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, 2024

Elaboró:	Revisó:	Aprobó:
Daniel Ernesto Fragoso Amariz. Profesional SDAE Martha Patricia Mateus González Profesional contratista SDAE	Sandy Patricia Guerrero Salcedo Contratista 064 de 2023 Edgar Mauricio Mera E Contratista 053 de 2023	Aprobó: Paola Rico Parada Subdirector de Diseño y Análisis Estratégico - SDAE

TABLA DE CONTENIDO

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 funcionen 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 JUSTIFICACIÓN

El desarrollo de un plan de tratamiento de riesgos de seguridad digital permitirá al Instituto para la Economía Social – IPES, planear, implementar, mantener y mejorar las acciones encaminadas a proteger los activos de información institucional, a través de la adopción de herramientas, sistemas, políticas, procedimientos, prácticas o mecanismos dinámicos y seguros, así como dar cumplimiento a la normatividad establecida por el estado Colombiano, entre ellas el Modelo de Seguridad y Privacidad de la Información – MSPI, el Decreto 1008 de 14 de junio 2018 y adoptar las buenas prácticas establecidas por estándares internacionales como ISO/IEC 27001:2022, ISO/IEC 27002:2022, ISO 31000:2018 y la guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión 5 emitida por el DAFP.

3 OBJETIVO

Presentar el plan de tratamiento definido para los riesgos de seguridad digital identificados por el Instituto para la Economía Social – IPES, el cual contribuirá al logro de los objetivos estratégicos, la visión institucional, el cumplimiento de los requisitos legales y reglamentarios vigentes y aplicables, la misionalidad y la preservación de la confidencialidad, integridad y disponibilidad de la información.

Los objetivos de este plan son:

a. Definir y aplicar los lineamientos para tratar de manera integral los riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación que el IPES pueda estar expuesto, y de esta manera alcanzar los objetivos, la misión y la visión institucional, protegiendo y preservando la integridad, confidencialidad, disponibilidad y autenticidad de la información.

b. Cumplir con los requisitos legales y reglamentarios pertinentes a la legislación colombiana.

c. Gestionar riesgos de Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación, de acuerdo con los contextos establecidos en la Entidad.

d. Fortalecer y apropiar conocimiento referente a la gestión de riesgos Seguridad y Privacidad de la información,

e. Seguridad Digital y Continuidad de la Operación.

4 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.

5 RESPONSABILIDADES

La Subdirección de Diseño y Análisis Estratégico como responsable de 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.

La Subdirección de Diseño y Análisis Estratégico será la encargada de 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.

El equipo del Sistema Integrado de Gestión se encargará de 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 PE01-FO-004 Mapa de Riesgos de Seguridad de la Información, con el fin de registrar la gestión adelantada, así como la revisión, seguimiento y monitoreo a los riesgos y su plan de tratamiento.

El equipo de seguimiento y evaluación está conformado por el/la Asesor/a de Control Interno, los servidores públicos y contratistas de su oficina asesora, quienes velarán por la adecuada elaboración e implementación del mapa de riesgos de cada proceso, promoviendo su apropiación, entendimiento y evaluación del mismo.

Los responsables de 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.

6 CONDICIONES GENERALES

- 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 PE01-FO-004 Mapa de Riesgos de Seguridad de la Información, para el registro del proceso de administración del riesgo.
- Utilizar el instructivo “Gestión de riesgos de seguridad digital" del IPES.

7 DEFINICIONES[1]

1. **Activo:** En el contexto de seguridad digital son elementos tales como aplicaciones de la organización, servicios web, redes, hardware, información física o digital, recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital, dentro de los cuales se puede mencionar:
   - Información.
   - Software.
   - Recursos físicos.
   - Servicios.
   - Personas y sus cualificaciones, habilidades y experiencias.
   - Elementos intangibles como la reputación y la imagen.

2. **Activo de información:** Conocimiento o datos que son de valor para la entidad. Ver modelo estándar de control interno para el Estado Colombiano, MECI 1000:2005, Numeral 2.2 Componente Información.

3. **Acceso a la Información Pública:** Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4).

4. **Archivo:** Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para

[1] DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA, Guía para la Administración del Riesgo y el

diseño de controles en entidades públicas V6 – 2022, Definiciones pág. 8.

servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3).

5. **Amenaza:** Situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización. (ISO/IEC 27000).

6. **Análisis de Riesgo:** Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).

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

8. **Auditoría:** Proceso sistemático, independiente y documentado para obtener evidencias de auditoria y obviamente para determinar el grado en el que se cumplen los criterios de auditoria. (ISO/IEC 27000).

9. **Bases de Datos Personales:** Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3).

10. **Causas:** Todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.

11. **Confidencialidad:** Propiedad de la información que la hace no disponible, es decir, divulgada a individuos, entidades o procesos no autorizados.

12. **Consecuencia:** Los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas.

13. **Control:** Medida que permite reducir o mitigar un riesgo. Entiéndase por las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida.

14. **Ciberseguridad:** Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).

15. **Ciberespacio:** Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009) interacción entre usuarios.

16. **Datos Abiertos:** Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6).

17. **Datos Personales:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).

18. **Datos Personales Públicos:** Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3).

