.A.S.

1.1. Objetivos Específicos

- Implementar programas de capacitación y sensibilización para todos los funcionarios, contratistas y proveedores del SETP TRANSFEDERAL S.A.S, enfocados en la importancia de la seguridad y privacidad de la información.
- Realizar un inventario y clasificación de los activos de información críticos para los procesos de SETP TRANSFEDERAL S.A.S.
- Implementar controles técnicos y administrativos para proteger la confidencialidad, integridad y disponibilidad de la información, alineados con los requisitos de la norma ISO 27001.
- Realizar evaluaciones periódicas de riesgos de seguridad de la información para identificar y priorizar las amenazas potenciales.
- Implementar medidas de control y mitigación de riesgos, basadas en los resultados de las evaluaciones, para prevenir incidentes de seguridad.
- Establecer un plan de respuesta a incidentes de seguridad que incluya procedimientos claros para la detección, análisis, contención, erradicación y recuperación.
- Realizar auditorías internas y revisiones periódicas para asegurar el cumplimiento de las normativas legales y regulatorias relacionadas con la seguridad y privacidad de la información.
- Mantener actualizados los registros y documentación necesaria para demostrar el cumplimiento de las obligaciones legales y regulatorias.

2. ALCANCE

El presente documento se aplica a todo el modelo de operación por procesos de SETP TRANSFEDERAL S.A.S, garantizando el cumplimiento de lo dispuesto en el Decreto 1083 de 2015, "por el cual se expide el Decreto Único Reglamentario del Sector de Función Pública", así como en el Decreto 1078 de 2015 en lo relacionado con la Política de Gobierno Digital y su Modelo de Seguridad y Privacidad de la Información establecido en la Resolución 500 de 2021. Todo ello se encuentra alineado con la norma NTC/IEC ISO 27001, asegurando un marco integral para la gestión de la seguridad de la información.

3. NORMATIVIDAD

3.1. Constitución, leyes y directivas

- **Constitución Política de Colombia**. Artículos 15, 20, 23 y 74.
- **Ley 23 de 1982.** Sobre derechos de autor.
- **Ley 44 de 1993.** Por la cual se modifica y adiciona la Ley 23 de 2082 y se modifica la Ley 29 de 2044 y Decisión Andina 351 de 2015 (Derechos de autor).
- **Ley 527 de 1999.** Por la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales y se establecen las entidades de certificación y se dictan otras disposiciones. **Ley 594 de 2000.** Por medio de la cual se regula el Derecho Fundamental de Petición y se sustituye un título del Código de Procedimiento Administrativo y de lo Contencioso Administrativo.
- **Ley 962 de 2005.** Por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos.
- **Ley 1221 del 2008.** Por la cual se establecen normas para promover y regular el Teletrabajo y se dictan otras disposiciones.
- **Ley 1266 de 2008.** Por la cual se dictan las disposiciones generales del Hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.
- **Ley 1273 de 2009**. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
- **Ley 1341 de 2009.** Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y las comunicaciones - TIC- Se crea la agencia Nacional de espectro y se dictan otras disposiciones
- **Ley 1474 de 2011.** Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.
- **Ley 1581 de 2012.** Por la cual se dictan disposiciones generales para la protección de datos personales.
- **Ley 2088 de 2012.** Por la cual se regula el trabajo en casa y se dictan otras disposiciones.
- **Ley 1712 de 2014.** Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
- **Ley 1915 de 2018.** Por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos.
- **Decisión Andina 351 de 1993.** Régimen común sobre derecho de autor y derechos conexos.
- **Directiva 26 de 2020.** Diligenciamiento de la información en el índice de transparencia y acceso a la información – ITA – de conformidad con las disposiciones del artículo 23 de la ley 1712 de 2014.

