"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
Año del Fortalecimiento de la Soberanía Nacional

San Isidro, 13 de Septiembre del 2022

RESOLUCION DIRECTORAL N° D000140-2022-PENSION65-DE

VISTO:

El Informe N° D000003-2022-PENSION65-CCAL, expedido por el Coordinador de Calidad, y el Informe N° D000244-2022-PENSION65-UAJ, expedido por la Unidad de Asesoría Jurídica del Programa Nacional de Asistencia Solidaria "Pensión 65" del Ministerio de Desarrollo e Inclusión Social; y,

CONSIDERANDO:

Que, mediante Decreto Supremo N° 081-2011-PCM, y sus modificatorias, se crea el Programa Nacional de Asistencia Solidaria "Pensión 65" con la finalidad de brindar protección social a los adultos mayores a partir de 65 años a más, que viven en situación de vulnerabilidad, entregándoles una subvención monetaria que les permita incrementar su bienestar; y mejorar sus mecanismos de acceso a los servicios públicos que brinda el Estado;

Que, mediante Resolución Ministerial N° 273-2017-MIDIS, se aprueba el Manual de Operaciones del Programa Nacional de Asistencia Solidaria "Pensión 65", documento técnico normativo de gestión que formaliza la estructura orgánica del Programa, orientando el esfuerzo institucional al logro de su misión, visión y objetivos estratégicos, describiendo entre otros aspectos, las funciones específicas de las unidades que lo integran y la descripción detallada y secuencial de los principales procesos técnicos y/o administrativos;

Que, el artículo 9 del Manual de Operaciones citado en el considerando anterior, establece como funciones de la Dirección Ejecutiva *"(…) d) Liderar, conducir y supervisar el Sistema de Gestión de la Calidad del Programa, conforme con las políticas y lineamientos establecidos por el MIDIS (…) i) emitir resoluciones directorales de su competencia (…)"*;

Que, la Ley N° 27658, Ley Marco de Modernización de la Gestión del Estado, declara al Estado peruano en proceso de modernización en sus diferentes instancias, dependencias, entidades, organizaciones y procedimientos, con la finalidad de mejorar la gestión pública y construir un Estado democrático, descentralizado y al servicio del ciudadano. Asimismo, el literal 5-A.1 del artículo 5 de la mencionada norma, señala que el Sistema Administrativo de Modernización de la Gestión Pública tiene por finalidad velar por la calidad de la prestación de los bienes y servicios;

Que, mediante Decreto Supremo N° 123-2018-PCM, se aprueba el Reglamento del Sistema Administrativo de Modernización de la Gestión Pública, cuyo artículo 3 señala que el mencionado sistema se rige bajo determinados principios siendo uno de ellos el referido a la eficacia y eficiencia, es decir, que las entidades públicas orientan su actuación hacia el logro de objetivos institucionales y el manejo racional y óptimo de los recursos;

Que, mediante Resolución Directoral N° 019-2019-MIDIS/P65 se conforma del Comité de Gestión de la Calidad del Programa Nacional de Asistencia Solidaria Pensión 65", el mismo que fue reconformado mediante Resolución Directoral N° 131-2019-MIDIS/P65-DE;

Que, mediante Resolución Directoral N° 266-2020-MIDIS/P65-DE, se aprobó en su artículo 7, el cambio de denominación del "Comité de Gestión de la Calidad" conformado mediante Resolución Directoral N° 131-2019-MIDIS/P65-DE, por el de "Comité de Sistemas de Gestión Integrados";

www.pension65.gob.pe
Av. República de Panamá Nro. 3505
San Isidro
Lima 24, Perú
T: (01) 705-2900

Que, mediante Resolución Directoral N° D000338-2021-PENSION65-DE, se aprobó la reconformación del Comité de Sistemas de Gestión Integrados del Programa Nacional de Asistencia Solidaria "Pensión 65" designado mediante Resolución Directoral N° 131-2019-MIDIS/P65-DE;

Que, mediante Resolución Directoral N° D000049-2022-PENSION65-DE, se formaliza la aprobación del "Plan de Desarrollo Anual del Sistema de Gestión Integral del Programa Nacional de Asistencia Solidaria "Pensión 65" para el período 2022", conforme a lo dispuesto mediante Acta N° 02 del 9 de marzo de 2022, del Comité de Sistemas de Gestión Integrados del Programa Nacional de Asistencia Solidaria "Pensión 65", el mismo que tiene como objetivo general fortalecer el Sistema de Gestión Integral del Programa Nacional de Asistencia Solidaria Pensión 65 en los procesos de Calidad y Antisoborno de la sede central y Unidades Territoriales, tomando como base la Norma Internacional ISO 9001:2015: Sistema de Gestión de la Calidad, así como la Norma Internacional ISO 37001:2016: Sistema de Gestión Antisoborno o sus equivalentes;

Que, mediante Informe N° D000003-2022-PENSION65-CCAL, el Coordinador de Calidad de este Programa Nacional hace de conocimiento que los miembros del Comité de Sistemas de Gestión Integrados, mediante Acta N° 05 de fecha 25 de agosto de 2022, aprobaron: i) Políticas de Seguridad de la Información, ii) Política del Sistema de Gestión Integral, iii) Procedimiento de Control de Documentos y Registros del Sistema de Gestión Integral, iv) Procedimiento de Auditorías Internas al Sistema de Gestión Integral, v) Procedimiento de Revisión por la Dirección del Sistema de Gestión Integral, vi) Procedimiento de Mejora Continua del Sistema de Gestión Integral, vii) Procedimiento de Salidas no conforme del Sistema de Gestión Integral, viii) Procedimiento de Gestión de riesgos y oportunidades del Sistema de Gestión Integral, ix) Matriz de contexto de la organización y x) Matriz de Partes Interesadas. Asimismo, se solicita la emisión del acto resolutivo correspondiente, que formalice los documentos antes referidos;

Que, mediante el Informe N° D000244-2022-PENSION65-UAJ, la Unidad de Asesoría Jurídica emite opinión favorable para la formalización de los documentos normativos aprobados por los miembros del Comité de Sistemas de Gestión Integrados, mediante Acta N° 05 de fecha 25 de agosto de 2022, a través del respectivo acto resolutivo, al estar conforme a las normas de la materia;

Que, estando a las competencias de la Dirección Ejecutiva y con el visado de la Jefa de la Unidad de Asesoría Jurídica y del Coordinador de Calidad del Programa Nacional de Asistencia Solidaria "Pensión 65"; y de conformidad con lo dispuesto en el Decreto Supremo N° 081-2011-PCM y posteriores modificatorias; y la Resolución Ministerial N° 273-2017-MIDIS, que aprueba el Manual de Operaciones del Programa Nacional de Asistencia Solidaria Pensión 65;

SE RESUELVE:

Artículo 1. – Formalizar las "Políticas de Seguridad de la Información" del Programa Nacional de Asistencia Solidaria "Pensión 65", aprobadas por los miembros del Comité de Sistemas de Gestión Integrados, mediante Acta N° 05 de fecha 25 de agosto de 2022, las mismas que forma parte integrante de la presente resolución.

Artículo 2.- Formalizar la "Política del Sistema de Gestión Integral" del Programa Nacional de Asistencia Solidaria "Pensión 65", aprobada por los miembros del Comité de Sistemas de Gestión Integrados, mediante Acta N° 05 de fecha 25 de agosto de 2022, la misma que forma parte integrante de la presente resolución.

Siempre con el pueblo

Artículo 3.- Formalizar el "Procedimiento de Control de Documentos y Registros del Sistema de Gestión Integral" del Programa Nacional de Asistencia Solidaria "Pensión 65", aprobado por los miembros del Comité de Sistemas de Gestión Integrados, mediante Acta N° 05 de fecha 25 de agosto de 2022, el mismo que forma parte integrante de la presente resolución.

Artículo 4.- Formalizar el "Procedimiento de Auditorías Internas al Sistema de Gestión Integral" del Programa Nacional de Asistencia Solidaria "Pensión 65", aprobado por los miembros del Comité de Sistemas de Gestión Integrados, mediante Acta N° 05 de fecha 25 de agosto de 2022, el mismo que forma parte integrante de la presente resolución.

Artículo 5.- Formalizar el "Procedimiento de Revisión por la Dirección del Sistema de Gestión Integral" del Programa Nacional de Asistencia Solidaria "Pensión 65", aprobado por los miembros del Comité de Sistemas de Gestión Integrados, mediante Acta N° 05 de fecha 25 de agosto de 2022, el mismo que forma parte integrante de la presente resolución.

Artículo 6.- Formalizar el "Procedimiento de Mejora Continua del Sistema de Gestión Integral" del Programa Nacional de Asistencia Solidaria "Pensión 65", aprobado por los miembros del Comité de Sistemas de Gestión Integrados, mediante Acta N° 05 de fecha 25 de agosto de 2022, el mismo que forma parte integrante de la presente resolución.

Artículo 7.- Formalizar el "Procedimiento de Salidas no conforme del Sistema de Gestión Integral" del Programa Nacional de Asistencia Solidaria "Pensión 65", aprobado por los miembros del Comité de Sistemas de Gestión Integrados, mediante Acta N° 05 de fecha 25 de agosto de 2022, el mismo que forma parte integrante de la presente resolución.

Artículo 8.- Formalizar el "Procedimiento de Gestión de riesgos y oportunidades del Sistema de Gestión Integral" del Programa Nacional de Asistencia Solidaria "Pensión 65", aprobado por los miembros del Comité de Sistemas de Gestión Integrados, mediante Acta N° 05 de fecha 25 de agosto de 2022, el mismo que forma parte integrante de la presente resolución.

Artículo 9.- Formalizar la "Matriz de contexto de la organización", aprobada por los miembros del Comité de Sistemas de Gestión Integrados, mediante Acta N° 05 de fecha 25 de agosto de 2022, la misma que forma parte integrante de la presente resolución.

Artículo 10.- Formalizar la "Matriz de Partes Interesadas", aprobada por los miembros del Comité de Sistemas de Gestión Integrados, mediante Acta N° 05 de fecha 25 de agosto de 2022, la misma que forma parte integrante de la presente resolución.

Artículo 11.- Dejar sin efecto todas las disposiciones normativas que se contrapongan a a los documentos formalizados en los artículos del 1 al 10 del presente acto resolutivo.

Artículo 12.- Notificar la presente resolución al Coordinador de Calidad del Programa Nacional de Asistencia Solidaria "Pensión 65", para los fines correspondientes.

Artículo 13.- Dispóngase que la Unidad de Comunicación e Imagen del Programa Nacional de Asistencia Solidaria "Pensión 65", en el plazo máximo de 02 días hábiles de emitido el presente acto resolutivo, efectúe su publicación en el portal institucional y el portal de transparencia estándar del Programa Nacional de Asistencia Solidaria "Pensión 65": http://www.gob.pe/pension65

Regístrese y comuníquese.

Firmado digitalmente,

HERNÁN E. PENA
Director Ejecutivo
Programa de Asistencia Solidaria Pensión 65

Siempre con el pueblo

Políticas de Seguridad de la Información

(Basado en la Norma ISO 27001:2013)

(Vs. 01)

Equipo de Implementación	Oficial de Seguridad de la Información	Comité de SGI	*12/09/2022*
Elaborado por	Revisado por	Aprobado por	Fecha de aprobación

Matriz de Control de Cambios en Documentos

Versión	Ítem	Modificación respecto a la versión anterior	Sustento	Unidad que solicitó el cambio	Observaciones

PR-GCAL-01-F05vs01

INDICE

1. OBJETIVO

Establecer los lineamientos y responsabilidades para el uso y administración de los activos de información que deben cumplir los usuarios, para garantizar la confidencialidad, integridad y disponibilidad de la información del PROGRAMA NACIONAL DE ASISTENCIA SOLIDARIA - PENSIÓN 65.

2. ALCANCE

El Alcance del sistema de gestión de seguridad de la información, basado en la norma ISO 27001, aplica a los procesos de "Afiliación, Verificación, Transferencia Monetaria, Pagaduría" a los usuarios del Programa Nacional de Asistencia Solidaria Pensión 65, realizados en la sede central en Lima.

Las actividades de estos procesos se llevan a cabo en nuestras instalaciones, ubicadas en: Avenida República de Panamá N°3505 - San Isidro - Lima - Perú

En cuanto a las interfaces que interactúan con el alcance son:

A) Interfaces y dependencias internas del Alcance SGI

Procesos del Alcance	Dependencias Internas	Interfaces de información	Interfaces de Procesos	Interfaces de personas	Interfaces tecnológicas
Todos los procesos del alcance del SGSI	Unidad de Recursos Humanos	Procedimientos, instructivos y formatos aplicados a la gestión de Recursos Humanos	Procesos de Selección, Capacitación y Rendimiento de Recursos Humanos.	Personal responsable de la gestión de Recursos Humanos	Correo electrónico SGD
Todos los procesos del alcance del SGSI	Unidad de Tecnologías de la Información	Procedimientos, instructivos y formatos aplicados a la gestión de Tecnologías de la Información	Procesos de Ciclo de Vida de Software, Infraestructura, Soporte.	Personal responsable de la gestión de las Tecnologías de la Información	Correo electrónico Servidor de Archivos Servidor de Dominio Servicios de Redes y Comunicaciones (Switches, Firewall, etc)
Todos los procesos del alcance del SGSI	Unidad de Administración	Procedimientos, instructivos y formatos aplicados a la gestión de Administración	Procesos de gestión de Proveedores e Infraestructura	Personal responsable de la gestión de Administración	Correo electrónico SGD
Todos los procesos del alcance del SGSI	Otras Unidades Internas	Procedimientos, instructivos y formatos aplicados.	Procesos de gestión	Personal responsable de la gestión de las unidades	Aplicaciones del Programa (SISOPE, AYZA,etc) Aplicaciones externas utilizadas en el Programa

B) Interfaces y dependencias externas del Alcance SGI

Procesos del Alcance	Dependencias Internas	Interfaces de información	Interfaces tecnológicas
Todos los procesos del alcance del SGSI	Entidades del Estado	Documentos administrativos	Aplicaciones externas utilizadas en el Programa
Todos los procesos del alcance del SGSI	Usuarios del Programa	Declaraciones Juradas Documentación del Usuario	Mesa de Partes Virtual Correo Electrónico
Todos los procesos del alcance del SGSI	Ciudadanos	Documentación de los Ciudadanos	Mesa de Partes Virtual Correo Electrónico
Todos los procesos del alcance del SGSI	Empresas de Servicio Eléctrico/Internet	Informes Técnicos	Servicios de Redes y Comunicaciones
Todos los procesos del alcance del SGSI	Otras Partes Interesadas Externas	Documentación de las Partes Interesadas	Portal Institucional Canales Oficiales de Comunicación del Programa