19. **Datos Personales Privados:** Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h).

20. **Datos Personales Mixtos**: Para efectos de esta guía es la información que contiene datos personales públicos junto con datos privados o sensibles.

21. **Datos Personales Sensibles:** Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013, art 3).

22. **Derecho a la Intimidad:** Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad,

que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural (Jurisprudencia Corte Constitucional).

23. **Disponibilidad:** Propiedad de ser accesible y utilizable a demanda por una entidad.

24. **Encargado del Tratamiento de Datos:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del responsable del Tratamiento. (Ley 1581 de 2012, art 3)

25. **Evaluación del riesgo:** Busca confrontar los resultados del análisis de riesgo inicial frente a los controles establecidos, con el fin de determinar la zona de riesgo final (Riesgo Residual).

26. **Gestión del riesgo**: Proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos.

27. **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).

28. **Identificación del riesgo:** Se deben establecer las fuentes o factores de riesgo, los eventos o riesgos, sus causas y sus consecuencias. Para el análisis se pueden involucrar datos históricos, análisis teóricos, opiniones informadas y expertas y las necesidades de las partes involucradas.

29. **Integridad:** Propiedad de exactitud y completitud

30. **Impacto**: son las consecuencias que genera un riesgo una vez se materialice.

31. **Información Pública Clasificada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).

32. **Información Pública Reservada**: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)

33. **Mapa de riesgos:** Documento con la información resultante de la gestión del riesgo.

34. **Política de administración de riesgos:** Declaración de la dirección y las intenciones generales de una organización con respecto a la gestión del riego.

35. **Plan de tratamiento de riesgos:** Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).

36. **Privacidad**: En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL la correlativa obligación de proteger dicha información en observancia del marco legal vigente.

37. **Probabilidad:** es la posibilidad de la amenaza aproveche la vulnerabilidad para materializar el riesgo

38. **Riesgo inherente:** Es aquel al que se enfrenta una entidad en ausencia de acciones de la dirección para modificar su probabilidad o impacto.

39. **Riesgo residual:** Nivel de riesgo que permanece luego de tomar medidas de tratamiento de riesgo.

40. **Riesgo de seguridad digital**: Combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos del ambiente físico, digital y las personas.

41. **Seguridad de la información:** Preservación de la confidencialidad, la integridad y la disponibilidad de la información. Además, puede involucrar otras propiedades como como: autenticidad, trazabilidad, no repudio y fiabilidad.

42. **Tolerancia al riesgo:** son los niveles aceptables de desviación relativa a la consecución de objetivos. Pueden medirse y a menudo resulta mejor, con las mismas unidades que los objetivos correspondientes. Para el riesgo de corrupción la tolerancia es inaceptable.

43. **Tratamiento del riesgo:** Es la respuesta establecida por la primera línea de defensa para la mitigación de los diferentes riesgos, incluyendo aquellos relacionados con la corrupción.

44. **Valoración de riesgos:** Establecer la probabilidad de ocurrencia del riesgo y el nivel de consecuencia o impacto, con el fin de estimar la zona de riesgo inicial (Riesgo Inherente).

45. **Vulnerabilidad:** es una falencia o debilidad que puede estar presente en la tecnología, las personas o en las políticas y procedimientos.

8 DESARROLLO DEL PLAN

8.1 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 riego.
- 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 27001:2022 a fin de 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.

8.2 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	01/03/2024	15/12/2024
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	22/02/2024	22/11/2024
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	3	• Matriz de riesgo corrupción del proceso	01/03/2024	15/12/2024

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.	18/04/2024	30/08/2024
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 gestión del riesgo.	01/05/2024	15/05/2024
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 sistemas y seguridad de la información que se realizan	13/06/2024	19/12/2204
Evaluación de la efectividad de los controles.	• Evaluación de riesgos incidentes de seguridad	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 o casos de incidentes de seguridad	02/02/2024	31/12/2024

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.	02/12/2024	31/12/2024
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.	02/03/2024	31/12/2024

Tabla 1. Actividades para la gestión del plan de tratamiento

8.3 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.

8.3.1. 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.

8.3.2. Monitoreo y Seguimiento

La entidad a través de la Subdirección de Diseño y análisis estratégico realizara un monitoreo mensual del plan a través del formato 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 Planeación estratégica y operativa, 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.

8.4 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 27002:2022, NTC-ISO/IEC 27001:2022, 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.

8.5 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.

8.6 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

9 ANEXOS

No se registran anexos.

10 MARCO NORMATIVO

- NTC-ISO/IEC 27001:2022
- NTC-ISO/IEC 27002:2022
- Ley 1712 de 2014
- MSPI - Modelo de Seguridad y Privacidad de la Información
- Política de Gobierno Digital

11 DOCUMENTOS ASOCIADOS

- Política de administración del riesgo del Instituto para la Economía Social

- PA03-MG-001 Matriz de riesgos gestión Información y Recursos Tecnológicos Sistemas
- Guía para la administración del riesgo y el diseño de controles en entidades públicas - emitida por el DAFP.V6 de 2022

12 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	06/12/2023	9. Actividades e indicadores	Se actualiza enfocando el plan de tratamiento de riesgos de seguridad digital de la vigencia