PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN-PESI 2024 -2027

Oficina de Tecnologías de la Información y las Comunicaciones
Secretaría de Educación Del Distrito

ALCALDÍA MAYOR DE BOGOTÁ D.C.
SECRETARÍA DE EDUCACIÓN
BOGOTÁ

Vigencia 2024-2027

Tabla de Contenido

1. INTRODUCCIÓN 4
2. OBJETIVO 5
   2.1. Objetivos Específicos 5
3. ALCANCE 6
4. AMBITO DE APLICACIÓN 7
5. MARCO LEGAL 8
6. ESTADO ACTUAL DE LA ENTIDAD RESPECTO AL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN 9
   6.1. Estado actual de la SED 9
   6.2. Brechas identificadas. 10
7. CIBERSEGURIDAD 11
   7.1. Campañas de sensibilización 13
8. ESTRATEGIAS DE SEGURIDAD DIGITAL 14
   8.1. Descripción de las estrategias específicas (ejes) 14
      8.1.1 Liderazgo de Seguridad de la Información. 15
      8.1.2 Gestión del riesgo 17
      8.1.3 Concientización 19
      8.1.4 Implementación de controles 22
      8.1.5 Gestión de incidentes 24
   8.2. Cronograma 27
9. RESPONSABLES DE LA SEGURIDAD 29
10. MESAS TÉCNICAS DE GOBIERNO Y SEGURIDAD DIGITAL 31
11. PRESUPUESTO 32
12. REVISIONES 33

GLOSARIO

ACTIVOS: en relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas...) que tenga valor para la organización.

ACTIVO DE INFORMACIÓN: bien de la entidad (representado en su información y datos) que tiene valor para los procesos de negocio, independientemente de su ubicación; puede ser un documento físico debidamente firmado, un archivo guardado en un servidor, un aplicativo o cualquier elemento que permita almacenar información valiosa o útil.

AMENAZAS: causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.

ANÁLISIS DE RIESGOS: uso sistemático de una metodología para estimar los riesgos e identificar sus fuentes, para los activos o bienes de información.

DISPONIBILIDAD: la disponibilidad consiste en asegurarse que los usuarios autorizados tengan acceso a la información y a los sistemas de apoyo, cuando se requiera, se trata de la propiedad de ser accesible y utilizable, bajo solicitud por una entidad autorizada.

CONTINUIDAD: la continuidad es el proceso de establecer por adelantado, las capacidades necesarias para evitar o mitigar el impacto de un acontecimiento que provoca la interrupción de las operaciones en una o más procesos.

CONFIDENCIALIDAD: propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

CONTROL: es toda actividad o proceso encaminado a mitigar o evitar un riesgo. Incluye políticas, procedimientos, guías, estructuras organizacionales, buenas prácticas, y que pueden ser de carácter administrativo, técnico o legal.

CONTROL DE ACCESO: una característica o técnica en un sistema de comunicaciones para permitir o negar el uso de algunos componentes o algunas de sus funciones.

ISO/IEC 27001:2022: norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa.

MEDIOS DE ALMACENAMIENTO DIGITAL: son todos aquellos dispositivos autorizados por la Secretaría de Educación del Distrito, que permiten el almacenamiento de información, los cuales pueden ingresar o salir de las instalaciones de la entidad con la respectiva autorización. Se incluyen equipos portátiles, teléfonos inteligentes, Ipods, reproductores mp3, memorias

USB/SD/Mini-SD, CDs, DVDs, cintas: respaldo y similares. Asimismo, se incluyen correos electrónicos y conexiones por donde pueda ser transportada la información de la Entidad.

MEDIO REMOVIBLE: medio que permite llevar o transportar información desde un computador a otro. Los medios removibles incluyen cintas, diskettes, discos duros removibles, CDs, DVDs, unidades de almacenamiento USB.

PROCEDIMIENTO: los procedimientos, definen específicamente como las políticas, estándares, mejores prácticas y guías que serán implementadas en una situación dada. Los procedimientos son independientes de la tecnología o de los procesos y se refieren a las plataformas, aplicaciones o procesos específicos. Son utilizados para delinear los pasos que deben ser seguidos por una dependencia para implementar la seguridad relacionada con dicho proceso o sistema específico. Generalmente los procedimientos son desarrollados, implementados y supervisados por el dueño del proceso o del sistema, los procedimientos seguirán las políticas de la organización, los estándares, las mejores prácticas y las guías tan cerca como les sea posible, y a la vez se ajustarán a los requerimientos procedimentales o técnicos establecidos dentro de la dependencia donde ellos se aplican.

RIESGO: efecto de la incertidumbre sobre los objetivos. Un efecto es una desviación de lo esperado: positivo o negativo.

SEGURIDAD DE LA INFORMACIÓN: preservación de la confidencialidad, integridad, y disponibilidad de la información en cualquier medio: impreso o digital. (ISO/IEC 27000).

SENSIBILIDAD: nivel de impacto que una divulgación no autorizada podría generar.

SERVICIO: es cualquier acto o desempeño que una persona puede ofrecer a otra, que es esencialmente intangible y que no conlleva ninguna propiedad. Su producción puede o no estar ligada a un producto físico.

GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN: procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).

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 27000).

VULNERABILIDAD: debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

1. INTRODUCCIÓN

En este documento se presenta el Plan Estratégico de Seguridad y Privacidad de la Información (PESI) para el periodo comprendido entre 2024-2027 herramienta la cual permite garantizar la protección de los activos de información de la Secretaría de Educación del Distrito, el cumplimiento normativo nacional como internacional, la identificación y mitigación de los riesgos digitales, así como la continuidad de los servicios que ofrece la entidad a toda la comunidad educativa manteniendo la confidencialidad, integridad y disponibilidad de la información.

El PESI, está enmarcado con la finalidad de suministrar a través del Modelo de Seguridad y Privacidad de la Información (MSPI) la planificación, implementación, verificación, monitoreo y mejora continua de los planes, proyectos, políticas, lineamientos y procedimientos de la estrategia de Gobierno Digital de la SED.

La SED ha adoptado una metodología que permite identificar y valorar los activos de información la cual actúa evaluando y dando el tratamiento adecuado a los riesgos identificados para así, mitigar y minimizar el impacto en la entidad.

En concordancia, el PESI articula la gestión del riesgo, lidera la seguridad y privacidad de la información, el estado actual y a futuro de la SED, cultura organizacional en ciberseguridad, define los roles y responsables de las estrategias, adopta los controles efectivos de seguridad y propone las mesas técnicas para su correcta implementación.

2. OBJETIVO

Garantizar la integridad, confidencialidad y disponibilidad de la información en la Secretaría de Educación del Distrito, a través del Modelo de Seguridad y Privacidad de la información, propendiendo la estrategia de Seguridad Digital de los activos y el tratamiento de riesgos informáticos.

2.1. Objetivos Específicos

- Incrementar el nivel de madurez de la SED en seguridad de la información y digital.
- Identificar y tratar los riesgos asociados a los activos de información.
- Realizar el seguimiento y mejora continua de implementación en los controles y procedimientos para la gestión de la seguridad de la información.
- Divulgar y fortalecer la cultura de seguridad y privacidad de la información.

