Miraflores, 27 de Diciembre del 2023

RESOLUCIÓN DE DIRECCIÓN EJECUTIVA N° 000268-2023-MIDIS/PNADP-DE

VISTOS:

El Informe N° 015-2023-MIDIS/PNADP-UTI del 17 de abril de 2023, de la Unidad de Tecnologías de la Información; el Memorando N° 2335-2023-MIDIS/PNADP-UPPM del 12 de diciembre de 2023, de la Unidad de Planeamiento, Presupuesto y Modernización; el Informe N° 099-2023-MIDIS/PNADP-UPPM-CMG de la Coordinadora de Modernización de la Gestión; y el Informe N° 436-2023-MIDIS/PNADP-UAJ del 27 de diciembre de 2023 de la Unidad de Asesoría Jurídica; y,

CONSIDERANDO:

Que, mediante Decreto Supremo Nº 032-2005-PCM, modificado por el Decreto Supremo Nº 062-2005-PCM, el Decreto Supremo Nº 012-2012-MIDIS y el Decreto Supremo Nº 002-2021-MIDIS, se crea el Programa Nacional de Apoyo Directo a los Más Pobres "JUNTOS", el cual tiene por finalidad ejecutar transferencias directas en beneficio de los hogares en condición de pobreza o pobreza extrema de acuerdo con el Sistema de Focalización de Hogares (SISFOH), priorizando progresivamente su intervención a nivel nacional. El Programa promueve en los hogares, con su participación y compromiso voluntario, el acceso a los servicios de salud y educación, orientados a mejorar la salud y nutrición preventiva materno-infantil y la escolaridad sin deserción;

Que, la población objetivo del Programa Nacional de Apoyo Directo a los Más Pobres "JUNTOS", son los hogares integrados por gestantes, niñas, niños y/o adolescentes en condición de pobreza, hasta que culminen la educación secundaria o cumplan diecinueve años, lo que ocurra primero. Los hogares se comprometen a cumplir los compromisos establecidos por el programa;

Que, mediante Resolución Ministerial N° 278-2017-MIDIS, se aprueba el Manual de Operaciones del Programa Nacional de Apoyo Directo a los Más Pobres "JUNTOS", el cual constituye el documento técnico normativo de gestión institucional, que determina la estructura orgánica, describe sus funciones generales, las funciones específicas de las unidades que lo integran, así como la descripción de los procesos estratégicos, misionales y de apoyo del Programa;

Que, en mérito a las normas señaladas, la Dirección Ejecutiva es la máxima autoridad ejecutiva y administrativa del Programa Nacional de Apoyo Directo a los Más Pobres "JUNTOS", teniendo entre sus funciones la emisión de Resoluciones de Dirección Ejecutiva en asuntos de su competencia;

Que, el artículo 20 del Manual de Operaciones establece que "La Unidad de Unidad de Tecnologías de la Información es responsable de planificar, ejecutar, monitorear y evaluar el desarrollo, implementación y mantenimiento de soluciones Tecnológicas de la Información (TI) en apoyo a las Unidades del Programa, y de la Secretaría de Gobierno Digital de la Presidencia del Consejo de Ministros (PCM)";

Que, mediante Informe N° 015-2023-MIDIS/PNADP-UTI del 17 de abril de 2023, la Unidad de Tecnologías de la Información formula la propuesta normativa denominada "Pautas para la gestión de riesgos de seguridad de la información", señalando que permitirá prevenir los efectos de las vulnerabilidades de los activos de información del Programa, garantizando la disponibilidad, confidencialidad e integridad de la información;

Que, con Memorando N° 2335-2023-MIDIS/PNADP-UPPM del 12 de diciembre de 2023, la Unidad de Planeamiento, Presupuesto y Modernización hace suyo y traslada el Informe N° 099-2023-MIDIS/PNADP-UPPM-CMG de la Coordinadora de Modernización de la Gestión, concluyendo que las "Pautas para la gestión de riesgos de seguridad de la información", se encuentra articulada a las normas de control interno, al macroproceso 'Modernización y gestión de la calidad', proceso de

'Gestión de la calidad' y al subproceso de 'Análisis y Mejora Continua' establecido en el Manual de Operaciones, y contribuye al componente insumo 'Normatividad vigente' y resultados esperados establecidos en la cadena de valor aprobada con Resolución de Dirección Ejecutiva N° 137-2020-MIDIS-PNADP-DE, emitiendo opinión favorable para su aprobación;

Que, con Informe N° 436-2023-MIDIS/PNADP-UAJ del 27 de diciembre de 2023, la Unidad de Asesoría Jurídica estima viable la emisión de la Resolución de Dirección Ejecutiva que apruebe el documento normativo antes indicado;

Con el visado de la Unidad de Tecnologías de la Información, de la Unidad de Planeamiento, Presupuesto y Modernización, y de la Unidad de Asesoría Jurídica;

En ejercicio de las facultades previstas en el Decreto Supremo N° 032-2005-PCM, modificado por el Decreto Supremo N° 062-2005-PCM, el Decreto Supremo N° 012-2012-MIDIS y el Decreto Supremo N° 002-2021-MIDIS; la Resolución Ministerial N° 068-2020-MIDIS; y estando a lo establecido por el Manual de Operaciones del Programa Nacional de Apoyo Directo a los Más Pobres "JUNTOS", aprobado por Resolución Ministerial N° 278-2017-MIDIS;

SE RESUELVE:

Artículo 1.- Aprobar las Pautas para la gestión de riesgos de seguridad de la información del Programa Nacional de Apoyo Directo a los Más Pobres "JUNTOS", que en anexo forma parte integrante de la presente Resolución.

Artículo 2.- Encargar a la Unidad de de Tecnologías de la Información la implementación y socialización del documento aprobado en el artículo 1 de la presente Resolución, entre los integrantes del Programa, y que las Unidades realicen las acciones necesarias para la aplicación respectiva.

Artículo 3.- Disponer que la Unidad de Comunicación e Imagen publique la presente Resolución en el Portal de Transparencia Estándar y en el Portal Institucional del Programa Nacional de Apoyo Directo a los Más Pobres "JUNTOS" (www.gob.pe/juntos), en el plazo de dos (02) días desde su emisión.

Regístrese y comuníquese.

DOCUMENTO

PAUTAS PARA LA GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Elaborado por:	Revisado por:	Aprobado por:
Miguel Santiago Ávila Jara Jefe de la Unidad de Tecnologías de la Información	Imelda Diana Silva Pretel Jefa de la Unidad de Planeamiento, Presupuesto y Modernización Jaime Erick Ríos Aquino Jefe de Unidad de Asesoría Jurídica	Jessica Cecilia Niño de Guzmán Esaine Directora Ejecutiva

Hoja de control de cambios

Versión	Fecha	Justificación	Textos Modificados	Responsable
01	Elaboración inicial del documento			UTI

INDICE

1. OBJETIVO

Establecer las pautas para identificar, analizar, evaluar y tratar los riesgos a los que están expuestos los activos de la información del Programa Nacional de Apoyo Directo a los Más Pobres "JUNTOS", en adelante el Programa JUNTOS; a fin de implementar medidas de control para garantizar la confidencialidad, integridad y disponibilidad de la información importante como parte del Sistema de Gestión de Seguridad de la Información.

