PRONIED
PROGRAMA NACIONAL
DE INFRAESTRUCTURA EDUCATIVA

Código: PE03.03 - PRONIED	Versión: 03

Procedimiento: *"Gestionar los riesgos organizacionales"*

	Unidad Orgánica	Visto y Sello
Elaborado por:	Oficina de Planeamiento y Presupuesto - PRONIED	 PRONIED PROGRAMA NACIONAL DE INFRAESTRUCTURA EDUCATIVA FIRMA DIGITAL Firmado digitalmente por CUELLAR SASIETA Magdalena Aurora FAU 20514347221 soft Motivo: Doy V° B° Fecha: 20.01.2021 00:05:35 -05:00
Validado por:	Oficina de Planeamiento y Presupuesto - PRONIED	 PRONIED PROGRAMA NACIONAL DE INFRAESTRUCTURA EDUCATIVA FIRMA DIGITAL Firmado digitalmente por PACHECO FLORES Ana Cecilia FAU 20514347221 soft Motivo: Doy V° B° Fecha: 15.01.2021 11:58:30 -05:00
Revisado por:	Unidad de Organización y Métodos - MINEDU	 FIRMA DIGITAL Firmado digitalmente por: ALVARADO LIZARME Patricia FAU 20131370998 hard Motivo: Soy el autor del documento Fecha: 23/12/2020 12:41:37-0500

Control de Cambios		
Versión	**Sección / Ítem**	**Descripción del cambio:**
01	----	Nuevo
02	I	Se modificó la descripción.
	II	Se modificó la descripción indicando a quienes está aplicado el procedimiento.
	III	Se precisó un responsable de hacer cumplir el procedimiento y un responsable del monitoreo.
	IV	Se reemplazó la norma legal del numeral 6 y 7 de la versión 01 por la norma legal precisada en el numeral 6. Se eliminó la norma legal del numeral 8 y 9 de la versión 01.
	V	Se eliminaron las siglas SGAS, SGC y SGSI. Se agregó la definición del término: Sistema de Gestión, producto, unidad funcional y unidad funcional responsable.
	VI	Se modificó la descripción del proveedor y entrada; agregándose otra entrada: productos priorizados (SCI). Se reemplazó la salida "Solicitud de acciones correctivas y oportunidad de mejora" por "Reporte o registro de monitoreo o materialización del riesgo".
	VII / actividad	Se mejoró la redacción de las actividades, asimismo se cita el formato codificado. Se agregaron las actividades N° 1, 2. 9, 10, 11, 12, 15, 17, 18, 19 y 20 Se ha consolidado la actividad N° 7 y 8 de la versión 01 por la actividad N° 8. Se ha consolidado la actividad N° 9 y 10 de la versión 01 por la actividad N° 13. Se dividió la actividad N° 11 de la versión 01 por la actividad N° 14 y 19.
	VII / área	Se modificó "órgano / unidad orgánica" por "unidad funcional responsable". Se agregó a la OPP.
	VII / responsable	Se modificó Coordinador del sistema de gestión por el Representante del equipo de trabajo. Se agregó un equipo de trabajo y al/a la Coordinador(a) / Especialista de Modernización.
	VIII	Se agregó 1 formato codificado.
	XI	Se definió un indicador de eficacia.
	XII	Se modificó la denominación y el contenido del anexo 1, 2, 3, 4, 5 y 6 de la versión 01 por los anexos 1, 4, 5, 6, 7 y 8, respectivamente. Se agregó el anexo 2 y 3. Se eliminaron los anexos 7, 8, 9, 10 y 11 de la versión 01.
03	IV	- Se ordenó por jerarquía de normas y antigüedad, agregándose la norma legal N° 10, 11 y 14
	V	- Se eliminó la definición de "riesgo inicial" - Se agregó el término "SGAS", "SGSI"

		- Se agregó la definición de “Puestos críticos” y “Vulnerabilidad” - Se actualizó la definición de “Causas”, “Consecuencias”, “Eventos” y “Riesgo”
	VI	- Se agregó como entrada: “Inventario de activos de información”, requerido para el SGSI - Se reemplazó la salida “Reporte o registro de monitoreo o materialización del riesgo” por “Matriz de riesgos (riesgo con efecto positivo)” y “Registro de monitoreo (riesgo materializado)”
	VII / actividad	- Se añadió una nota relacionada a las actividades a ser desarrolladas vía remota y/o presencial. - Se modificó la descripción de la actividad “N° 3 Identificar los riesgos” con relación a la incorporación de determinar los puestos críticos - Se agregó la actividad N° 5 relacionada a los riesgos identificados para el SGSI y la actividad N° 7 relacionada a los riesgos con efecto positivo - Se modificó la descripción de la actividad “N° 9 Analizar los riesgos” con relación a precisar la información a utilizar cuando se realice el análisis de un riesgo identificado y tratado con anterioridad - Se modificó la actividad N° 12 “Validar la matriz de riesgos” por la actividad N° 15 “Confirmar la matriz de riesgos”, en la que se describe que dicha confirmación se realiza mediante correo institucional - Se eliminó la actividad “N° 16 Solicitar la verificación de la eficacia” de la versión 02 - Se agregó en la actividad “N° 19 Analizar riesgo residual” una nota relacionada a que la medición de la eficacia del tratamiento del riesgo está referido al cálculo del riesgo residual - Las actividades N° 19, 20 y 21 de la versión 02 (responsable: OPP) fueron modificadas por las actividades N° 21, 22 y 23 (responsable: unidad funcional responsable)
	XI	Se modificó el término “aceptable” por “tolerable”, tanto en el nombre como fórmula del indicador.
	XII	- Se incorporó el anexo N° 3 “Cuadro de amenazas para el SGSI” y anexo N° 4 “Listado de vulnerabilidades para el SGSI” - Se modificó el anexo N° 6 “Escala de probabilidad del riesgo”, generándose dos tablas: Probabilidad del riesgo (exceptuado para riesgos de soborno o corrupción y Probabilidad para riesgos de soborno o corrupción - Se modificó el anexo N° 7 “Escala de impacto del riesgo”, generándose dos tablas: Escala de impacto del riesgo (exceptuado para riesgos de seguridad de la información) y Escala de impacto del riesgo de seguridad de la información - Se actualizó el diagrama de flujo (anexo N° 11)

PRONIED
PROGRAMA NACIONAL
DE INFRAESTRUCTURA EDUCATIVA
FIRMA DIGITAL

Firmado digitalmente por CUELLAR SASIETA Magdalena Aurora FAU 20514347221 soft
Motivo: Doy V° B°
Fecha: 20.01.2021 00:06:54 -05:00

MINISTERIO DE EDUCACIÓN
OFICINA DE PLANEAMIENTO Y PRESUPUESTO
V°B°
Director
PRONIED

I. OBJETIVO

- Establecer la metodología para la identificación, análisis, evaluación y definición de planes de acción para mitigar los riesgos, que puedan afectar al logro de los objetivos de los procesos y el cumplimiento de la misión del PRONIED.

II. ALCANCE

- Este procedimiento es de aplicación para todas las unidades funcionales del PRONIED.

III. RESPONSABLE

- El/La Director(a) de cada unidad funcional es el responsable de hacer cumplir el presente procedimiento.
- El/La Director(a) de la Oficina de Planeamiento y Presupuesto es el responsable de asegurar el seguimiento a la implementación del tratamiento de los riesgos.

IV. BASE NORMATIVA

1. Ley N° 27658, Ley Marco de Modernización de la Gestión del Estado, y sus modificatorias.
2. Ley N° 27785, Ley Orgánica del Sistema Nacional de Control y de la Contraloría General de la República, y sus modificatorias.
3. Ley N° 28716, Ley de Control Interno de las Entidades del Estado, y sus modificatorias.
4. Decreto Supremo N° 030-2002-PCM, Reglamento de la Ley Marco de Modernización de la Gestión del Estado.
5. Decreto Supremo N° 092-2017-PCM, que aprueba la Política Nacional de Integridad y Lucha contra la Corrupción.
6. Decreto Supremo N° 044-2018-PCM, que aprueba el Plan Nacional de Integridad y Lucha contra la Corrupción 2018 – 2021.
7. Decreto Supremo N° 004-2014-PCM, que aprueba la Política Nacional de Modernización de la Gestión Pública.
8. Decreto Supremo N° 004-2014-MINEDU, que crea el Programa Nacional de Infraestructura PRONIED.
9. Decreto Supremo N° 008-2020-SA, que declara en Emergencia Sanitaria a nivel nacional por el plazo de noventa (90) días calendario y dicta medidas de prevención y control del COVID-19, y sus prórrogas.
10. Resolución Ministerial N° 103-2020-PCM, que aprueba los "Lineamientos para la atención a la ciudadanía y el funcionamiento de las entidades del Poder Ejecutivo, durante la vigencia de la declaratoria de emergencia sanitaria producida por el Covid-19, en el marco del Decreto Supremo N° 008-2020-SA".
11. Resolución de Contraloría N° 320-2006-CG, que aprueba las Normas de Control Interno.
12. Resolución de Contraloría N° 146-2019-CG, que aprueba la Directiva N° 006-2019-CG/INTEG “Implementación del Sistema de Control Interno en las entidades del Estado”.
13. Resolución de Secretaría General N° 217-2018-MINEDU, que aprueba la Directiva N° 004-2018-MINEDU/SPE-OPEP-UNOME: denominada “Metodología para la gestión por procesos en el Ministerio de Educación”.
14. Norma Internacional ISO/IEC 27001:2013, Sistemas de Gestión de Seguridad de la Información – Requisitos.