3. ALCANCE

Se describen las estrategias que se ejecutaran en la Secretaría de Educación del Distrito, referentes a los temas de seguridad y privacidad de la Información, durante la vigencia 2024 – 2027, que permitan cumplir con las metas, objetivos y funciones de la política de Gobierno Digital.

El PESI esta alineado a los objetivos estratégicos y misionalidad de la Secretaría de Educación del Distrito, brindando la seguridad y privacidad de los activos de información propios de la entidad.

4. AMBITO DE APLICACIÓN

El Plan de Estratégico de Seguridad y Privacidad de la Información (PESI), así como la Política de Seguridad Digital, aplica a todos los niveles funcionales y organizacionales de la Secretaria de Educación del Distrito, a todos sus funcionarios, contratistas, proveedores, operadores, entidades adscritas, así como aquellas personas o terceros que en razón del cumplimiento de sus funciones y las de la SED compartan, utilicen, recolecten, procesen, intercambien o consulten su información, al igual que a las entidades de control, demás entidades relacionadas que accedan, ya sea interna o externamente a cualquier activo de información, independientemente de su ubicación.

De igual manera, este plan aplica a toda la información creada, procesada o utilizada por SED, sin importar el medio, formato, presentación o lugar en el cual se encuentre.

5. MARCO LEGAL

A continuación, se presenta la normatividad que relaciona, aplica y concierne al Plan Estratégico de Seguridad y Privacidad de la Información de la SED:

- 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*".
- 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*".
- Manual de Gobierno Digital – MINTIC.
- Modelo de Seguridad y Privacidad de la Información – MINTIC.

6. ESTADO ACTUAL DE LA ENTIDAD RESPECTO AL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

6.1. Estado actual de la SED

La Oficina de las Tecnologías de la Información y las Comunicaciones -OTIC-, de la Secretaría de Educación del Distrito, tiene el compromiso y responsabilidad de llevar a cabo la planeación, el desarrollo, la implementación y la constante mejora continua de las políticas, lineamientos, procedimientos y demás normas que den cumplimiento a brindar la integridad, la confidencialidad y disponibilidad de la seguridad de la información.

Por lo anterior, la OTIC, basándose en los estándares internacionales como la norma ISO 27001, así como el modelo de seguridad y privacidad de la información propuesto por el MINTIC. ha venido implementando una serie de políticas y lineamientos que permiten identificar un estado actual de seguridad del 80% de efectividad modo **gestionado.**

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	90	100	OPTIMIZADO
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	100	100	OPTIMIZADO
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	83	100	OPTIMIZADO
A.8	GESTIÓN DE ACTIVOS	83	100	OPTIMIZADO
A.9	CONTROL DE ACCESO	98	100	OPTIMIZADO
A.10	CRIPTOGRAFÍA	40	100	REPETIBLE
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	78	100	GESTIONADO
A.12	SEGURIDAD DE LAS OPERACIONES	76	100	GESTIONADO
A.13	SEGURIDAD DE LAS COMUNICACIONES	93	100	OPTIMIZADO
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	79	100	GESTIONADO
A.15	RELACIONES CON LOS PROVEEDORES	80	100	GESTIONADO
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	54	100	EFECTIVO
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	87	100	OPTIMIZADO
A.18	CUMPLIMIENTO	97,5	100	OPTIMIZADO
PROMEDIO EVALUACIÓN DE CONTROLES		80	100	GESTIONADO

Tabla 1. Evaluación controles NTC/ISO 27001:2013

Considerando que la información presentada corresponde al período 2024, posterior a la Declaración de Aplicabilidad (SOA), es necesario aclarar que los resultados expuestos no constituyen una conclusión definitiva sobre el nivel de madurez del Sistema de Gestión de Seguridad de la Información.

De conformidad con el enfoque de mejora continua (PHVA) establecido en la ISO/IEC 27001:2022, así como con los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI) del MINTIC, la información correspondiente a lo proyectado en el año 2026 se encuentra en proceso de construcción, a partir del

análisis, validación y consolidación de los datos, controles e indicadores generados durante el año 2025, los cuales permitirán actualizar la SOA, el análisis de riesgos y la medición del nivel de implementación y efectividad de los controles de seguridad de la información.

Así mismo, la entidad apropia las fases con relación al modelo de seguridad y privacidad de la información (MSPI), insumos para identificar el estado actual de la SED en seguridad de la información y tratamiento de riesgos digitales.

Las fases del modelo permiten definir metas específicas las cuales permiten a la entidad tener una visión y horizonte sobre la gestión en seguridad y privacidad de la información como se muestra a continuación:

Año	AVANCE PHVA		
	COMPONENTE	% de Avance Actual Entidad	% Avance Esperado
2024	Planificación	38%	40%
	Implementación	15%	20%
	Evaluación de desempeño	19%	20%
	Mejora continua	16%	20%
TOTAL		88%	100%

Tabla 2. % de avance actual ciclo PHVA

6.2. Brechas identificadas.

A través de los modelos de gobernanza de seguridad digital que en la entidad se han venido implementando, es importante abarcar los siguientes puntos de consolidación que permiten identificar y mejorar cada dominio de seguridad al que se busca llegar:

- En la evaluación de la efectividad de los controles se evidencia que se cuenta con el nivel de **gestionado.**
- Mantener actualizado el Manual de políticas de Seguridad y Privacidad de la Información.
- Realizar la detección y de análisis de vulnerabilidades interno y externo contra amenazas persistentes y en tiempo real.
- Establecer los planes de contingencia para garantizar la continuidad de los servicios.

7. CIBERSEGURIDAD

Dentro del marco de ciberseguridad, actualmente la Secretaría de Educación del Distrito -SED- cuenta con equipos que permiten tener una seguridad perimetral robusta a través de equipos como firewall perimetral, Forti-Mail, Analyzer, ambientes de pruebas y producción para aplicaciones y otros componentes que complementan equipos de filtrado de la plataforma seguridad lógica que corresponden al esquema de servicios de conectividad y seguridad perimetral, como una solución de forma global, es por ello que su operación y evolución debe ser continua y de crecimiento a medida que protejan no solo la infraestructura sino también los datos personales de toda la comunidad educativa, para esto, es necesario contar con herramientas de protección que se integren con las actuales.

Cualquiera de los ciberdelincuentes actuales puede eludir las defensas tradicionales a voluntad, por lo cual, las organizaciones quedan expuestas a los diferentes tipos de ataques cibernéticos que pueden costar mucho dinero y causar grandes daños desde el momento del ataque conocido hasta la remediación. Es por esto por lo que, las entidades de gobierno necesitan soluciones para amenazas avanzadas enfocadas en endpoints (Usuarios finales - Dispositivos tecnológicos de punto final, portátiles, equipos de escritorio, servidores), que se integren con la detección y respuesta a incidentes de ciberseguridad, al igual que complementen la estrategia con la gestión de vulnerabilidades en la infraestructura tecnológica.

