ALCALDÍA MAYOR
DE BOGOTÁ D.C.
DESARROLLO ECONÓMICO
Instituto para la Economía Social

IPES

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

SUBDIRECCIÓN DE DISEÑO Y ANÁLISIS ESTRATÉGICO

BOGOTÁ, ENERO 2026

Elaboró	Revisó:	Aprobó:
Rebeca González Bravo - Contratista SDAE Daniel Ernesto Fragoso Amariz - Profesional Especializado SDAE	Edgar Mauricio Mera Erazo – Contratista SDAE	Adriana Villamizar Navarro Subdirectora de Diseño y Análisis Estratégico

CONTENIDO

1. INTRODUCCIÓN 3
2. OBJETIVO 3
3. ALCANCE 3
4. RESPONSABLES 4
5. DEFINICIONES Y ABREVIATURAS 5
6. DESARROLLO 7
6.1. METODOLOGÍA 7
6.2. ACTIVIDADES E INDICADORES 9
6.2.1. Explicación de contenido actualizado 13
6.3. MONITOREO, SEGUIMIENTO Y EVALUACIÓN 14
6.3.1. Evaluación 14
6.3.2. Monitoreo y Seguimiento 15
6.4. RECURSOS 15
6.5. PRESUPUESTO 15
6.6. MEDICIÓN 15
7. MARCO NORMATIVO 17
8. DOCUMENTOS ASOCIADOS 17
9. CONTROL DE CAMBIOS 17

1. INTRODUCCIÓN

Reservar la seguridad de la información es un tema que se vuelve cada día más complejo y crítico debido al uso y masificación de las tecnologías de información y las comunicaciones en las organizaciones, por esto es prioritario para el Instituto para la Economía Social - IPES definir y adoptar prácticas integradas a sus procesos y operaciones, las cuales funcionan como estrategias para reducir o mitigar los riesgos de seguridad digital a los cuales se encuentran expuestos sus activos de información.

En el actual ecosistema digital, la preservación de la seguridad de la información ha trascendido de ser un requisito técnico a convertirse en un imperativo estratégico de alta complejidad. Ante un panorama de amenazas dinámico —caracterizado por la sofisticación de vectores de ataque como el ransomware dirigido y las Amenazas Persistentes Avanzadas (APT)—, sumado a la disolución de los perímetros tradicionales por la adopción de modelos de trabajo híbridos y la migración a la nube, el Instituto para la Economía Social (IPES) reconoce la urgencia de evolucionar su postura de ciberseguridad.

Este Plan de Tratamiento de Riesgos se establece como el instrumento rector para definir y adoptar controles integrales que fortalezcan nuestra resiliencia organizacional. Su propósito es salvaguardar los activos de información críticos, garantizando proactivamente la Confidencialidad, Integridad y Disponibilidad (CID) de los datos. Más allá del cumplimiento, este plan busca blindar la operación del IPES, asegurando la continuidad del negocio y la confianza digital necesaria para el cumplimiento exitoso de nuestra misionalidad institucional

El Instituto mantiene la confidencialidad, integridad, y disponibilidad de los activos de información, mediante un enfoque basado en riesgos y cuyo proceso es tomado como un componente importante para el gobierno corporativo, toma de decisiones, logro de los objetivos estratégicos y cumplimiento de su misionalidad.

Un componente fundamental desde la planificación del Sistema de Gestión de Seguridad de la Información y del proceso de identificación, análisis y evaluación de riesgos de seguridad digital, es la definición e implementación de un plan de tratamiento a estos riesgos, en el cual se determina implementar herramientas, sistemas, políticas, procedimientos, prácticas o mecanismos dinámicos y seguros que protejan la información y la infraestructura tecnológica que la soporta.

2. OBJETIVO

Contribuir al cumplimiento de los objetivos estratégicos, la visión institucional y los requisitos legales y reglamentarios, garantizando la seguridad digital, la privacidad de los datos y la protección del patrimonio público. Esto se logrará mediante la gestión integral de riesgos de seguridad, la priorización de la Infraestructura, y el fortalecimiento de capacidades que permitan medir la efectividad de los controles para asegurar un entorno digital confiable y seguro."