PRONIED
PROGRAMA NACIONAL
DE INFRAESTRUCTURA EDUCATIVA
FIRMA DIGITAL

Firmado digitalmente por CUELLAR SASIETA Magdalena Aurora FAU 20514347221 soft
Motivo: Doy V° B°
Fecha: 20.01.2021 00:07:27 -05:00

IV. BASE NORMATIVA

15. Norma Internacional ISO 37001:2016, Sistemas de Gestión Antisoborno – Requisitos con orientación para su uso.
16. Norma Internacional ISO 31000:2018, Gestión del Riesgo - principios y directrices.
17. Norma Internacional ISO 31010:2018, Técnicas de evaluación del riesgo.

V. SIGLAS Y DEFINICIONES

- **Causas**: Todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización o realización de un riesgo; es decir son los medios, circunstancias y agentes generadores del riesgo. Estos agentes son sujetos u objetos que tienen la capacidad de originar un riesgo; se pueden clasificar en cuatro categorías: personas, materiales, instalaciones y entorno.
- **Consecuencias**: Resultado de un evento que afecta a los objetivos.
  Nota 1: Una consecuencia puede ser cierta o incierta y puede tener efectos positivos o negativos, directos o indirectos sobre los objetivos.
  Nota 2: Las consecuencias se pueden expresar de manera cualitativa o cuantitativa.
- **Control:** Medida que mantiene y/o modifica un riesgo.
- **Dueño del riesgo:** Persona con la responsabilidad de gestionar un riesgo.
- **Evento:** Ocurrencia o cambio de un conjunto particular de circunstancias.
  Nota 1: Un evento puede tener una o más ocurrencias y puede tener varias causas y varias consecuencias.
  Nota 2: Un evento también puede ser algo previsto que no llega a ocurrir, o algo no previsto que ocurre.
- **FODA**: Se refiere a los cuatro aspectos a evaluar en el contexto de la organización (Fortalezas, Oportunidades, Debilidades y Amenazas).
- **Fuente de riesgo:** Elemento que, por sí solo o en combinación con otros, tiene el potencial de generar riesgo.
- **Gestión de riesgo:** Actividades coordinadas para dirigir y controlar la entidad con relación al riesgo.
- **Impacto:** Consecuencia de la materialización de un riesgo, expresado en términos económicos, como pérdidas financieras, mediante métodos cualitativos o cuantitativos.
- **Parte interesada:** Persona u organización que puede afectar; verse afectada o percibirse como afectada por una decisión o actividad.
- **Probabilidad:** Posibilidad de que algo suceda.
- **Proceso:** Secuencia de actividades mutuamente relacionadas que transforma una entrada o insumo en una salida o producto, añadiéndole valor en cada etapa de la cadena, utilizando recursos y siguiendo controles establecidos, con el fin de lograr la satisfacción a las necesidades de los clientes.

  Producto: Bien o servicio que proporcionan las entidades/dependencias del Estado a una población beneficiaria con el objeto de satisfacer sus necesidades; correspondiente al eje de gestión de riesgos, para la implementación del Sistema de Control Interno.
- **PRONIED:** Programa Nacional de Infraestructura Educativa.
- **Puestos críticos:** Son los que interfieren en la operación. Son los cargos que por alguno de los criterios determinados por la unidad funcional y/o la institución, según sus riesgos, requieren control exhaustivo. Puede ser por acceso a información clasificada, a la carga, a sitios sensibles, entre otros.
- **Riesgo:** Efecto de la incertidumbre en el cumplimiento de los objetivos de la Entidad.
- **Riesgo residual**: Es aquel riesgo que subsiste después de aplicar las acciones o medidas de control.

PRONIED
PROGRAMA NACIONAL DE INFRAESTRUCTURA EDUCATIVA
FIRMA DIGITAL

Firmado digitalmente por CUELLAR SASIETA Magdalena Aurora FAU 20514347221 soft
Motivo: Doy V° B°
Fecha: 20.01.2021 00:07:48 -05:00

MINISTERIO DE EDUCACIÓN - OFICINA DE PLANEAMIENTO Y PRESUPUESTO - V°B° Director - PRONIED

V. SIGLAS Y DEFINICIONES

- **SCI:** Sistema de Control Interno.
- **SGAS:** Sistema de Gestión Antisoborno.
- **SGSI:** Sistema de Gestión de Seguridad de la Información.
- **Sistema de Gestión**: Conjunto de elementos mutuamente relacionados o que interactúan para establecer la política y los objetivos, así como para cumplir con el logro de dichos objetivos. Una organización puede implementar diferentes sistemas de gestión, tales como: el de calidad, ambiental, seguridad de la información, seguridad y salud ocupacional, responsabilidad social, entre otros.
- **Tratamiento del riesgo:** Es el proceso destinado a modificar el riesgo. El tratamiento puede tener como objetivo prevenir, mitigar, compartir o transferir, aceptar o eliminar el riesgo.
- **Unidad funcional**: Es la unidad de organización que agrupa servidores civiles al interior de una estructura funcional (por ejemplo, Oficina de Planeamiento y Presupuesto, Oficina General de Administración, Unidad de Abastecimiento, etc.). El PRONIED cuenta con una estructura funcional que se desarrolla en su Manual de Operaciones y se representa mediante su organigrama.
- **Unidad funcional responsable**: Según sea el caso, representa a la unidad de organización que coordina la planificación, ejecución, seguimiento y evaluación del SCI o al dueño del proceso, que tiene la responsabilidad y la autoridad definida para establecer, mantener, controlar y mejorar el proceso y su interacción con otros procesos.
- **Vulnerabilidad**: Debilidad de un activo o control que puede ser explotado por una o más amenazas.

VI. ENTRADAS Y SALIDAS DEL PROCEDIMIENTO

Proveedor	Entrada
- Unidad funcional responsable	- Procesos - Productos priorizados (SCI) - Inventario de activos de información (valoración alto y crítico)
Salida	**Usuario**
- Matriz de riesgos	- Unidad funcional responsable - OPP
- Matriz de riesgos (riesgo con efecto positivo)	- Procedimiento: **PE03.02.04.01-PRONIED Realizar acciones correctivas y oportunidades de mejora**
- Registro de monitoreo (riesgo materializado)	

VII. ACTIVIDADES DEL PROCEDIMIENTO

Nº	Actividad	Área	Responsable	Registro

***Nota**: En caso las actividades del procedimiento puedan ser desarrolladas vía remota y/o presencial, se priorizará la modalidad remota, de acuerdo con la Resolución Ministerial N° 103-2020-PCM. Las actividades que por su naturaleza requieran ser presenciales, se realizarán cumpliendo las medidas establecidas en el Plan para la Vigilancia, Prevención y Control de COVID-19 en el trabajo del Programa Nacional de Infraestructura Educativa.*

MINISTERIO DE EDUCACIÓN OFICINA DE PLANEAMIENTO Y PRESUPUESTO PRONIED V°B° Director

PRONIED PROGRAMA NACIONAL DE INFRAESTRUCTURA EDUCATIVA FIRMA DIGITAL

Firmado digitalmente por CUELLAR SASIETA Magdalena Aurora FAU 20514347221 soft
Motivo: Doy V° B°
Fecha: 20.01.2021 00:08:16 -05:00

VII. ACTIVIDADES DEL PROCEDIMIENTO

Nº	Actividad	Área	Responsable	Registro
IDENTIFICACIÓN				
1	**Establecer equipo de trabajo** Establecer el equipo de trabajo, conformado por un mínimo dos (02) o más miembros y designar al representante del equipo, encargados de aplicar la metodología de gestión de riesgos en el ámbito de su competencia como dueño del riesgo, ya sea para un sistema de gestión o el SCI, e informar a la OPP de la designación del equipo de trabajo a través del correo electrónico institucional, para su posterior seguimiento.	Unidad funcional responsable	Director(a)	Correo electrónico
2	**Elaborar plan de trabajo** Elaborar plan de trabajo y coordinar con los demás miembros del equipo, las reuniones de trabajo necesarias para la aplicación de la metodología de gestión de riesgos. *Nota: De requerirlo, podrá solicitar la asistencia técnica de la OPP en cualquier fase del desarrollo de la citada metodología.*	Unidad funcional responsable	Representante del equipo de trabajo	Plan de trabajo
3	**Identificar los riesgos** Identificar los riesgos considerando el contexto de la organización (FODA), revisión de fichas de procesos y/o procedimientos del PRONIED que pueden afectar el logro de los objetivos, registro de incidentes y servicios no conformes, informes de control interno, otros documentos necesarios y/o aquellos sucesos que podrían crear, mejorar, prevenir, degradar, acelerar o retrasar el logro de dichos objetivos; asimismo determinar: - Tipo de riesgo, identificado de acuerdo a lo establecido en el **anexo N° 1** - Puestos críticos[1], esta información es obligatorio para los riesgos del SGAS y opcional, según se aplique, para otros riesgos	Unidad funcional responsable	Equipo de trabajo	Matriz de riesgos (Etapa I)

VII. ACTIVIDADES DEL PROCEDIMIENTO

Nº	Actividad	Área	Responsable	Registro
	- Activos de información, identificados en el "Inventario de Activos de Información" con valoración de altos y críticos que son impactados por el riesgo identificado, esta información aplica solo para el SGSI. La información identificada y determinada se registra en la sección I del **formato: FPE03.03.01-PRONIED Matriz de riesgos**. *[1]Cada vez que la unidad funcional contrate un(a) servidor(a) ligado al proceso donde se determinó el riesgo y/o realice funciones de una posición catalogada como crítica, este será considerado como crítico también y por ende se deberá actualizar la matriz para incluir al nuevo puesto crítico y subsecuentemente actualizar el listado de puestos críticos, realizando la comunicación correspondiente a la OPP.* *Nota: En caso corresponda al SCI, identificar los riesgos respecto al producto priorizado.*			
4	**Identificar las causas o amenazas** Identificar las causas[2] que generan el riesgo o las amenazas[3] a las que están expuestos los activos de información y registrarlas en la sección I (descripción y origen) del **formato: FPE03.03.01-PRONIED Matriz de riesgos**. *[2]Las causas se pueden identificar utilizando las "**Herramientas básicas de análisis de datos"** establecidas en el **anexo N° 2**.* *[3]Las amenazas se pueden identificar utilizando el "**Cuadro de amenazas para el SGSI**" establecido en el **anexo N° 3.*** ¿La gestión de riesgos corresponde al SGSI? Sí: Ir a la actividad N° 5. No: Ir a la actividad N° 6.	Unidad funcional responsable	Equipo de trabajo	Matriz de riesgos (Etapa I)
5	**Identificar las vulnerabilidades y el impacto en seguridad de la información**	Unidad funcional responsable	Equipo de trabajo	Matriz de riesgos (Etapa I)