A través de la solución tecnológica propuesta, la OTIC busca robustecer la postura de seguridad institucional definiendo un plan de acción, así:

- Iniciación: En esta etapa se busca consolidar y fortalecer la capacidad institucional para detectar, responder, gestionar y mitigar amenazas cibernéticas, para ello, se propone analizar el uso de servicios y tecnologías de ciberseguridad que permitan una respuesta extendida y automatizada mediante tecnologías XDR, la gestión centralizada de eventos de seguridad a través de soluciones SIEM y la administración integral de la exposición de la entidad en los distintos ámbitos de su infraestructura tecnológica, incluyendo servidores, aplicaciones web, entornos cloud y activos.

- Protección: Para esta etapa se propone fortalecer el esquema de ciberseguridad de la SED mediante el despliegue e implementación de las tecnologías definidas en la etapa de iniciación; estas tecnologías deberán ser ajustadas y afinadas conforme a los requerimientos técnicos, con el fin de garantizar el aseguramiento efectivo de los activos y plataformas tecnológicas involucradas.

- Correlación: Esta etapa busca mantener una visibilidad continua y una postura de seguridad integral sobre las plataformas tecnológicas de la entidad, a través de la definición e implementación de casos de uso alineados

con la misionalidad institucional. La correlación de eventos permitirá contar con un punto centralizado para la gestión, el análisis y la toma de decisiones frente a los riesgos de ciberseguridad identificados en los diferentes entornos tecnológicos.

Por último, la OTIC busca que estas fases se conviertan en un ciclo continuo que permita, a través de los diversos procesos internos, nutrirse con miras a fortalecer la postura existente y el despliegue de los controles de seguridad de la entidad.

En resumen, los controles de seguridad propuestos a considerar para las fases inicialmente descritas son:

- XDR – Extended Detection and Response: Tecnología que permite detectar y responder frente a anomalías y riesgos que se identifiquen en diversas fuentes asociadas a endpoints, permitiendo integración acorde a las cantidades definidas en el anexo técnico.

- Gestión de vulnerabilidades: Tecnología que permite medir que tan expuesta se encuentra la entidad y que brechas existen en servidores, aplicaciones Web, Nube Pública y Activos públicos en internet.

- SIEM – Security Information and Event Management: Tecnología que permite integrar diversas fuentes de logs de seguridad y que, a través de diversas configuraciones avanzadas, genera casos de uso para identificar cuando exista un ataque hacia un entorno misional.

7.1. Campañas de sensibilización

Elaboración de un plan de sensibilización en seguridad de la información que vaya de la mano con el Plan Institucional de Comunicación – PIC que tiene la entidad, que permita involucrar a todos sus funcionarios, contratistas, proveedores, operadores, entidades adscritas, así como a aquellas personas o terceros que tengan un vínculo con la SED, brindando las herramientas y consejos de seguridad que eviten:

- Suplantación de identidad
- Robos de información confidencial
- Correos de extorsión o Phishing
- Filtración de información sensible
- Perdida de datos
- Otros temas de seguridad

8. ESTRATEGIAS DE SEGURIDAD DIGITAL

La seguridad digital es un compromiso de responsabilidad compartida en el que intervienen todos los niveles organizacionales de la entidad (Central, local e institucional), mediante la Oficina de Tecnologías de la Información y las Comunicaciones -OTIC- se lideran las estrategias técnicas, culturales y procedimentales que reconocen la seguridad y privacidad de la información como parte fundamental para la misionalidad de la SED.

8.1. Descripción de las estrategias específicas (ejes)

De acuerdo con descrito en el modelo de seguridad y privacidad de la información (MSPI) y la resolución 500 de 2021, se describen las estrategias específicas que son recomendadas junto con su objetivo.

ESTRATEGIA / EJE	DESCRIPCIÓN/OBJETIVO
Liderazgo de seguridad de la información	Establecer el Modelo de Seguridad y Privacidad de la Información (MSPI) a través de la aprobación de la política general y demás lineamientos que se definan buscando proteger la confidencialidad, integridad y disponibilidad de la información teniendo como pilar fundamental el compromiso de la alta dirección y de los líderes de las diferentes dependencias y/o procesos de la Entidad a través del establecimiento de los roles y responsabilidades en seguridad de la información.
Gestión de riesgos	Determinar los riesgos de seguridad de la información a través de la planificación y valoración que se defina buscando prevenir o reducir los efectos indeseados tendiendo como pilar fundamental la implementación de controles de seguridad para el tratamiento de los riesgos.
Concientización	Fortalecer la construcción de la cultura organizacional con base en la seguridad de la información para que convierta en un hábito, promoviendo las políticas, procedimientos, normas, buenas prácticas y demás lineamientos, la transferencia de conocimiento, la asignación y divulgación de responsabilidades de todo el personal de la entidad en seguridad y privacidad de la información.

Implementación de controles	Planificar e implementar las acciones necesarias para lograr los objetivos de seguridad y privacidad de la información y mantener la confianza en la ejecución de los procesos de la Entidad, se pueden subdividir en controles tecnológicos y/o administrativos.
Gestión de incidentes	Garantizar una administración de incidentes de seguridad de la información con base a un enfoque de integración, análisis, comunicación de los eventos e incidentes y las debilidades de seguridad en pro de conocerlos y resolverlos para minimizar el impacto negativo de estos en la Entidad.

Tabla 3. Descripción de estrategias.
Fuente: Plantilla PESI - MINTIC

8.1.1 Liderazgo de Seguridad de la Información.

- **Planeación**

  - **Desarrollo de Estrategias de Seguridad de la Información**: Definir objetivos y metas a largo plazo para proteger la información crítica de la organización.
  - **Análisis de Requisitos Regulatorios**: Asegurar que las actividades de seguridad cumplan con las normativas, leyes y estándares del sector (como ISO 27001, GDPR, etc.).
  - **Evaluación de Recursos y Capacidades**: Determinar los recursos necesarios (tecnológicos, humanos, financieros) para implementar el plan de seguridad.
  - **Definición de Políticas y Procedimientos**: Establecer políticas claras para proteger la información y protocolos para su implementación.
  - **Planificación de Respuesta a Incidentes**: Crear planes para abordar posibles violaciones de seguridad, incluyendo protocolos de respuesta y recuperación.

- **Políticas y Procedimientos**

  - **Desarrollo y Aprobación de Políticas**: Crear y revisar políticas de seguridad, como control de acceso, uso de contraseñas, cifrado de datos, etc.
  - **Implementación de Procedimientos Operativos**: Asegurarse de que los procedimientos de seguridad estén bien documentados y sean accesibles para los colaboradores de la SED.

- **Entrenamiento Continuo**: Proporcionar formación regular sobre seguridad de la información para que todos los colaboradores entiendan y apliquen las políticas y procedimientos.
- **Revisión y Actualización de Políticas**: Establecer un proceso periódico para revisar y actualizar las políticas de seguridad según evoluciona la organización y las amenazas.