3. ALCANCE

El plan de tratamiento de riesgos definido en este documento, pretende realizar una eficiente gestión de riesgos de Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación, que permita integrar en los procesos de la entidad, buenas

prácticas que contribuyan a la toma de decisiones y prevenir incidentes que puedan afectar el logro de los objetivos. El plan de tratamiento de riesgos definido en este documento, aplica para los riesgos de seguridad digital identificados para el proceso de apoyo Gestión de Seguridad de la Información y Recursos Tecnológicos del Instituto para la Economía Social – IPES, cuyo nivel de riesgo se encuentren en las zonas “Extremo”, “Alto”, “Moderado” y “Bajo”.

Este plan se encuentra en el marco de las directrices dadas en la dimensión Gestión con Valores para Resultado de MIPG, y las políticas de Gobierno Digital y Seguridad Digital.

De conformidad con los lineamientos de la Política de Gobierno Digital y el Documento Maestro del MSPI (MinTIC V5), el presente plan priorizará las acciones de tratamiento de riesgos, implementación de controles y monitoreo sobre aquellos activos identificados y clasificados como Infraestructura Crítica Cibernética (ICC) y aquellos que soportan la operación de Servicios Esenciales de la entidad. Se garantizará la aplicación de controles de ciberseguridad específicos para estos activos críticos con el fin de asegurar la resiliencia organizacional, prevenir la interrupción de las funciones misionales y minimizar el impacto social y económico ante posibles incidentes de seguridad digital

4. RESPONSABLES

Responsable	Rol o Actividad a desarrollar
Oficial de Seguridad de la Información	Coordinar el proceso de gestión de riesgos de seguridad digital y privacidad, asegurando la alineación del Plan de Tratamiento de Riesgos (PTR) con los objetivos estratégicos de la entidad y el marco normativo vigente.
	Monitorear la implementación efectiva de los controles de seguridad (administrativos y técnicos) definidos por los líderes de proceso y brindar asesoría técnica sobre los controles del Anexo A (ISO 27001) para la mitigación de riesgos.
	Informar periódicamente al Comité de Sistemas y Seguridad de la Información sobre el estado de los riesgos críticos, la efectividad del plan de tratamiento y los incidentes materializados que afecten el perfil de riesgo de la entidad.
Subdirección de Diseño y Análisis Estratégico	Liderar el desarrollo e implementación del Sistema Integrado de Gestión se encargará de revisar y adecuar la metodología para la administración de los riesgos propuesta por el Departamento Administrativo de la Función Pública, a las necesidades del IPES, también brindará la asesoría y las herramientas a los procesos para la correcta identificación y valoración de riesgos en la entidad.
	Brindar acompañamiento en el desarrollo e implementación del proceso de administración de los riesgos de seguridad digital, este deberá recoger iniciativas, responsabilidades y armonizar los diferentes ejercicios para la implementación de un proceso más efectivo.

	Recoger iniciativas, responsabilidades y armonizar los diferentes ejercicios para la implementación de la metodología de Administración del Riesgo. A través de los referentes de los diferentes procesos se diligenciará el PA08-MR-001 Mapa de Riesgos con el fin de registrar la gestión adelantada, así como la revisión, seguimiento y monitoreo a los riesgos y su plan de tratamiento.
Equipo de seguimiento y evaluación (conformado por el/la Asesor/a de Control Interno, los servidores públicos y contratistas de su oficina asesora)	Velar por la adecuada elaboración e implementación del mapa de riesgos de cada proceso, promoviendo su apropiación, entendimiento y evaluación del mismo.
	Implementar las acciones definidas para tratar, reducir o mitigar los riesgos de seguridad digital, se encuentran relacionados en el plan de tratamiento de cada riesgo.
	Cumplimiento de los lineamientos para la administración del riesgo de seguridad digital de la Entidad.
	Utilizar la metodología propuesta por el Departamento Administrativo de la Función Pública “Guía para la administración del riesgo y el diseño de controles en entidades públicas V6 – 2022.
	Utilizar la Herramienta PA08-MR-001 Mapa de Riesgos para el registro del proceso de administración del riesgo.
	Utilizar el instructivo “Gestión de riesgos de seguridad digital" del IPES.