2. ALCANCE

Aplica a todos los procesos y/o actividades en los cuales se dispone de activos de información; así como en los puestos de interacción vinculantes de las unidades orgánicas del Programa JUNTOS.

3. BASE LEGAL

3.1 Ley N° 27658, Ley Marco de Modernización de la Gestión del Estado y modificatorias.
3.2 Ley Nº 29792, Ley de creación, organización y funciones del Ministerio de Desarrollo e Inclusión Social.
3.3 Decreto Supremo N° 103-2022-PCM que aprueba la Política Nacional de Modernización de la Gestión Pública al 2030.
3.4 Decreto Supremo N° 004-2019-JUS, que aprueba el Texto Único Ordenado de la Ley N° 27444 – Ley del Procedimiento Administrativo General.
3.5 Decreto Supremo N° 032-2005-PCM, que crea el Programa Nacional de Apoyo Directo a los Más Pobres "JUNTOS", modificado por los Decretos Supremos N° 062-2005-PCM N° 012-2012-MIDIS y 002-2021-MIDIS.
3.6 Resolución de Secretaría de Gobierno Digital N° 001-2017-PCM/SEGDI, que aprueba el Modelo de Gestión Documental en el marco del Decreto Legislativo N° 1310.
3.7 Resolución Ministerial N° 278-2017-MIDIS, que aprueba el Manual de Operaciones del Programa JUNTOS.
3.8 Resolución Ministerial Nº 138-2021-MIDIS, que aprueba el Manual Nº 004-2021-MIDIS – "Manual para la Gestión de Riesgos de Procesos en el Ministerio de Desarrollo e Inclusión Social".
3.9 Norma Internacional ISO/IEC 27001: Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos.
3.10 Norma Internacional ISO 31000:2018 Directrices para la Gestión de Riesgos
3.11 Norma Técnica Peruana NTP-ISO/IEC 27005:2018 Técnicas de la seguridad. Gestión de riesgos de seguridad de la información
3.12 Norma Técnica Peruana NTP-ISO/IEC 17799:2007 Tecnología de la Información. Código de Buenas Prácticas para la Gestión de la Seguridad de la Información.
3.13 Norma ISO/IEC 27005:2011 Tecnología de la Información. Técnicas de seguridad. Gestión de Riesgos de Seguridad de la Información.
3.14 Resolución de Dirección Ejecutiva Nº 205-2023-MIDIS/PNADP-DE, que aprueba la reconformación del Comité de Gobierno y Transformación Digital del Programa Nacional de Apoyo Directo a los Más Pobres "JUNTOS".
3.15 Resolución de Dirección Ejecutiva Nº 204-2023-MIDIS/PNADP-DE, que actualiza la denominación del Oficial de Seguridad y Confianza Digital del Programa Nacional de Apoyo Directo a los Más Pobres "JUNTOS".

4. SIGLAS Y DEFINICIONES

4.1 **Activo de información**: Es todo aquello que contenga información, que la institución valora y por lo tanto debe proteger.
4.2 **Administrador/a de riesgos de Seguridad de la información:** Este rol es asumido por el/la Oficial de Seguridad y Confianza Digital.
4.3 **Amenaza:** Causa potencial de un incidente no deseado que puede resultar en daño al sistema u organización.

4.4 **Análisis de riesgos:** Uso sistemático de información para identificar amenazas y estimar el riego.

4.5 **Confidencialidad:** Garantizar que la información sea accesible únicamente para quienes tengan acceso autorizado.

4.6 **Consecuencia:** Resultado de un acontecimiento que afecta los objetivos de la organización. Una consecuencia puede ser cierta o incierta y, en el contexto de la seguridad de la información, suele ser negativa.

4.7 **Control:** Medida que el Programa JUNTOS establece para afrontar o responder al riesgo. Los controles incluyen, pero no se limitan a cualquier, proceso, política, dispositivo, práctica u otras condiciones y/o acciones que mantengan y/o modifiquen un riesgo.

4.8 **Control existente:** Medida que el Programa JUNTOS viene realizando y que contribuye a afrontar el riesgo identificado.

4.9 **Criticidad:** Valor que determina la dependencia del proceso con el activo. A mayor valor de criticidad mayores consecuencias para el negocio supone la pérdida del activo.

4.10 **Disponibilidad:** Garantizar que los usuarios tengan acceso a la información y activos asociados para cuando sea necesario.

4.11 **Dueño/a del proceso:** Es quien tiene la responsabilidad y la autoridad definidas para diseñar, implementar, controlar y mejorar los procesos a su cargo, con el propósito de asegurar que se cumpla el resultado previsto.

4.12 **Equipo de gestión de riesgos de Seguridad de la información:** Es el equipo conformado para atender la gestión de riesgos y que es liderado por el Oficial de Seguridad y Confianza Digital.

4.13 **Evaluación de riesgos:** Procesos de comparación del riesgo estimado frente a los criterios de riesgo para determinar el significado de riesgo.

4.14 **Gestión del riesgo:** Conjunto de acciones y actividades que realiza el Programa JUNTOS para identificar, evaluar y tratar el riesgo.

4.15 **Impacto:** Magnitud de las consecuencias que pueden ocasionar a la entidad en caso de riesgo se materialice.

4.16 **Integridad:** Salvaguardar la exactitud e integridad de la información y activos asociados.

4.17 **Matriz de riesgo**: Instrumento que permite consolidar la información referente a los riesgos identificados en el Programa JUNTOS, lo cual incluye el tipo, causas, consecuencias y nivel de riesgo, así como los controles identificados para afrontarlos.

4.18 **Nivel del riesgo:** Magnitud de un riesgo o combinación, expresada en términos de la combinación de consecuencias y su probabilidad.

4.19 **Plan de tratamiento:** Documento que contiene controles, actividades, plazos, responsables, para afrontar los riesgos identificados.

4.20 **Probabilidad:** Posibilidad que algo suceda.

4.21 **Propietarios de los activos de la información:** Son los responsables de administrar, proteger y mantener los activos de la información haciéndolos accesibles a los usuarios; asimismo de monitorear el cumplimiento de los controles de seguridad en los activos que se encuentran bajo su custodia.

4.22 **Riesgo:** Es una combinación de las consecuencias que pueden seguir a la ocurrencia de un evento no deseado y de la probabilidad de la ocurrencia del evento.

