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, D.C.

ENERO 2025

Elaboró:	Revisó:	Aprobó:
Daniel Ernesto Fragoso Amariz. Profesional SDAE César Iván Vanegas Sánchez Profesional contratista SDAE	Edgar Mauricio Mera 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
Explicación del contenido actualizado 14

6.3. MONITOREO, SEGUIMIENTO Y EVALUACIÓN 17

6.3.1. Evaluación 17

6.3.2. Monitoreo y Seguimiento 17

6.4. RECURSOS 17

6.5. PRESUPUESTO 18

6.6. MEDICIÓN DEL PLAN DE TRATAMIENTO 18

7. MARCO NORMATIVO 18

8. DOCUMENTOS ASOCIADOS 18

9. CONTROL DE CAMBIOS 19

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.

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

Definir el plan de tratamiento para los riesgos de seguridad digital identificados por el Instituto para la Economía Social – IPES, con el fin de contribuir al logro de los objetivos estratégicos, la visión institucional, el cumplimiento de requisitos legales y reglamentarios, la protección de la información y la preservación de su confidencialidad, integridad y disponibilidad, mediante la implementación de lineamientos claros, la gestión integral de riesgos, el fortalecimiento del conocimiento en seguridad y privacidad, y el establecimiento de indicadores específicos que permitan medir la efectividad de las acciones y asegurar el cumplimiento de los objetivos del plan.

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.

4. RESPONSABLES

La como responsable de

Responsable	Rol o Actividad a desarrollar
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 V5 – 2020.
	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 solo 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.
- 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.

- **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

PLAN DE GESTIÓN DE RIESGOS							
Actividad	**Tareas**	**Responsable**	**Indicador**	**Meta**	**Productos**	**Fecha Inicio**	**Fecha Final**
Revisión y Actualización de los lineamientos para la administración del riesgo.	• Revisión y/o actualización de la política de administración del riesgo. • Revisión y/o Actualización de la metodología para la gestión del riesgo. • Actualización de Formato Mapa de Riesgos. Nota: Inicialmente la entidad procederá a realizar la revisión si la metodología vigente requiere o no cambios de conformidad con la normatividad vigente o cambios en la administración del IPES	Subdirección de Diseño y Análisis Estratégico	Número documentos estratégicos de lineamientos para la administración del riesgo actualizada	3	• Revisión Política de Administración del riesgo publicada. • Metodología para la gestión del riesgo publicada • Formato Mapa de Riesgos publicada	01/03/2025	22/03/2025
Plan de formación Capacitación y sensibilización	Socialización y entrenamiento a los encargados sobre el proceso de administración de Riesgos de seguridad digital.	Profesional en Seguridad de la Información - SDAE	Porcentaje de implementación del plan de formación y sensibilización	100%	• Plan de formación Capacitación y sensibilización	22/02/2025	22/11/2025
Proceso de administración de riesgos de seguridad digital.	• Identificación del riesgo. • Análisis del riesgo inherente. • Evaluación del riego inherente. • Definición de controles existentes. • Análisis del riesgo residual. • Selección de la opción de	Líderes de procesos	Porcentaje de implementación del Proceso de administración de riesgos de seguridad digital	100%	• Matriz de riesgo del proceso	01/03/2025	28/09/2025

PLAN DE GESTIÓN DE RIESGOS							
Actividad	**Tareas**	**Responsable**	**Indicador**	**Meta**	**Productos**	**Fecha Inicio**	**Fecha Final**
	tratamiento del riesgo. • Definición del plan de tratamiento. • Realimentación, revisión y verificación de los riesgos Identificados (Ajustes).						
Aceptación de los riesgos residuales y aprobación del plan de tratamiento.	• Generar documento con la aceptación de los riesgos residuales y documento con la aprobación del plan del Tratamiento.	Líderes de procesos	Número de aceptaciones de los riesgos residuales y aprobación del plan de tratamiento	Por demanda	• Documento con la aceptación de los riesgos residuales y documento con la aprobación del plan del Tratamiento.	18/04/2025	30/08/2025
Comunicación del riesgo.	• Presentar a las partes interesadas los resultados del proceso de administración o gestión del riesgo.	Profesional en Seguridad de la Información - SDAE Y SIG-MIPG	Número de Comunicación del riesgo generados	Por demanda	• Reportes de resultados del proceso de Administración O gestión del riesgo.	01/05/2025	15/05/2025
Seguimiento al plan de comités.	• Realizar seguimiento al estado de implementación de los comités y verificación de evidencias.	Profesional en Seguridad de la Información - SDAE Y SIG-MIPG	Porcentaje de efectividad de los comités	2	• Informe o reporte de los comités de seguridad que se realizan	13/06/2025	19/12/2025
Evaluación de la efectividad de los controles.	• Evaluación de riesgos residuales	Profesional en Seguridad de la Información - SDAE Y equipo SIG-MIPG	Número de evaluaciones de riesgos residuales realizadas sobre las programadas	Por demanda	• Reporte de Evaluación de riesgos residuales	19/09/2025	24/10/2025