3. TÉRMINOS Y DEFINICIONES

- **Activo de información:** Información que tiene valor para la entidad, pudiendo además ser aquel recurso (humano, tecnológico, etc.) que efectúa el tratamiento directo o indirecto de la información que soporta uno o más procesos del Programa. Hace referencia a la información y a los activos asociados a la información.
- **Control Lógico:** Están relacionados con el impedimento a nivel de software para los accesos de los usuarios.
- **Control Físico:** Están relacionados con el impedimento físico para los accesos de los usuarios.
- **Ciberseguridad:** Capacidad tecnológica de preservar el adecuado funcionamiento de las redes, activos y sistemas informáticos y protegerlos ante amenazas y vulnerabilidades en el entorno digital. Comprende la perspectiva técnica de la Seguridad Digital y es un ámbito del Marco de Seguridad Digital del país.
- **Confidencialidad:** Característica/propiedad por la cual la información no está disponible o revelada a individuos, entidades, o procesos no autorizados.
- **Contraseña:** Es una cadena de caracteres que se puede usar para iniciar sesión en un equipo y obtener acceso a archivos, programas y otros recursos.
- **Copia de respaldo (backup):** Copia de los datos de un archivo automatizado en un soporte que posibilite su recuperación.
- **Datos personales:** Son aquellos que identifican directa o indirectamente a una persona natural (titular de los datos); nombre, fecha de nacimiento, dirección de domicilio y del correo electrónico, números del DNI, RUC, teléfono, celular, seguro social y placa de vehículo; imagen, firma manuscrita y electrónica; y otros datos no sensibles.
- **Disponibilidad:** Característica/propiedad por la cual la información permanece accesible y disponible para su uso cuando lo requiera la persona autorizada.
- **Dispositivos BYOD:** Se caracteriza por el hecho de permitir al personal la incorporación de sus dispositivos móviles personales (portátiles, smartphones, tabletas) a las redes

	corporativas desde su casa, la propia oficina o cualquier otro lugar, aceptando su uso compartido, tanto para las tareas profesionales de uso corporativo como para las personales del personal. • **Hash:** Una función criptográfica hash- usualmente conocida como "hash"- es un algoritmo matemático que transforma cualquier bloque arbitrario de datos en una nueva serie de caracteres con una longitud fija. Independientemente de la longitud de los datos de entrada, el valor hash de salida tendrá siempre la misma longitud. • **Incidente de Seguridad de la Información:** Evento no deseado que tiene una probabilidad significativa de comprometer la confidencialidad, integridad y disponibilidad de la información y las operaciones involucradas a ella. • **Integridad:** Característica/propiedad por la cual la información conserva su exactitud y se encuentra completa. • **Log:** Registro de Información de un sistema. • **Propietario de Activo de Información:** Una persona o grupo de trabajo designado por la organización, quien tiene la responsabilidad de implementar los controles y/o disposiciones para el cuidado de los activos de información, bajo su responsabilidad. Es el responsable de la información y de los procesos que la manipulan, sean estos manuales, mecánicos o electrónicos. • **Recursos informáticos:** Todos los equipos computacionales, sistemas informáticos, aplicaciones, bases de datos, dispositivos extraíbles, y demás servidos que por su naturaleza registre, procese, almacene o transmita información electrónica o digital. • **Recovery Point Objective (RPO):** Cantidad de tiempo de inactividad o "downtime". Representa la cantidad de datos e información que una organización puede aceptar como pérdida considerable ante una contingencia, en ese umbral de tiempo debería estar siempre en un mínimo de tolerancia • **Recovery Time Objective (RTO):** Es el tiempo máximo que requiere una empresa para la recuperación de sus sistemas después de un incidente o desastre. • **SSH o Secure Shell:** es un protocolo de administración remota que le permite a los usuarios controlar y modificar sus servidores remotos a través de un mecanismo de autenticación. • **Seguridad de la Información:** Conjunto de actividades y prácticas orientadas a preservar la integridad, confidencialidad y disponibilidad de la información y los activos asociados a su tratamiento, independientemente de la forma en que éste se presente. • **Sistema de Gestión de Seguridad de la Información:** Es la parte del sistema integral de gestión, basado en un enfoque del riesgo del negocio para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información. • **Servidor de red:** Es un equipo que ofrece varios recursos compartidos de computadoras y otros servidores en una red informática. • **Sistema informático:** Sistema integrado por hardware, software y recursos humanos (administrador de la red informática, soporte técnico). • **UTI:** Unidad de Tecnologías de la Información • **UA:** Unidad de Administración • **URH:** Unidad de Recursos Humanos
4.	**DESARROLLO**
4.1	**POLÍTICA DE ORGANIZACIÓN DE LA SEGURIDAD (A.6)**
	La entidad permite prevenir, detectar y responder apropiadamente a eventos de Seguridad de la Información. Para ello, es necesario que se definan en forma clara las responsabilidades del personal en el contexto de la Seguridad de la Información.
4.1.1	**Funciones y responsabilidades de la seguridad de la información:** Se han establecido los roles y funciones de seguridad de la información en la entidad:
4.1.1.1	**Comité del Sistema de Gestión Integral (SGI)** a. Revisar, aprobar, establecer y comunicar a todo el programa el alcance, las políticas, los planes, los objetivos e información documentada relacionada con el Sistema de Gestión.

	b. Supervisar la implementación y efectividad de la Política de Seguridad de la Información. c. Asegurar que los recursos necesarios para el Sistema de Gestión estén disponibles. d. Definir la gestión de riesgo, aprobar el plan de tratamiento de los riesgos, los riesgos residuales y supervisar la eficacia de los controles implementados. e. Supervisar el cumplimiento de los controles organizativos y técnicos aplicados para cumplir con la preservación de la Seguridad de la Información. f. Revisar la eficacia de los controles de seguridad de la información aplicados a intervalos planificados.
4.1.1.2	**Oficial de Seguridad de la Información** a. Gestionar y mantener el Sistema de Seguridad de la Información. b. Aplicar el procedimiento de Gestión de Riesgos y Oportunidades c. Proporcionar apoyo al Comité del Sistema de Gestión en todo lo relacionado a la Seguridad de la Información. d. Proponer ante el Comité del Sistema de Gestión las modificaciones a la documentación perteneciente al Sistema de Gestión. e. Programar auditorías enfocadas en la seguridad de la información, para evaluar las prácticas de Seguridad de la Información. f. Supervisar que la información y todos los sistemas en el ámbito del alcance estén adecuadamente protegidos. g. Velar por el cumplimiento de la Seguridad de la Información.
4.1.1.3	**Personal** a. Conocer y cumplir con lo establecido en la Política de Seguridad de la información aprobada y vigente. b. Notificar los incidentes de seguridad de la información conforme a los canales de comunicación establecidos. c. Mantener la confidencialidad sobre toda la información, datos de carácter personal y de terceros a los que se tenga acceso en virtud de su trabajo. Obligación que subsistirá incluso después de finalizar su relación con la organización. d. Acceder únicamente a la información que han sido autorizados para el desarrollo de sus funciones en función de su perfil de puesto o responsabilidades. e. Queda terminantemente prohibido hacer entrega, por cualquier medio y sin autorización, de listados o de bases de datos a personas no autorizadas, ya sea de forma total o parcial. f. Participar en las pruebas del **PL-GTEC-02 PLAN DE CONTINGENCIA INFORMÁTICO**, ante eventuales caídas de los sistemas de información y aplicaciones informáticas. g. Velar por la seguridad y confidencialidad de la información contenida en sus equipos, especialmente cuando se encuentren fuera de las dependencias de la institución.
4.1.2	**Separación de Funciones** Se han segregado las funciones y áreas de responsabilidad para reducir las oportunidades de mal uso de los activos del Programa. Se tienen considerada en las: **a. POLITICA DE GESTION DE ACCESOS** **b. POLITICA DE SEGURIDAD FISICA Y EQUIPOS.** **c. POLITICA DE CONTRASEÑAS SEGURAS**
4.1.3	**Contacto con autoridades y Grupos de Interés** A efectos de poder comunicar incidentes de seguridad de la información a las autoridades pertinentes, se cuenta con el documento **ANEXO 1 – LISTA DE CONTACTOS DE AUTORIDADES Y GRUPOS DE INTERÉS**, en donde se encuentran identificados. Así mismo, se identifican Grupos de Interés en donde se tiene participación a fin de realizar consultas relacionadas a seguridad de la información, se cuenta con el documento Lista de Contactos de Autoridades y Grupos de Interés, en donde se encuentran identificados.

4.1.4	**Seguridad de la información en gestión de proyectos** La entidad debe integrar la seguridad de la información en las metodologías de gestión de proyectos para garantizar que los riesgos de seguridad de la información son identificados y tratados independientemente al tipo de proyecto. Los proyectos se registran y se evalúan sus riesgos de seguridad de Información en los registros documentos de proyectos.
4.2	**POLITICA DE EQUIPOS MÓVILES (A.6.2.1)**
	La política de seguridad de dispositivos móviles brinda lineamientos para el aseguramiento en el uso y administración de los dispositivos como teléfonos celulares, tabletas y laptops.
4.2.1	**Identificación de los dispositivos móviles** El registro de los dispositivos móviles (los smartphones, tabletas y laptops) lo realiza la **UNIDAD DE ADMINISTRACIÓN.**
4.2.2	**Asignación de Equipos** El equipo previo a su asignación se realizarán tareas de limpieza lógica y física. En el caso del chip del equipo se debe asignar considerando la jerarquía de puestos.
4.2.3	**Instalación y Configuración de Aplicaciones** La administración de los recursos de los dispositivos móviles pertenecientes a la entidad estará a cargo del personal de la UTI a partir de una solicitud (**APLICATIVO WEB GLPI)**. El proceso de instalación y configuración de las aplicaciones de los dispositivos móviles será realizado por la UTI. Los perfiles de usuarios y las características en las capacidades de los equipos serán definidos en función de la importancia de la información procesada o almacenada en cada tipo de usuario que utilizan los smartphones y tabletas del Programa. En el caso de smartphones de la institución, se utiliza un software de administración como el Mobile Data Management (MDM).
4.2.4	**Autenticación y Acceso** Se protegerá el acceso a los dispositivos móviles según: a. Los privilegios de cada perfil de usuario del 3.2.2. b. Asimismo, se podrá considerar también la importancia de la información que se almacena o se protege en cada equipo. En caso de smartphones se recomienda el uso del patrón de inicio de sesión.
4.2.5	**Control de Acceso a aplicaciones desde el dispositivo móvil** Para el caso de las aplicaciones instaladas en el celular se manejan los siguientes controles de acceso: a. Ayza – IMEI generado del mismo aplicativo y activado desde la UTI. b. Otras aplicaciones – Usuario y contraseña
4.2.6	**Parches y Actualización** Toda actualización será realizada por la Unidad de Tecnologías de la Información. Todos los usuarios de dispositivos móviles utilizarán la última o la más segura versión de las aplicaciones. Los parches y aplicaciones serán obtenidos de manera formal, provenientes del fabricante. Asimismo, contarán con servicios de soporte del fabricante.
4.2.7	**Controles Físicos** El personal protegerá sus dispositivos móviles, no debiendo entregarlos a otra persona, en particular en aquellos dispositivos inteligentes que almacenan información de **uso interno** del Programa.
4.2.8	**Información almacenada** Se realiza copia de seguridad de la información del dispositivo.
4.2.9	**Seguridad del Sistema Operativo** En los dispositivos móviles se instala un software de detección y prevención de malware.

4.2.10	**Pérdida o Robo** Ante alguna pérdida o robo se debe informar inmediatamente a su jefe inmediato, a la Unidad de Administración para la suspensión del servicio y correspondiente bloqueo y también a la Unidad de Tecnologías de la Información para el bloqueo del acceso a los aplicativos.
4.2.10	**Responsabilidad del personal** a. Velar por la seguridad de los dispositivos móviles entregados. b. Asegurar que ninguna persona utilice el dispositivo móvil de propiedad del Programa violando la presente política, que no se realicen actividades ilegales, contrarias a la moral y las buenas costumbres y que no utilice el acceso para fines ajenos a las actividades propias de su función como colaborador. c. Todo dispositivo móvil que tenga instalado los aplicativos de Pensión 65, tanto el aplicativo como el dispositivo móvil asumirán los controles implementados por la Entidad. d. Toda la información contenida en los aplicativos de Pensión 65 y aquella que se haya generado por estos, que sean propios del desempeño del personal y que se encuentre contenida en los dispositivos móviles es de propiedad única y exclusiva de Pensión 65, y es clasificada bajo todo concepto como **USO INTERNO**. e. Queda prohibido la manipulación de las configuraciones de los smartphones y tabletas, incluye las aplicaciones. f. En caso de pérdida o robo, se debe de comunicar inmediatamente a UA, UTI y su jefe inmediato. g. Cuando el personal se retire de las instalaciones y no lleve el dispositivo móvil consigo, g.1. En caso sea una Laptop, deberá colocar la cadena de seguridad en la Laptop, g.2. En caso sea otro dispositivo móvil éste deberá ser guardado en un cajón con llave; y en ambos casos, la puerta de su oficina deberá ser cerrada con llave, si es el caso. g.3. Adicionalmente, cuando el dispositivo móvil sea una laptop se debe tener en cuenta que: El protector de pantalla debe estar configurado y activado obligatoriamente. g.4. Deben bloquearse luego de diez (10) minutos de inactividad. h. Adicionalmente cuando desarrollen fuera del lugar habitual de trabajo: h.1. Se deberán proteger los dispositivos móviles contra el robo. h.2. No se deberá dejar solo, o sin vigilar, un equipo que contenga información importante, sensible o crítica; siempre que sea posible se dejará bajo llave. h.3. Cuando la información sea altamente confidencial, se usarán técnicas de encriptación para evitar el acceso no autorizado o la divulgación de la información almacenada. h.4. Revisar si se cuenta con un antivirus activo y/u otros procedimientos contra software malicioso. h.5. Se deberá asegurar que la información sensible almacenada en estos dispositivos móviles tiene copia de seguridad recuperable en caso de pérdida o robo del dispositivo. h.6. Se deberá prestar un cuidado especial en proteger los dispositivos móviles que estén conectados a las redes. Solo se deberán hacer accesos remotos a la información de la empresa pasando por mecanismos de seguridad de control de accesos y después de conseguir con éxito identificarse y autenticarse. i. El personal encargado de los dispositivos móviles son los máximos responsables de su seguridad y como tales deberán asumir las sanciones impuestas ante un posible incidente de segurida.

4.3	POLÍTICA DE USO DE DISPOSITIVOS MÓVILES PERSONALES PARA USO DEL PROGRAMA (BYOD)
4.3.1	El Programa retendrá el control sobre su información mientras se accede a dicha información a través de dispositivos que no pertenecen a la organización. Las reglas de la presente Política aplican para todos los dispositivos móviles personales para el uso del Programa de la sede central denominados en ingles por sus siglas BYOD (Bring Your Own Device), dentro o fuera de las instalaciones de la organización.
4.3.2	**Copias de seguridad para información** El usuario se conecta a la red interna y guarda todos los documentos dentro de su carpeta personal, de la cual se realiza un backup periódico. En el caso de teléfonos móviles, estos no manejan o no tienen acceso a archivos de la red, solo a navegación y lectura de correo electrónico.
4.3.3	**Software de seguridad instalado** Todos los equipos BYOD deben tener instalado un software antivirus instalado por el propio usuario del equipo.
4.3.4	**Método de autenticación** El usuario tiene acceso a los servicios informáticos del Programa a través de una Virtual Private Networt o VPN (Red privada virtual) configurada con su usuario asignado de la red interna.
4.3.5	**Responsabilidad del Personal** a. Cuando se utilicen BYOD fuera de las instalaciones del Programa, no deben ser dejados desatendidos. b. Cuando se utiliza BYOD en lugares públicos, el propietario debe tener la precaución de que los datos no puedan ser leídos por personas no autorizadas. c. Se deben instalar periódicamente parches y actualizaciones. d. No se permite hacer lo siguiente con los BYOD: d.1. Permitir el acceso a cualquiera que no sea el personal propietario del dispositivo. d.2. Almacenar material ilegal en el dispositivo. d.3. Instalar software sin licencia. e. No conectarse a redes Wi-Fi desconocidas.