4.23 **Riesgo residual:** Nivel de riesgo obtenido de la valoración realizada después de la implementación de controles establecidos para el riesgo.

4.24 **Seguridad de la Información:** Preservar la confidencialidad, integridad y disponibilidad de la información; además de también pudiendo involucrar características como la autenticidad, responsabilidad, no repudio y fiabilidad.

4.25 **Usuarios de los activos de información:** Son aquello servidores, personal temporal, consultores y proveedores de bienes y/o servicios y personas externas a la entidad que utilizan los activos de la información de esta, para desarrollar sus actividades.

4.26 Vulnerabilidad: Debilidad de un activo o grupo de activos que puede ser explotados por una o más amenazas.

4.27 SI: Seguridad de la Información.

4.28 UTI: Unidad de Tecnologías de la Información.

5. DESARROLLO

5.1 Organización para la gestión del riesgo de seguridad de la información (SI)

A continuación, se presentan los roles y responsabilidades para ejecutar la gestión de riesgos de seguridad de la información:

TABLA Nº 01: ROLES DEL EQUIPO PARA LA GESTIÓN DE RIESGOS DE SI

ROL	RESPONSABILIDADES
Oficial de Seguridad y Confianza Digital	• Participar en todas las etapas de la gestión de riesgos de seguridad de la información. • Realizar capacitaciones sobre la gestión de riesgos de seguridad de la información. • Brindar asistencia a los dueños de procesos sobre la gestión de riesgos de seguridad de la información. • Reportar de manera semestral al Comité de Gobierno y Transformación Digital, el estado de cumplimiento de las acciones de tratamiento detalladas en el Plan de tratamiento de riesgos de seguridad de la información (PNADP-UTI-GMC-F-006).
Dueño/a del proceso	• Participar en las etapas de evaluación de riesgos, tratamiento de riesgos y la aceptación del riesgo. • Puede designar otros especialistas y/o analistas a participar del proceso.
Servidores/as del Programa	• Según sea necesario en el ámbito de su competencia.
Comité de Gobierno y Transformación Digital	• Aprobar la Matriz de gestión de riesgos de seguridad de la información (PNADP-UTI-GMC-F-005)[1].

Elaboración: UTI

Si bien los roles presentados en la Tabla N° 01 son los mínimos requeridos para poder llevar a cabo el proceso, es posible que se asignen roles adicionales en caso sea necesario.

5.2 Metodología para la gestión de riesgos de seguridad de la información

La metodología a emplear considera las etapas establecidas en la norma ISO/IEC 27005, las mismas que se muestran en la siguiente imagen:

[1] El/La Jefe/a de la Unidad de Tecnologías de la Información, socializa la Matriz de riegos mediante Memorando Múltiple.

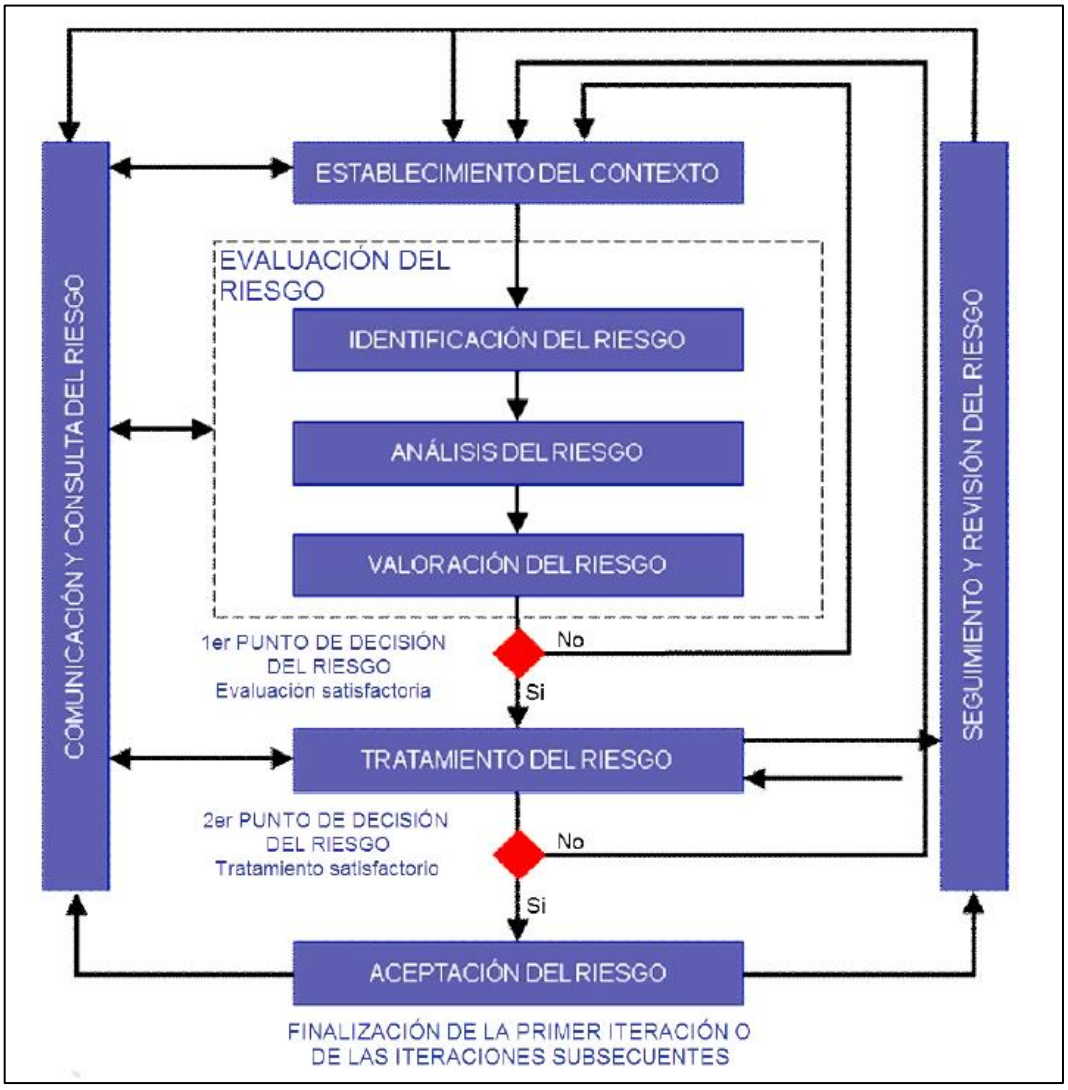

Ilustración n° 1: Etapas del proceso de gestión del riesgo de seguridad de la información
Fuente: NTP-ISO/IEC 27005

5.3 Evaluación del riesgo

El objetivo de esta etapa es identificar los posibles riesgos a partir de las amenazas identificadas y las vulnerabilidades detectadas, teniendo en cuenta los controles existentes, y así poder obtener una valoración del nivel de los riesgos que nos permita priorizarlos adecuadamente.