➢ **Riesgos**

- **Evaluación de Riesgos**: Identificar, evaluar y clasificar los riesgos relacionados con la seguridad de la información.
- **Análisis de Impacto en el Negocio (BIA)**: Determinar el impacto de la pérdida de información crítica o la interrupción de los servicios.
- **Desarrollo de Planes de Mitigación de Riesgos**: Crear estrategias para mitigar los riesgos identificados, como controles técnicos y operativos.
- **Gestión de Riesgos Residuales**: Monitorear los riesgos que no pueden ser completamente mitigados y asegurar que se gestionen adecuadamente.

➢ **Monitoreo**

- **Monitoreo Continuo de Seguridad**: Establecer herramientas y procesos para monitorear la red, los sistemas y las aplicaciones en busca de posibles amenazas.
- **Auditorías de Seguridad**: Realizar auditorías periódicas para evaluar la eficacia de los controles de seguridad implementados.
- **Monitoreo de Cumplimiento Normativo**: Asegurarse de que la organización cumpla con los requisitos regulatorios y las mejores prácticas de seguridad.
- **Gestión de Incidentes de Seguridad**: Implementar sistemas de alerta temprana y respuesta rápida para gestionar incidentes de seguridad de manera eficiente.

➢ **Mejora Continua**

- **Revisión y Análisis de Desempeño de Seguridad**: Evaluar regularmente los resultados de las políticas y procedimientos de seguridad mediante KPIs (Indicadores Clave de Desempeño).
- **Auditorías Internas y Externas**: Realizar auditorías periódicas para identificar áreas de mejora y asegurar la eficacia de las estrategias de seguridad.

- **Lecciones Aprendidas de Incidentes**: Después de cualquier incidente de seguridad, realizar una evaluación post-mortem para entender las causas y tomar acciones correctivas.
- **Actualización de Herramientas y Tecnologías**: Asegurar que las herramientas de seguridad estén siempre actualizadas con las últimas tecnologías y amenazas emergentes.
- **Capacitación y Sensibilización Continua**: Asegurar que los colaboradores reciban formación continua para estar al tanto de las últimas amenazas y mejores prácticas.

8.1.2 Gestión del riesgo

➢ **Planeación**

- **Desarrollo de la Estrategia de Gestión de Riesgos**: Establecer objetivos, metas y prioridades para la gestión de riesgos en la organización. Definir cómo la organización gestionará y tratará los riesgos en sus procesos.
- **Definición del Alcance y los Límites de la Gestión de Riesgos**: Establecer los límites de los riesgos a gestionar y definir qué áreas o procesos se incluirán en la gestión de riesgos.
- **Asignación de Recursos para la Gestión de Riesgos**: Determinar qué recursos humanos, tecnológicos y financieros se necesitarán para llevar a cabo las actividades de gestión de riesgos.
- **Desarrollo del Plan de Acción de Riesgos**: Crear un plan detallado que describa cómo se identificarán, evaluarán, mitigarán y monitorearán los riesgos.
- **Establecimiento de Roles y Responsabilidades**: Definir claramente quién será responsable de las distintas fases del proceso de gestión de riesgos (por ejemplo, identificar riesgos, evaluarlos, mitigarlos, etc.).

➢ **Políticas y Procedimientos**

- **Desarrollo de Políticas de Gestión de Riesgos**: Redactar y aprobar políticas que guíen cómo la organización abordará la identificación, evaluación, mitigación y monitoreo de riesgos. Las políticas deben incluir el marco de riesgos y las responsabilidades.
- **Elaboración de Procedimientos Operativos**: Documentar procedimientos detallados para la gestión diaria de riesgos. Estos procedimientos deben incluir cómo se deben identificar los riesgos, cómo realizar evaluaciones periódicas y qué hacer en caso de un incidente o riesgo materializado.

- **Implementación de una Metodología para Evaluación de Riesgos**: Establecer una metodología clara y coherente para identificar, evaluar y tratar los riesgos. Esto puede incluir el uso de matrices de riesgos, análisis cualitativos y cuantitativos, etc.
- **Comunicación de Políticas**: Asegurar que todos los colaboradores de la entidad comprendan y apliquen las políticas de gestión de riesgos a través de formación y difusión.

➢ **Riesgos**

- **Identificación de Riesgos**: Realizar actividades periódicas para identificar los riesgos que pueden afectar a la organización.
- **Evaluación de Riesgos**: Utilizar herramientas y técnicas de evaluación de riesgos para valorar la probabilidad e impacto de los riesgos identificados (por ejemplo, matrices de probabilidad e impacto, análisis FODA, etc.).
- **Análisis de Impacto en el Negocio (BIA)**: Evaluar cómo los riesgos potenciales pueden afectar las operaciones y los activos críticos de la organización, priorizando los riesgos según su gravedad y su impacto.
- **Desarrollo de Estrategias de Mitigación de Riesgos**: Definir acciones concretas para reducir o eliminar los riesgos identificados (por ejemplo, la implementación de controles preventivos, la adopción de nuevas tecnologías, etc.).
- **Monitoreo de Riesgos Emergentes**: Mantener una vigilancia activa sobre nuevos riesgos que puedan surgir debido a cambios en el entorno, tecnologías o el mercado.

➢ **Monitoreo**

- **Monitoreo Continuo de Riesgos**: Implementar procesos de monitoreo continuo para evaluar de forma constante los riesgos en los diferentes procesos de la organización, utilizando métricas e indicadores clave de desempeño (KPIs).
- **Evaluación de Efectividad de las Medidas de Mitigación**: Hacer seguimiento de las estrategias de mitigación implementadas para asegurarse de que sean efectivas y que los riesgos estén siendo gestionados adecuadamente.
- **Auditorías y Revisión de Cumplimiento**: Realizar auditorías internas o externas para revisar el cumplimiento de las políticas y procedimientos establecidos y evaluar la eficacia del sistema de gestión de riesgos.

- **Evaluación de Eventos y Lecciones Aprendidas**: Después de cualquier incidente o crisis, llevar a cabo un análisis para identificar las causas y cómo mejorar la gestión futura de riesgos.

➢ **Mejora Continua**

- **Revisión Periódica de la Gestión de Riesgos**: Establecer un ciclo de revisión periódica de las políticas, procedimientos y estrategias de gestión de riesgos para asegurar que sigan siendo pertinentes y efectivas frente a cambios en el entorno y nuevos riesgos.
- **Lecciones Aprendidas de Incidentes y Fallos**: Tras cualquier incidente, realizar sesiones de retroalimentación para aprender de los errores cometidos y hacer ajustes en las políticas o procedimientos para evitar que se repitan.
- **Capacitación y Sensibilización Continua**: Ofrecer programas de capacitación periódicos para que los colaboradores y directivos sean más conscientes de los riesgos y cómo gestionarlos, además de fomentar una cultura organizacional de gestión de riesgos.
- **Actualización de Herramientas de Evaluación y Monitoreo**: Asegurarse de que las herramientas y técnicas utilizadas para la evaluación y el monitoreo de riesgos se mantengan actualizadas y mejoradas conforme surgen nuevas amenazas y tecnologías.
- **Integración con otras Áreas de Gestión**: Alinear y coordinar la gestión de riesgos con otras áreas de la organización (como la gestión de la seguridad, la calidad, la continuidad del negocio, etc.) para una visión global e integrada del riesgo.