4.3.6	**Responsabilidad del Programa** a. Realizar el inventario de los equipos BYOD y mantenerlo actualizado. Para lo cual se solicitará a todas las unidades el reporte de estos equipos mediante el **ANEXO 5 -LISTADO DE DISPOSITIVOS BYOD.** b. Concientizar en el uso de los equipos BYOD c. Atender las solicitudes de actualización y configuraciones del dispositivo siempre y cuando estén relacionado con las actividades de trabajo en el Programa. d. El Programa tiene el derecho de ver, editar y borrar todos los datos que se encuentran almacenados, transferidos o procesados en BYOD. e. El responsable del sistema está autorizado a configurar cualquier BYOD en conformidad con la presente política y a controlar su uso a través de [software para gestión de dispositivos móviles si procede]. f. Se tiene el derecho de realizar el borrado completo de todos los datos del BYOD si considera que es necesario para la protección de los datos del Programa, sin el consentimiento del propietario del dispositivo. g. El Programa no abonará al personal (los propietarios de BYOD) ningún costo por el uso del dispositivo con fines laborales. h. Todas las violaciones de seguridad relacionadas con BYOD deben ser reportadas inmediatamente al Oficial de Seguridad de la Información, o quien haga sus veces.
4.4	**POLITICA DE TRABAJO REMOTO (A.6.2.2)**
	El trabajo remoto utiliza tecnología de comunicaciones para permitir que el personal trabaje en forma remota desde un lugar externo a la entidad. La entidad ha brindado instrucciones a todo el personal para que se cumplan los mismos lineamientos establecidos de seguridad en los ambientes de trabajo remoto, en el caso que el equipo sea un equipo considerado personal (BYOD) adicionalmente se aplicará la **POLÍTICA DE USO DE DISPOSITIVOS MÓVILES PERSONALES PARA USO DEL PROGRAMA (BYOD).** Entre ellos tenemos los siguientes:
4.4.1	Es responsabilidad del Personal: a. Asegurarse que en el sitio en donde se realizará el trabajo remoto debe ser un ambiente en donde se reduzca la probabilidad de la amenaza de acceso no autorizado a información o recursos por parte de otras personas que utilizan el lugar o ambientes en donde se realiza el trabajo remoto. b. Asegurarse que el lugar tenga fácil acceso a la red inalámbrica (wifi) para hacer el trabajo, que no se tengan problemas de señal baja del wifi que puedan impactar en el trabajo, es decir, contar con conexión a internet de alta velocidad confiable. c. Verificar la seguridad de las redes domésticas, es decir, el acceso a la red inalámbrica tenga clave de acceso. d. Verificar que el Sistema operativo del equipo asignado y aplicaciones cuenten con las últimas actualizaciones. e. Verificar que los equipos tengan instalado y actualizado el antivirus. f. Verificar que los equipos cuenten con bloqueo automático por inactividad. g. No utilizar otra herramienta de comunicación o de videoconferencia a la establecida por la entidad. Si se necesita utilizar otra herramienta de comunicaciones, debe ser aprobada por la UTI. h. Está prohibido almacenar la información de trabajo en los equipos, toda la información se almacena en la plataforma que brinda la UTI. i. No realizar actividades ilícitas ni vulnerar las políticas del Programa o utilizar el acceso remoto suministrado para obtener lucro comercial.

4.4.2	Es responsabilidad del Programa: a. La concientización, sensibilización del personal sobre la necesidad de proteger sus contraseñas de acceso, y no compartirlas con nadie, ni siquiera con los miembros de su familia. b. Establecer qué personal tienen permitido el acceso a sistemas internos del Programa. c. Efectuar monitoreos regularmente de las conexiones remotas, especialmente se debe prestar atención a los intentos de conexión sospechosos. d. Verificar que los equipos de trabajo remoto tienen instalado y correctamente configurado el software VPN o un software de administración remota. e. Realizar la anulación de las autorizaciones y derechos de acceso cuando finalicen las actividades remotas. f. Llevar un registro de los incidentes de seguridad de la información por este tipo de modalidades.
4.4.3	Se llevará un registro de incidentes a fin de corregir eventuales fallas en la seguridad de este tipo de accesos según la **POLÏTICA DE INCIDENTES**.
4.5	**POLITICA DE SEGURIDAD DE LA INFORMACIÓN DE LOS RECURSOS HUMANOS (A.7)**
	La seguridad de la información de los recursos humanos involucra a toda persona que utiliza la información de la entidad para el desempeño de sus actividades (en el caso de personal de proveedores se desarrolla en la Política de Seguridad de la Información de Proveedores), por lo tanto, se establece que:
4.5.1	**Previo al empleo**
4.5.1.1	**Selección** a. El proceso de selección se desarrolla en el marco de la **DI-GRHH-04 DIRECTIVA PARA LA SELECCIÓN DE PERSONAL BAJO EL REGIMEN ESPECIAL DE CONTRATACIÓN ADMINISTRATIVA DE SERVICIOS – CAS, DECRETO LEGISLATIVO N° 1057, EN EL PROGRAMA NACIONAL DE ASISTENCIA SOLIDARIA PENSIÓN 65** b. Todos los candidatos presentan los anexos de postulación a modo de declaración jurada. c. En el caso del candidato que resulta ganador del proceso de selección, la Unidad de Recursos Humanos realiza la verificación de la información del postulante en la plataforma PIDE (antecedentes policial, judicial y penal).
4.5.1.2	**Términos y condiciones de empleo** Se establecen obligaciones y responsabilidad del personal de Pensión 65 respecto a la seguridad de la información.

	En las siguientes cláusulas del **CONTRATO ADMINISTRATIVO DE SERVICIOS:** a. CLÁUSULA DÉCIMO CUARTA: DERECHO DE PROPIEDAD Y CONFIDENCIALIDAD DE LA INFORMACIÓN a.1. Las obras, creaciones intelectuales, científicas, entre otros, que se hayan realizado en el cumplimiento de las obligaciones del presente contrato con los recursos y medios de la entidad, son de propiedad de LA ENTIDAD. En cualquier caso, los derechos de autor y demás derechos de cualquier naturaleza sobre cualquier material producido bajo las estipulaciones de este Contrato son cedidos a LA ENTIDAD en forma exclusiva. a.2. La información obtenida por el trabajador dentro del cumplimiento de sus obligaciones, así como sus informes y toda clase de documentos que produzca, relacionados con la ejecución de sus labores será confidencial. b. CLÁUSULA NOVENA: OBLIGACIONES GENERALES DE EL CONTRATADO b.1. No divulgar, revelar, entregar o poner a disposición de terceros, dentro o fuera del centro de trabajo salvo autorización expresa de LA ENTIDAD, la información proporcionada por ésta para la prestación del servicio y, en general, toda información a la que tenga acceso o la que pudiera producir con ocasión. b.2. Adoptar las medidas de seguridad que garanticen la integridad de la documentación que se proporciona. En los siguientes artículos del **REGLAMENTO INTERNO DE SERVIDORES INTERNOS:** a. Articulo 21 Obligaciones del Servidor Civil a.1. Usar y cuidar los bienes, equipos, materiales e implementos de trabajo, enseres y valores que se le hayan asignado para el cumplimiento de su labor, siendo responsables de la reparación de los daños que provoquen en caso de deterioro o pérdida por el uso indebido y/o irresponsable, sin perjuicio de la sanción administrativa, de ser el caso. a.2. Guardar absoluta reserva y discreción sobre aquellas actividades, asuntos, procesos, gestiones y documentos producidos, proporcionados u obtenidos, así como de toda documentación e información que con motivo del ejercicio de sus funciones haya podido conocer; así como de toda información, que por su naturaleza sea de carácter reservado o confidencial. a.3. Cumplir con las normas de seguridad informática y obligaciones referidas al uso de internet, software y correo electrónico que otorga el Programa. b. Articulo 22 Prohibiciones del Servidor Civil b.1. Alterar, modificar, falsificar, ocultar o destruir documentos de trabajo, así como extraer documentos del Programa, inclusive aquellos que no tengan carácter reservado; salvo autorización del funcionario responsable, atendiendo los requerimientos de la labor de la entidad
4.5.1.3	Asimismo, una vez que el personal comienza a laborar contará con los accesos apropiados para desempeñar sus actividades.
4.5.2	**Durante el Empleo**

4.5.2.1	**Concientización, educación y formación en seguridad de la información** Todo el personal recibe concientización, entrenamiento, formación y actualizaciones regulares en seguridad de la información relevantes para su función laboral. a. Las capacitaciones de seguridad de la información se establecen en el **PLAN DE DESARROLLO PERSONAL-PDP**, para lo cual las áreas comunican sus necesidades de capacitación. b. Las charlas seguridad de la información se realizan mediante un **PLAN DE SENSIBILIZACIÓN**. c. Además, se realizan inducciones al nuevo personal de aspectos de seguridad de la información.
4.5.2.2	**Proceso disciplinario** En el **REGLAMENTO INTERNO DE SERVIDORES CIVILES** en el CAPITULO IX REGIMEN DISCIPLINARIO se encuentra definido el proceso disciplinario administrativo para adoptar medidas aplicables al personal que han cometido una falta a los lineamientos establecidos por la Entidad, este proceso disciplinario debe también usarse como disuasivo para prevenir que el personal falte a las políticas y procedimientos de seguridad de la información de PENSION 65.
4.5.3	**Finalización o cambio de la relación laboral o puesto de trabajo.** Las responsabilidades y las funciones de la seguridad de la información que siguen vigentes luego de la finalización de la relación contractual o el cambio del puesto de trabajo son establecidas en la **DI-GRHH-05 DIRECTIVA PARA LA ENTREGA Y RECEPCIÓN DE CARGO DE LOS SERVIDORES DEL PROGRAMA NACIONAL DE ASISTENCIA SOLIDARIA PENSIÓN 65**. a. Los derechos de acceso a la información y a las instalaciones de procesamiento; del personal y terceros debe ser removido o modificado al producirse el término de la relación laboral o contrato. b. La Unidad de Recursos Humanos debe enviar un correo electrónico a la UTI para la actualización o eliminación de las cuentas de usuarios, a fin de mantener actualizado los accesos a los sistemas de información y servicios informáticos. c. Los jefes de Unidad deben comunicar a la UTI los accesos de los terceros a los recursos informáticos y aplicaciones que deben ser retirados.

4.5.4	**Consideraciones de Seguridad de la Información al personal** a. Cuando el personal inicia la relación laboral se le asignan los permisos apropiados para desempeñar su trabajo, como: a.1. Permisos a las aplicaciones informáticas internas y/ externas a.2. Permisos a una cuenta de correo del Programa a.3. Permiso a una computadora con carpetas locales y una carpeta en red b. Cuando el personal termina su relación laboral b.1. Se remueven los permisos brindados, como: i) Permisos a las aplicaciones informáticas internas y/ externas: Se eliminan los accesos. ii) Permisos a una cuenta de correo del Programa: Se realizar una copia de seguridad del correo y después se elimina el correo. iii) Permiso a una computadora: Se eliminan los archivos locales y archivos de carpetas de red del usuario en mención. b.2. Dado que los archivos de la computadora en local y en red del usuario son eliminados, es responsabilidad del personal realizar una copia de seguridad sin violar las Políticas de Seguridad de la Información del Programa. b.3. Dado que la cuenta del correo del Programa es eliminada, es responsabilidad del personal realizar la copia de seguridad sin violar las Políticas de Seguridad de la Información del Programa. b.4. En el caso de la cuenta del correo del Programa, la persona podrá solicitar la entrega de los mensajes contenidos en su correo dado que antes de su desvinculación se ha realizado la copia de seguridad del mismo, esta solicitud siempre debe realizarse de la manera más específica posible para evitar violar las Políticas de Seguridad de la Información del Programa.
4.6	**POLITICA DE GESTION ACTIVOS (A. 8)**
4.6.1	**Responsabilidad por Activos**
4.6.1.1	**Inventario y Propiedad de los Activos de Información** a. Se tienen identificados los activos de información asociados a los procesos, sus propietarios y ubicación. El inventario es realizado por Unidad de Administración y será actualizado una vez al año o ante cualquier modificación de la información registrada, lo que suceda primero. b. La responsabilidad de los activos de información está referida al propietario de la información y de los procesos que la manipulan, sean estos manuales, mecánicos o electrónicos. Aunque tenga autoridad formal, no significa que tenga derechos de propiedad sobre el activo.
4.6.1.2	**Uso Aceptable de los Activos** a. El uso de los activos de información debe ser para propósitos de las actividades del Programa de acuerdo con las políticas y procedimientos que se definan y considerando criterios de buen uso. b. No se debe divulgar información que haya sido clasificada como “Uso Interno”, salvo tenga una respuesta satisfacción de la consulta por parte de la Unidad de Asesoría Jurídica. c. Se deben cumplir con los requisitos legales, contractuales y normativos relativos al uso de activos de información, incluyendo las políticas de seguridad que deben mantenerse alineadas con las leyes vigentes. d. Se deben gestionar adecuadamente los elementos de control de acceso, como contraseñas (control lógico) así como llaves de cerradura (control físico). e. El personal que ponga en riesgo los activos de información, se le aplicará medidas disciplinarias de acuerdo con el Reglamento Interno de Trabajo. Esta sanción estará sujeta a la gravedad del incidente ocasionado y conforme a las normas establecidas.