VII. ACTIVIDADES DEL PROCEDIMIENTO

Nº	Actividad	Área	Responsable	Registro
	Identificar las vulnerabilidades[4] de los activos de información que podrían ser explotados por las amenazas identificadas previamente y el impacto en seguridad de la información del riesgo identificado, ya sea en: - Confidencialidad - Integridad - Disponibilidad - Ley de Protección de Datos Personales La información identificada se registra en la sección I del **formato: FPE03.03.01-PRONIED Matriz de riesgos**. *[4]Las vulnerabilidades se pueden identificar utilizando el "**Listado de vulnerabilidades para el SGSI**" establecido en el **anexo N° 4**.* *Nota 1: Es posible que el impacto se de en más de un aspecto de seguridad, es decir, puede ser que el riesgo impacte a la confidencialidad, integridad y disponibilidad simultáneamente.* *Nota 2: Se puede tomar como fuente de impactos de seguridad lo identificado en la matriz de activos de información.*			
6	**Describir consecuencia y efecto del riesgo** Describir para cada riesgo identificado las posibles consecuencias que podría ocurrir si se materializa el riesgo, asimismo, el tipo de efecto del riesgo que puede ser positivo o negativo y registrarlas en la sección I del **formato: FPE03.03.01-PRONIED Matriz de riesgos**. De acuerdo al tipo de efecto del riesgo: - **Positivo**: Ir a la actividad N° 7. - **Negativo**: Ir a la actividad N° 8. *Nota: Un efecto es una desviación respecto a lo previsto. Puede ser positivo, negativo o ambos, y puede*	Unidad funcional responsable	Equipo de trabajo	Matriz de riesgos (Etapa I)

PRONIED
PROGRAMA NACIONAL DE INFRAESTRUCTURA EDUCATIVA
FIRMA DIGITAL

Firmado digitalmente por CUELLAR SASIETA Magdalena Aurora FAU 20514347221 soft
Motivo: Doy V° B°
Fecha: 20.01.2021 00:09:04 -05:00

MINISTERIO DE EDUCACIÓN · OFICINA DE PLANEAMIENTO Y PRESUPUESTO · V°B° · Director · PRONIED

VII. ACTIVIDADES DEL PROCEDIMIENTO				
Nº	**Actividad**	**Área**	**Responsable**	**Registro**
	abordar, crear o resultar en oportunidades y amenazas.			
7	**Seleccionar riesgos con efecto positivo** Seleccionar todos los riesgos con efecto positivo de la Matriz de riegos (riesgo con efecto positivo) para ser evaluados y tratados como oportunidad de mejora, de ser el caso, mediante el procedimiento **PE03.02.04.01-PRONIED Realizar acciones correctivas y oportunidades de mejora**. **Fin del procedimiento**	Unidad funcional responsable	Equipo de trabajo	Matriz de riesgos (riesgo con efecto positivo)
8	**Identificar los controles existentes** Identificar los controles existentes y el nivel correspondiente de acuerdo a lo establecido en el **anexo N° 5** y registrarlos en la sección II del **formato: FPE03.03.01-PRONIED Matriz de riesgos**.	Unidad funcional responsable	Equipo de trabajo	Matriz de riesgos (Etapa I)
ANÁLISIS Y EVALUACIÓN				
9	**Analizar los riesgos** Analizar los riesgos de acuerdo a los criterios de la "**Escala de probabilidad del riesgo**" establecida en el **anexo N° 6** y la "**Escala de impacto del riesgo**" establecida en el **anexo N° 7** y registrarlos en la sección III del **formato: FPE03.03.01-PRONIED Matriz de riesgos**. En caso corresponda a un nuevo análisis de un riesgo identificado y tratado con anterioridad, se debe registrar la información del riesgo residual calculado (sección VI) en una nueva matriz de riesgos como riesgo (sección III). La presente indicación aplica para las mediciones posteriores que se realizarán a los riesgos.	Unidad funcional responsable	Equipo de trabajo	Matriz de riesgos (Etapa I)
10	**Calcular el nivel de riesgo**	Unidad funcional responsable	Equipo de trabajo	Matriz de riesgos (Etapa I)

PRONIED PROGRAMA NACIONAL DE INFRAESTRUCTURA EDUCATIVA FIRMA DIGITAL

Firmado digitalmente por CUELLAR SASIETA Magdalena Aurora FAU 20514347221 soft
Motivo: Doy V° B°
Fecha: 20.01.2021 00:09:30 -05:00

MINISTERIO DE EDUCACIÓN OFICINA DE PLANEAMIENTO Y PRESUPUESTO V°B° Director PRONIED

VII. ACTIVIDADES DEL PROCEDIMIENTO				
Nº	**Actividad**	**Área**	**Responsable**	**Registro**
	Calcular el nivel de riesgo multiplicando los valores de la probabilidad y el impacto, determinados en la actividad N° 6. De acuerdo a la siguiente formula: **Nivel de riesgo = Probabilidad x Impacto** Identificar el nivel de riesgo de acuerdo a la **Matriz de impacto y probabilidad** establecida en el **anexo N° 8** y la tabla **de Niveles de riesgo** establecida en el **anexo N° 9**. Las valoraciones de los riesgos se registran en la sección III del **formato: FPE03.03.01-PRONIED Matriz de riesgos**. ¿El valor del riesgo obtenido se encuentra establecido como tolerable? - Sí: Se acepta el riesgo, Ir a la actividad N° 12. - No: Ir a la actividad N° 11. *Nota: Al aceptar el riesgo, no aplica (N.A.) realizar un plan de tratamiento de riesgos, es decir, no se ejecuta la etapa II de la matriz de riesgos.*			
TRATAMIENTO Y COMUNICACIÓN				
11	**Determinar el tratamiento del riesgo** Determinar el tratamiento para el riesgo definiendo el tipo de tratamiento[5], las acciones o controles necesarios para reducir el riesgo no tolerable, el registro o evidencia por presentar, responsables, recursos, plazos, teniendo en cuenta los controles ya existentes o implementados en cada uno de los procesos de PRONIED y registrarlos en la sección IV del **formato: FPE03.03.01-PRONIED Matriz de riesgos**.	Unidad funcional responsable	Equipo de trabajo	Matriz de riesgos (Etapa I)

VII. ACTIVIDADES DEL PROCEDIMIENTO

Nº	Actividad	Área	Responsable	Registro
	En caso la gestión de riesgos corresponda al SGSI se deben definir los controles de seguridad de la información a implementar, considerando los controles listados en la tabla A.1 del anexo A de la ISO 27001:2013. *[5]Las opciones para tratar el riesgo pueden implicar una o más de las opciones definidas en la tabla **Tipos de tratamiento del riesgo** establecido en el **anexo N° 10**.* *Nota: Al seleccionar opciones para el tratamiento del riesgo, se debe tomar en cuenta a las unidades funcionales que pueden afectar o verse afectadas por el tratamiento del riesgo determinado.*			
12	**Presentar la matriz de riesgos** Visar y presentar la matriz de riesgos, de acuerdo a la etapa que corresponda (Etapa I: Evaluación y tratamiento o Etapa II: Seguimiento y revisión), al(a la) coordinador(a) / especialista de Modernización de la OPP, cada vez que se realice alguna modificación y/o actualización a la matriz de riesgos.	Unidad funcional responsable	Representante del equipo de trabajo	Matriz de riesgos (Etapa I / Etapa II)
13	**Revisar la matriz de riesgos** Revisar que la matriz de riesgos cumpla con la metodología establecida; de acuerdo a la etapa que corresponda (Etapa I: Evaluación y tratamiento o Etapa II: Seguimiento y revisión). ¿Cumple la metodología establecida? - Sí: Ir a la actividad N° 15. - No: Ir a la actividad N° 14.	OPP	Coordinador(a) / Especialista de Modernización	Matriz de riesgos (Etapa I / Etapa II)
14	**Subsanar observaciones** Subsanar las observaciones identificadas en la matriz de riesgos, por la OPP. Luego ir a la actividad N° 12.	Unidad funcional responsable	Equipo de trabajo	Matriz de riesgos (Etapa I / Etapa II)
15	**Confirmar la matriz de riesgos**	OPP	Coordinador(a) / Especialista de Modernización	Matriz de riesgos