8.1.3 Concientización

➢ **Planeación**

- **Desarrollo del Plan de Concientización**: Diseñar un plan estratégico que defina los objetivos, metas y acciones necesarias para aumentar la concientización en seguridad de la información en toda la SED.
- **Definir Públicos Objetivos**: Identificar y segmentar a los distintos grupos dentro de la SED para personalizar el contenido y los enfoques de concientización según sus roles y necesidades.
- **Establecer Recursos y Presupuesto**: Determinar los recursos (humanos, financieros, tecnológicos) necesarios para llevar a cabo las actividades de concientización y establecer un presupuesto adecuado.
- **Planificación de Canales y Herramientas de Comunicación**: Definir qué canales y herramientas se utilizarán para comunicar los mensajes

de concientización, como intranet, correos electrónicos, sesiones presenciales, videos, gamificación, etc.

- **Cronograma de Actividades**: Crear un calendario con las actividades y campañas de concientización a realizar, asegurándose de que haya un flujo constante de mensajes y recursos.

➢ **Políticas y Procedimientos**

- **Desarrollo de Políticas de Seguridad y Concientización**: Establecer políticas que fomenten la responsabilidad en el manejo de la seguridad de la información y promuevan la concientización continua.
- **Procedimientos de Capacitación y Formación**: Crear procedimientos claros para la implementación de programas de formación y concientización, estableciendo los procesos para la evaluación, planificación y seguimiento de estas actividades.
- **Incorporación de Evaluaciones en Políticas**: Definir procedimientos para evaluar regularmente el nivel de concientización y asegurarse de que los colaboradores comprendan y sigan las políticas de seguridad de la información.

➢ **Riesgos**

- **Identificación de Riesgos Relacionados con el Comportamiento Humano**: Identificar los riesgos asociados a la falta de concientización, como el phishing, la filtración accidental de datos, o el uso indebido de dispositivos.
- **Evaluación del Nivel de Concientización**: Realizar encuestas, pruebas de phishing y otros métodos para evaluar el nivel de concientización actual entre los colaboradores y detectar áreas de riesgo.
- **Desarrollo de Estrategias de Mitigación de Riesgos**: Definir e implementar estrategias para reducir los riesgos humanos relacionados con la seguridad de la información, como la capacitación en la detección de amenazas, el fortalecimiento de las políticas de contraseñas, y la promoción de buenas prácticas de seguridad.
- **Simulacros y Pruebas de Seguridad**: Organizar simulacros de incidentes de seguridad, como ataques de phishing, para medir la reacción de los colaboradores y reforzar la importancia de estar alerta ante amenazas.
- **Evaluación de los Impactos de la Falta de Concientización**: Establecer métricas para evaluar cómo la falta de concientización

puede afectar los procesos y activos de la organización, como pérdidas financieras, daño a la reputación o incidentes de seguridad.

- **Monitoreo**

  - **Monitoreo de la Participación en las Actividades de Concientización**: Supervisar la participación en los programas de concientización, como las tasas de finalización de cursos, la asistencia a eventos o la participación en simulacros.
  - **Seguimiento del Comportamiento de los Colaboradores**: Monitorear el comportamiento de los colaboradores en relación con las políticas de seguridad de la información, identificando patrones que puedan indicar falta de comprensión o cumplimiento de las normas.
  - **Evaluación de la Eficacia de los Programas**: Implementar indicadores clave de desempeño (KPIs) para medir el éxito de las campañas de concientización, como la reducción de incidentes de seguridad causados por errores humanos, el aumento en la detección de phishing o la mejora en las encuestas de satisfacción.
  - **Auditorías de Cumplimiento**: Realizar auditorías internas para asegurar que los colaboradores están cumpliendo con las políticas de seguridad y que están aplicando correctamente las prácticas aprendidas en las actividades de concientización.
  - **Retroalimentación y Encuestas de Seguimiento**: Realizar encuestas regulares para obtener retroalimentación sobre la efectividad de los programas y áreas donde aún pueda haber confusión o resistencia.

- **Mejora Continua**

  - **Revisión Periódica de las Iniciativas de Concientización**: Evaluar de forma continua las iniciativas de concientización, analizando qué está funcionando y qué no, y haciendo ajustes para mejorar la efectividad de los programas.
  - **Actualización de Contenidos de Formación**: Asegurarse de que los materiales de formación se mantengan actualizados con las últimas amenazas y tendencias en ciberseguridad. Esto incluye el uso de nuevos enfoques como gamificación o aprendizaje interactivo.
  - **Adaptación a Nuevas Amenazas y Cambios Organizacionales**: Ajustar las estrategias de concientización según evolucionen los riesgos y amenazas en el panorama de seguridad, y también conforme la organización cambie (incorporación de nuevas tecnologías, procesos, o políticas).

- **Análisis de Tendencias de Incidentes**: Revisar los incidentes de seguridad recurrentes para identificar si son causados por falta de concientización y tomar medidas correctivas en los programas de formación.
- **Fomentar una Cultura de Seguridad a Largo Plazo**: Promover una cultura organizacional que valore la seguridad de la información de forma continua, alentando la participación de todos los colaboradores en mantener prácticas seguras en el día a día.

8.1.4 Implementación de controles

➢ **Planeación**

- **Desarrollo del Plan de Implementación de Controles**: Establecer un plan detallado que defina los tipos de controles necesarios (preventivos, detectivos, correctivos) y la forma en que serán implementados, alineados con los objetivos de seguridad de la información y la gestión de riesgos.
- **Definición de Objetivos de los Controles**: Establecer los objetivos específicos de los controles, como la protección de datos confidenciales, la prevención de accesos no autorizados, la detección de intrusiones, etc.
- **Identificación de Recursos Necesarios**: Determinar los recursos necesarios para implementar los controles, incluyendo personal capacitado, herramientas tecnológicas y presupuesto.
- **Priorización de Controles**: Evaluar y priorizar los controles según el nivel de riesgo y el impacto potencial de las amenazas en la organización. Esto puede hacerse a través de una evaluación de riesgos que identifique qué controles son más urgentes.
- **Planificación de la Implementación en Etapas**: Definir un cronograma para la implementación de los controles, organizando la ejecución por fases o etapas si es necesario, para facilitar su integración con los procesos existentes.

➢ **Políticas y Procedimientos**

- **Desarrollo de Políticas de Seguridad para la Implementación de Controles**: Crear políticas que definan claramente los controles a implementar, así como los procedimientos relacionados. Esto incluye políticas sobre la gestión de acceso, protección de datos, seguridad de la red, control de cambios, etc.
- **Desarrollo de Procedimientos Operativos**: Elaborar procedimientos detallados sobre cómo los controles se implementarán en el día a día.

Estos procedimientos deben ser claros, accesibles y aplicables a diferentes equipos de la organización (TI, RRHH, Finanzas, etc.).