4.6.1.3	**Devolución de los Activos** a. Todo el personal y los usuarios de proveedores externos deben devolver todos los activos del Programa en su poder al término de su empleo, contrato o servicio. b. En el caso del personal se debe seguir la **DI-GRHH-05-01 DIRECTIVA PARA LA ENTREGA Y RECEPCIÓN DE CARGO DE LOS SERVIDORES DEL PROGRAMA NACIONAL DE ASISTENCIA SOLIDARIA PENSIÓN 65**.
4.6.1.4	**Clasificación de Activos de Información** a. La clasificación de la información es de acuerdo con la **LEY Nº 27806 DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA**: a.1. **Uso Interno:** Activos de información cuyo contenido sólo debe ser de uso y divulgación para el personal interno y que solo podrán ser divulgados a terceras partes teniendo firmado un acuerdo de confidencialidad, siempre y cuando su divulgación no impacte a la Entidad. **a.2.** **Uso Público:** Información no sensible de acceso público y que su divulgación no genera impacto a la Entidad. b. El propietario de la información es el encargado de la clasificación de los activos de información que están bajo su responsabilidad siguiendo los lineamientos legales.
4.6.2	**Manejo de Medios**
4.6.2.1	**Gestión de medios removibles/extraíbles** a. Todo los medios reutilizables y su contenido que ya no son necesarios deben hacerse irrecuperables, para lo cual se cuenta con el procedimiento Borrado Seguro Elimina Medios de la **DIRECTIVA PARA LA ADMINISTRACIÓN, ASIGNACIÓN, USO Y CONTROL DE LOS BIENES MUEBLES, PATRIMONIALES PARA EL PROGRAMA NACIONAL PENSION 65**. b. Los medios de almacenamiento se almacenan en un entorno seguro según las especificaciones del fabricante. c. En los casos que se tengan medios removibles con información considerada confidencial o la integridad de los datos es importante, se debería utilizar técnicas de cifrado (ZIP o RAR) para proteger los datos en estos medios removibles/extraíbles.
4.6.2.2	**Eliminación de Soportes (Disposición de Medios)** a. Se debe disponer de los medios de forma segura cuando ya no sean necesarios para lo cual se cuenta con el procedimiento Borrado Seguro Elimina Medios de la **DIRECTIVA PARA LA ADMINISTRACIÓN, ASIGNACIÓN, USO Y CONTROL DE LOS BIENES MUEBLES, PATRIMONIALES PARA EL PROGRAMA NACIONAL PENSION 65**. b. Todo medio de almacenamiento de información debe ser almacenado y eliminado de forma segura. c. Debe identificarse los elementos que puedan requerir su eliminación.
4.6.2.3	**Transferencia de medios físicos** a. Se debe proteger los medios que contienen información contra el acceso no autorizado, el mal uso o la corrupción durante el transporte, para lo cual la entidad debe contar con transporte o mensajeros confiables para la protección de sus activos de información. b. Toda información confidencial en medios físicos debe contener una protección física adicional como un embalaje.
4.7	**POLÍTICA DE CONTRASEÑAS SEGURAS**

	a. Las contraseñas son un aspecto fundamental de la seguridad de la información. Una contraseña mal elegida o protegida puede resultar en un agujero de seguridad para toda la organización. Por ello, todos los usuarios de la empresa son responsables de velar por la seguridad de las contraseñas. b. Se debe concienciar y controlar que los usuarios sigan buenas prácticas de seguridad en la selección, uso y protección de claves o contraseñas, las cuales constituyen un medio de validación de la identidad de un usuario y consecuentemente un medio para establecer derechos de acceso a las instalaciones, equipos o servicios informáticos. c. Los usuarios son responsables del uso de las claves o contraseñas de acceso que se le asignen para la utilización de los equipos o servicios informáticos del programa. d. Todas las contraseñas de cuentas que den acceso a recursos y servicios de la empresa deberán seguir las siguientes directrices generales: d.1. Todas las contraseñas de sistema (root, administradores, cuentas de administración de aplicaciones, cuentas de email, etc) deben ser cambiados al menos una vez cada 3 meses. d.2. Se deben cambiar las claves en el primer ingreso al sistema. (Para las aplicaciones internas) d.3. Cada vez que se cambien éstas deben ser distintas por lo menos de las últimas tres anteriores. d.4. Las contraseñas no deben ser incluidas en mensajes de correo electrónico, ni ningún otro medio de comunicación electrónica. Tampoco deben ser comunicadas las contraseñas en conversaciones telefónicas, ni redes sociales, incluido WhatsApp. d.5. En la medida de lo posible, las contraseñas serán generadas automáticamente con las características recomendadas en esta política y se les comunicará a los usuarios su contraseña siempre en estado “expirado” para obligar al usuario a cambiarla en el primer uso que hagan de la cuenta o servicio. d.6. Las contraseñas por defecto asociadas a los sistemas o aplicaciones nuevas deberán ser cambiadas antes de poner estos sistemas en producción. También se desactivarán aquellas cuentas “por defecto” que no sean imprescindibles. d.7. Todas las contraseñas de sistema y de usuario de recursos y servicios deben respetar las recomendaciones descritas en la presente política. d.8. Las claves no deben ser almacenadas en un sistema de registro automatizado (por ej., macros o explorador). d.9. No se deben utilizar las mismas claves personales para fines privados y para fines comerciales. e. Algunos servicios en los que sea crítico el mantener la seguridad de la contraseña podrán determinar medidas adicionales de protección de la misma.
4.7.1	**Selección y custodia de contraseñas**

4.7.1.1 Recomendaciones generales para la selección de contraseñas

Las contraseñas son usadas con múltiples propósitos en la empresa como pueden ser las contraseñas de cuentas de usuario intranet, servicios Web, cuentas de correo electrónico, protectores de pantalla en los recursos de los usuarios, administración de dispositivos remotos, etc.

La seguridad de este tipo de autentificación se basa en dos premisas:

a. La contraseña personal sólo la conoce el usuario.

b. La contraseña es lo suficientemente "fuerte" para no ser descifrada: La contraseña para ser considerada "fuerte" (segura) debe poseer las siguientes características:

b.1. Debe tener al menos 8 caracteres.

b.2. Utiliza caracteres de tres de los cuatro grupos siguientes, y siempre que uno de ellos deberá ser un símbolo:

i) Letras minúsculas.
ii) Letras mayúsculas.
iii) Números (por ejemplo, 1, 2, 3).
iv) Símbolos (por ejemplo, ¡, @, Ñ, =\`{}[]:";'<>?,./) -, etc.).

b.3. No utilizar contraseñas que se puedan adivinar fácilmente, como pueden ser:

i) Una cadena de caracteres derivada del nombre de la cuenta del usuario.

ii) Una cadena de caracteres formada por la repetición de caracteres.

iii) Una palabra contenida en un diccionario (de lengua española o extranjera).

iv) Una palabra de diccionario seguida o precedida de un carácter (p.ej. "palabra1" o "Xpalabra" o "palabra!".

v) Un nombre de pila: Nombres de familiares, amigos, mascotas, ciudades, etc.

vi) Fechas de cumpleaños u otra información personal tales como dirección o número de teléfono.

vii) Conjuntos de letras o números que sigan un patrón sencillo, tales como aaabbb, qwerty, abcdef, 123321, etc.

viii) Una clave no debe ser una palabra que se encuentre en el diccionario, en un dialecto o jerga de ningún idioma, como tampoco ninguna de estas palabras escritas hacia atrás.

c. Las contraseñas no deben ser almacenadas por escrito nunca. Intente crear contraseñas que pueda recordar fácilmente. Una forma de recordarlo con facilidad es crear una contraseña basada en una frase fácilmente recordable.

4.7.1.2 Recomendaciones para la protección de la contraseña

	a. Se recomienda cambiar la contraseña en el primer momento de acceder a la cuenta, para que la nueva contraseña sea distinta a la que va en la solicitud. b. No comparta las cuentas y contraseñas con nadie, incluyendo administrativos, secretarias, etc. Todas las contraseñas deben ser tratadas como información sensible y confidencial. c. A continuación, se presenta una lista de cosas que NO se deben hacer: c.1. No utilice la misma contraseña. c.2. No revele su contraseña por teléfono a NADIE, incluso aunque le hablen en nombre del servicio de informática o de un superior suyo en la organización. c.3. Las claves generadas por el usuario no deben ser distribuidas por ningún medio (oral, escrito, electrónico, etc.); las claves deben ser cambiadas si existen indicios de que puedan estar en riesgo las mismas claves o el sistema (en ese caso, se debe informar un incidente de seguridad). c.4. Nunca escriba la contraseña en papel y lo guarde. Tampoco almacene contraseñas en ficheros de ordenador sin cifrar o proveerlo de algún mecanismo de seguridad. c.5. No revele su contraseña a sus superiores, ni a ninguna persona. c.6. No hable sobre una contraseña delante de otras personas. c.7. No revele su contraseña en ningún cuestionario o formulario, independientemente de la confianza que le inspire el mismo. c.8. No comparta la contraseña con familiares. c.9. No revele la contraseña a sus compañeros cuando se marche de vacaciones. c.10. No utilice la característica de “Recordar Contraseña” existente en algunas aplicaciones. c.11. No se debe llevar un registro de las claves, a menos que un método seguro haya sido aprobado por el responsable del sistema.
4.7.1.3	**Recomendaciones sobre contraseñas de servicios y servidores informáticos.** Estas últimas recomendaciones van dirigidas a aquéllos que administran o son responsables de algún servidor o servicio que sea accesible a distintos usuarios (externos o internos): a. Tener unos criterios para la creación y asignación de contraseñas lo más similares posibles a los Requisitos obligatorios expuestos en esta Política. b. Los servidores y dispositivos se deben configurar con cuentas separadas para los que tienen privilegios de administración y los que no. c. Los usuarios se deberían autenticar con cuentas que no tuvieran más privilegios que los necesarios para hacer uso del servicio. d. El acceso a los privilegios correspondientes (para administrar la máquina) debe hacerse mediante mecanismos de “escalado de privilegios”; en este caso además quedará traza de qué usuario ha accedido a estos privilegios especiales. e. Sólo se tendrán los privilegios especiales el tiempo que sea estrictamente necesario. f. Se deberá dar de baja a aquellos usuarios que dejen de pertenecer al colectivo al que va destinado el servicio.

4.7.1.4	**Gestión de la clave del usuario** Cuando se asignan y utilizan claves de usuarios, se deben seguir las siguientes reglas: a. Deben mantener sus claves en forma confidencial, como se establece en este documento. b. Cada usuario puede utilizar solamente su propio nombre de usuario asignado de forma exclusiva. c. Cada usuario debe tener la posibilidad de escoger su propia clave, en los casos corresponda. d. Las claves utilizadas para el primer acceso al sistema deben ser exclusivas y seguras, según lo establecido precedentemente. e. Las claves de primer acceso deben ser comunicadas al usuario de forma segura, y se debe verificar previamente la identidad del usuario. f. El sistema de gestión de claves debe requerir que el usuario modifique la clave de primer acceso cuando ingrese al sistema por primera vez. g. Los sistemas informáticos deben requerir que el usuario escoja contraseñas seguras. h. El sistema de gestión de claves debe requerir que los usuarios cambien sus claves cada tres meses. i. Si el usuario solicita una nueva clave, el sistema de gestión de claves debe determinar la identidad del usuario. j. El usuario debe confirmar la recepción de la clave. k. La contraseña no debe ser visible en la pantalla durante el inicio de sesión. l. Si un usuario ingresa una clave incorrecta tres veces consecutivas, el sistema debe bloquear la cuenta de usuario en cuestión. m. Las claves creadas por el fabricante del software o hardware deben ser cambiadas durante la instalación inicial. n. Los archivos que contienen claves deben ser guardados en forma separada de los datos de sistema de la aplicación.
4.8	**POLITICA DE GESTION DE ACCESOS (A.9)**
	La presente política tiene como finalidad controlar los accesos a la información, mantener el acceso autorizado del personal y prevenir accesos no autorizados a los sistemas de información y a los servicios de red del Programa.
4.8.1	**Requerimientos para el Control de Accesos**
4.8.1.1	Todos los accesos a los activos de información tanto lógicos como físicos deben basarse en la necesidad y rol del usuario. Se deberá tomar en cuenta los siguientes aspectos: a. Los requerimientos de seguridad de cada una de las aplicaciones. b. Identificación de toda la información relacionada a las aplicaciones y los riesgos a la que está expuesta. c. Coherencia entre las políticas de control de accesos y las políticas de gestión de activos de información. d. Uso de perfiles de usuarios estandarizados definidos según roles. e. Revisión periódica de los controles de acceso. f. Revocación de los derechos de acceso.
4.8.1.2	El personal del Programa y/o terceros solo deben tener acceso a redes y servicios a los que fueron específicamente autorizados a utilizar.
4.8.1.3	El procedimiento de **PR-GTEC-08 ACCESOS DE USUARIOS A LOS SERVICIOS DE LA UNIDAD DE TECNOLOGÍAS DE LA INFORMACIÓN** brinda el proceso de solicitud alta/modificación de los accesos a los servicios de la Unidad de Tecnologías de la Información
4.8.2	**Gestión de Acceso del Personal**

4.8.2.1	**Registro y baja de usuarios** El procedimiento de **PR-GTEC-08 ACCESOS DE USUARIOS A LOS SERVICIOS DE LA UNIDAD DE TECNOLOGÍAS DE LA INFORMACIÓN** brinda el proceso de solicitud alta y baja de los accesos a los servicios de la Unidad de Tecnologías de la Información. Según dicho procedimiento: a. Los responsables de cada unidad solicitan a UTI el alta b. Para el personal la Unidad de Recursos Humanos comunica la baja. c. Para los proveedores la Unidad de Administración también comunica la baja
4.8.2.2	**Gestión de derechos de acceso privilegiados** a. Debe restringirse y controlarse la asignación y uso de los derechos de acceso privilegiados. b. Se identifica los derechos de acceso privilegiado asociados a cada sistema o proceso, así como los usuarios a los que se les está otorgando el acceso. c. Deben asignarse privilegios de acceso alineados a la política de control de acceso basados como requisito mínimo para sus roles y funciones. d. Debe definirse requisitos para la expiración de los derechos de acceso privilegiados. e. Revisar constantemente las cuentas de los usuarios con los accesos privilegiados y si están alineados a sus funciones. f. Debe definirse los privilegios y/o permisos para cada rol en los sistemas de información de Pensión65.
4.8.2.3	**Gestión de la información de autenticación secreta de los usuarios** a. Se verifica la identidad del usuario antes de proporcionarle la información de autenticación secreta nueva, sustitutiva o temporal. b. La entrega de la autenticación temporal debe hacerse en forma segura y única para cada individuo.
4.8.2.4	**Revisión de los derechos de acceso de usuario** a. El Especialista en Infraestructura de la UTI en forma semestral revisa los derechos de los accesos de los usuarios para verificar si están de acuerdo con las solicitudes de altas/bajas/modificaciones. En el caso de usuarios que no debe estar activos o usuarios que se deba actualizar sus accesos, se notifica al jefe de UTI y al Oficial de Seguridad de la Información, o quien haga sus veces, vía correo electrónico y se procede a darles de baja o actualizar.
4.8.2.5	**Eliminación o ajuste de los derechos de acceso** a. Para la baja y cambios de los accesos, los responsables de las Unidades Orgánicas deben informar y solicitar a UTI la cancelación o desactivación de los accesos. b. Los derechos de acceso de todo el personal a información e instalaciones de procesamiento de información deben ser eliminadas como consecuencia de la desvinculación de su empleo, contrato o acuerdo o ser ajustado ante cambios. c. Deben reducirse o eliminarse todos los derechos de acceso a la información y los activos asociados a las instalaciones de procesamiento de información antes de la finalización del empleo o cambio.
4.8.3	**Responsabilidades del Personal** a. Todo el personal es responsable de la confidencialidad de la contraseña asignada, y de las consecuencias por las acciones que terceras personas puedan hacer con el uso de la misma. b. Está prohibido compartir las contraseñas asignadas. c. El personal debe de bloquear su estación de trabajo si por algún motivo se retira de su puesto de trabajo.