5. DEFINICIONES Y ABREVIATURAS

- **Acceso a la Información Pública:** Derecho a conocer y acceder a información pública.
- **Activo:** Elementos usados por la organización en el entorno digital.
- **Activo de información:** Conocimiento o datos valiosos para la entidad.
- **Amenaza:** Situación que puede causar daño a un sistema.
- **Análisis de Riesgo:** Proceso para determinar el nivel de riesgo.
- **Archivo:** Conjunto de documentos acumulados como testimonio o información.
- **Auditoría:** Proceso para evaluar el cumplimiento de criterios establecidos.
- **Autorización:** Consentimiento para el tratamiento de datos personales.
- **Bases de Datos Personales:** Conjunto organizado de datos personales.
- **Causas:** Factores que pueden provocar riesgos.
- **Ciberespacio:** Ambiente físico y virtual de interacción digital.
- **Ciberseguridad:** Capacidad de minimizar riesgos cibernéticos.
- **Confidencialidad:** Propiedad que limita el acceso no autorizado a la información. **Consecuencia:** Efecto de la materialización de un riesgo.

- **Control:** Medida para mitigar riesgos.
- **Datos Abiertos:** Datos accesibles y reutilizables por cualquier ciudadano.
- **Datos Personales:** Información vinculada a una persona natural.
- **Datos Personales Privados:** Información íntima relevante sólo para el titular
- **Datos Personales Públicos:** Datos accesibles como el estado civil o profesión
- **Datos Personales Sensibles:** Información que puede afectar la intimidad o generar discriminación.
- **Derecho a la intimidad:** Derecho a una esfera privada libre de intervenciones.
- **Disponibilidad:** Propiedad de ser accesible cuando se requiera.
- **Encargado del Tratamiento de Datos:** Persona que gestiona datos por cuenta del responsable.
- **Evaluación del riesgo:** Comparación de riesgos frente a controles.
- **Gestión de incidentes de seguridad de la información:** Procesos para manejar incidentes de seguridad.
- **Gestión del riesgo:** Proceso para garantizar el logro de objetivos ante riesgos. **Identificación del riesgo:** Determinación de fuentes y consecuencias de riesgos.
- **Impacto: Consecuencia de la materialización de un riesgo.**
- **Información Pública Clasificada:** Información protegida por requisitos legales
- **Información Pública Reservada:** Información cuyo acceso puede ser restringido. **Integridad:** Propiedad de exactitud y completitud de la información.
- **Mapa de riesgos:** Documento que organiza los riesgos identificados.
- **Plan de tratamiento de riesgos:** Documento con acciones para mitigar riesgos.
- **Política de administración de riesgos:** Declaración sobre cómo gestionar riesgos. **Privacidad: Derecho a proteger datos personales y clasificados.**
- **Probabilidad:** Posibilidad de que un riesgo se materialice.
- **Riesgo de seguridad digital:** Combinación de amenazas y vulnerabilidades digitales.
- **Riesgo inherente:** Riesgo presente sin medidas de mitigación.
- **Riesgo residual:** Riesgo que queda tras aplicar controles.
- **Seguridad de la información:** Protección de la confidencialidad, integridad y disponibilidad.
- **Tolerancia al riesgo:** Nivel aceptable de riesgo para cumplir objetivos.
- **Tratamiento del riesgo:** Respuesta para reducir riesgos.
- **Valoración de riesgos:** Estimación de probabilidad e impacto del riesgo
- **Vulnerabilidad:** Falencia en tecnología, personas o procedimientos.

6. DESARROLLO

6.1. METODOLOGÍA

Para la definición del plan de tratamiento de riesgos de seguridad digital se señalan las actividades desarrolladas previamente:

- Comprensión del contexto.
- Identificación del riesgo.
- Análisis del riesgo inherente:

Para este paso, la entidad adopta las escalas de valoración de 5 niveles propuestas por el DAFP:

TABLA DE PROBABILIDAD

Nivel	Descriptor	Criterio de Frecuencia / Probabilidad	Valor
5	Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 5.000 veces al año. O es casi seguro que el evento ocurra en la mayoría de las circunstancias.	100%
4	Alta	La actividad se ejecuta entre 500 y 5.000 veces al año. O es probable que el evento ocurra en la mayoría de las circunstancias.	80%
3	Media	La actividad se ejecuta entre 24 y 500 veces al año. O el evento podría ocurrir en algún momento.	60%
2	Baja	La actividad se ejecuta entre 3 y 24 veces al año. O el evento puede ocurrir en algún momento.	40%
1	Muy Baja	La actividad se ejecuta máximo 2 veces por año. O el evento puede ocurrir solo en circunstancias excepcionales (rara vez).	20%