5.3.1 Identificación de activos de información

a) El Equipo de gestión de riesgos de Seguridad de la Información identifica los activos de información relevantes del Programa Juntos; para lo cual se recomienda tener en cuenta que no son solo elementos de hardware y software, sino que estos pueden incluir más elementos.

b) Se debe identificar al propietario de cada activo, para asignarle una responsabilidad y rendición. El propietario del activo puede no tener derechos de propiedad sobre el activo, pero tiene la responsabilidad de su producción, desarrollo, mantenimiento, uso y seguridad, según corresponda. El propietario del activo con frecuencia es la persona más idónea para determinar el valor que el activo tiene para la organización.

c) Las categorías de los activos se describen en la siguiente tabla:

TABLA Nº 02: CATEGORÍA DE ACTIVOS

CATEGORÍA	DESCRIPCIÓN
Procesos / Servicios	• Procesos o servicios cuya interrupción, modificación o degradación hacen que se dificulte llevar a cabo la misión del Programa JUNTOS. • Procesos o servicios que contengan actividades relacionados con algún tipo de información confidencial para el Programa JUNTOS. • Procesos que son necesarios para que el Programa JUNTOS cumpla con los requerimientos legales, contractuales y otros aplicables.
Datos e información	Planes estratégicos, nóminas, archivos de carácter personal, contratos, correos, documentos, reportes, entre otros.
Equipos Informáticos (Hardware)	Servidores, dispositivos móviles (smartphone, tablet, etc.), dispositivos de red (router, switches, etc.), dispositivos USB, discos duros externos, medios de respaldo (datos, sistemas operativos, software), entre otros.
Software	Sistemas operativos (Microsoft Windows, Linux, etc.), aplicaciones de servidor, aplicaciones de cliente (Google Chrome, Internet Explorer, etc.), software de seguridad (Antivirus, firewall), aplicaciones de usuario (Adobe Acrobat Reader, Microsoft Office, etc.), aplicaciones de desarrollo, servidor de correo, entre otros.
Personas	Interno (servidores) y externo (terceros).
Redes de Comunicaciones	WAN, MAN, LAN, DMZ, VLAN's, VPN, nodos, entre otros.
Instalación Física	Espacio físico donde se llevan a cabo procesos de la institución.
Equipamiento Auxiliar	Generadores eléctricos, sistema de control de acceso, HVAC (calefacción, ventilación y aire acondicionado), sistema de detección, control de incendio, etc.
Computadoras Personales	Equipo informático (PC o laptop) utilizado por los servidores para llevar a cabo las funciones propias del cargo.

Elaboración: UTI

d) El inventario de activos de información se debe realizar de manera conjunta entre los miembros del "Equipo de gestión de riesgos de seguridad de la información".

e) Los activos identificados, se registran en la sección **"Identificación de activos"** del formato "Inventario de Activos de Información" (PNADP-UTI-GMC-F-004).

5.3.2 Valoración de los activos

a) Equipo de gestión de riesgos de SI, junto con las unidades del Programa involucradas, realiza la ponderación de activos con el fin de determinar en términos cualitativos la criticidad de los distintos activos.

b) En ese sentido, se evalúan tres aspectos: Confidencialidad, Disponibilidad e Integridad, de manera independiente. Para lo cual se utiliza la Tabla n° 03 de Nivel de impacto.

TABLA Nº 03: ESCALAS DE NIVEL DE IMPACTO				
CATEGORÍA	VALOR	DESCRIPCIÓN		
		CONFIDENCIALIDAD	DISPONIBILIDAD	INTEGRIDAD
BAJO	4	Se divulgan datos no relevantes al interior del Programa. Pequeño o nulo efecto en el desarrollo de los procesos y en el cumplimiento de los objetivos de Juntos	El evento puede tener un pequeño o nulo efecto en el desarrollo de los procesos y en el cumplimiento de los objetivos del Programa.	Se generan algunos datos inconsistentes menores o ausencia mínima de datos.
MEDIO	6	Se divulgan datos de un ámbito específico o sistema no fundamental al interior del Programa. La divulgación se da sobre un ámbito limitado con efectos de menor envergadura sobre los procesos.	El evento tiene efectos de menor envergadura en los procesos que pueden ser asumidos sin mayores problemas por las áreas. No afecta mayormente el cumplimiento de los objetivos.	Se generan datos inconsistentes o incompletos en una aplicación o activo de impacto menor. El evento tiene efectos de menor envergadura en los procesos que pueden ser asumidos sin mayores problemas por las áreas.
ALTO	8	Se divulgan datos puntuales de un activo de información relevante de la organización. La divulgación puede tener efectos significativos para el Programa en términos estratégicos y/o reputación.	El evento provoca deterioro en el desarrollo de los procesos, dificultando o atrasando el cumplimiento normal de los objetivos, impidiendo que se desarrolle de forma adecuada.	Se presentan inconsistencias en varios sistemas o se comprometen sistemas relevantes. El evento tendrá efectos significativos para el Programa en el desarrollo de procesos y cumplimiento de objetivos.
MUY ALTO	10	Se divulgan datos de una aplicación estratégica, datos confidenciales o se divulgan muchos datos de la organización. El evento tiene efectos graves para la organización ocasionando importantes pérdidas.	El evento tiene efectos graves en el desarrollo de procesos y cumplimiento de los objetivos, impidiendo que estos se desarrollen.	Se presentan inconsistencias en sistemas estratégicos o en la mayoría de los sistemas del Programa. El evento tiene efectos graves en el desarrollo de procesos y cumplimiento de los objetivos, impidiendo que estos se desarrollen.

Elaboración: UTI

c) Cuantificado cada uno de esos aspectos el "Impacto" corresponde al promedio de la valoración de cada uno de ellos, según la siguiente formula[2]:

$$Impacto = \frac{Confidencialidad + Disponibilidad + Integridad}{3}$$

d) La valoración de cada uno de los aspectos se registra en la sección **"Valoración del activo (criticidad)"** del formato "Inventario de Activos de Información" (PNADP-UTI-GMC-F-004).

[2] El resultado debe ser redondeado hacía arriba.

e) El "Equipo de gestión de riesgos de seguridad de la información" realiza el análisis del riesgo a los activos de información priorizados, teniendo como base la valoración del activo.

5.3.3 Análisis de riesgos

El Equipo de gestión de riesgos de SI, evalúa las características por cada activo identificado de acuerdo a la Tabla Nº 04. Cabe mencionar que el análisis de riesgo, solo aplica a los activos de información que tengan una criticidad mayor o igual a un valor de 8, para los demás no es aplicable.