3.2. Decretos

- **Decreto 2364 de 2012.** Por medio del cual se reglamenta el artículo 7° de la Ley 527 de 1999, sobre la firma electrónica y se dictan otras disposiciones.
- **Decreto 2609 de 2012.** Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado.
- **Decreto 884 de 2012** Por medio del cual se reglamenta la Ley 1221 de 2008 y se dictan otras disposiciones.
- **Decreto 1377 de 2013.** Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
- **Decreto 886 de 2014.** Por el cual se reglamenta el Registro Nacional de Bases de Datos.
- **Decreto 103 de 2015.** Por medio del cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
- **Decreto 1499 de 2017.** Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.
- **Decreto 1008 del 2018.** Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.
- **Decreto 612 de 2018.** Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.
- **Decreto 2106 de 2019.** Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública.
- **Decreto 1287 de 2020.** Por el cual se reglamenta el Decreto Legislativo 491 del 28 de marzo de 2020, en lo relacionado con la seguridad de los documentos firmados durante el trabajo en casa, en el marco de la Emergencia Sanitaria.
- **Decreto 620 de 2020.** Por el cual se subroga el título 17 de la parte 2 del libro 2 del Decreto 1078 de 2015, para reglamentarse parcialmente los artículos 53, 54, 60, 61 y 64 de la Ley 1437 de 2011, los literales e), j) y literal a) del parágrafo 2 del artículo 45 de la Ley 1753 de 2015, el numeral 3 del artículo147 de la Ley 1955 de 2019, y el artículo 9° del Decreto 2106 de 2019, estableciendo los lineamientos generales en el uso y operación de los servicios ciudadanos digitales.
- **Decreto 338 de 2022.** Por el cual se adiciona el Titulo 21 a la parte 2 del libro 2 del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones.
- **Decreto 767 de 2022.** Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- **Decreto 88 de 2022.** Por el cual se adiciona el Título 20 a la Parte 2 del Libro 2 del Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, Decreto 1078 de 2015, para reglamentar los artículos 3, 5 Y 6 de la Ley 2052 de 2020, estableciendo los conceptos, lineamientos, plazos y condiciones para la digitalización y automatización de trámites y su realización en línea.

3.3. Resoluciones del Ministerio de Tecnologías de la Información y las Comunicaciones

- **Resolución 2339 de 2024.** Por la cual se actualiza la Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de los servicios del Ministerio/Fondo de Tecnologías de la Información y las Comunicaciones, se definen lineamientos frente al uso y manejo de la información y se deroga la resolución 0448 de 2022
- **Resolución 1838 de 2022.** Por la cual se reglamentan las modalidades de teletrabajo, se establecen las condiciones de trabajo en casa y se definen los lineamientos de desconexión laboral en el MINTIC, y se deroga la resolución 1151 del 16 de mayo de 2019.
- **Resolución 500 de 2021.** Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la Política de Gobierno Digital
- **Resolución 1519 de 2020.** Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos.

3.4. Documentos de Política Publica

- **CONPES 3995 de 2020.** Confianza y Seguridad Digital
- **CONPES 3854 de 2017.** Política Nacional de Seguridad digital.
- **CONPES 3701 de 2011.** Lineamientos de Política para Ciberseguridad y Ciberdefensa.
- **CONPES 4069 de 2022.** Política Nacional de Ciencia, tecnología e innovación 2022 – 2031.

4. ESTADO ACTUAL DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

4.1. Nivel de Madurez Inicial del Modelo de Seguridad y Privacidad de la Información – MSPI

El Sistema Estratégico de Transporte Público de Neiva - SETP TRANSFEDERAL S.A.S realizó el autodiagnóstico sobre la implementación del Modelo de Seguridad y Privacidad de la Información, utilizando el instrumento de evaluación entregado por el Ministerio TIC de la Política Nacional de Gobierno Digital, el resultado del diagnóstico para el año 2024 un promedio del 10% en la implementación.

El resultado muestra un nivel de madurez INICIAL del modelo de Seguridad y Privacidad de la Información en El Sistema Estratégico de Transporte Público de Neiva - SETP TRANSFEDERAL S.A.S, sobre el que se cuenta con un nivel de cumplimiento bajo.

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	10	100	INICIAL
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	10	100	INICIAL
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	10	100	INICIAL
A.8	GESTIÓN DE ACTIVOS	10	100	INICIAL
A.9	CONTROL DE ACCESO	10	100	INICIAL
A.10	CRIPTOGRAFÍA	0	100	INEXISTENTE
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	10	100	INICIAL
A.12	SEGURIDAD DE LAS OPERACIONES	10	100	INICIAL
A.13	SEGURIDAD DE LAS COMUNICACIONES	10	100	INICIAL
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	10	100	INICIAL
A.15	RELACIONES CON LOS PROVEEDORES	0	100	INEXISTENTE
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	10	100	INICIAL
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	10	100	INICIAL
A.18	CUMPLIMIENTO	10	100	INICIAL
PROMEDIO EVALUACIÓN DE CONTROLES		**9**	**100**	INICIAL

Ilustración 1. Línea base producto de seguimiento de controles 2024.

Ilustración 2. Análisis de brechas - Controles de Anexo A de la Norma ISO 27001:2013.