TABLA DE IMPACTO

Nivel	Descriptor	Criterio Económico / Reputacional	Valor
5	Catastrófico	Mayor a 500 SMLMV. Afectación de imagen a nivel nacional con efecto sostenido.	100%

4	Mayor	Entre 100 y 500 SMLMV. Afectación de imagen a nivel de sector administrativo, departamental o municipal.	80%
3	Moderado	Entre 50 y 100 SMLMV. Afecta la imagen con usuarios relevantes.	60%
2	Menor	Entre 10 y 50 SMLMV. Conocimiento interno, junta directiva o proveedores.	40%
1	Leve	Menor a 10 SMLMV. Afecta la imagen solo de un área interna.	20%

- Evaluación del riesgo.
- Definición de controles existentes.
- Análisis del riesgo residual.
- Selección de la opción de tratamiento del riesgo.
- Definición del plan de tratamiento.

El Instituto para la Economía Social - IPES se encuentra trabajando en la implementación del Sistema de Gestión de Seguridad de la Información - SGSI, y en su integración al Sistema Integrado de Gestión, por lo tanto, los riesgos identificados son los que pueden afectar la disponibilidad, integridad y confidencialidad de la información y las acciones definidas contribuyen a la preservación de estos principios de seguridad de la información. Las medidas que se implementarán serán comparadas con los controles del Anexo A de la NTC-ISO/IEC 27001:2013 a fin que no sean omitidos controles necesarios.

En el plan de tratamiento se determinan los siguientes ítems:

- **Opciones de manejo:** El propósito de esta etapa es seleccionar e implementar opciones o estrategias para abordar el riesgo y con base en ella diseñar las acciones a aplicar. Las opciones para el tratamiento de los riesgos son:
  - **Reducir el riesgo** mediante la aplicación de controles apropiados de manera que el riesgo residual se pueda reevaluar como aceptable.
  - **Asumir el riesgo** significa que se reconoce la exposición a la pérdida, pero no se toman acciones relativas a un riesgo en particular y la pérdida es aceptada, en caso de que ocurra.
  - **Evitar el riesgo** la acción que da origen al riesgo particular.
  - **Compartir o transferir el riesgo** a entidades como aseguradoras o proveedores que puedan gestionar de manera eficaz el riesgo particular, siempre que no resulte un costo superior al del riesgo mismo.
  - Los riesgos de corrupción no pueden ser aceptados conforme a los lineamientos del DAFP

- **Acción para tratar el riesgo:** Describir las medidas o controles a implementar con el fin de lograr el tratamiento del riesgo.
- **Soporte:** Relaciona la evidencia que soportará el cumplimiento de la acción definida para tratar el riesgo.

- **Documentos asociados al control:** Describen los documentos existentes y que de alguna manera se relacionan con la implementación del control.
- **Responsable:** Proceso o rol encargado de la implementación y ejecución de las acciones que tratarán el riesgo.
- **Tiempo de ejecución:** Fechas de inicio y terminación de la implementación de las acciones.
- **Indicador**: Relaciona las métricas que miden la implementación de la acción.

El plan del tratamiento del riesgo se registra en las columnas “Plan de tratamiento de riesgos” del Formato Mapa de Riesgos.