TABLA Nº 04: CAMPOS DE ANALISIS DE RIESGOS

CAMPO	DESCRIPCIÓN
Amenaza asociada al activo.	Indicar cuál es la causa potencial de un incidente no deseado que puede resultar en daño al sistema u organización.
Vulnerabilidad asociada al activo.	Indicar cuál es la debilidad del activo o grupo de activos que puede ser explotados por una o más amenazas.
Descripción de Controles actuales.	Indicar qué controles se encuentran actualmente implementados por el Programa Juntos, que mitigan el nivel de riesgo de los activos.
Aplica SoA (Si / No).	Determinar si corresponde a la aplicación de un control de acuerdo con el anexo A, de la norma ISO/IEC 27001.
Cláusula de control SoA.	Indicar el numeral del anexo A, al cual corresponde el control identificado.

Elaborado: UTI

A continuación, se procede a realizar el análisis de riesgos para los activos de información definidos.

5.3.4 Análisis de amenazas

Se identifica las amenazas y sus orígenes. Una amenaza tiene el potencial de causar daños a activos tales como información, procesos y sistemas, por lo tanto, a las organizaciones. Para ello en el **Anexo 01**, se muestra un listado de posibles amenazas que pueden afectar a los activos priorizados.

Algunas amenazas pueden afectar a más de un activo. En tales casos pueden causar diferentes impactos dependiendo los activos que se vean afectados.

5.3.5 Análisis de vulnerabilidades

Se identifica las vulnerabilidades que pueden ser explotadas por las amenazas para causar daños a los activos o a la institución.

La sola presencia de una vulnerabilidad no causa daño por sí misma, dado que es necesario que haya una amenaza presente para explotarla. Una vulnerabilidad que no tiene una amenaza correspondiente puede no requerir de la implementación de un control, pero es recomendable reconocerla y monitorearla para determinar los cambios.

Conviene anotar que un control implementado de manera incorrecta o que funciona mal, o un control que se utiliza de modo incorrecto podrían por sí solo constituir una vulnerabilidad. Al respecto en el **Anexo 02**, se presenta un listado de vulnerabilidades que pueden afectar a los activos de información priorizados.

5.3.6 Identificación de controles

Es importante, la identificación de los controles existentes para evitar trabajo o costos innecesarios, por ejemplo, en la duplicación de estos. Además, mientras se identifican los controles existentes es recomendable hacer una verificación para garantizar que los controles funcionan correctamente. Si el control no funciona como se espera se

pueden presentar vulnerabilidades. Cabe mencionar que, los controles vigentes se encuentran en la Declaración de aplicabilidad del SoA.

La amenaza, vulnerabilidad y controles actuales asociados al activo se registran en la sección **"Análisis de Riesgos"** de la Matriz de gestión de riesgos de seguridad de la información (PNADP-UTI-GMC-F-005).

5.4 Valoración del nivel del riesgo

Culminado el análisis de riesgos de cada activo de información, el Equipo de gestión de riesgos de SI procede a realizar la valoración del nivel de riesgo de acuerdo lo siguiente:

5.4.1 Determinación del impacto

El cálculo del nivel de impacto proviene de la identificación del nivel de criticidad del activo registrado en la sección **"Valoración del activo (Criticidad)"** del formato "Inventario de Activos de Información" (PNADP-UTI-GMC-F-004).

5.4.2 Determinación de la probabilidad

a) Para determinar la probabilidad de la materialización del riesgo se evalúan dos aspectos: (1) Nivel de amenaza y (2) Nivel de la vulnerabilidad, las mismas que se identificaron en el análisis del riesgo; para lo cual se debe evaluar cada aspecto entre un valor entre 4 al 10 de acuerdo a la siguiente tabla:

TABLA Nº 05: NIVEL DE PROBABILIDAD DE OCURRENCIA DE AMENAZA Y VULNERABILIDAD

CATEGORÍA	VALOR	DESCRIPCIÓN	FRECUENCIA
BAJO	**4**	Es poco probable la materialización del riesgo.	Nunca o no sea ha presentado en los últimos 05 años.
MEDIO	**6**	Es probable la materialización del riesgo.	Al menos una vez se ha presentado en los últimos 05 años.
ALTO	**8**	Es muy probable la materialización del riesgo.	Al menos una vez se ha presentado en los últimos 02 años.
MUY ALTO	**10**	Es extremadamente probable la materialización del riesgo.	Al menos una vez se ha presentado en el último año.

b) Finalmente, el nivel de probabilidad se calcula de la siguiente forma:

$$\boldsymbol{Probabilidad = \frac{Nivel\ de\ Amenaza + Nivel\ de\ vulnerabilidad}{2}}$$

5.4.3 Determinación del Nivel de Riesgo

Luego se procede a la valoración del riesgo (R), el mismo que se calcula de acuerdo con la expresión matemática que se presenta a continuación:

Donde:

$$\mathbf{R = P \times I}$$

R: Riesgo **P:** Probabilidad **I:** Impacto

En la siguiente tabla se presenta el "Mapa de riesgos" en el cual se muestra el nivel de riesgos resultado del "Impacto" y "Probabilidad".

TABLA Nº 06: MAPA DE RIESGO DE SEGURIDAD DE LA INFORMACIÓN

			IMPACTO			
			BAJO	MEDIO	ALTO	MUY ALTO
			4	6	8	10
PROBABILIDAD	MUY ALTA	10	40 Medio	60 Alto	80 Muy Alto	100 Muy Alto
	ALTA	8	32 Medio	48 Alto	64 Alto	80 Muy Alto
	MEDIA	6	24 Bajo	36 Medio	48 Alto	60 Alto
	BAJA	4	16 Bajo	24 Bajo	32 Medio	40 Medio

Sobre lo planteado, se presenta en la siguiente imagen el rango de los niveles de riesgo por rangos.

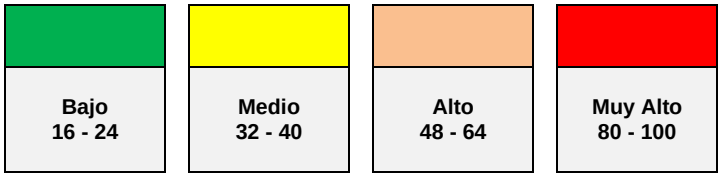

Ilustración nº 2: Rango de Niveles

5.4.4 Aceptación de la evaluación

En este punto se revisa la evaluación del riesgo y el equipo decide si está de acuerdo con el resultado de la evaluación. En caso no estar de acuerdo, se puede volver a realizar la evaluación del riesgo, hasta que sea satisfactoria.
Los riesgos que tienen un nivel de aceptación bajo son aceptados por lo cual no afectan a la información contenida en dichos activos de información.