- **Establecimiento de Criterios de Éxito y Evaluación**: Definir los criterios mediante los cuales se evaluará la efectividad de los controles implementados. Estos criterios pueden incluir la reducción de incidentes de seguridad, la mejora en tiempos de respuesta a incidentes, o el cumplimiento de normativas.
- **Desarrollo de Procedimientos de Auditoría**: Crear procedimientos que aseguren que los controles se auditen periódicamente para verificar su funcionamiento y cumplimiento con las políticas de seguridad.

➢ **Riesgos**

- **Evaluación de Riesgos y Necesidad de Controles**: Realizar una evaluación de riesgos detallada para identificar áreas clave donde se necesiten controles específicos. Identificación de activos críticos, vulnerabilidades, amenazas y el impacto de posibles incidentes.
- **Implementación de Controles para Mitigar Riesgos Identificados**: Asegurarse de que los controles seleccionados estén alineados con los riesgos prioritarios identificados en la evaluación. Implementar controles de acceso para mitigar el riesgo de accesos no autorizados.
- **Priorización de Controles en Función de los Riesgos**: Priorizar la implementación de controles basándose en el nivel de riesgo, comenzando con aquellos controles que mitiguen los riesgos más altos o aquellos que tienen un mayor impacto en la organización.
- **Establecer Controles de Contingencia**: Desarrollar controles para la gestión de riesgos residuales (aquellos que no pueden ser completamente mitigados), como planes de contingencia y recuperación ante desastres.

➢ **Monitoreo**

- **Monitoreo Continuo de la Eficacia de los Controles**: Establecer sistemas para monitorear de manera continua la efectividad de los controles implementados. Incluir herramientas de detección de intrusos, monitoreo de accesos a sistemas, auditorías de seguridad, etc.
- **Auditorías Periódicas de Controles**: Realizar auditorías regulares para evaluar el cumplimiento de las políticas de seguridad y la efectividad de los controles. Incluir auditorías internas o externas y revisiones de sistemas de control de acceso, protección de datos, etc.

- **Pruebas de Control y Simulacros**: Llevar a cabo simulacros y pruebas de los controles para asegurar que respondan adecuadamente en situaciones de estrés o crisis, como ataques de phishing, incidentes de violación de datos, o desastres naturales.
- **Monitoreo de Cumplimiento de Normativas y Estándares**: Asegurarse de que los controles implementados cumplen con las normativas, estándares y regulaciones aplicables (como ISO 27001, GDPR, PCI-DSS, etc.), y realizar seguimiento de cualquier cambio en los requisitos legales.

➢ **Mejora Continua**

- **Revisión Periódica de los Controles Implementados**: Establecer un ciclo de revisión periódica de los controles de seguridad para asegurarse de que siguen siendo relevantes y efectivos frente a los riesgos actuales y emergentes.
- **Análisis de Incidentes y Lecciones Aprendidas**: Después de un incidente de seguridad o vulnerabilidad, analizar cómo los controles respondieron y si hubo fallos en su implementación o cobertura. Aplicar las lecciones aprendidas para mejorar los controles y prevenir futuros incidentes.
- **Ajustes Basados en el Desempeño**: Usar métricas e indicadores para evaluar el desempeño de los controles y hacer ajustes cuando sea necesario. Por ejemplo, si un control no está funcionando como se esperaba, investigar sus causas y realizar cambios en la estrategia o las herramientas utilizadas.
- **Capacitación y Sensibilización Continuas sobre Controles**: Asegurar que los colaboradores y personal clave reciban formación continua sobre el uso y la importancia de los controles implementados, para garantizar su cumplimiento y eficacia.
- **Evaluación de Nuevas Tecnologías y Técnicas de Control**: Mantenerse actualizado sobre nuevas tecnologías y metodologías de control que puedan mejorar la protección de la información, como la adopción de nuevas soluciones de ciberseguridad, automatización de procesos de control, o inteligencia artificial aplicada a la seguridad.

8.1.5 Gestión de incidentes

➢ **Planeación**

- **Desarrollo del Plan de Respuesta a Incidentes**: Crear un plan estructurado que detalle cómo la organización identificará, responderá y recuperará ante incidentes de seguridad. Este plan debe incluir las

fases de preparación, identificación, contención, erradicación, recuperación y lecciones aprendidas.

- **Definición de Roles y Responsabilidades**: Establecer claramente los roles y responsabilidades del personal involucrado en la gestión de incidentes. Definir quién será el responsable de la coordinación general, la comunicación, la investigación técnica y la toma de decisiones.
- **Priorización de Tipos de Incidentes**: Clasificar los posibles incidentes según su gravedad y prioridad. Identificar qué tipos de incidentes (violación de datos, ataques DDoS, malware, etc.) requieren una respuesta inmediata y qué otros pueden ser tratados con un enfoque diferente.
- **Planificación de Recursos y Herramientas**: Identificar los recursos tecnológicos, humanos y financieros necesarios para gestionar eficazmente los incidentes. Definir herramientas de monitoreo, software de gestión de incidentes y equipos de respuesta.
- **Desarrollo de Canales de Comunicación**: Establecer canales de comunicación claros para la notificación de incidentes, tanto internamente como con partes externas, como proveedores de servicios o autoridades regulatorias, en caso de incidentes graves.

➢ **Políticas y Procedimientos**

- **Elaboración de Políticas de Gestión de Incidentes**: Redactar políticas que establezcan los procedimientos estándar para gestionar los incidentes de seguridad. Las políticas deben definir cómo se clasifican los incidentes, los protocolos de respuesta y las expectativas de tiempo de respuesta.
- **Desarrollo de Procedimientos Operativos**: Crear procedimientos detallados para cada fase del ciclo de vida de un incidente. Los procedimientos deben ser claros y prácticos, asegurando que todo el personal conozca las acciones a seguir en caso de un incidente.
- **Integración de Políticas de Comunicación**: Desarrollar políticas sobre cómo se deben comunicar los incidentes tanto interna como externamente. Divulgar la información a los colaboradores, partes interesadas, autoridades legales y públicos, si fuera necesario.
- **Procedimientos de Escalación**: Definir y documentar los procedimientos para escalar incidentes de seguridad según su gravedad. Elevar un incidente de bajo impacto a uno de mayor nivel, o cómo coordinar la respuesta con otros equipos o proveedores externos.

- **Riesgos**

    - **Evaluación de Riesgos Relacionados con Incidentes**: Identificar y evaluar los riesgos que pueden generar incidentes de seguridad, tales como fallos de infraestructura, errores humanos, ataques externos, etc. Priorizar los incidentes con mayor probabilidad o impacto.
    - **Análisis de Impacto en el Negocio (BIA)**: Evaluar cómo diferentes tipos de incidentes afectarán a los activos críticos y las operaciones de negocio. Asegurar que el plan de respuesta a incidentes contemple estos impactos y cómo mitigarlos de manera efectiva.
    - **Desarrollo de Estrategias de Mitigación**: Implementar controles preventivos y estrategias para reducir la probabilidad de incidentes. Implementar sistemas de detección de intrusos, actualizaciones de seguridad, capacitación de colaboradores, etc.
    - **Gestión de Riesgos Residuales**: Identificar los riesgos que no pueden ser completamente eliminados, asegurando que haya estrategias de respuesta a incidentes bien definidas para gestionarlos de manera adecuada si ocurren.