6.2. ACTIVIDADES E INDICADORES

LINEAMIENTOS ESTRATEGICOS							
Actividad	**Tareas**	**Responsable**	**Indicador**	**Meta**	**Productos**	**Fecha Inicio**	**Fecha Final**
Actualización Metodológica	Revisar y actualizar la Política y Metodología de Administración del Riesgo para integrar lineamientos de Seguridad Digital,	Subdirección de Diseño y Análisis Estratégico (SDAE)	Número documentos estratégicos de lineamientos para la administración del riesgo actualizados	3	Política de Administración del Riesgo, Metodología y Formato de Mapa de Riesgos publicados	01/03/2026	22/03/2026
CULTURA DE RIESGOS							
Capacitación y Sensibilización	Socialización y entrenamiento a los encargados y líderes de proceso sobre la identificación y valoración de riesgos de seguridad digital	Profesional en Seguridad de la Información (SDAE)	Porcentaje de implementación del plan de formación y sensibilización	100%	Registros de asistencia y material de capacitación (Plan de formación)	22/02/2026 -	22/11/2026
VALORACIÓN DE RIESGOS (CICLO PHVA)							
Identificación y Análisis	Identificar activos, amenazas y vulnerabilidades. Analizar probabilidad e impacto para determinar el riesgo	Líderes de procesos / SDAE	Porcentaje de implementación del Proceso de administración de riesgos de seguridad digital	100%	Matriz de riesgos de seguridad digital por proceso (Mapa de Riesgos)	01/03/2026	28/09/2026

	inherente en todos los procesos						
Definición del Plan de Tratamiento:	Seleccionar controles (Anexo A ISO 27001) para mitigar, transferir, evitar o aceptar los riesgos. Definir acciones concretas para riesgos inaceptables	Líderes de procesos	Número de aceptaciones de riesgos residuales y aprobación del plan	100%	Plan de Tratamiento de Riesgos (PTR) consolidado y documentado	18/04/2026	- 30/08/2026
Aceptación de Riesgos:	Generar documentos formales donde los dueños de los riesgos aceptan el nivel de riesgo residual resultante tras la aplicación de controles	Líderes de procesos / Comité	Documentos de aceptación de riesgo residual firmados	100%	Actas de aceptación de riesgo residual y aprobación del PTR	18/04/2026	30/08/2026
COMUNICACIÓN Y CONSULTA							
Comunicación de Resultados:	Presentar a las partes interesadas (internas y externas) y a la Alta Dirección los resultados del mapa de riesgos y la exposición de la entidad	Profesional en Seguridad (SDAE) y Equipo SIG-MIPG	Número de reportes de comunicación del riesgo generados	Por demanda	Reportes de resultados del proceso de gestión de riesgos	01/05/2026	15/05/2026
MONITOREO Y REVISIÓN							
Seguimiento a Comités:	Realizar seguimiento al estado de implementación de los comités de seguridad y verificación de evidencias de gestión de riesgos	Profesional en Seguridad (SDAE) y SIG-MIPG	Porcentaje de efectividad de los comités	2	Informes de seguimiento a los comités de seguridad	13/06/2026	18/12/2026

Evaluación de Efectividad de Controles	Evaluar si los controles implementados han sido efectivos para reducir la probabilidad o impacto (cálculo de riesgo residual real)	Profesional en Seguridad (SDAE) / Oficina de Control Interno	Número de evaluaciones de riesgos residuales realizadas	Por demanda	Reporte de Evaluación de efectividad de controles y riesgos residuales	19/09/2026	24/10/2026
Medición de Indicador de Impacto	Calcular el indicador estratégico de tratamiento de riesgos definido en la política (Fórmula: Controles implementados / Controles establecidos * 100)	Subdirección de Diseño y Análisis Estratégico (SDAE)	Tratamiento de riesgos de seguridad digital	> 90%	Reporte de indicadores del plan de tratamiento	01/11/2026	- 11/12/2026
MEJORA CONTINUA							
Acciones de Mejora	Identificar oportunidades de mejora basadas en los resultados de la evaluación de controles y definir acciones correctivas	Profesional en Seguridad (SDAE) y Equipo SIG-MIPG	**Número de Oportunidades de mejora identificadas**	**Por demanda**	Plan de mejoramiento del proceso de riesgos	09/10/2026	31/10/2026

6.2.1. Explicación de contenido actualizado

Cada fila en la Matriz de Gestión de Riesgos anterior asegura la gestión integral y alineada con los principios de la norma ISO 27001 y las mejores prácticas en seguridad de la información. A continuación la explicación de cada actividad y su contribución al proceso general de gestión de riesgos:

Identificación de riesgos

Argumento: La identificación es el primer paso crítico en la gestión de riesgos, ya que permite detectar todas las amenazas potenciales que pueden afectar la seguridad de la información. Sin una identificación exhaustiva de los riesgos, el IPES estaría expuesto a amenazas desconocidas. Esta actividad se asegura de que todos los riesgos relevantes se registren y evalúen adecuadamente.