5.5 Tratamiento y control del riesgo

a) El tratamiento de los riesgos consiste en tomar decisiones frente a los diferentes niveles de riesgo identificados de acuerdo con la estrategia establecida.

b) Se deben seleccionar controles para reducir, aceptar/retener, evitar o transferir los riesgos y se debe definir un plan para el tratamiento del riesgo.

c) El equipo de gestión de riesgos de SI debe definir la estrategia que se debe de tomar para afrontar el riesgo de acuerdo con su nivel, en función a lo establecido en la ilustración n° 3:

Evitar

Se debe evitar la actividad o la acción que da origen al riesgo particular.

Cuando los riesgos identificados se consideran muy altos, o si los costos para implementar otras opciones de tratamiento del riesgo exceden los beneficios, se puede tomar una decisión para evitar por completo el riesgo, mediante el retiro de una actividad o un conjunto de actividades planificadas o existentes, o mediante el cambio en las condiciones bajo las cuales se efectúa tal actividad.

Por ejemplo, para los riesgos causados por la naturaleza, puede ser una alternativa más eficaz en términos de costo, transferir físicamente las instalaciones de procesamiento de la información a un lugar donde no exista el riesgo o esté bajo control.

Mitigar

Los riesgos se reducen mediante la selección de controles, de manera tal que el riesgo residual se pueda reevaluar como aceptable.
Se deben seleccionar controles adecuados y justificados que satisfagan los requisitos identificados en la valoración y el tratamiento del riesgo.
En esta selección se deberían tener en cuenta los criterios de aceptación del riesgo, así como requisitos legales, reglamentarios y contractuales; así como, los costos y tiempo para la implementación de los controles, o los aspectos técnicos, ambientales y culturales. Con frecuencia es posible disminuir el costo total de la propiedad de un sistema con controles de seguridad de la información adecuadamente seleccionados.

Transferir

El riesgo se debe transferir a otra parte que pueda gestionar de manera más eficaz el riesgo particular dependiendo de la evaluación del riesgo.

Asumir

La decisión sobre la retención del riesgo sin acción posterior se debería tomar dependiendo de la evaluación del riesgo.
Aceptar los riesgos con conocimiento y objetividad, siempre y cuando satisfagan claramente la política y los criterios de la institución para la aceptación de los riesgos.

Ilustración n° 3: Estrategias de tratamiento de los riesgos

d) La actuación del Programa JUNTOS para la gestión de los riesgos conlleva a tomar estrategias según el nivel de riesgo, evaluando la implementación de controles y medidas factibles en costo/eficacia teniendo en consideración las ya existentes y el nivel de esfuerzo para su aplicación. La Tabla N° 07 detalla las estrategias por nivel de riesgo identificado.

TABLA Nº 07: ESTRATEGIAS DE TRATAMIENTO DE RIESGOS

	Evitar	Mitigar	Transferir	Asumir	¿Require Plan de Tratamiento?
Bajo	--	--	--	X	No
Medio	--	X	X	--	Sí
Alto	--	X	X	--	Sí
Muy Alto	X	X	X	--	Sí

e) En los casos que aplique la ejecución de un Plan se debe evaluar si aplica la implementación de controles de la Declaración de aplicabilidad del SoA[3].

f) Todas las acciones señaladas en el presente numeral deben ser registradas en la sección de **"Tratamiento"** de la Matriz de gestión de riesgos de seguridad de la información (PNADP-UTI-GMC-F-005).

5.5.1 Aplicación del tratamiento

En el caso de los niveles de riesgos medio a muy alto, corresponde realizar acciones para disminuir el riesgo para ello se debe aplicar las estrategias señaladas en la ilustración nº 3.

Para ello el equipo de riesgos debe utilizar el formato Plan de tratamiento de riesgos de seguridad de la información (PNADP-UTI-GMC-F-006), identificando acciones a realizar de acuerdo con la estrategia seleccionada.

5.6 Seguimiento y monitoreo

El/la Oficial de Seguridad y Confianza Digital es responsable de monitorear y revisar periódicamente el cumplimiento de lo señalado en el Plan de tratamiento de riesgos de seguridad de la información, para lo cual debe:

a) Verificar la implementación de las medidas de prevención y mitigación, a través de las medidas de control, siendo de importancia contar con las evidencias o medios de verificación que dan cuenta de la implementación de esas medidas.

ESTADOS DE IMPLEMENTACIÓN	
No implementado	De 0% hasta el 50% de actividades culminadas
Parcialmente implementado	De 51% hasta el 99% de actividades culminadas
Implementado	El 100% de actividades culminadas

Nota: Actividad culminada es aquella actividad finalizada y que se puede evidenciar

b) La información señalada debe ser ingresada en el Plan de tratamiento de riesgos de seguridad de la información (PNADP-UTI-GMC-F-006).

c) La gestión del riesgo, es un proceso dinámico por lo que resulta importante un monitoreo constante a fin de identificar los cambios que pudieran afectar al Programa. El monitoreo constante debe considerar los siguientes aspectos:

- ✓ Activos nuevos.
- ✓ Modificaciones necesarias de los valores de los activos.
- ✓ Nuevas amenazas que podrían estar activas dentro o fuera del Programa y que no se han valorado.
- ✓ Probabilidad de aparición de nuevas vulnerabilidades o incremento en las vulnerabilidades existentes.
- ✓ Vulnerabilidades identificadas que se exponen a nuevas amenazas o que vuelven a surgir.
- ✓ Incidentes de la seguridad de la información.

5.7 Aceptación del riesgo de seguridad de la información

5.7.1 El/la Coordinador/a de Modernización de la Gestión evalúa la eficacia de la implementación de los controles después de seis meses, según la metodología

[3] Son los controles de seguridad de la información que se colocan en el registro de "Declaración de aplicabilidad SoA".

establecida en el **Anexo 03**: Evaluación de la eficacia de controles y lo registra en la sección **"Determinación del nivel de eficacia de los controles (implementados)"** del Plan de tratamiento de riesgos de seguridad de la información (PNADP-UTI-GMC-F-006).

5.7.2 Posteriormente, determina el nivel del riesgo residual, según lo señalado en el **Anexo 04** y registra los resultados en la sección **"Evaluación del riesgo residual"** del Plan de tratamiento de riesgos de seguridad de la información (PNADP-UTI-GMC-F-006).