- **Monitoreo**

    - **Monitoreo Continuo de Seguridad**: Implementar sistemas y herramientas para el monitoreo proactivo de la infraestructura y redes de la organización en busca de señales de incidentes, como actividades inusuales o vulnerabilidades que podrían ser explotadas.
    - **Alertas y Notificaciones**: Configurar alertas automáticas para detectar incidentes a medida que ocurren. Las alertas deben ser claras y contener suficiente información para iniciar una investigación sin demora.
    - **Análisis Forense en Tiempo Real**: Cuando se detecte un incidente, realizar un análisis forense para determinar el alcance del evento, cómo ocurrió, y qué activos fueron afectados.
    - **Monitoreo de KPIs de Incidentes**: Establecer indicadores clave de desempeño (KPIs) para medir la efectividad de la gestión de incidentes, como el tiempo de respuesta, el tiempo de recuperación y el impacto financiero de los incidentes.

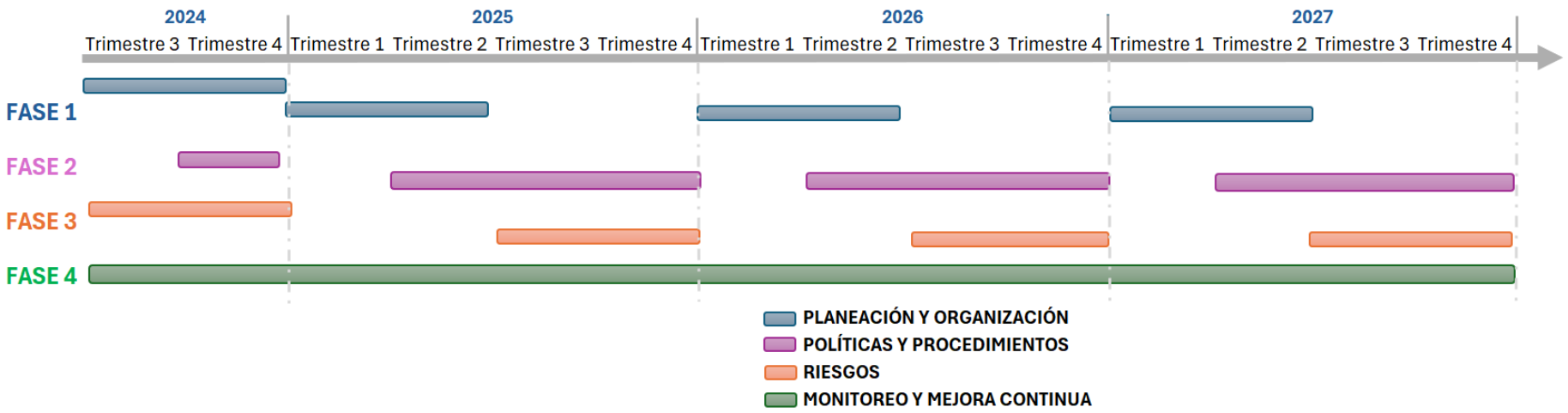
- **Mejora Continua**

    - **Análisis Post-Mortem y Lecciones Aprendidas**: Después de cada incidente, realizar un análisis exhaustivo para determinar qué salió bien y qué se puede mejorar. Las lecciones aprendidas deben ser documentadas y comunicadas a los equipos responsables.

- **Actualización de Políticas y Procedimientos**: Usar las lecciones aprendidas para actualizar las políticas y procedimientos de gestión de incidentes. Esto asegura que la organización esté mejor preparada para futuros incidentes.
- **Entrenamiento Continuo**: Asegurar que los equipos involucrados en la gestión de incidentes reciban formación regular sobre las mejores prácticas, nuevas amenazas y tecnologías emergentes. Incluir simulacros de incidentes para practicar la respuesta en situaciones reales.
- **Evaluación de Herramientas y Tecnología de Gestión de Incidentes**: Realizar una revisión continua de las herramientas y tecnologías utilizadas para la gestión de incidentes. Asegurar que sean adecuadas para detectar, mitigar y responder a incidentes con rapidez.
- **Mejora de los Procesos de Respuesta**: Asegurar que los procesos de respuesta a incidentes sean más ágiles y eficaces a medida que la organización aprende y adapta sus tácticas y estrategias. Simplificar procedimientos, automatizar ciertos pasos o implementar nuevas tecnologías.
- **Auditorías y Revisiones Periódicas**: Realizar auditorías periódicas de la efectividad del proceso de gestión de incidentes, verificando la correcta implementación de controles, la velocidad de respuesta, y la coherencia de los procedimientos.

8.2. Cronograma

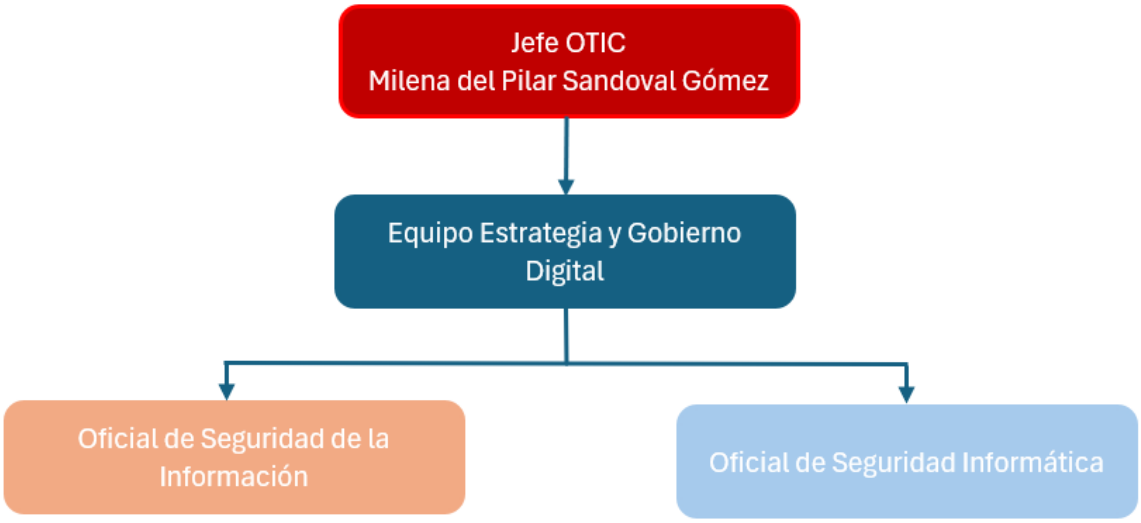
El equipo de Estrategia y Gobierno Digital, a través del Oficial responsable de la seguridad y privacidad de la información, así como del tratamiento de riesgos identificados, deberá hacer seguimiento de la implementación y cumplimiento del cronograma de actividades propuestos durante la vigencia 2024 – 2027.