VII. ACTIVIDADES DEL PROCEDIMIENTO				
Nº	**Actividad**	**Área**	**Responsable**	**Registro**
	Confirmar mediante el correo electrónico institucional la correcta aplicación de la metodología en la elaboración de la matriz de riesgos, dicha confirmación se registra de acuerdo a la etapa que corresponda (Etapa I: Evaluación y tratamiento o Etapa II: Seguimiento y revisión) y remitir al(a la) director(a) de la unidad funcional responsable.			(Etapa I / Etapa II)
16	**Aprobar y difundir la matriz de riesgos** Aprobar la matriz de riesgos, mediante el visado de dicha matriz, de acuerdo a la etapa que corresponda (Etapa I: Evaluación y tratamiento o Etapa II: Seguimiento y revisión) y difundir mediante correo electrónico la matriz de riesgos a los involucrados en el proceso y al(a la) coordinador(a) / especialista de Modernización de la OPP. Según sea el caso: - **Riesgo tolerable / Tratamiento implementado**: Ir a la actividad N° 21. - **Tratamiento por implementar**: Ir en paralelo a la actividad N° 17, N° 18 y N° 21. *Nota: La información registrada en la matriz de riesgos aprobada, no puede ser modificada o alterada sin coordinación previa con la OPP.*	Unidad funcional responsable	Director(a)	Matriz de riesgos (Etapa I / Etapa II)
IMPLEMENTACIÓN Y/O MONITOREO				
17	**Realizar seguimiento a la implementación del tratamiento** Realizar el seguimiento a la implementación de los planes de tratamiento establecidos que buscan reducir los riesgos no tolerables, actualizando su estado en la sección V del **formato: FPE03.03.01-PRONIED Matriz de riesgos**. Los estados pueden ser:	OPP	Coordinador(a) / Especialista de Modernización	Matriz de riesgos (Etapa II)

VII. ACTIVIDADES DEL PROCEDIMIENTO

Nº	Actividad	Área	Responsable	Registro
	- **Sin implementación**: Cuando ninguno de los planes establecidos se ha iniciado. - **En implementación**: Cuando los planes establecidos están en proceso de implementación. - **Implementado**: Cuando los planes establecidos han sido implementados. - **N.A (no aplica)**: Cuando el riesgo es tolerable (no cuenta con plan de tratamiento de riesgos).			
18	**Implementar plan de tratamiento** Implementar el plan de tratamiento de acuerdo a lo determinado en la matriz de riesgos y dentro del plazo establecido; comunicando a través del correo electrónico institucional los avances y enviando los registros o evidencias de la implementación finalizada.	Unidad funcional responsable	Equipo de trabajo	Correo electrónico
19	**Analizar el riesgo residual** De acuerdo a la fecha determinada para la medición de la eficacia analizar el riesgo residual de acuerdo a los criterios de la "**Escala de probabilidad del riesgo**" establecida en el **anexo N° 6** y la "**Escala de impacto del riesgo**" establecida en el **anexo N° 7** y registrarlos en la sección IV del **formato: FPE03.03.01-PRONIED Matriz de riesgos**. *Nota: La medición de le eficacia del tratamiento del riesgo está referido al cálculo del riesgo residual, en la fecha establecida en la matriz de riesgos (sección V. Seguimiento al plan de tratamiento).*	Unidad funcional responsable	Equipo de trabajo	Matriz de riesgos (Etapa II)
20	**Calcular el nivel de riesgo residual** Calcular el nivel de riesgo residual multiplicando los valores de la probabilidad y el impacto, determinados en la actividad precedente. De acuerdo a la siguiente formula:	Unidad funcional responsable	Equipo de trabajo	Matriz de riesgos (Etapa II)

VII. ACTIVIDADES DEL PROCEDIMIENTO

Nº	Actividad	Área	Responsable	Registro
	Nivel de riesgo residual = Probabilidad x Impacto Identificar el nivel de riesgo de acuerdo a la **Matriz de impacto y probabilidad** establecida en el **anexo N° 8** y la tabla **de Niveles de riesgo** establecida en el **anexo N° 9**. Las valoraciones de los riesgos se registran en la sección VI del **formato: FPE03.03.01-PRONIED Matriz de riesgos**. *Nota: Se considera que las medidas de tratamiento fueron eficaces cuando hubo una disminución en la valoración del riesgo (Riesgo residual es menor al Riesgo inicial).* Luego ir a la actividad N° 12.			
21	**Monitorear los riesgos** Monitorear periódicamente el comportamiento de los riesgos, con el objetivo de: - Asegurar que los controles sean eficaces y eficientes en el diseño y funcionamiento. - Obtener más información para mejorar la evaluación de riesgos - Aprender lecciones a partir de los eventos, los cambios, las tendencias, los éxitos y los fracasos. - Detectar cambios en el contexto interno y externo. En caso la gestión de riesgos corresponda al SGAS, cada unidad funcional del PRONIED realiza la evaluación y revisión de los riesgos de soborno con una frecuencia mínima anual o cuando la situación lo amerite, realizando la coordinación respectiva con la OPP. De acuerdo al resultado del monitoreo:	Unidad funcional responsable	Representante del equipo de trabajo	Matriz de riesgos (Etapa II)

VII. ACTIVIDADES DEL PROCEDIMIENTO

Nº	Actividad	Área	Responsable	Registro
	- **Materialización del riesgo**: Ir a la actividad N° 23. - **Necesidad de revaluación**: Ir a la actividad N° 22.			
22	**Solicitar revaluación del riesgo** Solicitar mediante el correo electrónico institucional, al equipo de trabajo de la unidad funcional responsable, la revaluación del riesgo identificado, de acuerdo a la necesidad que amerite. *Nota: La revaluación del riesgo es para asegurar que el ciclo completo de la gestión de riesgos se repita según sea necesario para garantizar un control eficaz.* Luego ir a la actividad N° 2.	Unidad funcional responsable	Representante del equipo de trabajo	Correo electrónico
23	**Presentar registro de monitoreo por materialización del riesgo** Presentar el registro de monitoreo por materialización del riesgo para su tratamiento de acuerdo al procedimiento **PE03.02.04.01-PRONIED Realizar Acciones Correctivas y Oportunidades de Mejora.** **Fin del procedimiento**	Unidad funcional responsable	Representante del equipo de trabajo	Registro de monitoreo (riesgo materializado)

VIII. DOCUMENTOS RELACIONADOS

Nº	Documento
1	Formato: FPE03.03.01-PRONIED Matriz de riesgos

IX. PROCESO

Nombre	Tipo
PE03 Gestionar el desarrollo de la organización	Estratégico

X. SEGUIMIENTO

Ninguno

XI. INDICADOR

Nombre	Fórmula
Porcentaje de riesgos tolerables	$\%\ Riesgos\ aceptables = \frac{\text{N° Riesgos tolerables}}{\text{N° Total de Riesgos}} x100\%$

XII. ANEXOS

1. Tipos de riesgo
2. Herramientas básicas para análisis de datos
3. Cuadro de amenazas para el SGSI
4. Listado de vulnerabilidades para el SGSI
5. Niveles de control
6. Escala de probabilidad del riesgo
7. Escala de impacto del riesgo
8. Matriz de impacto y probabilidad
9. Niveles de riesgo
10. Tipos de tratamiento del riesgo
11. Diagrama de flujo

XIII. OTROS

1. No aplica

PRONIED
PROGRAMA NACIONAL
DE INFRAESTRUCTURA EDUCATIVA
FIRMA DIGITAL

Firmado digitalmente por CUELLAR SASIETA Magdalena Aurora FAU 20514347221 soft
Motivo: Doy V° B°
Fecha: 20.01.2021 00:12:11 -05:00

Anexo N° 1

Tipos de riesgo

TIPO DE RIESGO	DESCRIPCIÓN
Riesgo Estratégico	Se asocia con la forma en que se gestiona la entidad. El manejo del riesgo estratégico se enfoca en asuntos globales relacionados con la misión y el cumplimiento de los objetivos estratégicos, la clara definición de políticas y el diseño y conceptualización de la entidad por parte de la Alta Dirección.
Riesgo Operativo	Comprende los riesgos relacionados tanto con la parte operativa como técnica de la entidad, incluye riesgos provenientes de deficiencias en los sistemas de información, en la definición de los procesos, en la estructura organizacional, en la desarticulación entre dependencias, lo cual conduce a ineficiencias, oportunidades de corrupción incluyendo el soborno e incumplimiento de los compromisos institucionales.
Riesgo Financiero	Se relaciona con el manejo de los recursos de la entidad e incluye, la ejecución presupuestal, la elaboración de los estados financieros, los pagos, manejos de excedente de tesorería y manejo sobre los bienes. De la eficiencia y transparencia en el manejo de los recursos, así como su interacción con las demás áreas dependerá en gran parte el éxito o fracaso de la entidad.
Riesgo de Cumplimiento	Se asocian con la capacidad de la entidad para cumplir con los requisitos legales, contractuales, de ética pública y en general con su compromiso ante la comunidad.
Riesgo de Tecnología	Se asocia con la capacidad de la entidad para que la tecnología disponible satisfaga sus necesidades actuales y futuras, y soporte el cumplimiento de su misión.
Riesgo de Reputación	Posibilidad de pérdidas por la disminución de la confianza en la integridad de la institución que surge cuando el buen nombre de la entidad es afectado. El riesgo de reputación puede presentarse a partir de otros riesgos inherentes en las actividades de una organización.
Riesgo de Seguridad de la información	Son los riesgos que se generan a partir de la disponibilidad, protección, integridad y acceso a la información de la organización a través de su infraestructura, métodos y procesos de generación, almacenamiento, transporte, consulta y análisis. Son aquellos riesgos que atenten contra la disponibilidad, confidencialidad e integridad de la información independiente del medio en que esta se encuentre.
Riesgo de Corrupción	Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado. El riesgo de corrupción en la administración pública se relaciona a la comisión de delitos tales como: cobro indebido, colusión, peculado, malversación, cohecho, tráfico de influencias y enriquecimiento ilícito, entre otros.
Riesgo de Soborno	Relacionado a la oferta, promesa, entrega, aceptación o solicitud de una ventaja indebida de cualquier valor (que pude ser naturaleza financiera o no financiera), directamente o indirectamente, e independiente de su ubicación, en violación de la ley aplicable, como incentivo o recompensa para que una persona actué o deje de actuar en relación con el desempeño de las obligaciones de esa persona.