5. DESARROLLO

5.1. PROCESO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Sistema Estratégico de Transporte Público de Neiva - SETP TRANSFEDERAL S.A.S. deberá adoptar en su modelo de Seguridad y Privacidad de la Información a nivel estratégico que permita garantizar continuamente la seguridad y privacidad de la información en la entidad, por medio de la definición de políticas, programas, lineamientos, estrategias y actividades.

5.2. OBJETIVOS ESPECÍFICOS DE LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LAINFORMACIÓN DEL SISTEMA ESTRATÉGICO DE TRANSPORTE PÚBLICO SETP TRANSFEDERAL S.A.S

Sistema Estratégico de Transporte Público de Neiva - SETP TRANSFEDERAL S.A.S. establece los siguientes objetivos estratégicos en materia de seguridad de la información:

- Desarrollar e implementar un marco normativo robusto que garantice la protección integral de los activos de información de la empresa.
- Implementar un sistema de gestión de riesgos que permita identificar, evaluar y controlar las amenazas relacionadas con la seguridad de la información, privacidad y continuidad operativa de los servicios prestados.
- Crear e implementar protocolos efectivos de respuesta ante incidentes de seguridad informática, garantizando una gestión oportuna que minimice el impacto sobre las operaciones de la empresa.
- Fortalecer los sistemas de protección tanto físicos como digitales para salvaguardar la información empresarial, asegurando su confidencialidad, integridad, disponibilidad y autenticidad en todos los procesos.
- Establecer directrices específicas para la gestión documental segura, contemplando tanto documentos físicos como digitales, bajo estándares de protección de datos y privacidad.
- Promover una cultura organizacional enfocada en la seguridad de la información, mediante programas de capacitación y sensibilización que impulsen la mejora continua del Sistema de Gestión de Seguridad de la Información.
- Asegurar el cumplimiento de la normatividad colombiana vigente en materia de seguridad informática, protección de datos personales y gestión documental aplicable a la empresa.
- Diseñar e implementar un Plan de Continuidad del Negocio que garantice la prestación ininterrumpida de los servicios públicos esenciales para la ciudad de Neiva.

5.3. ALCANCE DEL SISTEMA DE GESTIÓN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

Asegurar la confidencialidad, integridad y disponibilidad de la información en la gestión y control de la prestación del Servicio Público de las Tecnologías de la Información y las Comunicaciones.

5.4. ÁMBITO DE APLICACIÓN

La presente política se aplica de manera integral a toda la estructura organizacional del Sistema Estratégico de Transporte Público de Neiva - SETP TRANSFEDERAL S.A.S. abarcando:

El personal vinculado directamente con la empresa que desarrollen actividades para la organización.

Las entidades y organismos de control que interactúen con la información institucional, así como terceros que por razones justificadas requieran acceder, procesar, almacenar o transmitir datos de la empresa.

Toda la información generada, adquirida, procesada o almacenada por el Sistema Estratégico de Transporte Público de Neiva - SETP TRANSFEDERAL S.A.S., independientemente de:

- Su formato de presentación (físico o digital)
- Su ubicación (instalaciones propias o sistemas externos)
- Su naturaleza (administrativa, operativa o técnica)
- Su medio de conservación o transmisión

5.5. PLAN DE IMPLEMENTACIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

El Plan de implementación de Seguridad y Privacidad de la Información se ejecuta de acuerdo con el siguiente cronograma, al cual se le hace seguimiento mes a mes:

Gestión	Actividades	Tareas	Responsable de la Tarea	Evidencia	Fechas Programación Tareas		Fecha de Seguimiento
					Fecha Inicio	Fecha Final	
Activos de Información	Definir lineamientos para el levantamiento de activos de información	Actualizar la metodología o la documentación de la gestión de levantamiento de activos de información, en el caso que aplique	Planeación Estrategica	Documentación actualizada	01-may-25	30-may-25	30-dic-25

	Identificación y/o Actualización activos de información	Validar activos de información en el instrumento con el que cuenta la entidad	Planeación Estrategica	Documentación revisada	01-jun-25	30-jun-25	30-dic-25
		Identificar nuevos activos de información en cada dependencia	Planeación Estrategica	Acta de Reunión	01-jun-25	30-jun-25	30-dic-25
	Publicación de Activos de Información	Validar y aceptar los activos de información para su publicación en sistema de gestión de la entidad	Planeación Estrategica	Oficio de aprobación	1-jul-25	30-jul-25	01-ago-25
Gestión de Riesgos	Actualización de lineamientos de riesgos	Apoyar cuando se requiera la actualización de la política, metodología y lineamientos de la gestión de riesgos	Planeación Estrategica	Correos electrónicos, Documentación actualizada en Sistema de Gestión Página web	01-jul-25	30-jul-25	30-dic-25
	Identificación de Riesgos de Seguridad y Privacidad de la Información	Contexto, Identificación, Análisis y Evaluación de Riesgos - Seguridad y Privacidad de la Información y Seguridad Digital	Planeación Estrategica	Correos electrónicos Mapas de riesgos	1-ago-25	30-ago-25	30-dic-25
		Realimentación, revisión y verificación de los riesgos identificados (Ajustes)	Planeación Estrategica	Correos electrónicos Mapas de riesgos	1-ago-25	30-ago-25	v