4.8.4	**Control de Acceso al Sistema y a las Aplicaciones**
4.8.4.1	**Restricción del acceso a la información** a. El acceso a la información y a las funciones del sistema tienen controles de seguridad (por ejemplo, usuario y contraseña, doble autenticación), a fin de evitar accesos no autorizados a recursos o información, b. Así mismo los derechos de acceso ya sea de lectura, escritura, borrar y ejecutar deben ser controlados, también los datos y aplicaciones que son accedidos por el usuario. c. Dentro de los aspectos que deben ser tomados en consideración para definir los controles, se incluyen: c.1. Procedimiento de inicio de sesión seguros. c.2. Identificación y autenticación de usuarios. c.3. Restricción del uso de herramientas utilitarias del sistema operativo con capacidades de eludir y/o sobrescribir los controles de seguridad. c.4. Se debe cancelar sesiones inactivas luego de un periodo determinado en las aplicaciones críticas y sistemas operativos. c.5. El personal cambia su contraseña de acuerdo a la aplicación y al tiempo de uso de la contraseña. c.6. Las cuentas de usuarios se bloquean al tercer intento del Active Directory. **c.7.** Para activar su cuenta, deben de comunicarse al Especialista en Infraestructura de la UTI.
4.8.4.2	**Procedimientos seguros de inicio de sesión** Se realiza a través de contraseñas fuertes o el uso de multifactor de autenticación para el inicio de sesión.
4.8.4.3	**Lineamiento de Contraseñas seguras** Todas las contraseñas a los recursos de red deben de considerar lo referente a la **POLÍTICA DE CONTRASEÑAS SEGURAS**.
4.8.4.4	**Uso de programas utilitarios privilegiados** a. El uso de programas utilitarios está restringido y se limita el uso solo para usuarios autorizados y debe ser también controlado. b. Todo programa utilitario debe pasar por un proceso de identificación, autenticación y autorización de uso, así como su registro, definición y documentación.
4.8.4.5	**Control de acceso al código fuente del programa** a. El acceso al código fuente de los programas sólo es accesible por los desarrolladores. b. Las bibliotecas de programas fuente se mantendrán en los sistemas en producción para tener un backup de los sistemas por cuestiones de contingencia
4.9	**POLITICA DE CRIPTOGRAFIA (A.10)**
4.9.1	**Controles Criptográficos**
4.9.1.1	**Aplicativos Web** Las aplicaciones web expuestas al público trabajan con un certificado digital para SSL (Secure Sockets Layer), el cual es utilizado para el acceso a los diferentes servicios que forman parte de su plataforma. El certificado digital es un mecanismo que permite autenticar un sitio web en internet de manera que se conserve protegida la información del Programa y sus clientes, puesto que toda comunicación viajará de manera cifrada por la red.
4.9.1.2	**Desarrollo de Aplicaciones** En el desarrollo de aplicaciones, en el caso que se manejen claves criptográficas; estas son distintas para desarrollo y producción, y no se guardan en el repositorio colaborativo. Estas claves criptográficas se utilizan sobre todo para funciones hash de las contraseñas a la hora de almacenarlas en la base de datos.

4.9.1.3	**Transferencia de Información** Como buena práctica de compartir archivos y mantener su integridad con entidades externas, se obtiene el hash del archivo mediante un algoritmo de hasheado seguro y este se remite al destinatario.
4.9.1.4	**Claves de cifrado para ingreso a servicios** Para conectarse a servicios como el SSH (Secure Shell) se pueden utilizan un cifrado asimétrico donde se generan una clave pública y una clave privada. Las claves de cifrado privadas nunca son expuestas o guardadas en algún repositorio colaborativo.
4.9.1.5	**Firmas Digitales** Las firmas digitales utilizan algoritmos seguros de cifrado que son administrados por las autoridades correspondientes.
4.10	**POLITICA DE SEGURIDAD FISICA Y EQUIPOS (A.11)**
	El alcance de la presente política abarca a las instalaciones y equipos que se encuentran dentro del alcance del SGSI. Esta política debe de ser conocida y cumplida por todo el personal y terceros que laboren o tengan relación con la entidad. La Unidad de Administración realiza las gestiones de planeación e implementación. La Unidad de Tecnologías de la información envía las propuestas sobre la seguridad de la información.
4.10.1	**Áreas de Seguridad**
4.10.1.1	**Perímetro de seguridad física** a. Los criterios para determinar un área segura son los detallados a continuación: a.1. Dónde se procesa información a.2. Dónde se almacena información a.3. Dónde se cuenta con información confidencial a.4. La relación de las áreas seguras se encuentra en el **ANEXO 3 - LISTA ÁREAS SEGURAS**. b. En el caso que amerite, el perímetro de seguridad física estará claramente definido. Las especificaciones técnicas de seguridad dependerán del nivel de protección que se requiera implementar. c. Las áreas donde funcionan las instalaciones de procesamiento de información y cualquier otra que sea considerada como crítica y que pudiera afectar el funcionamiento de los sistemas de información son protegidas de accesos no autorizados. d. Las instalaciones de procesamiento de información son físicamente sólidos; los muros, paredes y pisos externos son sólidos y todas las puertas exteriores están protegidas contra accesos no autorizados mediante mecanismos de control.
4.10.1.2	**Controles de acceso físico** a. En los accesos a la Entidad se cuenta con controles que aseguran el acceso físico sólo al personal debidamente autorizado. **b.** Se cuenta con control de acceso biométrico en la puerta de acceso a la oficina.

4.10.1.3	**Seguridad en oficinas, despachos e instalaciones** a. Existen controles de seguridad física, los cuales se mencionan en el **ANEXO 3 - LISTA DE ÁREAS SEGURAS.** b. El personal autorizado (personal y proveedores) no debe facilitar el acceso a las instalaciones a personas desconocidas. c. Las áreas dedicadas al procesamiento de información identificados en el registro de Lista de Áreas Seguras deben ser ubicadas en un lugar que no presente riesgos desde el punto de vista de acceso al público. d. El control de Acceso a los Centros de Datos del Programa se realiza mediante: d.1. Registro de Control de Accesos d.2. Dispositivo Biométrico (Huella) d.3. Cámaras
4.10.1.4	**Protección contra amenazas externas y del ambiente** a. Los equipos se encuentran ubicados y protegidos de tal forma que se reducen los riesgos como resultado de las amenazas y los peligros del medio ambiente, y las oportunidades de acceso no autorizado. b. Los equipos de red y los equipos de comunicaciones (Switch, Router, Access Point) ubicados dentro del Centro de Datos deberán estar conectados a una unidad de alimentación eléctrica por batería UPS (Sistema de Alimentación Ininterrumpida) con autonomía mínimo de media hora.
4.10.1.5	**Trabajo en las áreas seguras** a. Las actividades realizadas en las áreas identificadas como seguras, según **ANEXO 3 - LISTA DE ÁREAS SEGURAS**, deben ser supervisadas por la Unidad de Administración para evitar amenazas. b. No se debe brindar información a personas no autorizadas.
4.10.2	**Equipos**
4.10.2.1	**Ubicación y protección del equipamiento** a. Los equipos se encuentran ubicados y protegidos de tal forma que se reduzcan los riesgos como resultado de las amenazas y los peligros del medio ambiente, y las oportunidades de acceso no autorizado. b. Está completamente prohibido Fumar en las instalaciones del Programa. c. La computadora personal es de uso exclusivo para el usuario del Programa, para el desarrollo de sus actividades y fines organizacionales, siendo responsable de su buen uso. d. El personal debe respetar y no modificar por ningún motivo la configuración de hardware y software establecida por el área de soporte técnico de la UTI. e. El personal está prohibido de abrir los equipos de cómputo o dispositivos informáticos excepto el personal especializado de soporte técnico de la UTI. f. Las computadoras personales del Programa no deben ser alterados (cambios de procesador, adición de memoria o tarjetas) ni movidos de su punto de red a otro sin el consentimiento, evaluación técnica y autorización del área responsable.
4.10.2.2	**Seguridad en el cableado** a. El cableado de energía o de telecomunicaciones se encuentra protegido de cualquier intercepción o daño. b. El cableado de suministro de energía eléctrica y telecomunicaciones en las zonas de tratamiento de información cuenta con un sistema de puesta a tierra (pozo a tierra), el que es revisado anualmente para garantizar su adecuado funcionamiento. c. La UTI debe garantizar que el cableado estructurado cumpla con las normas internacionales aprobadas por la TIA-EIA (Asociación de Industrias de Telecomunicaciones y Asociación de Industrias Electrónicas) u otra organización reconocida.

4.10.2.3	**Mantenimiento de equipos** a. El mantenimiento de los equipos se realizará de acuerdo con lo establecido en el Procedimiento **PR-GTEC-02 MANTENIMIENTO DE EQUIPOS.**
4.10.2.4	**Retiro de activos de información** a. Los equipos informáticos (PC´s, Laptops, Discos externos, etc.) y Software son propiedad del Programa, por lo que, para el retiro de dichos equipos, software y/o información, se debe contar con la autorización expresa correspondiente. b. Una vez que se tenga la autorización, se debe de registrar la salida del activo de información según **DIRECTIVA PARA LA ADMINISTRACIÓN, ASIGNACIÓN, USO Y CONTROL DE LOS BIENES MUEBLES, PATRIMONIALES PARA EL PROGRAMA NACIONAL PENSION 65.**
4.10.2.5	**Seguridad de equipos fuera del local** a. El uso de equipos fuera de sus instalaciones debe ser autorizado de manera expresa por los Jefes utilizando la **DIRECTIVA PARA LA ADMINISTRACIÓN, ASIGNACIÓN, USO Y CONTROL DE LOS BIENES MUEBLES, PATRIMONIALES PARA EL PROGRAMA NACIONAL PENSION 65**, asimismo, el personal autorizado será responsable de su custodia.
4.10.2.6	**Disposición o reutilización segura de equipos** a. Se deben de verificar todos los equipos para asegurar que cualquier dato sensible y software con licencia se haya eliminado antes de su reutilización o cuando se disponga a eliminarse, para lo cual se debe de realizar de acuerdo con el procedimiento Borrado Seguro y Eliminación de Medios de la **DIRECTIVA PARA LA ADMINISTRACIÓN, ASIGNACIÓN, USO Y CONTROL DE LOS BIENES MUEBLES, PATRIMONIALES PARA EL PROGRAMA NACIONAL PENSION 65.**
4.10.2.7	**Equipo desatendido por el usuario y Pantalla y escritorios limpios** a. Se cuenta con la Política de Pantallas y Escritorios Limpios**,** en donde se dan los lineamientos para la protección de la información. En caso de incumplimiento se reporta como incidente de seguridad.
4.11	**POLITICA DE ESCRITORIOS Y PANTALLAS LIMPIAS (A.11.2.9)**
	Esta política se aplica a la protección de cualquier tipo de información, en cualquiera de sus formas y que pueden estar contenidas en escritorios, estaciones de trabajo, computadores portátiles, medios ópticos, medios magnéticos, documentos en papel y en general cualquier tipo de información que es utilizada por los directivos, todo el personal y terceros.
4.11.1	**Ubicación de escritorios y equipos** a. Los lugares de trabajo de los usuarios deben localizarse preferentemente en ubicaciones que no queden expuestas al acceso de personas externas. De esta forma se protege tanto el equipamiento tecnológico como los documentos que pudiera estar utilizando el usuario. b. Los equipos que queden ubicados cerca de zonas de atención o tránsito de público deben situarse de forma que las pantallas no puedan ser visualizados por personas externas.
4.11.2	**Equipos Desatendidos** a. Toda vez que un usuario se ausenta de su lugar de trabajo debe de bloquear su estación de trabajo, así estas tengan instaladas protectores de pantalla. b. En el caso que no lo realice el usuario, el equipo debe de bloquearse a los 10 minutos.

4.11.3	**Escritorios Limpios** a. Toda vez que un usuario se ausenta de su lugar de trabajo debe guardar en lugar seguro cualquier documento, medio magnético u óptico removible que contenga información. b. Al finalizar la jornada de trabajo, el usuario debe guardar en un lugar seguro los documentos y medios que contengan información de **USO INTERNO**. c. La información confidencial o sensible, cuando se imprima se debe retirar inmediatamente de las impresoras.
4.11.4	**Pantallas Limpias** a. Las estaciones de trabajo y equipos portátiles tienen bloqueo automático en un lapso de 10 minutos. b. La pantalla de autenticación a la red debe requerir solamente la identificación de la cuenta y una clave y no entregar otra información. **c.** Toda vez que el usuario se ausente de su lugar de trabajo debe bloquear su estación de trabajo o laptop de forma de proteger el acceso a las aplicaciones y servicios del Programa.
4.12	**POLITICA DE SEGURIDAD DE LAS OPERACIONES (A.12)**
	La presente política tiene como fin garantizar la operación correcta y segura en las instalaciones de procesamiento de información del Programa, minimizar el riesgo de fallos de los sistemas, proteger la integridad de software y de la información y monitorear las actividades de procesamiento de información para detectar acciones no autorizadas.
4.12.1	**Procedimientos y Responsabilidades Operacionales**
4.12.1.1	**Procedimientos documentados de operación** Los procedimientos documentados de la operación de la seguridad de la información están definidos en la **MATRIZ DE DOCUMENTOS NORMATIVOS DEL PROGRAMA PENSION 65** del procedimiento **PR-GCAL-01-05 Control de Documentos y Registros del SGI.**

4.12.1.2	**Gestión de Cambios** a. Todo cambio en los procesos, sistemas o instalaciones de procesamiento de la información que afecten a la seguridad de la información son registrado en el **ANEXO 2 - REGISTRO DE CAMBIOS**. b. Los cambios que están relacionados a tecnología se registran en dicho anexo, y se deberá de considerar lo siguiente: b.1. En el caso de instalación de actualizaciones de software para Servidores y Estaciones de Trabajo: i) Todas las actualizaciones de Windows Update se deben realizar fuera del horario de oficina. ii) Las actualizaciones del sistema operativo del servidor se descargan en forma manual y mediante configuración las actualizaciones se realizan fuera del horario de oficina. De igual forma las actualizaciones de la base de datos. iii) Las actualizaciones de los sistemas se realizan dentro del horario de trabajo del personal. b.2. En el caso de cambios en las Configuraciones de los Equipos de Comunicación: i) Para realizar cambios en las configuraciones de los equipos de comunicación router o switches, se programan para realizarlos fuera del horario de trabajo a fin de no afectar los servicios de la red. ii) En caso de una actualización del firmware se evaluará las mejoras en la seguridad o performance del equipo antes de proceder a su aplicación, considerándose en todos los casos el realizar una copia de seguridad de todas las configuraciones aplicadas al equipo como paso previo. c. En el caso de cambios en Configuraciones de Equipos de Seguridad c.1. El Especialista en Infraestructura de la UTI es responsable de la administración y monitoreo de las soluciones de seguridad basadas en hardware y/o software respectivamente. c.2. El Especialista en Infraestructura de la UTI debe de revisar periódicamente las actualizaciones de seguridad que los fabricantes de hardware y/o software publican a fin de evaluar y programar su instalación. c.3. Se debe de coordinar con el Especialista en Infraestructura de la UTI la fecha y hora para que todo cambio se realice sin que afecte a los servicios. c.4. Realizado el cambio a cargo del Especialista en Infraestructura de la UTI, le enviará un correo electrónico al Oficial de Seguridad de la Información, o a quien haga sus veces, indicando que se ejecutó el cambio correctamente. d. Los cambios que no están relacionados a tecnología se registran en la hoja registro de cambios de los documentos normativos.
4.12.1.3	**Gestión de la Capacidad** Se supervisa el uso de los recursos de los servidores y se hacen proyecciones de los futuros requisitos de capacidad tecnológica para asegurar el desempeño requerido de los sistemas de información, para lo cual se debe de realizar los siguiente: a. Se identifican los requerimientos de capacidad teniendo en cuenta la criticidad del sistema para del Programa. b. Se realizan proyecciones de los nuevos requisitos del negocio y del sistema para el aprovisionamiento de recursos. c. Se revisan y desinstalan aplicaciones, sistemas, bases de datos o entornos obsoletos. d. Se asegura, mediante las revisiones periódicas, el ancho de banda para servicios de alta demanda de recursos en caso sea críticos para la Entidad.