Evaluación y análisis de riesgos

Argumento: Una vez identificados, los riesgos deben evaluarse en términos de impacto y probabilidad para comprender su nivel de criticidad. Esta actividad permite clasificar los riesgos y establecer prioridades, lo que es esencial para asignar recursos y tomar decisiones informadas sobre las medidas de tratamiento necesarias.

Definición de controles

Argumento: Es fundamental seleccionar controles que respondan específicamente a los riesgos identificados y evaluados. La definición de controles garantiza que el IPES pueda mitigar, evitar, transferir o aceptar los riesgos de manera estructurada y eficaz. Además, esta actividad asegura que los controles estén alineados con los requisitos del Anexo A de ISO 27001, lo cual es esencial para la conformidad.

Implementación de acciones de mitigación

Argumento: Esta actividad es el paso práctico en la gestión de riesgos, donde se implementan los controles definidos para reducir los riesgos a niveles aceptables. Documentar estas acciones y asignar responsables asegura una ejecución ordenada y permite realizar un seguimiento preciso del avance.

Monitoreo y Seguimiento de Riesgos

Argumento: Los riesgos son dinámicos y pueden cambiar con el tiempo. Por ello, es esencial monitorear y revisar los riesgos periódicamente para detectar nuevas amenazas, evaluar cambios en los riesgos existentes y ajustar los controles. Este monitoreo continuo garantiza que el IPES pueda responder rápidamente a cualquier cambio en el entorno de riesgo.

Evaluación de la eficacia de controles

Argumento: Implementar controles no es suficiente; es necesario evaluar periódicamente su efectividad para asegurarse de que están cumpliendo su propósito. Mediante auditorías y pruebas de control, esta actividad asegura que los controles son eficaces y, si no lo son, permite implementar mejoras.

Capacitación y sensibilización

Argumento: La gestión de riesgos de seguridad de la información no solo depende de medidas técnicas, sino también de una cultura organizacional de seguridad. Capacitar al personal asegura que todos comprendan su rol en la seguridad de la información, reduciendo los riesgos relacionados con el factor humano, como el phishing o el acceso no autorizado.

Revisión y mejora continua

Argumento: La mejora continua es un principio clave de ISO 27001 y garantiza que el Sistema de Gestión de Seguridad de la Información (SGSI) evolucione y mejore con el tiempo. Esta actividad permite al IPES identificar áreas de oportunidad, ajustar políticas y fortalecer sus controles de seguridad, alineándose constantemente con los objetivos estratégicos y el contexto cambiante.

Comunicación de resultados

Argumento: La gestión de riesgos no solo es responsabilidad del equipo de seguridad, sino de toda la organización. Comunicar los resultados del proceso de gestión de riesgos asegura que la alta dirección esté informada y pueda tomar decisiones estratégicas, además de promover la transparencia y el compromiso de todos los niveles de la entidad.

6.3. MONITOREO, SEGUIMIENTO Y EVALUACIÓN

Periódicamente se revisará el valor de los activos, impactos, amenazas, vulnerabilidades y probabilidades en busca de posibles cambios, que exijan la valoración interactiva de los riesgos de seguridad de la información. Los riesgos son dinámicos como la misma Entidad por tanto podrá cambiar de forma o manera radical sin previo aviso. Por ello es necesaria una supervisión continua que detecte:

- Nuevos activos o modificaciones en el valor de los activos
- Nuevas amenazas
- Cambios o aparición de nuevas vulnerabilidades
- Aumento de las consecuencias o impactos
- Incidentes de seguridad de la información.
- Análisis periódico de la efectividad de los controles de seguridad implementados para asegurar que sigan siendo adecuados frente a los riesgos actuales.
- Revisión de cumplimiento con normativas y estándares como ISO 27001 y regulaciones locales (por ejemplo, MSPI en Colombia).

6.3.1. Evaluación

Con el propósito de conocer los estados de cumplimiento de los objetivos de la gestión de los riesgos de seguridad de la información, el proceso de gestión de riesgos de seguridad digital será revisado y evaluado en un término cuatrimestral, incluyendo el plan de tratamiento, y las actividades, permitiendo identificar las acciones de mejora y la gestión de conocimiento frente al mismo.