	Aceptación de Riesgos Identificados	Aceptación, aprobación riesgos identificados y planes de tratamiento	Planeación Estrategica	Memorandos de aceptación mapas de riesgos	1-sept-25	11-sept-25	30-dic-25
	Publicación	Publicación mapas de riesgos de los procesos Sistema de Gestión	Planeación Estrategica	Mapas de riesgos publicados Sistema de Gestión	15-sept-25	30-sept-25	30-dic-25
	Seguimiento Fase de Tratamiento	Seguimiento implementación de controles y planes de tratamiento de riesgos los identificados (verificación de evidencias)	Planeación Estrategica	Seguimiento mapas de riesgo	01-dic-25	30-dic-25	30-dic-25
Plan de Cambio y Cultura de Seguridad y Privacidad de la Información	Plan de Cambio y Cultura de Seguridad y Privacidad de la Información Ejecutar el n	Elaborar la documentación del Plan de Cambio, Cultura y Apropiación de Seguridad y Privacidad de la Información	Planeación Estrategica	Documentación actualizada en Sistema de Gestión	01-oct-25	10-oct-25	2-jul-25
		Implementar las estrategias del Plan de Cambio, Cultura y Apropiación de Seguridad y Privacidad de la Información	Planeación Estrategica	Correo electrónico, listados de asistencia	11-oct-25	31-dic-25	31-dic-25

Matriz de verificación de Requisitos Legales de Seguridad de la Información	Elaborar la Matriz de verificación de Requisitos Legales de Seguridad de la Información	Elaborar la Matriz de verificación de Requisitos Legales de Seguridad de la Información	Planeación Estrategica	Documentación actualizada en Sistema de Gestión	1-oct-25	30-oct-25	30-dic-25
Planeación	Revisión Manual Políticas de Seguridad de la Información y Resolución de Seguridad de la Información	Actualizar cuando se requiera los Manuales, Políticas, Resoluciones, documentación del MSPI y la documentación estratégica del procesos de Seguridad y privacidad de la Información.	Planeación Estrategica	Documentación actualizada en Página Web	01-may-25	30-dic-25	30-dic-25
Seguridad Digital	Seguridad Digital	Actualizar el documento de autodiagnóstico de la entidad en la implementación de Seguridad y Privacidad de la Información.	Planeación Estrategica	Documento de Diagnostico de MINTIC para Medición del MSPI	01-may-25	30-dic-25	30-dic-25
Revisión de los controles de la norma ISO 27001:2013	Revisión de los controles de la norma ISO 27001:2013,	Aplicar la herramienta diseñada para realizar la validación del cumplimiento de la Política General de Seguridad y Privacidad de la Información	Planeación Estrategica	Herramienta diligenciada	01-may-25	30-jun-25	1-jul-25

Plan de diagnóstico de IPV4 a IPV6	Plan de diagnóstico de IPV4 a IPV6	Elaborar el documento de diagnóstico de IPV4 a IPV6	Planeación Estrategica	Documentación	01-jul-25	30-dic-25	30-dic-25

6. RECURSOS

SISTEMA ESTRATÉGICO DE TRANSPORTE PÚBLICO SETP TRANSFEDERAL S.A.S, en el marco de la gestión de Seguridad y Privacidad de la información, dispone de los siguientes recursos.

RECURSOS	VARIABLE
Humanos	Equipo de trabajo de la empresa
Logísticos	Gestión de recursos para realizar socializaciones, transferencia de conocimientos y seguimiento a la gestión de riesgos.
Financieros	Recursos para la adquisición de conocimiento, recursos humanos, técnicos, y desarrollo de auditorías con un costo aproximado de 192.400.000

7. SEGUIMIENTO DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Nombre	Formula	Cumplimiento		
		Alto	Medio	Bajo
Porcentaje de cumplimiento actividades identificadas en el plan de seguridad y privacidad de la información.	Porcentaje de cumplimiento = (Número de actividades cumplidas / Número total de actividades) * 100	75% al 100%	50% al 74%	0% al 49%