4.12.1.4	**Separación de los ambientes de Desarrollo, Pruebas y Producción** a. Los ambientes de Desarrollo y Producción cuentan con el nivel de separación necesario para prevenir problemas operacionales, así como los controles de acceso adecuados para cada uno de ellos. b. El acceso a los ambientes de Desarrollo está restringido exclusivamente a personal de Desarrollo del Programa. c. El personal de la UTI es responsable de la administración, mantenimiento, operatividad continua, seguridad y rendimiento aceptable de los ambientes de Desarrollo y Producción. d. Las pruebas se realizan utilizando datos de prueba. En los casos en los que no se pueda recrear los datos de prueba y la Entidad así lo requiera, la copia de datos de producción puede ser usada para las pruebas siempre y cuando el uso de ésta sea autorizado y analizado por el propietario del activo de información relacionado y previamente tratada para el resguardo de los datos.
4.12.2	**Controles de software malicioso** a. Las aplicaciones de terceros utilizado por la Entidad deben ser autorizado por el Especialista en Infraestructura de la UTI. b. Para reducir la presencia de códigos maliciosos (virus, gusanos, troyanos, spyware, entre otros) en los sistemas de información y los medios de procesamiento, el sistema de antivirus debe encontrarse habilitado en los equipos del Programa, así como en los equipos de personal de terceros o visitas que requieran ingresar a la red del Programa. c. El sistema de antivirus debe contar con una actualización diaria y configurada para realizar revisiones programadas para la detección de virus en los equipos del Programa. d. El Especialista en Infraestructura de la UTI es responsable de instalar, configurar, monitorear y controlar el sistema de antivirus en las estaciones de trabajo. **e.** Todo incidente de infección de virus informático debe ser reportado inmediatamente según la **POLÍTICA DE INCIDENTES.**
4.12.3	**Respaldo de Información** a. Los usuarios que tienen asignada una computadora son responsables de realizar la copia de la información en las carpetas compartidas. b. El respaldo y las pruebas de recuperación de la información de bases de datos, File Server y Aplicativos Institucionales se realizan de acuerdo con el procedimiento **PR-GTEC-01 RESPALDO DE LA INFORMACIÓN.**
4.12.4	**Registro de Eventos** a. Los tipos de eventos de advertencias y errores generados por el servidor son registrados y son monitoreados según el procedimiento **PR- GTEC-07 MONITORIZACIÓN DE SERVIDORES Y SERVICIOS DE TECNOLOGÍAS DE LA INFORMACIÓN**. b. Se monitorea el uso de aplicaciones del sistema, tipo de acceso; direcciones y protocolos de red; alarmas configuradas por el sistema de monitoreo; activación y desactivación de los sistemas de protección, tales como sistemas de antivirus y registros de las transacciones realizadas por los usuarios en las aplicaciones. c. Los eventos cuando tengan impactos a los servicios brindados, se les deberán de registrar como incidentes de seguridad y seguir el instructivo establecido.

4.12.5	**Protección de información de Registros (eventos)** a. Los registros de eventos (log) se protegen contra alteración, eliminación y/o accesos no autorizados a los registros de eventos (logs). Para ello se cuentan con controles de acceso a los repositorios. b. Los logs tal como los otros recursos cuentan con políticas de accesos, de acuerdo con ellos solo pueden acceder a los usuarios privilegiados, estos logs no pueden ser modificados por usuarios no privilegiados.
4.12.6	**Registro de los usuarios administrador** Todas las actividades de los usuarios super administrador son registradas y esos registros son protegidos, además se menciona que los logs son almacenados en los servidores y equipos; así mismo se revisan regularmente para mantener la responsabilidad de los usuarios privilegiados. Esta información queda almacenada en el Log de Auditoría del sistema.
4.12.7	**Sincronización de relojes** Todos los equipos de la red se conectan al servicio NTP para su sincronización de actualización de los relojes y se verifica con la hora oficial peruana de la Marina de Guerra del Perú.
4.12.8	**Instalación de software en los sistemas operativos** a. Se revisa periódicamente el software instalado y las licencias que se han adquirido para asegurar que solo Software legal y aprobado se está utilizando. b. Se mantiene un registro de software permitido en el **ANEXO 4 - LISTA DE SOFTWARE PERMITIDO**: b.1. Se debe estar familiarizado con la Ley de derechos de autor, a fin de comprender las consecuencias de su incumplimiento, incluyendo las sanciones y responsabilidades por daños y perjuicios. b.2. Se debe mantener actualizada la lista de software permitido. b.3. Se debe desinstalar todo el software sin licencia o cualquier software que no aparezca en la lista de software aprobado y compatible. Así mismo desinstalar el software que ya no se usa en los equipos. b.4. Exigir que el software se adquiera a través de un proceso de compra formal para asegurar que se obtienen las aprobaciones adecuadas, y que los registros de compra, recepción, e inventario son creados y mantenidos.
4.12.9	**Gestión de Vulnerabilidades técnicas** a. Se debe realizar una vez al año un análisis de vulnerabilidades técnicas de los sistemas de información en uso y de la infraestructura tecnológica. b. Los hallazgos y recomendaciones de esta revisión deben ser analizadas e implementadas, de ser el caso. c. El Especialista en Infraestructura de la UTI es el encargado de ejecutar el análisis o escaneo de la red informática, así como la auditoría de seguridad de la red, actualizaciones de los sistemas operativos y análisis de vulnerabilidad mediante software especializado, como también reportará al director de la UTI sobre el estado de la red informática del Programa.
4.12.10	**Restricciones en la instalación de software por usuarios** a. Los usuarios no cuentan con acceso para instalar aplicativos en sus equipos, el Especialista en Infraestructura de la UTI es el encargado de realizar las instalaciones. b. El Especialista en Infraestructura de la UTI se asegura que el software que se va a instalar se encuentre registrado en el **ANEXO 4 - LISTA DE SOFTWARE PERMITIDO.**

4.12.11	**Controles de auditoría de sistemas de información** a. Se debe planificar y acordar los requisitos y las actividades de auditoría que implican la verificación de los sistemas operativos para minimizar las interrupciones en los procesos del Programa. b. Se debe controlar el alcance de las verificaciones, estas deben limitarse a accesos de sólo lectura al software y a los datos; en caso de que las verificaciones afecten la disponibilidad del sistema deben realizarse fuera de horario de oficina. c. Todo acceso a los sistemas debe ser supervisado y registrado para poder realizar revisiones posteriores. d. Se establecen en el **PROGRAMA DE AUDITORÍAS INTERNAS.**
4.13	**POLITICA DE SEGURIDAD DE LAS COMUNICACIONES (A.13)**
	La presente política tiene como fin asegurar la protección de la información en las redes y los recursos de tratamiento de la información y mantener la seguridad en la información que se transfiere dentro de una organización y con cualquier y entidad externa.
4.13.1	**Gestión de la seguridad de Red**
4.13.1.1	**Controles de red** a. Todos los servidores de red que están conectados a la red informática son de acceso restringido solo al personal técnico especializado de la UTI. b. Los incidentes de seguridad detectados en los ambientes gestionados son notificados según **PR-GTEC-03 PROCEDIMIENTO DE ATENCIÓN DE INCIDENCIAS** para las acciones respectivas. c. El Especialista en Infraestructura de la UTI debe administrar, monitorear, controlar las redes de cómputo, garantizar la seguridad de la información en la red y proteger los servicios conectados a la red. Así mismo, es responsable de la configuración de la red cableada e inalámbrica y garantizar la disponibilidad de los servicios a su cargo.
4.13.1.2	**Seguridad de los Servicios de Red** a. La seguridad en los servicios de las redes es administrada y gestiona por el Especialista en Infraestructura de la UTI. b. Los equipos de comunicaciones cumplen los requisitos mínimos de seguridad establecidos. c. Los usuarios de red cuentan con el Active Directory instalado en el servidor interno para separar los archivos compartidos entre los usuarios.
4.13.1.3	**Segregación de Redes** La red interna debe estar segregada, para ello se tiene habilitado: a. LAN de Pensión 65 (Internet) b. LAN de Usuarios (Internet) c. LAN de Teléfonos d. LAN de Wifi e. LAN DMZ (Zona Desmilitarizada) f. LAN de Servidores g. Entre otras.
4.13.2	**Transferencia de Información**

4.13.2.1	**Políticas y procedimientos de transferencia de información** La entidad ha establecido controles internos para asegurarse que la información transmitida dentro del Programa está protegida, para lo cual se cuentan con lineamientos de responsabilidades de los usuarios, controles de accesos, lineamientos de uso aceptable de activos de información, además de contar con antivirus actualizado para prevenir software malicioso. En el caso que se realice un intercambio de información con cualquier entidad externa, se debe mantener la seguridad en el intercambio de información. a. Para el envío de información: a.1. Los intercambios de información deben realizarse utilizando el protocolo SFTP y una clave que se le asignara previa petición. a.2. Adicionalmente, se utiliza el algoritmo MD5 y SHA1 para identificar de forma única a los documentos remitidos a las entidades. a.3. Se remitirán los oficios firmados por la dirección ejecutiva siguiendo el **ANEXO 6 - FORMATO PARA EL ENVÍO DE DOCUMENTACIÓN A UNA ENTIDAD EXTERNA**. b. Para la recepción de información: b.1. Las entidades responden mediante un oficio por mesa de partes indicando el enlace de descarga o la forma descargar del archivo solicitado. b.2. Todos los archivos externos deberán ser revisados previa a su apertura: i) Evaluar su procedencia y si el remitente es desconocido ii) Evaluar la extensión del archivo, a fin de que no sea un archivo ejecutable iii) Preferiblemente pasarlo por un software antivirus o antimalware
4.13.2.2	**Acuerdos de transferencia de información** El intercambio de información por parte de las entidades públicas se encuentra normado a través del DL 1211 Decreto legislativo que aprueba medidas para el fortalecimiento e implementación de servicios públicos integrados a través de ventanillas únicas e intercambio de Información entre entidades públicas. Asimismo, se celebran convenios con entidades establecido en la **DI-GUPPO-01 DIRECTIVA PARA LA GESTIÓN DE CONVENIOS DE COOPERACIÓN INTERINSTITUCIONAL PARA EL PROGRAMA DE ASISTENCIA SOLIDARIA PENSIÓN 65 Y LOS ORGANISMOS PÚBLICOS O PRIVADOS, NACIONALES O EXTRANJEROS**. Con ello, ambas organizaciones se rigen bajo los acuerdos de confidencialidad y no divulgación de la información establecidos.
4.13.2.3	**Mensajería electrónica** Se aborda en el 3.20 **POLÍTICA DE CORREO ELECTRÓNICO**.
4.13.2.4	**Acuerdos de confidencialidad o no divulgación** a. Todo el personal y proveedores externos (que aplique) cuentan con acuerdos de confidencialidad o no-divulgación los cuales detallan los aspectos de seguridad que deben de cumplir, estos lineamientos se encuentran en el documento Acuerdo de Confidencialidad. b. Las obligaciones de confidencialidad inician una vez firmado el acuerdo de confidencialidad, sobreviviendo después del cese de labores y extendiéndose de manera permanente. **c.** Los acuerdos de confidencialidad y/o no divulgación se revisan anualmente o cuando se requiera para verificar que los requisitos de seguridad son los adecuados o pertinentes de acuerdo a la necesidad del Programa.
4.14	**POLITICA DE ADQUISICION, DESARROLLO Y MANTENIMIENTO DE SISTEMAS (A.14)**

	La presente política tiene como fin garantizar que la seguridad de la información sea parte integral de los sistemas de información en todo el ciclo de vida. Incluyendo los requisitos para los sistemas de información que proporcionan los servicios a través de redes públicas.
4.14.1	**Requisitos de Seguridad de los Sistemas de Información**
4.14.1.1	**Análisis y Especificación de los Requisitos de Seguridad de la Información** La entidad cuenta con la directiva **DI-GTEC-03 CICLO DE VIDA DEL SOFTWARE DEL PROGRAMA NACIONAL DE ASISTENCIA SOLIDARIA PENSIÓN 65**, en este se establecen las actividades del ciclo de desarrollo de software. a. Para todos los sistemas desarrollados, se determinan (si aplica) los requerimientos de seguridad de información antes de comenzar la fase de desarrollo de la aplicación, con el fin de evitar o minimizar fallas de seguridad en los sistemas de información a desarrollar. b. El Líder del Proyecto es quien valida si se cumplen con los requerimientos de seguridad establecidos. Estos requisitos de seguridad se deben de establecer desde el requerimiento del usuario, o en todo caso, el Líder del Proyecto proporciona lineamientos básicos de seguridad. c. Estos requerimientos deben ser incorporados en cada fase del ciclo de desarrollo como son: Análisis de Requerimientos, Diseño, Desarrollo, Pruebas e Implantación.
4.14.1.2	**Aseguramiento de los Servicios de Aplicación en las Redes Públicas** La información involucrada en los servicios de aplicación que pasan a través de redes públicas es protegida de acuerdo con los requisitos de seguridad definidos en el punto anterior.
4.14.1.3	**Protección de las Transacciones de los Servicios de Aplicación** La información implicada en las transacciones de los servicios de aplicación se protege para prevenir la transmisión incompleta, la omisión de envío, la alteración del mensaje, la divulgación, la duplicación o repetición del mensaje no autorizados. Esta protección se detalla en el análisis que realizan por cada desarrollo.
4.14.2	**Seguridad en los Procesos de Desarrollo y Soporte**
4.14.2.1	**Política de Desarrollo Seguro** Se cuenta con una política de desarrollo seguro e ingeniería de software, la cual se detalla en la **POLÍTICA DE DESARROLLO SEGURO**. La política de desarrollo seguro está basada en los siguientes principios: a. A partir de un mínimo modelo de permisos y luego ir escalando privilegios; b. Limpiar la codificación de pruebas o comentarios; c. Nunca confiar en los datos que se ingresa en la aplicación; d. Hacer seguimiento de las versiones y tecnologías usadas ya que estás van evolucionando o se vuelven obsoletas; e. Las claves pasan por un proceso de encriptación; f. Los cambios que se soliciten deben pasar por un proceso de evaluación y deben ser documentados, g. Colocar puntos de control y auditoria en los puntos más críticos o vulnerables.
4.14.2.2	**Procedimiento de Control de Cambio del Sistema** a. Se ha determinado que se realiza el versionamiento de software con herramientas de versionado como GIT, Mercurial (TortoiseHg). Esta actividad permite gestionar y controlar los cambios realizados que finalmente modifican el ambiente productivo siendo un requerimiento fundamental para realizar dichas modificaciones. b. Se deben realizar las revisiones de la funcionalidad con respecto a seguridad de la información en la fase de pruebas.