6.3.2. Monitoreo y Seguimiento

La entidad a través de la Subdirección de Diseño y análisis estratégico realizará un monitoreo mensual del plan a través del formato FO-264 Bitácora Plan, y los cortes de análisis de seguimiento al interior de la entidad se realizarán trimestralmente, según lo establecido en el procedimiento PE01-PD-004, dado que el esquema de seguimiento y medición al sistema de gestión de riesgos de la seguridad de la información es fundamental para contextualizar la toma de decisiones de manera oportuna.

6.4. RECURSOS

Para el desarrollo del plan de tratamiento de riesgos de seguridad digital, el Instituto para la Economía Social – IPES dispone de los siguientes recursos:

Humanos: La Subdirección de Diseño y Análisis Estratégico dispone de personal responsable de la coordinación e implementación de herramientas, sistemas, políticas, procedimientos, prácticas o mecanismos dinámicos y seguros para el tratamiento de los riesgos. Asimismo, se dispone del apoyo de los demás procesos que intervienen en el desarrollo del plan.

Técnicos: Se dispone de documentación técnica como; NTC-ISO/IEC 27002:2015, NTC-ISO/IEC 27001:2013, la guía para la administración del riesgo y el diseño de controles en entidades públicas v5, la política de administración del riesgo, el mapa de riesgos para el registro y evidencia del proceso.

Físicos: Se cuenta con la infraestructura tecnológica y física para el desarrollo de actividades como socializaciones, transferencia de conocimientos, comunicación del riesgo, seguimiento y evaluación a la gestión de los riesgos financieros: El Instituto dispone de recursos financieros para la implementación de las acciones que requieran la contratación de servicios o la compra de bienes, los cuales son descritos en los planes de compras anuales.

6.5. PRESUPUESTO

La alta dirección del Instituto para la Economía Social – IPES demuestra su compromiso frente a la seguridad de la información, mediante la asignación de presupuesto o recursos financieros para la implementación del plan de tratamiento de riesgos de seguridad digital, por lo tanto, los Líderes de procesos o dueños de los riesgos realizarán la estimación y asignación del presupuesto anual para este objetivo.

6.6. MEDICIÓN

La medición al cumplimiento del plan de tratamiento se realiza a través de un macro indicador de gestión, el cual tiene por objetivo medir el porcentaje de implementación de las acciones definidas en el plan:

INDICADOR TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL	
Tipo de indicador:	Gestión
Nombre:	Tratamiento de riesgos de seguridad digital

Fórmula:	$\frac{No.\ de\ controles\ del\ PTR\ implementados}{No.de\ controles\ establecidos\ en\ el\ PTR}$ (V1/V2) *100 V1: Cantidad de controles del plan de tratamiento implementados en el año V2: Cantidad de controles establecidos en el plan de tratamiento anual
Meta:	90%
Periodicidad en la medición:	Anual
Fuente de la información:	Mapa de riesgos
Responsable de la medición:	Subdirección de Diseño y Análisis Estratégico

Tabla 2. Indicador para la medición del plan de tratamiento

Adicionalmente, para evaluar si las acciones implementadas realmente están protegiendo a la entidad y reduciendo la exposición al riesgo, se establece un indicador de efectividad. Este indicador mide la materialización de riesgos frente al universo de riesgos gestionados, permitiendo identificar fallas en los controles o cambios en el entorno de amenazas, alineado con los indicadores de impacto sugeridos por el Modelo de Seguridad y Privacidad de la Información.

INDICADOR DE EFECTIVIDAD Y MATERIALIZACIÓN DE RIESGOS	
Tipo de indicador:	Efectividad / Impacto
Nombre:	Materialización de riesgos de seguridad y privacidad
Fórmula:	Total de riesgos activos en el mapa —---------- x 100 No. de riesgos materializados
Meta:	< 5%
Periodicidad en la medición:	Semestral
Fuente de la información:	Reporte de Incidentes (Mesa de Ayuda) y Mapa de Riesgos
Responsable de la medición:	Oficial de Seguridad de la Información

Tabla 3. Indicador de efectividad y materialización de riesgos.