Anexo N° 2

Herramientas básicas para análisis de datos

1. LLUVIA DE IDEAS

¿Qué es?

Es una técnica que permite aprovechar el pensamiento creativo de un equipo para identificar posibles causas y soluciones de problemas, potenciales oportunidades de mejoramiento de la calidad.

¿Cuándo se usa?

- Cuando exista la necesidad de liberar la creatividad de los equipos
- Cuando se desee generar un número extenso de ideas
- Cuando se desee involucrar a todos los miembros de un proceso

¿Cómo se elabora?

a. Fase de generación
   - Nombrar al coordinador del grupo.
   - El coordinador explica concretamente el tema a tratar.
   - El coordinador concede la palabra a cada uno de los miembros por turno hasta agotar las ideas.
   - Las ideas se deben escribir en un lugar visible por todos.
   - Las ideas propuestas pueden servir como base a otras ideas
   - En esta etapa, las ideas no deben ser criticadas.
   - En esta fase, las ideas pueden recogerse de otras formas, por ejemplo, escribiéndose en un formato preestablecido o realizándose de manera silenciosa por un espacio de tiempo previamente definido.

b. Fase de aclaración
   - Proceder a la aclaración de cada una de las ideas
   - Se puede criticar o apoyar, cuestionar las ideas, no a las personas.
   - Se puede unir dos ideas si son similares.

c. Fase de votación
   - Se procede en función a su importancia o incidencia en el problema.
   - Se puede emplear sistema de ponderación para calificar las ideas.
   - Debe ser secreta para evitar influencias hacia determinadas ideas.
   - Si el número de ideas es grande, reducir a la mitad
   - Utilizar sistema de ponderación.

d. Fase de ordenamiento
   - Listar las ideas de “mayor a menor”, resolviendo una por una.
   - Agrupar.
   - Revisar la lista (rehacer según orden de importancia).

Consideraciones a tomar en cuenta

- El líder facilita, posibilita el compromiso y la fluidez.
- Todos son iguales, igual valoración.
- Todos entienden el tema a tratar.
- Se alienta la generación de ideas (aliente la extravagancia).
- No criticar ni alabar.
- No personas extrañas.
- Fijar un límite de tiempo (10 a 30 minutos).

2. CINCO PORQUÉS

¿Qué es?

Es una metodología que nos permite identificar consecuencias y causas.

¿Cuándo se usa?

Cuando se necesita realizar el análisis de un problema para identificar el efecto.

¿Cómo se elabora?

a. Se define el problema o el efecto
b. Luego se hace la pregunta ¿Por qué se ha producido el problema?
c. Se anota la o las respuestas
d. Luego se hace la pregunta ¿Por qué... (considerando las respuestas anteriores)?
e. Se repite el ejercicio 5 veces
f. Se considera la respuesta al quinto porque la causa raíz del problema

Consideraciones a tomar en cuenta

- En caso el equipo de mejora considere dos o más respuestas ante una pregunta evaluar las respuestas a considerar en la secuencia de preguntas siguientes.
- De ocurrir el caso anterior se obtendría más de una causa raíz ante el problema o efecto planteado.

Ejemplo de aplicación

Situación en una organización se presenta el siguiente problema: Las responsabilidades, autoridades y competencias del personal no han sido definidas en su totalidad. El documento SOF-RH-DDP-001.00 “Descripción de funciones y competencias” que contiene las funciones, responsabilidades, autoridades, competencias y niveles de comunicación para cada puesto de trabajo aún está en proceso de elaboración.

- Pregunta 1: ¿Por qué no se han definido las funciones, responsabilidades, autoridades, competencias y niveles de comunicación?
- Respuesta 1: Porque aún no se ha definido formalmente la estructura organizacional.
- Pregunta 2: ¿Por qué no se ha definido formalmente la estructura organizacional?
- Respuesta 2: Porque no se ha realizado un estudio técnico de respaldo
- Pregunta 3: ¿Por qué no se ha realizado un estudio técnico de respaldo?
- Respuesta 3 Por que el personal actual tiene labores que no le permiten realizar esta labor

- Pregunta 4: ¿Por qué personal actual tiene labores que no le permiten realizar esta labor?
- Respuesta 4: Porque no cuenta con personal de apoyo que le permita cumplir con los entregables a tiempo.
- Pregunta 5: ¿Por qué no cuenta con personal de apoyo que le permita cumplir con los entregables a tiempo?
- Respuesta 5: Porque no se ha presentado la solicitud de contratación de personal de apoyo.

  Causa Raíz: *No se cuenta con personal de apoyo que permita cumplir con los entregables del área sin descuidar las labores cotidianas.*

3. DIAGRAMA CAUSA – EFECTO (DIAGRAMA DE ISHIKAWA O DIAGRAMA DE ESPINAS DE PESCADO)

¿Qué es?

Es el diagrama que muestra la relación entre una característica de calidad y los factores. El diagrama causa – efecto sea tal vez la herramienta más útil con la que un equipo de mejora de procesos cuenta para determinar las causas que dan origen a una situación no deseada dentro de un proceso.

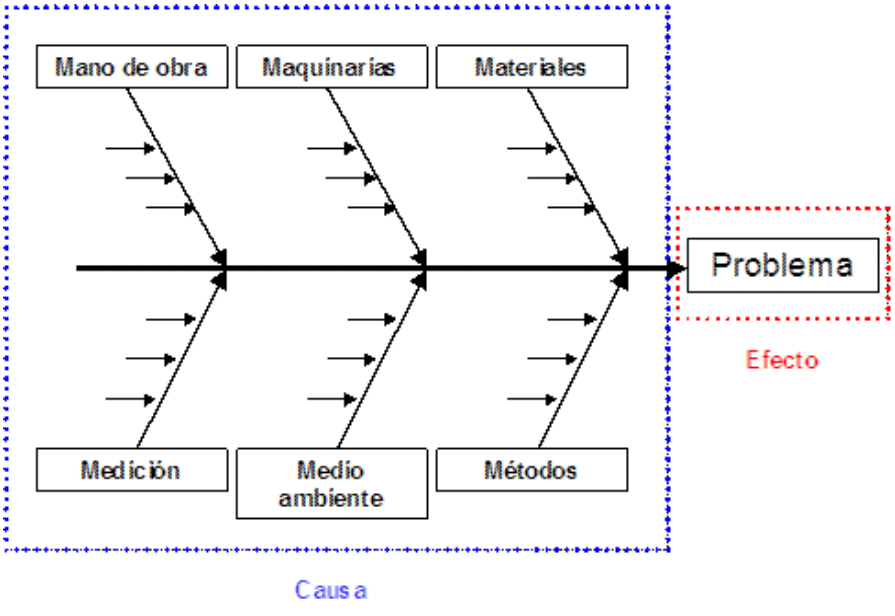
¿Cuándo se usa?

El diagrama causa – efecto se usa cuando se requiere determinar las causas – raíz de un problema, agrupándolas en causas comunes.

¿Cómo se elabora?

La elaboración de un diagrama causa efecto contempla los siguientes pasos:

a. Usar la siguiente plantilla



b. Conformar un equipo de trabajo para desarrollar la herramienta.

c. Nombrar a un coordinador para que lidere el uso de la herramienta.

d. Identificar el problema y escribirlo en el casillero “PROBLEMA” del diagrama. El problema (o “efecto”), es la característica que queremos mejorar o controlar. Se debe describir de manera clara y concisa, para que la “lluvia de ideas” respecto a la causa de dicho problema genere la mayor cantidad de ideas.

e. Escribir las causas primarias que afectan a dicha característica. Cada una de estas causas representa a uno de los seis principales factores que afectan a los procesos:

   - Las máquinas del proceso: hardware y software, equipos, instrumentos, entre otros, que son utilizados para ejecutar el proceso.
   - Los materiales que se usan en el proceso: insumos, información, entre otros, que ingresan al proceso.
   - Los métodos del proceso: conocimientos, documentos normativos, políticas, manuales, etc.
   - La mano de obra involucrada en el proceso: el recurso humano que participan en la ejecución del proceso.
   - La medición de los procesos: indicadores sobre calidad, oportunidad, cantidad, entre otros que miden el proceso hoy.
   - El medio ambiente que rodea al proceso: factores externos, tales como el clima, el gobierno, el entorno, la sociedad, etc. El equipo realizará el trabajo con ayuda de la herramienta “Lluvia de ideas” para la generación de posibles causas que originen el problema.

f. Escribir las causas secundarias que afectan a las primarias sobre una línea (a manera de espina).