4.14.2.3	**Revisión Técnica de Aplicaciones después de Cambios en la Plataforma Operativa** a. Se debe verificar y garantizar que los cambios realizados en los sistemas operativos no tengan un impacto adverso en las actividades y operaciones críticas del Programa. b. Se deben realizar pruebas con la finalidad de evidenciar posibles inconvenientes, con la finalidad de evidenciar el cumplimiento de los requisitos de seguridad de la información solicitados y determinar si estos cumplen con los criterios de aceptación definidos en la etapa de análisis. c. En caso las funcionalidades no satisfagan los requerimientos mínimos de seguridad, el Líder de Proyectos o quien haga a sus veces, debe emitir un informe que especifique las deficiencias de seguridad encontradas y recomendar los controles compensatorios en caso fuesen identificados, para que éstas sean aprobadas por la UTI aceptando los riesgos encontrados.
4.14.2.4	**Restricciones en Cambios a Paquetes de Software** Las modificaciones a paquetes de software deben limitarse solo a cambios necesarios y todos los cambios deberían ser estrictamente controlados. La UTI debe considerar el impacto ocasionado, ya que se hace responsable por el mantenimiento del software como consecuencia de los cambios.
4.14.2.5	**Principios de la Ingeniería de Sistemas Seguros** Se han establecido los principios de ingeniería de sistemas seguros, los cuales se encuentran en la **POLÍTICA DE DESARROLLO SEGURO**.
4.14.2.6	**Entorno de Desarrollo Seguro** Se ha determinado un ambiente seguro de Desarrollo; solo las personas autorizadas podrán tener acceso a dicho ambiente, de acuerdo con las funciones o actividades asignadas.
4.14.2.7	**Desarrollo contratado Externamente** La UTI supervisa y realiza el seguimiento de las actividades de desarrollo de sistemas subcontratados, considerando: a. El acuerdo de licencias, la propiedad del código y los derechos de propiedad intelectual relacionado con el contenido de terceros. b. Los requisitos contractuales para el diseño, la codificación y las pruebas seguras. c. Las pruebas de aceptación para la calidad y precisión de los entregables. d. La presentación de pruebas de que se probaron los requisitos de seguridad para establecer los niveles mínimos aceptables de seguridad y calidad.
4.14.2.8	**Pruebas de Seguridad de Sistemas y Pruebas de Aceptación de Sistemas** Se realizan pruebas para validar el cumplimiento de los requerimientos establecidos por la necesidad del usuario. El responsable de las pruebas debe revisar el cumplimiento de los requisitos mínimos de seguridad establecidos en el análisis del requerimiento.
4.14.3	**Datos de Prueba**

4.14.3.1	**Protección de los Datos de Prueba** a. Se tiene establecido el uso de mecanismos de protección de datos para el caso en que se requiera migrar datos del ambiente de producción hacia el ambiente de desarrollo, con la finalidad de utilizarlos en las diversas etapas de los proyectos. b. Esta actividad se realiza a demanda y para ello el responsable del proyecto deberá solicitar autorización al Administrador de Base de Datos o quien haga a sus veces, registrando la solicitud que deberá contener como mínimo el nombre y cargo del solicitante, fecha, nombre del sistema, descripción de información requerida y motivo, autorizaciones correspondientes para la extracción de la información especificada.
4.15	**POLITICA DE DESARROLLO SEGURO (A.14.2.1)**
	La presente política tiene como fin garantizar que los desarrollos de las aplicaciones cuenten con lineamientos de ingeniería de software para el desarrollo seguro. Es política de Pensión 65 ejecutar los proyectos de desarrollo y mantenimiento de aplicaciones en base a un proceso de ingeniería definido que considere los siguientes lineamientos:
4.15.1	Se asegura el entorno de desarrollo considerando que sólo los miembros del equipo de desarrollo son los únicos que tienen acceso al mismo.
4.15.2	Se considera la implementación de ambientes de desarrollo, pruebas y producción de manera separada para las aplicaciones.
4.15.3	El ciclo de vida de desarrollo de software está determinado en el procedimiento Ciclo de Vida del Software.
4.15.4	Se recolectan las necesidades del usuario para desarrollar sus requerimientos y priorizarlos; se establece los requerimientos del producto, se identifican las interfaces tempranamente.
4.15.5	Los requerimientos se analizan y validan para asegurar que son necesarios; balanceando restricciones frente a necesidades; y asegurando que el producto funcionará en el ambiente de producción.
4.15.6	El diseño del producto debe incluir el diseño de las interfaces, así como un análisis de lo que debe desarrollarse, comprarse o reusarse. Los manuales deben incluir la documentación de uso final que brinde soporte al mismo.
4.15.7	La integración de los componentes del producto se debe realizar definiendo y siguiendo el procedimiento establecido. Las compatibilidades de las interfaces deben ser aseguradas y el producto integrado evaluado antes de su entrega.
4.15.8	Se verifica el producto con la finalidad de asegurar que satisface los requerimientos especificados, para lo cual se deben seleccionar los productos a verificar, establecer el ambiente donde el producto será verificado y realizar la verificación, siguiendo procedimientos y criterios establecidos. Los resultados de la verificación deben ser analizados.
4.15.9	Se verifica el producto con la finalidad de asegurar que satisface los requerimientos especificados, para lo cual se deben seleccionar los productos a verificar, establecer el ambiente donde el producto será verificado y realizar la verificación, siguiendo procedimientos y criterios establecidos. Los resultados de la verificación deben ser analizados.
4.15.10	Se valida el producto con la finalidad de demostrar que funciona bien en el ambiente de producción, para el cual ha sido planeado. Involucra la selección de productos a validar, establecer el ambiente de validación y realizar la validación siguiendo procedimientos y criterios establecidos. Los resultados de la validación deben ser analizados. La validación del producto debe ser realizada por el usuario o sus representantes formalmente autorizados.
4.15.11	Los programas fuentes se almacenan en repositorios seguros en los servidores del Programa. De esta manera se controlan las versiones de los sistemas.
4.15.12	Los Sistemas que sean utilizados en Pensión 65 deberán cumplir con los siguientes requisitos mínimos de seguridad: a. Los usuarios deben desconectar de la aplicación a los 15 minutos de inactividad. b. La base de datos utilizada debe contar con un programa de backup full e incremental. c. Los desarrolladores deberán firmar un acuerdo de confidencialidad. d. Otras que la UTI solicite.

4.15.13	Se utilizan técnicas de programación segura para los desarrollos, estas comprenden aspectos como: a. Las aplicaciones exigen a los usuarios que utilicen contraseñas seguras, no se ofrece una "forma alternativa" de ingreso a la aplicación (backdoor). b. Reutilizar componentes en los cuales confiamos, se han utilizado anteriormente sin problemas.
4.15.14	**Seguridad por defecto.** Cuando una aplicación se despliega en su entorno de producción, utiliza una serie de opciones de configuración que se establecen por defecto. Estas opciones por defecto deben ser tales que la aplicación sea segur, por defecto una aplicación debería tener habilitada la expiración de contraseñas y una política de complejidad de claves adecuada.
4.15.15	**Ejecución con los mínimos privilegios.** El principio de mínimos privilegios establece que las cuentas deben tener el menor nivel de privilegios posible para realizar las tareas de negocio. Este nivel de privilegios abarca tanto permisos de usuarios como permisos sobre recursos como CPU, memoria, red, sistema de ficheros, etc.
4.15.16	**Defensa en profundidad.** Una aplicación deberá implementar a distintas medidas en varias capas para prevenir inyecciones SQL.
4.15.17	**Detección de intrusos.** La detección de intrusiones requiere la existencia de tres elementos: a. Capacidad para incluir en el log eventos relevantes de seguridad. b. Procedimientos que aseguren que los logs son monitorizados con regularidad. c. Procedimientos para responder adecuadamente a una intrusión una vez ha sido detectada.
4.15.18	Toda la información de seguridad relevante debe ser registrada en un log (registro de información de un sistema).
4.15.19	**Evitar la seguridad por ocultación** La seguridad por ocultación es un mecanismo de seguridad débil y generalmente falla cuando es el único control existente. La seguridad de un sistema nunca debe recaer en la ocultación de secretos -no puede depender de mantener en secreto el código fuente.
4.15.20	**Solucionar correctamente los problemas de seguridad.** Una vez que se ha detectado un problema de seguridad, es fundamental desarrollar pruebas para reproducirlo y detectar la causa raíz. Una vez que se desarrolla una solución válida es clave garantizar que no se introducen problemas de regresión.
4.15.21	Se considera la ejecución de pruebas de seguridad o análisis de vulnerabilidad como: a. Análisis Estático del Código Fuente de la Aplicación b. Análisis Dinámica del funcionamiento de la aplicación
4.16	**POLITICA DE SEGURIDAD CON PROVEEDORES (A.15)**
	Esta política tiene como finalidad garantizar la protección de los activos de información del Programa que son accesibles por los proveedores. Por lo que se define los siguientes aspectos:
4.16.1	Todo proveedor que presta servicios a la Entidad deberá firmar el documento **ANEXO 8 - LINEAMIENTOS DE SEGURIDAD DE LA INFORMACIÓN PARA LOS PROVEEDORES**.
4.16.2	Todo proveedor debe firmar un **ACUERDO DE CONFIDENCIALIDAD**.
4.16.3	Los proveedores sólo podrán desarrollar para la Entidad, aquellas actividades cubiertas bajo el correspondiente contrato u Orden de Servicio.
4.16.4	El proveedor proporcionará los datos completos de la persona de contacto, quien será el encargado de recibir todo tipo de directivas de seguridad de la información. El proveedor proporcionará la relación de personas, perfiles, funciones y responsabilidades asociadas al servicio provisto, e informará puntualmente de cualquier cambio (alta, baja, sustitución o cambio de funciones o responsabilidades) que se produzca en dicha relación.

4.16.5	Todo proveedor deberá velar porque su personal que presta los servicios directamente a la Entidad cumpla con las políticas de seguridad de la información recogidas en el presente documento. En caso de incumplimiento, la Entidad se reserva el derecho de solicitar al proveedor el cambio de personal, sin perjuicio del derecho del Programa de resolver el contrato de prestación de servicios en los términos establecidos en el contrato.
4.16.6	El proveedor deberá garantizar que todo su personal que realiza servicios para la Entidad cuente con formación y capacitación apropiada para el desarrollo del servicio contratado, tanto a nivel específico en las materias correspondiente a la actividad asociada, como de manera transversal en materia de seguridad de la información.
4.16.7	Cualquier tipo de intercambio de información que se produzca entre la Entidad y el proveedor se entenderá que ha sido realizado dentro del marco establecido por el contrato, de modo que dicha información tendrá el carácter de confidencial y no podrá ser utilizada en ningún caso fuera de dicho marco, ni para fines diferentes a los asociados al contrato.
4.16.8	La Entidad podrá realizar auditorías para verificar que el proveedor cumple con los requisitos de seguridad establecidos.
4.16.9	Se les proporciona los accesos a los proveedores (Solicitud/modificación), los cuales deben revisarse de manera frecuente ante cambios o baja del servicio.
4.17	**POLITICA DE GESTION DE INCIDENTES (A.16)**
	La presenta política tiene como fin garantizar un enfoque consistente y eficaz para la gestión de incidentes de seguridad de la información, incluyendo la comunicación de eventos de seguridad y debilidades de la información.
4.17.1	**Responsabilidades y procedimientos** La Entidad cuenta con los procedimientos: **a. PR-GTEC-03 ATENCIÓN DE INCIDENCIAS** b. **PL-GTEC-02 PLAN DE CONTINGENCIA INFORMÁTICO** **c. PR-GCAL-07 MEJORA CONTINUA DEL SGI** Los cuales brindan los lineamientos y responsabilidades de la gestión de incidentes.
4.17.2	**Reporte de eventos y debilidades de seguridad de la información** Todos los usuarios deben comunicar las debilidades, eventos o incidentes a UTI mediante los canales establecidos **(APLICATIVO WEB GLPI).** En el caso de usuarios externos deben seguir la **POLITICA DE SEGURIDAD CON PROVEEDORES** informando oportunamente.
4.17.3	**Evaluación, decisión y respuesta sobre los eventos de seguridad de información** Los eventos de seguridad dependiendo de su nivel de impacto se clasifican en 02: a. Incidentes Menores: Son atendidos siguiendo el procedimiento **PR-GTEC-03 ATENCIÓN DE INCIDENCIAS** b. Incidentes Graves: Son atendidos siguiendo el **PL-GTEC-02 PLAN DE CONTINGENCIA INFORMÁTICO** Se cuenta con un equipo de respuestas ante incidentes de seguridad digital en cumplimiento de la Resolución Ministerial N°360-2009-PCM y del Decreto de Urgencia N°007-2020, Decreto supremo Nº 029-2021- PCM.
4.17.4	**Aprender de los incidentes de seguridad de la información** En caso aplique se podrá aplicar **PR-GCAL-07 MEJORA CONTINUA DEL SGI** mejorar los procesos en base a incidentes ya presentados y así para poder solucionar futuros incidentes en base a las acciones ya realizadas.
4.17.5	**Recolección de evidencia** Los distintos procedimientos mencionados han definido acciones para la identificación, recolección y conservación de la información que puede servir como evidencia para propósitos de acción disciplinaria y legal.
4.18	**POLITICA DE SEGURIDAD EN LA CONTINUIDAD DE NEGOCIO (A.17)**
	La presente política tiene como fin establecer los lineamientos para la Gestión de los Aspectos de Seguridad de la Información para la Continuidad del Negocio del Programa.
4.18.1	Se ha considerado a los procesos de tecnologías de la Información como procesos críticos.

4.18.2	Se ha definido que los tiempos objetivos de recuperación de los procesos críticos de tecnologías de la información se encuentran detallados en el **PL-GTEC-01 PLAN DE CONTINUIDAD OPERATIVA** del Programa.
4.18.3	La entidad cuenta con un **PL-GTEC-02 PLAN DE CONTINGENCIA INFORMÁTICO** en donde se han identificado los distintos eventos de seguridad de la información.
4.18.4	La UTI ha determinado que los actuales controles de seguridad de la información implementados son los mismos que se deben de considerar en el **PL-GTEC-02 PLAN DE CONTINGENCIA INFORMÁTICO**.
4.18.5	El Oficial de Seguridad debe supervisar el cumplimiento de los controles de seguridad en el proceso de Contingencia.
4.18.6	Se ha definido el documento Pruebas del Plan de Contingencia Informático, para garantizar la disponibilidad ante cualquier eventualidad.
4.18.7	El Especialista en Infraestructura de la UTI es responsable de completar el formato Checklist de Pruebas de Contingencia para evidenciar la ejecución de las pruebas y el cumplimiento de los tiempos definidos en el **PL-GTEC-02 PLAN DE CONTINGENCIA INFORMÁTICO**.
4.18.8	Se tiene establecida y definida una estructura de personal con la responsabilidad, autoridad y competencia necesaria para la ejecución del Plan de Contingencia.
4.18.9	Una vez realizadas las pruebas planificadas, se debe de presentar el Informe de Pruebas de Contingencia.
4.18.10	Se tienen definidas e implementadas instalaciones de procesamiento de información redundantes con capacidad suficiente para garantizar la disponibilidad del negocio.
4.19	**POLITICA DE CUMPLIMIENTO (A.18)**
	La presente política tiene como fin establecer los lineamientos para asegurar el cumplimiento de cualquier requisito reglamentario, regulación u obligación contractual y de todos los requisitos de Seguridad de la Información implementados por la entidad. Asimismo, brinda lineamientos para mantener la conformidad de los sistemas de información de acuerdo con las políticas y normas de Seguridad de la Información establecidas.
4.19.1	**Cumplimiento**
4.19.1.1	**Identificación de la legislación aplicable y de los requisitos contractuales** El Oficial de Seguridad de la Información, o a quien haga sus veces, se encarga de registrar o actualizar la legislación aplicable en materia de Seguridad de la Información en la **MATRIZ DE DOCUMENTOS NORMATIVOS DEL PROGRAMA PENSION 65**, a partir de las solicitudes realizadas a la Unidad de Asesoría Jurídica en relación a nuevas normas, regulaciones y/o leyes relacionadas a la seguridad de la información que aplican a la Entidad. Asimismo, el Oficial de Seguridad de la Información revisa las normas y leyes con la finalidad de velar por su cumplimiento en el alcance del SGSI, para lo cual coordina con las jefaturas involucradas en la interpretación de los requisitos con la finalidad de identificar los controles existentes, documentos, prácticas y otros que dan cumplimiento a las nuevas exigencias normativas registradas
4.19.1.2	**Derechos de propiedad intelectual (DPI)** Se supervisa el cumplimiento al uso de productos registrados de software y los respectivos acuerdos contractuales relacionados a los derechos de propiedad intelectual, no permitiendo la instalación de software piratas.
4.19.1.3	**Protección de los registros de la organización** Se debe cumplir con el resguardo de los registros de backups según los lineamientos establecidos en el **PR- GTEC-01 PROCEDIMIENTO DE RESPALDO DE LA INFORMACIÓN**, con ello se debe garantizar la confidencialidad y disponibilidad de dicha información.