2024
2025
2026
2027
Trimestre 3 Trimestre 4 Trimestre 1 Trimestre 2 Trimestre 3 Trimestre 4 Trimestre 1 Trimestre 2 Trimestre 3 Trimestre 4 Trimestre 1 Trimestre 2 Trimestre 3 Trimestre 4
FASE 1
FASE 2
FASE 3
FASE 4
PLANEACIÓN Y ORGANIZACIÓN
POLÍTICAS Y PROCEDIMIENTOS
RIESGOS
MONITOREO Y MEJORA CONTINUA

9. RESPONSABLES DE LA SEGURIDAD

La Oficina de las Tecnologías de la Información y las Comunicaciones –OTIC- de la Secretaría de Educación del Distrito (SED) conformada mediante Decreto 310 del 29 de julio 2022, "*Por el cual se modifica la estructura organizacional y las funciones de la Secretarla de Educación del Distrito*", en su compromiso con el cierre de la brecha digital y el apoyo a los procesos Administrativos a través del uso de las TIC a nivel central, local e institucional, tiene la responsabilidad de brindar los servicios de acceso a Internet y la disponibilidad de cada una de las aplicaciones web de uso interno y externo de la SED así como el de proteger el acceso a la información y los servicios informáticos entregados y usados por la Entidad.

Por lo anterior, el equipo que se muestra a continuación será el encargo de liderar la implementación del Plan Estratégico de Seguridad y Privacidad de la Información -PESI- de la Entidad:



FUNCIONES Y/O ACTIVIDADES	RESPONSABLE
• Coordinar la implementación del Plan Estratégico de Seguridad y Privacidad de la Información enmarcado en la seguridad y los lineamientos del MSPI	Jefe Oficina de Tecnologías de la Información y las Comunicaciones

FUNCIONES Y/O ACTIVIDADES	RESPONSABLE
• Implementación de buenas prácticas para la protección de datos. • Proyectar, actualizar y dar cumplimiento a las políticas y procedimientos para la protección de datos. • Dar respuesta a los titulares de los datos cuando existan requerimientos. • Registrar las bases de datos de la entidad ante la SIC. • Coordinar y monitorear los sistemas de interoperabilidad para el uso y tratamiento de los datos personales.	Oficial de datos (OTIC)
• Gestionar estrategias para la seguridad de la información. • Proyectar, actualizar y dar cumplimiento a las políticas y procedimientos para la seguridad de la información. • Identificar y gestionar riesgos de seguridad. Crear y difundir los planes de campaña de sensibilización en la entidad. • Medir el nivel de madurez de la entidad frente a la implementación de los controles definidos en la norma ISO 27001:2022. • Coordinar los equipos de seguridad. • Desarrollar, implementar y supervisar las políticas enfocadas en riesgos digitales. • Realizar el levantamiento de los activos de información.	Oficial de Seguridad de la Información (Equipo de Estrategia y Gobierno Digital)
• Desarrollar, implementar y supervisar las políticas de ciberseguridad. • Coordinar el equipo de ciberseguridad. • Monitorear los permisos, identidades y recursos a nivel de infraestructura. • Aseguramiento de las aplicaciones, garantizar la seguridad desde el diseño hasta su paso a producción. • Realizar el tratamiento de riesgos de los activos de información. • Campañas de sensibilización en identificación de riesgos digitales.	Oficial de Seguridad Informática (Equipo de Estrategia y Gobierno Digital)

10. MESAS TÉCNICAS DE GOBIERNO Y SEGURIDAD DIGITAL

Las mesas técnicas que se llevaran a cabo por el grupo responsable de coordinar, monitorear y supervisar la implementación del PESI, asegurando que exista un apoyo gerencial y compromiso de la alta dirección, que garantice el desarrollo de las propuestas e iniciativas en materia de seguridad de la información para la SED.

De acuerdo con la resolución No 001 del 14 de julio de 2025, el equipo técnico de las políticas Gobierno Digital y Seguridad Digital a cargo de la Oficina de Tecnologías de la Información y las Comunicaciones, el cual estará conformado por:

- ✓ El(la) jefe de la Oficina de Tecnologías de la Información y las Comunicaciones o su delegado (a)
- ✓ El (la) jefe de la Oficina Asesora de Planeación o su delegado
- ✓ El (la) jefe de la Oficina Asesora de Comunicaciones Prensa o su delegado.

11. PRESUPUESTO

Teniendo en cuenta lo definido en las estrategias, los planes y las metas a través del cronograma de actividades, se deberá contar con un presupuesto mínimo a lo largo de la vigencia, el cual deberá contar con las actualizaciones y correcciones, a que hayan lugar, para mantener el Plan Estratégico alineado a su misionalidad, esto, podrá sufrir cambios o adiciones en cada línea de servicio (componente) propuesto debido a las actualizaciones tecnológicas y/o necesidades de la SED, así como también el presupuesto estará sujeto de acuerdo a la disponibilidad presupuestal de cada año durante su vigencia.

Línea de Servicio	Nombre	2024	2025	2026	2027
INFRAESTRUCTURA	LICENCIAMIENTOS Y SOPORTE SEGURIDAD PERIMETRAL	$ 1.608.402.000	$ 2.100.000.000	$2.741.477.244	$ 2.561.732.023
	PROYECTO DRP	$ 1.453.824.309	Por establecer	Por establecer	Por establecer
total		$ 3.062.226.309	$ -	$ -	$ -
HERRAMIENTAS DE CIBERSEGURIDAD PROPUESTAS	GESTOR DE VULNERABILIDADES	$ -	$ -	$ -	Por establecer
	SIEM (Gestión de Información y Eventos de Seguridad)	$ -	$ -	$ -	Por establecer
	XDR (Detección y Respuesta Ampliadas)	$ -	$ -	$ -	Por establecer
total		$ -	$ -	$ -	$ -

12. REVISIONES

El Plan Estratégico de Seguridad y Privacidad de la Información – PESI, de la Secretaría de Educación del Distrito, tendrá revisiones periódicas y se realizaran actualizaciones pertinentes, siguiendo las políticas de Gobierno y Seguridad Digital.

CONTROL DE CAMBIOS

Versión	Fecha	Elaborado Por	Revisado Por	Aprobó	Descripción
V.1.0	28/01/2025	Henry Alexander Moyan Montenegro	Jairo Alberto Orduz Salamanca	Milena del Pilar Sandoval Gómez	Creación PESI
V.2.0	27/01/2026	Henry Alexander Moyan Montenegro	Jasson Smith Castro León	Milena del Pilar Sandoval Gómez	Actualización PESI

Firma:

Aprobado por: MILENA DEL PILAR SANDOVAL GOMEZ
Jefe Oficina de Tecnologías de la información y las Comunicaciones-OTIC

Elaborado: Henry Alexander Moyan Montenegro - Profesional Contratista Oficina OTIC

Revisado: Jasson Smith Castro León - Profesional Especializado Oficina OTIC