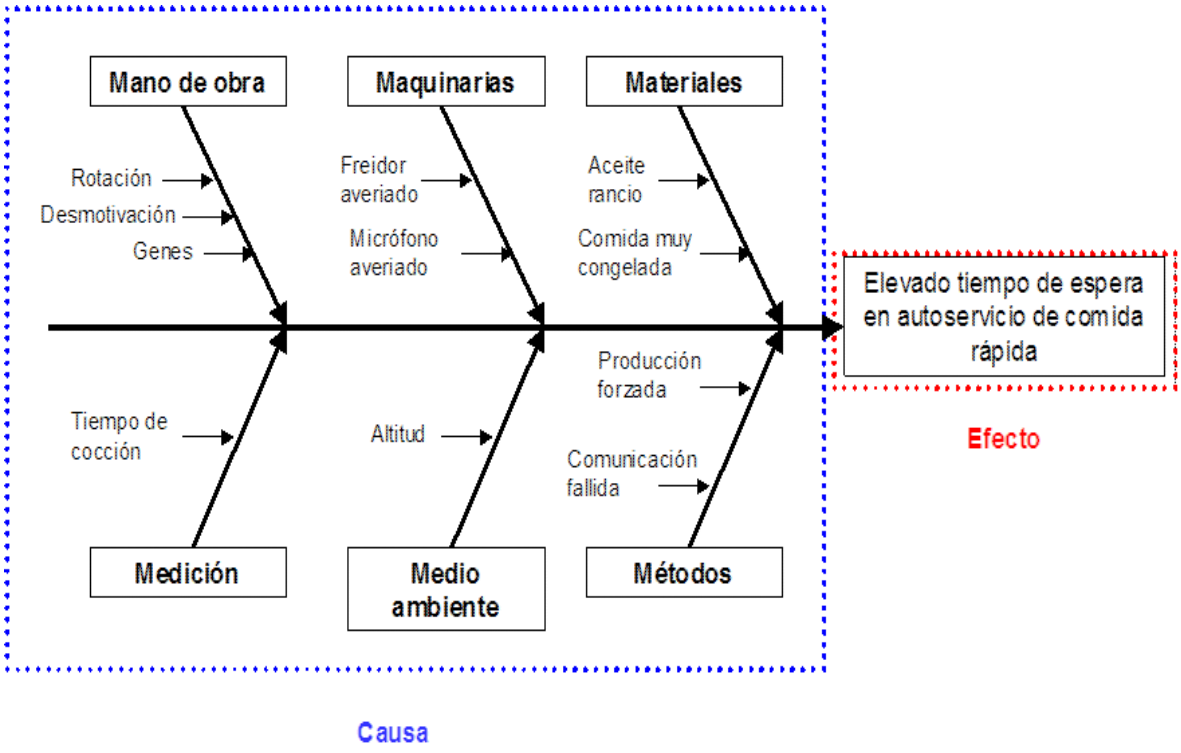
g. Escribir las causas terciarias que afectan a las secundarias.

h. Repetir si es necesario, para alguna causa, hasta agotar la “lluvia de ideas”.

Consideraciones a tomar en cuenta

- Los diagramas causa-efecto identifican causas posibles de un problema, por lo que se requiere de un análisis de datos para confirmar los resultados del uso de esta herramienta, por lo que lo ideal es escoger "causas medibles".
- La construcción de un diagrama causa efecto es más efectiva luego de construir el diagrama del proceso.
- Durante la construcción del diagrama causa efecto, se debe tener cuidado en captar todas las ideas, expresándolas tan concretamente como sea posible.
- No debatir ni criticar las ideas.
- Reunir las ideas repetidas.
- Construir un diagrama por cada problema.
- Reunir “problemas” sobre los que sea posible actuar.
- Con la finalidad de aumentar ideas, sobre problemas en los que hubo dificultad para generarlas durante el ejercicio en equipo, se puede exhibir el diagrama en murales con tránsito de personas relacionadas al “problema” e invitando a que dichas personas, utilizando papeles adhesivos, planteen ideas.

Ejemplo de aplicación



PRONIED
PROGRAMA NACIONAL
DE INFRAESTRUCTURA EDUCATIVA
FIRMA DIGITAL

Firmado digitalmente por CUELLAR SASIETA Magdalena Aurora FAU 20514347221 soft
Motivo: Doy V° B°
Fecha: 20.01.2021 00:14:22 -05:00

Anexo N° 3

Cuadro de amenazas para el SGSI

TIPO	AMENAZAS PARA EL SGSI
Daño Físico	Incendio
	Daño por agua
	Contaminación
	Accidente Importante
	Destrucción del equipo o los medio
	Polvo, corrosión, congelación
Eventos Naturales	Fenómeno Climático
	Fenómeno sísmico
	Fenómeno volcánico
	Fenómeno meteorológico
	Inundación
Pérdida de servicios esenciales	Fallas del sistema de aire acondicionado o del suministro de agua
	Perdida del suministro de electricidad
	Falla del equipo de telecomunicaciones
Perturbación debida a radiación	Radiación electromagnética
	Radiación térmica
	Pulsos electromagnéticos
Compromiso de información	Intercepción de señales de interferencia comprometedoras
	Espionaje remoto
	Interceptación de comunicaciones
	Robo de medios o documentos
	Robo de equipos
	Hallazgo de medios reciclados o descartados
	Divulgación
	Datos de fuentes no confiables
	Adulteración del Hardware
	Adulteración del software
	Detección de posición
Fallas Técnicas	Falla de equipo
	Mal funcionamiento del equipo
	Saturación del sistema de información
	Mal funcionamiento del software
	Brecha / fisura de mantenimiento de sistemas de información
Acciones no autorizadas	Uso no autorizado del equipo
	Copia fraudulenta del software
	Uso de software falsificado o copiado
	Corrupción de datos
	Procesamiento ilegal de datos
Compromiso de Funciones	Error en el uso
	Abuso de derechos
	Falsificación de derechos
	Negación de acciones
	Brecha de disponibilidad del personal
	Hacking

TIPO	AMENAZAS PARA EL SGSI
Interacción Humana	Ingeniería social
	Intrusión en el sistema, incursiones
	Acceso no autorizado al sistema
	Crimen informático (acoso cibernético)
	Acto fraudulento (reproducción de archivos, suplantación, intercepción)
	Soborno informático
	Falsificación o usurpación de la dirección
	Intrusión en el sistema
	Bomba/Terrorismo
	Equipo de guerra informática
	Ataque al sistema (ej. DDOS)
	Penetración en el sistema
	Adulteración/ manipulación del sistema
	Ventaja de defensa
	Ventaja política
	Explotación económica
	Robo de información
	Intrusión en la privacidad personal
	Asalto a un empleado
	Chantaje
	Búsqueda de información propietaria
	Abuso informático
	Fraude y robo
	Soborno por información
	Ingreso de datos falsificados o corruptos
	Intercepción
	Códigos maliciosos (ej. Virus, bomba lógica, troyano)
	Venta de información personal
	Disfunciones del sistema (bugs)
	Intrusión en el sistema
	Sabotaje al sistema

MINISTERIO DE EDUCACIÓN
OFICINA DE PLANEAMIENTO Y PRESUPUESTO
V°B°
Director
PRONIED

PRONIED
PROGRAMA NACIONAL
DE INFRAESTRUCTURA EDUCATIVA
FIRMA DIGITAL

Firmado digitalmente por CUELLAR SASIETA Magdalena Aurora FAU 20514347221 soft
Motivo: Doy V° B°
Fecha: 20.01.2021 00:15:01 -05:00

Anexo N° 4

Listado de vulnerabilidades para el SGSI

N°	VULNERABILIDADES PARA EL SGSI
1	Mantenimiento insuficiente / instalación fallida de medios de almacenamiento
2	Falta de esquemas de reemplazo periódicos
3	Susceptibilidad a la humedad, al polvo y a la suciedad
4	Sensibilidad a la radiación electromagnética
5	Falta de control eficiente del cambio de configuración
6	Susceptibilidad a variación de voltaje
7	Susceptibilidad a variaciones de temperatura
8	Almacenamiento no protegido
9	Falta de cuidado al descartarlo
10	Copia no controlada
11	Pruebas al software inexistentes o insuficientes
12	Errores conocidos en el software
13	No hacer "logout" cuando se sale de la estación de trabajo
14	Disposición o reutilización de medios de almacenamiento sin borrar apropiadamente
15	Falta de evidencia de auditoria
16	Asignación equivocada de derechos de acceso
17	Software ampliamente distribuido
18	Aplicar programas de aplicación a datos incorrectos en términos del tiempo
19	Interfaz de usuario complicada
20	Falta de documentación
21	Seteo incorrecto de parámetros
22	Fechas incorrectas
23	Falta de mecanismos de identificación y autentificación como la autentificación de usuarios
24	Tablas de claves no protegidas
25	Mala administración de claves
26	Habilitación de servicios innecesarios
27	Software inmaduro o nuevo
28	Especificaciones no claras o incompletas para los desarrolladores
29	Falta de control de cambios eficaz
30	Descarga y uso incontrolado de software
31	Falta de copias de respaldo
32	Falta de protección física del edificio, puertas y ventanas
33	No producir informes de gestión
34	Falta de pruebas de envió o recepción de mensaje
35	Líneas de comunicación no protegidas
36	Tráfico delicado no protegido
37	Juntas malas en el cableado
38	Punto de falla única
39	Falta de identificación y autentificación de destinador y destinatario
40	Arquitectura de red insegura
41	Transferencia de claves en claro
42	Gestión inadecuada de la red (capacidad de recuperación del ruteo)
43	Conexiones no protegidas de la red publica
44	Ausencia del personal