6. FORMATOS

- Inventario de activos de información (PNADP-UTI-GMC-F-004).
- Matriz de gestión de riesgos de seguridad de la información (PNADP-UTI-GMC-F-005).
- Plan de tratamiento de riesgos de seguridad de la información (PNADP-UTI-GMC-F-006)

7. ANEXOS

- Anexo 01: Tipos de amenazas
- Anexo 02: Tipos de vulnerabilidades
- Anexo 03: Evaluación de la eficacia de controles
- Anexo 04: Determinación del riesgo residual

Inventario de activos de información

PNADP-UTI-GMC-F-004/Rev.01

Fecha de Actualización

IDENTIFICACIÓN DE ACTIVOS											Valoración del Activo (criticidad)			> =	8
Proceso / Proyecto	Sub Proceso/ Actividad	Unidad	Código del Activo	Nombre del Activo	Categoría	Descripción del activo	Tipo de Soporte	Ubicación	Responsable del Proceso / Propietario del Activo	Estado	Confidencialidad	Disponibilidad	Integridad	VA	Priorizado
			A-0001							Activo	10	8	8	8.67	SI
			A-0002							Activo	0	0	0	0.00	NO
			A-0003							Activo	0	0	0	0.00	NO

Nota: Ejemplo referencial de llenado.

Matriz de gestión de riesgos de seguridad de la información

PNADP-UTI-GMC-F-005/Rev.01

Fecha de Actualización

EVALUACIÓN DEL RIESGO																		TRATAMIENTO		
Activos Priorizados						ANÁLISIS DE RIESGOS						Valoración del nivel de riesgo								
Sub Proceso/ Actividad	Unidad	Código del Activo	Nombre del Activo	Descripción del Activo	VA	Código de Riesgo	Amenaza asociada al Activo	Vulnerabilidad asociada al Activo	Descripción de Controles actuales	¿Aplica SoA? (Sí / No)	Control SoA	Impacto (I)	Probabilidad (P)			Valor del riesgo	Nivel de Riesgo	Estrategia	¿Aplica Plan? (Sí / No)	Control a implementar
												VA	Nivel de la amenaza	Nivel de la vulnerabilidad	Probabilidad					
		A-0001			9.00	RG-0001						9.00	4	4	4	36	Medio	Mitigar	Si	
						RG-0002						9.00	6	4	5	45	Medio	Mitigar	Si	
		A-0002			7.00	RG-0003						7.00	6	8	7	49	Alto	Mitigar	Si	
						RG-0004						7.00	4	4	4	28	Medio	Mitigar	Si	

Nota: Ejemplo referencial de llenado.

Plan de tratamiento de riesgos de seguridad de la información

PNADP-UTI-GMC-F-006/Rev.01

Fecha de Actualización

Sub Proceso/ Actividad	Unidad	Código del Activo	Código de Riesgo	Control a implementar	¿Aplica SoA? (Sí / No)	Control SoA	Actividades	Fecha de implementación	Responsable de la implementación	Medio de verificación	Estado de Implementación (*)	Determinación de la Eficacia del Control					Evaluación del riesgo residual	
												Periodicidad	Oportunidad	Tecnológico	Valor de Eficacia	Nivel de Eficacia	Nivel de riesgo inicial	Nivel de riesgo final
		A-0001	RG-0001					00/00/0000				3	2	1	6	Regular	Bajo	
			RG-0002					00/00/0000				3	2	2	12	Bueno	**Bajo**	

(*) No implementado (De 0% hasta el 50% de actividades culminadas) / Parcialmente implementado (De 51% hasta el 99% de actividades culminadas) / Implementado (El 100% de actividades culminadas).

Nota: Ejemplo referencial de llenado.

Anexo 01: Tipos de amenazas

Nº	TIPOS DE AMENAZAS	DESCRIPCIÓN
1	Obtención de Credenciales	Utilización de herramientas informáticas o técnicas para probar contraseñas con el fin de acceder a un sistema.
2	Ingeniería social	Consiste en utilizar artilugios, tretas y otras técnicas para engañar a las personas, a fin de que ellas revelen información de interés para el atacante, por ejemplo: las contraseñas de acceso.
3	Código Malicioso/ Virus	Se define así a todo programa o fragmento del mismo que genera algún tipo de problema en el sistema en el cual se ejecuta, interfiriendo de esta forma con su normal funcionamiento.
4	Denegación del Servicio	Ataques externos que buscan que un recurso informático no esté disponible para los usuarios previstos.
5	Daños físicos en equipos	Daños a equipos que pueden ser ocasionados por acciones intencionadas, por negligencia a usuarios o por accidentes.
6	Fuga de información confidencial	Ocurre cuando la información confidencial empresa es obtenida por personal no autorizado y divulgada a personas fuera de la institución para fines ajenos a la misma.
7	Secuestro de Datos (Ransomware)	Es un tipo de código malicioso que impide la utilización de los equipos o sistema que infecta, cifrando la información y solicitando un rescate para su desencriptación.
8	Phishing	Envío masivo de mensajes electrónicos que simulan ser notificaciones oficiales de entidades o empresas legítimas, con el fin de obtener datos personales de los usuarios.
9	Intrusiones	Acceso de personal no autorizado a la red interna de la institución.
10	Robo de identidad	Ocurre cuando alguien obtiene y utiliza, mediante medios informáticos, información personal ajena (nombre, número de tarjeta de crédito, información bancaria, número de afiliado a un sistema de salud, etc.) sin su autorización, con el propósito de realizar actividades fraudulentas.
11	Condiciones ambientales adversas	Daño de activos de información por condiciones ambientales adversas, como humedad, temperatura ambiental, etc.
12	Emergencias (terremotos, incendios, etc.)	Emergencias naturales o accidentes no previstos que puedan dañar activos de la información.
13	Otras	Otras que no se hayan considerado al momento de la elaboración del documento y que puedan ser importantes para la gestión del riesgo de seguridad de la información.

Anexo 02: Tipos de vulnerabilidades

Nº	Tipos de Vulnerabilidades	Concepto
1	Seguridad de Recursos Humanos	Falta de entrenamiento en seguridad, carencia de toma de conciencia en seguridad, falta de mecanismos de monitoreo, falta políticas para el uso correcto de las telecomunicaciones, no eliminar accesos al término del contrato de trabajo, carencia de procedimiento que asegure la entrega de activos al término del vínculo laboral, servidores desmotivados.
2	Control de Acceso	Segregación inapropiada de redes, falta de política de escritorio y pantalla limpia, falta de protección al equipo de comunicación móvil, política incorrecta para el control de acceso, password sin modificarse.
3	Seguridad Física y Ambiental	Control de acceso físico inadecuado de oficinas, locales de las Unidades Territoriales, ubicación en áreas sujetas a inundaciones, almacenes desprotegidos, carencia de programas para sustituir equipos, mal cuidado de equipos, susceptibilidad de equipos a variaciones de voltaje.
4	Gestión de Operaciones y comunicación	Complicadas interfases de usuarios, control de cambios, inadecuado, gestión de red inadecuada carencia de mecanismos que aseguren el envío y recepción de mensajes, carencia de tareas segregadas, carencia de control copiado, falta de protección en redes públicas de conexión.
5	Mantenimiento, Desarrollo y Adquisición de Sistemas de Información	Protección inapropiada de llaves criptográficas, políticas incompletas para el uso de criptografía, carencia de validación de datos procesados, carencia de ensayos de software, mala selección de ensayos de datos.