Con el fin de evaluar la conformidad con la Ley 1581 de 2012 y garantizar la protección de los derechos de los titulares (Habeas Data), se establece el siguiente indicador específico para medir la efectividad de los controles de privacidad implementados sobre los datos personales sensibles y públicos gestionados por la entidad:

INDICADOR DE CUMPLIMIENTO NORMATIVO (LEY 1581)	
Tipo de indicador:	Cumplimiento / Impacto
Nombre:	Efectividad en la Protección de Datos Personales
Fórmula:	(Controles de privacidad implementados / Controles de privacidad requeridos por Ley 1581) * 100
Meta:	100%
Periodicidad en la medición:	Semestral
Fuente de la información:	Registro Nacional de Bases de Datos (RNBD) y Auditoría Interna.
Responsable de la medición:	Subdirección de Diseño y Análisis Estratégico

Tabla 4. Indicador para la medición del cumplimiento normativo Ley 1581

7. MARCO NORMATIVO

- NTC-ISO/IEC 27001:2013
- NTC-ISO/IEC 27002:2015
- Ley 1712 de 2014
- Modelo de Seguridad y Privacidad de la Información
- Política de Gobierno Digital

8. DOCUMENTOS ASOCIADOS

- Política de administración del riesgo del Instituto para la Economía Social
- PA03-MG-001 V11 Matriz de riesgos gestión Información y Recursos Tecnológicos Sistemas
- Guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión 6 emitida por el DAFP.

9. CONTROL DE CAMBIOS

VERSIÓN	FECHA	ÍTEM MODIFICADO	DESCRIPCIÓN DEL CAMBIO
1		Elaboración del documento	Todo el documento
2	24/01/2019	Nombre del documento 7 definiciones 11 referencias Bibliográfica	Lineamientos decreto 612 de 2018 Actualización de definiciones Actualización de referencias
3	10/01/2020	10 Marco Normativo 11 documentos Asociados 12 anexo	Se incluyen los numerales, teniendo en cuenta la estructura del documento estratégico
4	20/01/2021	9. Actividades e indicadores	Se actualiza enfocando el plan de tratamiento de riesgos de seguridad digital de la vigencia
5	18/01/2022	9. Actividades e indicadores	Se actualiza enfocando el plan de tratamiento de riesgos de seguridad digital de la vigencia
6	20/12/2022	9. Actividades e indicadores	Se actualiza enfocando el plan de tratamiento de riesgos de seguridad digital de la vigencia
7	28/01/2024	10.Marco Normativo 11.documentos Asociados 12.anexo	Se incluyen los numerales, teniendo en cuenta la estructura del documento estratégico
8	20/12/2025	9. Actividades e indicadores	Se actualiza enfocando el plan de tratamiento de riesgos de seguridad digital de la vigencia
9	22/01/2026	2. Objetivo 3. Alcance 4. Responsables 6. Desarrollo	Se ajustó la redacción para incluir explícitamente la gestión del Riesgo, la priorización de la Infraestructura y Servicios Esenciales, en cumplimiento del MSPI V5 y Guía DAFP Inclusión de Rol Estratégico: Se agregó al Oficial de Seguridad de la Información con funciones

		6.1 Metodología 6.2 Actividades e indicadores 6. 6 Medición 8. Documentos Asociados	específicas de articulación estratégica, monitoreo de controles y reporte a la Alta Dirección, diferenciándolo de la operación general Actualización Metodológica (DAFP V6): Se adoptaron las escalas de 5 niveles para Probabilidad (Frecuencia) e Impacto (Económico/Reputacional). Se incluyó la nota explícita de que los riesgos de corrupción no pueden ser aceptados Fortalecimiento en Privacidad: Se adiciona una actividad específica para el tratamiento de riesgos de cumplimiento de la Ley 1581 de 2012, enfocada en controles de consentimiento, transferencia internacional y protección de datos sensibles Nuevos Indicadores de Impacto: Se incorporaron dos nuevos indicadores para medir la efectividad real del plan, complementando la medición de gestión: 1. Materialización de Riesgos (Incidentes vs. Riesgos Identificados) 2. Efectividad en Privacidad (Cumplimiento Ley 1581) alineado con indicador SGIN11. Inclusión de la Guía para la administración del riesgo y el diseño de controles en entidades públicas Versión 6 y el Documento Maestro del MSPI Versión 5