PLAN DE GESTIÓN DE RIESGOS							
Actividad	**Tareas**	**Responsable**	**Indicador**	**Meta**	**Productos**	**Fecha Inicio**	**Fecha Final**
Mejora continua.	• Identificación de las oportunidades de mejora acorde a los resultados obtenidos durante la evaluación de la efectividad de los controles del plan de tratamiento.	Profesional en Seguridad de la Información - SDAE Y equipo SIG-MIPG	Número de Oportunidades de mejora acorde a los resultados obtenidos durante la evaluación de la efectividad de los controles del plan	Por demanda	• Oportunidades de mejora acorde a los resultados obtenidos durante la evaluación de la efectividad de los controles del plan De tratamiento generados.	09/10/2025	31/10/2025
Monitoreo y revisión.	• Generación, presentación y reporte de indicadores del plan de tratamiento.	Profesional en Seguridad de la Información y equipo SIG-MIPG	Número de Monitoreos y revisiones realizadas	Por demanda	• Reporte de indicadores del plan de tratamiento.	01/11/2025	11/12/2025

Tabla 1. Actividades para la gestión del plan de tratamiento

SUGERIDO

PLAN DE GESTIÓN DE RIESGOS							
Actividad	**Tareas**	**Responsable**	**Indicador**	**Meta**	**Productos**	**Fecha Inicio**	**Fecha Final**
Identificación de Riesgos	- Realizar análisis de contexto interno y externo. - Identificar riesgos y amenazas.	Líder de cada proceso Subdirección de Análisis Estratégico	Número de riesgos identificados	100% de los riesgos relevantes	Mapa de riesgos actualizado	Anual	Revisión trimestral
Evaluación y Análisis de Riesgos	- Determinar impacto y probabilidad. - Clasificar los riesgos según niveles de tolerancia y apetito de riesgo.	Líder de cada proceso	Número de riesgos evaluados y clasificados	100% de los riesgos identificados	Informe de evaluación de riesgos	Anual	Revisión trimestral
Definición de Controles	- Seleccionar controles adecuados para mitigar riesgos. - Ajustar controles a los requisitos del Anexo A de ISO 27001.	Subdirección de Análisis Estratégico	Número de controles implementados	90% de implementa ción anual	Informe de controles implementados	Continuo	Actualización trimestral
Implementación de Acciones de Mitigación	- Aplicar controles definidos en el plan de tratamiento. - Documentar acciones y asignar responsables.	Líderes de cada proceso				Continuo	

			Porcentaje de acciones completadas	100% de acciones implementadas	Documentación de acciones de mitigación		Revisión trimestral
Monitoreo y Seguimiento de Riesgos	- Realizar monitoreos periódicos de riesgos residuales y emergentes. - Revisar cambios en el perfil de riesgo.	Subdirección de Análisis Estratégico	Número de monitoreos realizados	100% de riesgos monitoreados	Reportes de seguimiento de riesgos	Mensual	Revisión trimestral
Evaluación de la Eficacia de Controles	- Realizar auditorías y pruebas de control. - Analizar la efectividad de los controles aplicados.	Equipo de Auditoría Interna Profesional de Seguridad	Número de auditorías completadas	100% de controles auditados	Informes de auditoría de controles	Trimestral	Informe anual
Capacitación y Sensibilización	- Socializar políticas de seguridad y riesgos. - Capacitar al personal en prácticas de seguridad de la información.	Subdirección de Recursos Humanos Equipo SIG-MIPG	Porcentaje de personal capacitado	90% del personal anual	Programa de capacitación y registros de asistencia	Anual	Revisión trimestral

Revisión y Mejora Continua	- Identificar oportunidades de mejora según los resultados de evaluación. - Ajustar políticas y procedimientos.	Subdirección de Análisis Estratégico	Número de mejoras implementadas	100% de mejoras identificadas	Informe de mejora continua y actualizaciones	Trimestral	Revisión anual
Comunicación de Resultados	- Presentar resultados a la alta dirección y a las partes interesadas.	Profesional en Seguridad de la Información	Número de reportes de comunicación generados	100% de resultados reportados	Reportes de resultados del proceso de gestión	Trimestral	Informe anual

Explicación del 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:

1. **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.

2. **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.

3. **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.

4. **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.

5. **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.

6. **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.

7. **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.

8. **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.

9. **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 del riesgo.**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 DEL PLAN DE TRATAMIENTO

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

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 5 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