Anexo 03: Evaluación de la eficacia de controles

Implementado el control, es necesario evaluar la eficacia de las actividades de control registradas, determinándose si son controles necesarios o innecesarios, o son controles que generan más costos que beneficios, esto como respuesta a los riesgos. Para ello, se utiliza la información detallada en la tabla siguiente:

Tabla A3.01: Determinación del nivel de eficacia de los controles

Calificación	Valor
Criterio: Periodicidad	
Permanente	3
Periódico	2
Ocasional	1
Criterio: Oportunidad	
Correctivo	3
Preventivo	2
Detectivo	1
Criterio: Automatización	
Automatizado	3
Semiautomatizado	2
Manual	1

En la tabla siguiente, se encuentran algunos aspectos a tomar en cuenta para la asignación del valor al realizar la determinación del nivel de eficacia de los controles señalados en la Tabla N° A3.01.

Tabla A3.02: Aspectos a considerar para la asignación del valor a los criterios

Criterio: Periodicidad	Permanente	Se aplica en forma constante cada vez que se ejecuta el proceso, actividades o tareas.
	Periódico	Pueden ser anuales, semestrales y mensuales, dependiendo de la ejecución de los procesos, actividades o tareas.
	Ocasional	Se aplican en forma ocasional, de acuerdo con el criterio del responsable del proceso.
Criterio: Oportunidad	Controles correctivos	Identifica desviaciones cuando el riesgo se ha materializado. Permiten el restablecimiento de la actividad después de ser detectado un evento no deseable y la modificación de las acciones que propiciaron su ocurrencia. Estos controles actúan cuando ya se han presentado hechos que implican pérdidas para el Programa JUNTOS.

Tabla A3.02: Aspectos a considerar para la asignación del valor a los criterios		
	Controles preventivos	Actúan sobre la causa de los riesgos, con el fin de disminuir su probabilidad de ocurrencia y constituyen la primera línea de defensa. Ejemplos: Revisión de firmas y saldo antes de efectuar un pago.
	Controles detectivos	Sirven para supervisar la ejecución del proceso, ofrecen la segunda barrera de seguridad frente a los riesgos
Criterio: Automatización	Automatizada	Son aplicados a través de sistemas de información automatizados. Aseguran la correcta captación de la información y procedimientos de autorización y aprobación por parte de los responsables.
	Semiautomatizada	Su aplicación es parcialmente automatizada, combina acciones de control manuales. Ejemplos: Verificaciones de documentos, autorizaciones, registro de datos en aplicativos.
	Manual	Son ejecutados por el personal que interviene en el proceso, las acciones de control son manuales. Ejemplos: Registro en formatos, firmas para autorizar, cálculos manuales, conciliaciones manuales, entre otros.

El valor total de la eficacia de los controles establecidos, es resultado de la multiplicación de los valores determinados por los tres criterios que se señalan en la tabla anterior.

Los resultados de la evaluación de la eficacia, se realiza de acuerdo con lo detallado en la tabla siguiente:

Tabla A03.03: Asignación del nivel de eficacia de los controles	
Calificación total	**Valor**
Insuficiente	De 1 a 3
Regular	De 4 a 6
Bueno	De 8 a 12
Óptimo	De 18 a 27

NOTA: Se consideran controles eficaces, cuando se obtienen resultados: Bueno y Óptimo.

La información determinada en esta etapa se debe ingresar en la sección “Determinación del nivel de eficacia de los controles (implementados)”, del Plan de tratamiento.

Anexo 04: Determinación del riesgo residual

Evaluar el Riesgo residual

Finalmente, se determina el riesgo residual, para lo cual se debe tomar en cuenta la eficacia de las actividades de control implementadas o existentes, dado que es un remanente después del tratamiento del riesgo, se da la valoración del riesgo residual de acuerdo con la siguiente ilustración.

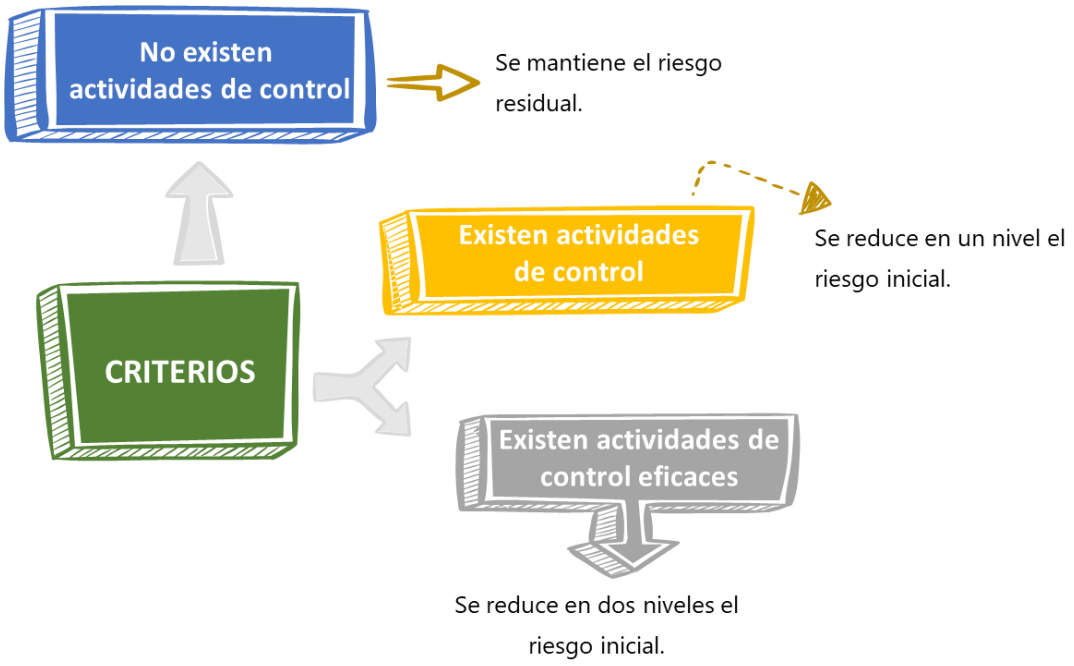

Ilustración n° 4: Infografía de la valoración del riesgo residual
Fuente: UPPM-CMG

Aceptación del riesgo residual

Se acepta el riesgo residual, cuando éste corresponde a nivel Bajo o Medio. Caso contrario, se volverá a analizar las causas, consecuencias y se plantearán nuevos controles. Este análisis de reproceso se realiza en un nuevo ciclo de evaluación.