N°	VULNERABILIDADES PARA EL SGSI
45	Procedimientos inadecuados del reclutamiento
46	Capacitación de seguridad insuficiente
47	Uso incorrecto del software y hardware
48	Falta de conciencia de seguridad
49	Falta de mecanismos de monitoreo
50	Trabajo no supervisado del personal externo o de limpieza
51	Falta de políticas para el uso correcto de medios de telecomunicaciones y mensajería
52	Uso inadecuado o negligente del control de acceso físico a edificios y ambientes
53	Ubicaciones en un área susceptible a las inundaciones
54	Red inestable de energía eléctrica
55	Falta de protección física del edificio, puertas y ventanas
56	Falta de un procedimiento formal para el registro y baja de usuarios
57	Falta de proceso formal para revisar el derecho de acceso (supervisión)
58	Disposiciones inexistentes o insuficientes (respecto de la seguridad) en contratos con clientes y/o terceros
59	Falta de procedimientos de monitoreo de instalaciones de procesamiento de la información
60	Falta de auditorías regulares (supervisión)
61	Falta de procedimientos de identificación y evaluación del riesgo
62	Falta de informes de fallas registradas en los registros del administrador y del operador
63	Respuesta inadecuada del mantenimiento del servicio
64	Inexistencia o insuficiencia de acuerdo sobre el nivel de servicio
65	Falta de procedimiento de control de cambios
66	Falta de procedimiento formal para el control de la documentación de la empresa
67	Falta de procedimiento formal para la supervisión del registro de la empresa
68	Falta de proceso formal para autorización de información pública disponible
69	Falta de asignación apropiada de responsabilidades de seguridad en la información
70	Falta de planes de continuidad
71	Falta de una política de uso de correos electrónicos
72	Falta de procedimientos para introducir software en sistemas operativos
73	Faltas de registro en los historiales del administrador y del operador
74	Falta de procedimientos para manejo de la información clasificada
75	Falta de responsabilidades sobre la seguridad de la información en las descripciones de puestos
76	Ausencia o insuficiencia de disposiciones (concernientes a la seguridad de la información en contratos con empleados)
77	Falta de proceso disciplinario definido en caso de incidentes en la seguridad de la información
78	Falta de política formal sobre el uso de computadoras portátiles
79	Falta de control de activos que se encuentran fuera del local
80	Inexistencia o insuficiencia de la política de "escritorio despejado y pantalla despejada"
81	Falta de autorización al acceso a las instalaciones de procesamiento de la información
82	Falta de mecanismos de monitoreo establecidos para las rupturas de la seguridad
83	Falta de revisiones regulares de la gestión
84	Falta de procedimientos para reportar debilidades en la seguridad
85	Falta de procedimientos sobre el cumplimiento de disposiciones respecto de derechos intelectuales

MINISTERIO DE EDUCACIÓN - V°B° - Director - PRONIED

PRONIED PROGRAMA NACIONAL DE INFRAESTRUCTURA EDUCATIVA
FIRMA DIGITAL

Firmado digitalmente por CUELLAR SASIETA Magdalena Aurora FAU 20514347221 soft
Motivo: Doy V° B°
Fecha: 20.01.2021 00:15:48 -05:00

Anexo N° 5

Niveles de control

NIVEL	DESCRIPCIÓN
Muy deficiente	El control no ha sido aplicado; no existen responsables definidos de la ejecución del control ni una supervisión de los responsables; no permite restringir la acción que genera el riesgo, no existen protocolos para proceder ante riesgo advertido por el control; no hay evidencia de documentos que acrediten su cumplimiento y registro temporal.
Deficiente	El control no ha sido informado a todos los colaboradores, no todos lo aceptan; se ejecuta a veces, no se supervisa; no existen responsables para su ejecución; permite restringir en parte la acción que genera el riesgo, no cuenta con protocolos; no hay evidencia de documentos que acrediten su cumplimiento y registro temporal.
Insuficiente	El control ha sido informado a todos los colaboradores, pero no todos lo aceptan; se ejecuta y supervisa a veces; no existen responsables para ejecutarlo; permite restringir en parte la acción que genera el riesgo, cuenta con protocolos; hay evidencia de documentos que acrediten su cumplimiento mas no su registro temporal.
Mejorable	El control ha sido informado y es aceptado por los colaboradores; no existen herramientas para su gestión; se ejecuta según los tiempos establecidos, no siempre se supervisa; existen responsables para su ejecución; permite restringir en parte la acción que genera el riesgo, cuenta con protocolos; hay evidencia de documentos que acreditan su cumplimiento y registro temporal.
Apropiada	El control ha sido informado a todo el PRONIED, es aceptado por los colaboradores, existen herramientas que permiten gestionarlo; se ejecuta y da seguimiento en los tiempos establecidos; existen responsables para su ejecución; permite restringir la acción que genera el riesgo, cuenta con protocolos; hay evidencia de documentos que acreditan su cumplimiento y registro temporal.

PRONIED
PROGRAMA NACIONAL
DE INFRAESTRUCTURA EDUCATIVA
FIRMA DIGITAL

Firmado digitalmente por CUELLAR SASIETA Magdalena Aurora FAU 20514347221 soft
Motivo: Doy V° B°
Fecha: 20.01.2021 00:16:34 -05:00

Anexo N° 6

Escala de probabilidad del riesgo

PROBABILIDAD DEL RIESGO*		
NIVEL	**VALOR**	**DESCRICPIÓN**
Baja	**4**	El evento puede ocurrir solo bajo circunstancias excepcionales
		Ocurrencia del evento una (01) vez al año
		Muy baja probabilidad de ocurrencia entre 1% y 25% relacionado al proceso que se aplica
Media	**6**	El evento puede ocurrir en algún momento.
		Ocurrencia del evento por lo menos dos (02) veces al año y a lo más seis (06) veces al año
		Baja probabilidad de ocurrencia entre 26% y 50% relacionado al proceso que se aplica
Alta	**8**	El evento puede ocurrir en casi cualquier circunstancia
		Ocurrencia del evento por lo menos siete (07) veces al año y doce (12) veces al año
		Significativa probabilidad de ocurrencia entre el 61% y 80% relacionado al proceso que se aplica
Muy Alta	**10**	Se espera la ocurrencia del evento en la mayoría de las circunstancias
		Ocurrencia del evento más de doce (12) veces al año
		Casi con certeza se espera la ocurrencia del evento entre 81% y 100% relacionado al proceso que se aplica

**No aplica para riesgos de soborno o corrupción*.

PROBABILIDAD PARA RIESGOS DE SOBORNO O CORRUPCIÓN		
NIVEL	**VALOR**	**DESCRICPIÓN**
Baja	**4**	Ocurrencia del evento una (01) vez cada tres (03) años
Media	**6**	Ocurrencia del evento una (01) vez cada dos (02) años
Alta	**8**	Ocurrencia del evento una (01) vez al año
Muy Alta	**10**	Ocurrencia del evento dos (02) veces al año

PRONIED
PROGRAMA NACIONAL
DE INFRAESTRUCTURA EDUCATIVA
FIRMA DIGITAL

Firmado digitalmente por CUELLAR SASIETA Magdalena Aurora FAU 20514347221 soft
Motivo: Doy V° B°
Fecha: 20.01.2021 00:16:59 -05:00

Anexo N° 7

Escala de impacto del riesgo

ESCALA DE IMPACTO DEL RIESGO*				
NIVEL	VALOR	DESCRIPCIÓN		
		IMPACTO EN LA REPUTACIÓN Y/O LEGAL	IMPACTO EN LAS ACTIVIDADES	PÉRDIDAS
Bajo	4	Se toma conocimiento de la acción y no es necesaria su atención por las unidades funcionales.	Paralización de algún sistema administrativo del PRONIED durante máximo cuatro (04) horas laborables de un día.	Pérdida bruta menor o igual a 1UIT
		Sin publicidad en medios formales como diarios y televisión.	El personal se dedica menos del 10% de su tiempo laboral para manejar el impacto.	
		Sin investigación interna en cada unidad funcional.	Interrupción de los sistemas CORE del PRONIED durante máximo diez (10) horas laborables al año.	
		Sin impacto normativo y/o legal, pérdida insignificante.	Sin impacto en el cumplimiento de las metas.	
Medio	6	Recibe atención de la Alta Dirección.	Paralización de algún sistema administrativo del PRONIED por un día (01) completo hasta dos (02) días.	Pérdida bruta mayor a 1 UIT y menor o igual a 10 UIT
		Cobertura moderada de medios de comunicación nacionales.	El personal se dedica entre el 21% y el 30% de su tiempo laboral para manejar el impacto.	
		Observaciones del Órgano de Control Institucional sobre la gestión interna del PRONIED.	Interrupción de los sistemas CORE del PRONIED durante máximo treinta (30) horas laborables al año.	
		Desfase de cumplimiento de normativas, pudiendo generar pérdidas.	Desviación del 1% al 10% respecto de la meta planteada.	

MINISTERIO DE EDUCACIÓN
OFICINA DE PLANEAMIENTO Y PRESUPUESTO
V°B°
Director
PRONIED

PRONIED
PROGRAMA NACIONAL
DE INFRAESTRUCTURA EDUCATIVA
FIRMA DIGITAL

Firmado digitalmente por CUELLAR SASIETA Magdalena Aurora FAU 20514347221 soft
Motivo: Doy V° B°
Fecha: 20.01.2021 00:17:15 -05:00

ESCALA DE IMPACTO DEL RIESGO*				
NIVEL	**VALOR**	**DESCRIPCIÓN**		
		IMPACTO EN LA REPUTACIÓN Y/O LEGAL	**IMPACTO EN LAS ACTIVIDADES**	**PÉRDIDAS**
Alto	**8**	Recibe atención del Sector.	Paralización de algún sistema administrativo del PRONIED por más de dos (02) días y menos de cuatro (04) días.	Pérdida bruta mayor a 10 UIT y menor o igual a 90 UIT
		Cobertura de medios de comunicación nacionales.	El personal se dedica entre el 31% y el 40% de su tiempo laboral para manejar el impacto.	
		Hallazgo del Órgano de Control Institucional sobre la gestión interna del PRONIED.	Interrupción de los sistemas CORE del PRONIED entre treinta (30) y sesenta (60) horas laborables al año.	
		Sanciones administrativas y contingencias legales, ocasiona pérdidas.	Desviación del porcentaje de participación del monto contratado de 11% al 25% respecto de la meta planteada.	
Muy Alto	**10**	Recibe atención del Sector y del Congreso.	Paralización de algún sistema administrativo del PRONIED por más de cuatro (04) días.	Pérdida bruta mayor a 90 UIT
		Alta cobertura de medios de comunicación nacionales y cobertura por medios de comunicación extranjeros.	El personal se dedica más del 40% de su tiempo laboral para manejar el impacto.	
		Hallazgo de la Contraloría sobre la gestión interna del PRONIED.	Interrupción de los sistemas CORE del PRONIED por más de sesenta (60) horas laborables al año.	
		Contingencias judiciales y multas impuestas, pérdidas muy significativas.	Desviación de más del 25% respecto de la meta planteada.	

**No aplica para riesgos de seguridad de la información.*

MINISTERIO DE EDUCACIÓN – OFICINA DE PLANEAMIENTO Y PRESUPUESTO – PRONIED – Director

PRONIED
PROGRAMA NACIONAL
DE INFRAESTRUCTURA EDUCATIVA
FIRMA DIGITAL

Firmado digitalmente por CUELLAR SASIETA Magdalena Aurora FAU 20514147231 soft
Motivo: Doy V° B°
Fecha: 20.01.2021 00:17:34 -05:00

ESCALA DE IMPACTO DEL RIESGO DE SEGURIDAD DE LA INFORMACIÓN		
NIVEL	**VALOR**	**DESCRICPIÓN**
Bajo	**4**	El impacto es leve y se puede prescindir del mismo en un tiempo limitado, no afecta la confidencialidad, integridad y disponibilidad de la información o activos de información.
Medio	**6**	El impacto sobre la confidencialidad, integridad y disponibilidad de la información o activos de información es limitado en tiempo y alcance. Su efecto es para un proceso de soporte o actividad específica que puede subsanarse en corto plazo.
Alto	**8**	Impacta en forma grave a un área o servicio específico de la institución, se puede llegar a comprometer activos de información o documentos internos clasificados como confidenciales, paralizar o retrasar procesos claves de la institución por un tiempo considerable. Su efecto está limitado dentro de la institución.
Muy Alto	**10**	Impacta en forma severa en la institución al punto de comprometer la confidencialidad o integridad de los activos de información o información crítica de la institución o la continuidad de las operaciones por paralización de los servicios críticos más allá de los tiempos tolerables por el negocio. El impacto es a toda la institución y su efecto se siente en todo el personal involucrado y a partes externas.

PRONIED
PROGRAMA NACIONAL
DE INFRAESTRUCTURA EDUCATIVA
FIRMA DIGITAL

Firmado digitalmente por CUELLAR SASIETA Magdalena Aurora FAU 20514347221 soft
Motivo: Doy V° B°
Fecha: 20.01.2021 00:17:52 -05:00

Anexo N° 8

Matriz de impacto y probabilidad

MATRIZ DE IMPACTO Y PROBABILIDAD

			IMPACTO			
			Bajo	Medio	Alto	Muy alto
			4	6	8	10
PROBABILIDAD	Muy alto	10	40 (RM)	60 (RA)	80 (RMA)	100 (RMA)
	Alta	8	32 (RM)	48 (RA)	64 (RA)	80 (RMA)
	Media	6	24 (RB)	36 (RM)	48 (RA)	60 (RA)
	Baja	4	16 (RB)	24 (RB)	32 (RM)	40 (RM)

Leyenda:

- RB: Riesgo Bajo
- RM: Riesgo Medio
- RA: Riesgo Alto
- RMA: Riesgo Muy Alto

MINISTERIO DE EDUCACIÓN OFICINA DE PLANEAMIENTO Y PRESUPUESTO V°B° Director PRONIED

PRONIED
PROGRAMA NACIONAL DE INFRAESTRUCTURA EDUCATIVA
FIRMA DIGITAL

Firmado digitalmente por CUELLAR SASIETA Magdalena Aurora FAU 20514347221 soft
Motivo: Doy V° B°
Fecha: 20.01.2021 00:18:12 -05:00

Anexo N° 7

Niveles de riesgo

NIVELES DE RIESGO			
NIVEL	**VALORES POR INTERVALOS (RANGO)**	**TOLERANCIA AL RIESGO**	**DESCRIPCIÓN**
Riesgo Bajo (RB)	[16 - 24]	Tolerable 	Se acepta el riesgo, manteniendo el monitoreo sobre las actividades de control vigentes, sin embargo, no debe dejarse de evaluar las causas que podrían conllevar a que el riesgo se traslade a otro nivel superior.
Riesgo Medio (RM)	[32 - 40]	No tolerable 	Se deben establecer acciones / controles necesarios para el tratamiento del riesgo.
Riesgo Alto (RA)	[48 - 64]		
Riesgo Muy Alto (RMA)	[80 - 100]		

PRONIED
PROGRAMA NACIONAL DE INFRAESTRUCTURA EDUCATIVA
FIRMA DIGITAL

Firmado digitalmente por CUELLAR SASIETA Magdalena Aurora FAU 20514347221 soft
Motivo: Doy V° B°
Fecha: 20.01.2021 00:18:29 -05:00

Anexo N° 10

Tipos de tratamiento del riesgo

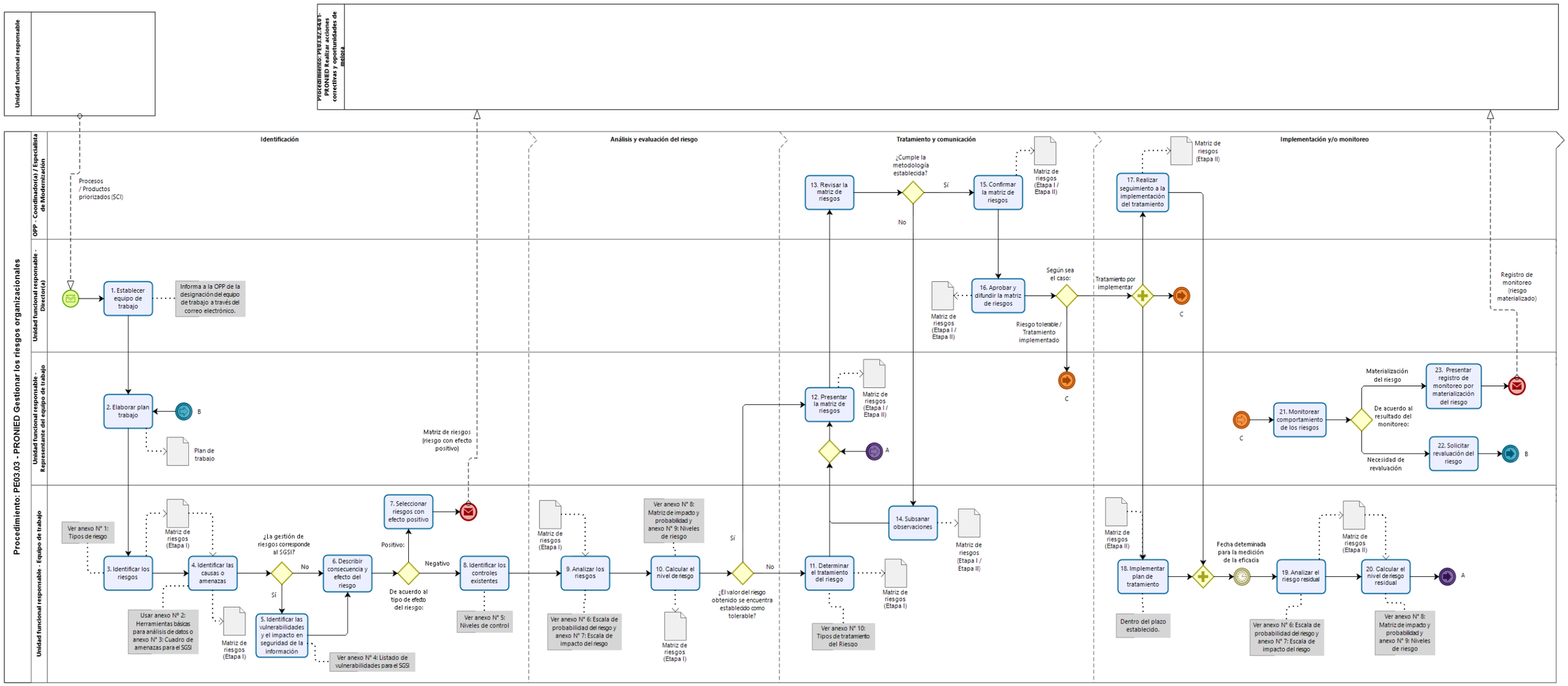
TIPOS DE TRATAMIENTO DEL RIESGO	
TIPO	**DESCRIPCIÓN**
Evitar	Implica tomar las medidas para prevenir un riesgo adverso o caso contrario no proseguir con la actividad riesgosa cuando esto sea factible.
Mitigar	Implica tomar las medidas necesarias tendientes a reducir la probabilidad y el impacto, o ambos casos a la vez.
Compartir o Transferir	Implica compartir parte del riesgo con terceros o simplemente dar a otra parte la responsabilidad de su gestión.
Aceptar	Implica aceptar el riesgo sin gestionarlo; toda vez que, no causa ningún efecto, por consiguiente, no se requiere ningún tratamiento.

MINISTERIO DE EDUCACIÓN
OFICINA DE PLANEAMIENTO Y PRESUPUESTO
V°B°
Director
PRONIED

PRONIED
PROGRAMA NACIONAL
DE INFRAESTRUCTURA EDUCATIVA
FIRMA DIGITAL

Firmado digitalmente por CUELLAR SASIETA Magdalena Aurora FAU 20514347221 soft
Motivo: Doy V° B°
Fecha: 20.01.2021 00:18:49 -05:00

Anexo N° 11
Diagrama de flujo



MINISTERIO DE EDUCACIÓN
OFICINA DE PLANEAMIENTO Y PRESUPUESTO
V°B°
Director
PRONIED

PRONIED
PROGRAMA NACIONAL
DE INFRAESTRUCTURA EDUCATIVA
FIRMA DIGITAL

Firmado digitalmente por CUELLAR SASIETA Magdalena Aurora FAU 20514347221 soft
Motivo: Doy V° B°
Fecha: 20.01.2021 00:19:26 -05:00