4.19.1.4	**Protección y privacidad de la información de carácter personal** Se cuenta con la **DI-GTEC-04-01-DIRECTIVA TRATAMIENTO Y PROTECCIÓN DE DATOS PERSONALES** que permite el cumplimiento de la Ley de Protección de Datos Personales Nº 29733 y su reglamento.
4.19.2	**Revisión**
4.19.2.1	**Revisión independiente de la seguridad de la información** Se debe supervisar el cumplimiento del de manera que se permita evaluar la efectividad de los controles implementados.
4.19.2.2	**Cumplimiento de las políticas y normas de seguridad** Los jefes de las Unidades son los responsables de supervisar el cumplimiento de las directivas, políticas, procedimientos y del procesamiento de la información dentro de su área de responsabilidad. Esta revisión se debe realizar al menos en forma anual. Si se detectan incumplimientos, estos se deberán de registrar como no conformidades y se deben de tratar inmediatamente de acuerdo con lo establecido en el **PR-GCAL-07 MEJORA CONTINUA DEL SGI**.
4.19.2.3	**Comprobación del cumplimiento técnico** Se debe supervisar que anualmente se realicen evaluaciones técnicas especializadas para verificar el cumplimiento de los controles técnicos implementados. Se establecen en el **PROGRAMA DE AUDITORÍAS INTERNAS.** El resultado de estas evaluaciones debe ser revisados y se tiene que tomar acciones inmediatas para remediar las brechas/riesgos identificados.
4.20	**POLITICA DE CORREO ELECTRÓNICO**
4.20.1	**Consideraciones Generales** a. El servicio de correo electrónico que se brinda al personal y proveedores es de propiedad exclusiva del Programa. El correo electrónico y su contraseña respectiva son confidenciales, personales e intransferibles. b. La entidad se reserva el derecho de activar las opciones de auditoría sobre los mensajes enviados o recibidos para verificar el cumplimiento de las políticas establecidas para el uso del correo electrónico. c. El personal del Programa y los proveedores son responsables de asegurar que ninguna persona ajena utilice su correo electrónico violando las políticas de seguridad, que no se realice actividades ilegales y que no utilice el acceso para fines ajenos a los del Programa. d. El Oficial de Seguridad de la Información, o a quien haga sus veces, como parte de la gestión de incidentes de seguridad es responsable de realizar las investigaciones y tomar las acciones que correspondan en coordinación con las direcciones y/o jefaturas, se amerita solicitar la revocación del privilegio si se detecta un mal uso del correo electrónico.
4.20.2	**Apertura del Correo Electrónico** a. Cuando el personal inicia la relación laboral y mediante una solicitud de la Unidad contratante a la UTI, se le crea el correo electrónico al personal. b. En el caso de proveedores será a solicitud expresa de la Unidad contratante.

4.20.3	**Cierre del Correo Electrónico** a. Cuando el personal termina su relación laboral y mediante una solicitud de la URH a la UTI, se le da de baja al correo electrónico, previo a la generación de una copia de seguridad. b. En el caso de proveedores NO se realizará una copia de seguridad, salvo a solicitud de la Unidad contratante.
4.20.4	**Copia de Respaldo del Correo Electrónico** La copia de respaldo se realiza: a. Se descarga el archivo de respaldo del correo electrónico en mención. b. El archivo descargado se colocará en una carpeta de almacenamiento (Google Drive, por ejemplo). c. Al momento de retiro del personal del Programa, se recomienda que el personal solicite copia de su correo electrónico caso contrario se eliminara la copia almacenada.
4.20.5	**Recomendaciones de Seguridad al Personal** a. El personal y proveedores de servicio deben velar por el correcto uso de su cuenta de correo electrónico institucional siendo de carácter privado y de su propiedad exclusiva. b. La cuenta de correo electrónico institucional es personal e intransferible, no permitiéndose que terceras personas hagan uso de ella. c. Si un personal o proveedor de servicio recibe un mensaje por error, no debe revelar, copiar, distribuir o utilizar su contenido, inmediatamente debe enviar al emisor una notificación sobre el hecho y proceder a eliminar el mensaje de su buzón de correo electrónico institucional. d. Uso indebido o inapropiado del correo electrónico: d.1. El personal o proveedores de servicio no deben enviar correos a personas que estén fuera de las actividades laborales o mensajes considerados ofensivos. En caso de que el Programa reciba quejas, denuncias o reclamos por estas prácticas, se cancelará su cuenta y se informará ante el responsable de la Unidad, para las medidas pertinentes según corresponda. d.2. El personal o proveedores de servicio no deben abrir ningún archivo recibido por correo electrónico, de cuenta desconocida, sin previamente verificar el remitente y/o su contenido (se aplica especialmente a saludos, tarjetas, juegos u otros archivos). d.3. Es prohibida la difusión de contenido para fines ajenos al Programa, como la transferencia de música, videos, imágenes inapropiadas, o software pirata. e. Al terminar la relación laborar con el Programa: e.1. Dado que la cuenta del correo electrónico del Programa, es responsabilidad del personal realizar la copia de seguridad sin violar las Políticas de Seguridad de la Información del Programa. e.2. En el caso de la cuenta del correo electrónico del Programa, la persona podrá solicitar la entrega de los mensajes contenidos en su correo dado que antes de su desvinculación se ha realizado la copia de seguridad del mismo, esta solicitud siempre debe realizarse de la manera más específica posible para evitar violar las Políticas de Seguridad de la Información del Programa.
5.	**REGISTROS**
5.1	No aplica

6.	ANEXOS
6.1	ANEXO 1: LISTA DE CONTACTOS DE AUTORIDADES Y GRUPOS DE INTERÉS
6.2	ANEXO 2: REGISTRO DE CAMBIOS
6.3	ANEXO 3: LISTA DE ÁREAS SEGURAS
6.4	ANEXO 4: LISTA DE SOFTWARE PERMITIDO
6.5	ANEXO 5: LISTA DE DISPOSITIVOS BYOD
6.6	ANEXO 6: FORMATO PARA EL ENVÍO DE DOCUMENTACIÓN A UNA ENTIDAD EXTERNA
6.7	ANEXO 7: LINEAMIENTOS DE SEGURIDAD DE LA INFORMACIÓN PARA EL PERSONAL
6.8	ANEXO 8: LINEAMIENTOS DE SEGURIDAD DE LA INFORMACIÓN PARA LOS PROVEEDORES DE SERVICIOS

ANEXO 1
LISTA DE CONTACTOS DE AUTORIDADES Y GRUPOS DE INTERÉS

Nº	Tipo (Autoridad o Grupo de Interés)	Nombre	Motivo del contacto	Nombre de Contacto Externo	Correo	Teléfono	URL
1							

ANEXO 2
REGISTRO DE CAMBIOS

Tipo de Cambio	Fecha de Solicitud	Solicitante	Justificación del Cambio	Detalle del Cambio	Autorizado Por	Fecha Autorización	Responsable del Cambio	Fecha Ejecución del Cambio	Se evaluó Riesgos de S.I.	Observaciones

ANEXO 3
LISTA DE ÁREAS SEGURAS

N°	Área Segura	Descripción	Ubicación	Controles de Seguridad	Temporalidad

ANEXO 4
LISTADO DE SOFTWARE PERMITIDO

NOMBRE DEL SOFTWARE	AREA QUE NECESITA

ANEXO 5
LISTADO DE DISPOSITIVOS BYOD

NOMBRE Y APELLIDOS	PUESTO	DISPOSITIVO BYOD	CONFIGURACIONES OBLIGATORIAS	APLICACIONES Y BASES DE DATOS CON ACCESO PERMITIDO	APLICACIONES Y BASES DE DATOS CON ACCESO PROHIBIDO

ANEXO 6
FORMATO PARA EL ENVÍO DE DOCUMENTACIÓN A UNA ENTIDAD EXTERNA

(Cabecera)
(Datos del remitente)
(Asunto)
(Referencia)

(Cuerpo del Mensaje)

(Introducción del mensaje)

(Documentación a enviar)
Se remite la siguiente documentación:

Nombre del documento	Hashes del documento	Descripción o Comenta
Documento_01. extensión	MD5: SHA3:	El documento contiene
Documento_02. extensión	MD5: SHA3:	El documento contiene

(Alojamiento de la información a enviar – Opción 01)
Cabe resaltar, que la información se encuentra alojada en el servidor SFTP del MIDIS, al que se podrá acceder mediante el siguiente enlace: sftp://XX.XX.XX.XX/Folder

Para cualquier apoyo con el acceso al servidor comunicarse con la persona encargada NOMBRE_ENCARGADO, mediante el correo: NOMBRE_ENCARGADO@pension65.gob.pe.

(Alojamiento de la información a enviar – Opción 02) – Recomendable sólo con el uso de un adecuado control de acceso como contraseña o control de permisos al recurso
Cabe resaltar, que la información se encuentra en el siguiente enlace de https://docs.google.com/mirecurso.extension

Para cualquier apoyo o coordinación adicional favor de comunicarse con la persona encargada XYZ, mediante el correo: XYZ@pension65.gob.pe.

Sin otro particular, aprovecho la oportunidad para manifestarle mis sentimientos de estima personal.

Atentamente,

En relación a ello, recomendamos establecer los mecanismos necesarios para preservar la confidencialidad de la información requerida, conforme a la Ley N°29733 de Protección de Datos Personales y su Reglamento aprobado por XXXX.

ANEXO 7
LINEAMIENTOS DE SEGURIDAD DE LA INFORMACIÓN PARA EL PERSONAL

Es un deber del personal conocer y respetar las normas de seguridad de la información establecidas en la entidad.

AMBITO	LINEAMIENTO DE SEGURIDAD
ORGANIZACIÓN	a. Conocer y cumplir con lo establecido en la Política de Seguridad de la información aprobada y vigente. b. Notificar los incidentes de seguridad de la información conforme a los canales de comunicación establecidos. c. Mantener la confidencialidad sobre toda la información, datos de carácter personal y de terceros a los que se tenga acceso en virtud de su trabajo. Obligación que subsistirá incluso después de finalizar su relación con la organización. d. Acceder únicamente a la información que han sido autorizados para el desarrollo de sus funciones en función de su perfil de puesto o responsabilidades. e. Queda terminantemente prohibido hacer entrega, por cualquier medio y sin autorización, de listados o de bases de datos a personas no autorizadas, ya sea de forma total o parcial. f. Velar por la seguridad y confidencialidad de la información contenida en sus equipos, especialmente cuando se encuentren fuera de las dependencias de la institución.
EQUIPOS MÓVILES	a. Velar por la seguridad de los dispositivos móviles entregados. b. Asegurar que ninguna persona utilice el dispositivo móvil de propiedad del Programa violando la presente política, que no se realicen actividades ilegales, contrarias a la moral y las buenas costumbres y que no utilice el acceso para fines ajenos a las actividades propias de su función como colaborador. c. Todo dispositivo móvil que tenga instalado los aplicativos de Pensión 65, tanto el aplicativo como el dispositivo móvil asumirán los controles implementados por la Entidad. d. Toda la información contenida en los aplicativos de Pensión 65 y aquella que se haya generado por estos, que sean propios del desempeño del personal y que se encuentre contenida en los dispositivos móviles es de propiedad única y exclusiva de Pensión 65, y es clasificada bajo todo concepto como **USO INTERNO**. e. Periodicidad de sincronización del AYZA de la información de recogida en campo máximo 24 horas después recogida esta, para evitar una posible pérdida de Información. f. Queda prohibido la manipulación de las configuraciones de los smartphones y tabletas, incluye las aplicaciones. g. En caso de pérdida o robo, se debe de comunicar inmediatamente a UA, UTI y su jefe inmediato. h. Cuando el personal se retire de las instalaciones y no lleve el dispositivo móvil consigo, h.1. En caso sea una Laptop, deberá colocar la cadena de seguridad en la Laptop, h.2. En caso sea otro dispositivo móvil éste deberá ser guardado en un cajón con llave; y en ambos casos, la puerta de su oficina deberá ser cerrada con llave, si es el caso.

	h.3. Adicionalmente, cuando el dispositivo móvil sea una laptop se debe tener en cuenta que: El protector de pantalla debe estar configurado y activado obligatoriamente. h.4. Deben bloquearse luego de diez (10) minutos de inactividad. i. Adicionalmente cuando desarrollen fuera del lugar habitual de trabajo: i.1. Se deberán proteger los dispositivos móviles contra el robo. i.2. No se deberá dejar solo, o sin vigilar, un equipo que contenga información importante, sensible o crítica; siempre que sea posible se dejará bajo llave. i.3. Cuando la información sea altamente confidencial, se usarán técnicas de encriptación para evitar el acceso no autorizado o la divulgación de la información almacenada. i.4. Revisar si se cuenta con un antivirus activo y/u otros procedimientos contra software malicioso. i.5. Se deberá asegurar que la información sensible almacenada en estos dispositivos móviles tiene copia de seguridad recuperable en caso de pérdida o robo del dispositivo. i.6. Se deberá prestar un cuidado especial en proteger los dispositivos móviles que estén conectados a las redes. Solo se deberán hacer accesos remotos a la información de la empresa pasando por mecanismos de seguridad de control de accesos y después de conseguir con éxito identificarse y autenticarse. El personal encargado de los dispositivos móviles son los máximos responsables de su seguridad y como tales deberán asumir las sanciones impuestas ante un posible incidente de seguridad.
EQUIPOS BYOD	a. Cuando se utilicen BYOD fuera de las instalaciones del Programa, no deben ser dejados desatendidos. b. Cuando se utiliza BYOD en lugares públicos, el propietario debe tener la precaución de que los datos no puedan ser leídos por personas no autorizadas. c. Se deben instalar periódicamente parches y actualizaciones. d. Notificar a la UTI y a su jefe inmediato antes de eliminar, vender o entregar un BYOD a terceros para su reparación. e. No se permite hacer lo siguiente con los BYOD: e.1. Permitir el acceso a cualquiera que no sea el personal propietario del dispositivo. e.2. Almacenar material ilegal en el dispositivo. e.3. Instalar software sin licencia. No conectarse a redes Wi-Fi desconocidas.
TRABAJO REMOTO	a. Asegurarse que en el sitio en donde se realizará el trabajo remoto debe ser un ambiente en donde se reduzca la probabilidad de la amenaza de acceso no autorizado a información o recursos por parte de otras personas que utilizan el lugar o ambientes en donde se realiza el trabajo remoto. b. Asegurarse que el lugar tenga fácil acceso a la red inalámbrica (wifi) para hacer el trabajo, que no se tengan problemas de señal baja del wifi que puedan impactar en el trabajo, es decir, contar con conexión a internet de alta velocidad confiable.

	c. Verificar la seguridad de las redes domésticas, es decir, el acceso a la red inalámbrica tenga clave de acceso. d. Verificar que el Sistema operativo del equipo asignado y aplicaciones cuenten con las últimas actualizaciones. e. Verificar que los equipos tengan instalado y actualizado el antivirus. f. Verificar que los equipos cuenten con bloqueo automático por inactividad. g. No utilizar otra herramienta de comunicación o de videoconferencia a la establecida por la entidad. Si se necesita utilizar otra herramienta de comunicaciones, debe ser aprobada por la UTI. h. Está prohibido almacenar la información de trabajo en los equipos, toda la información se almacena en la plataforma que brinda la UTI. i. No realizar actividades ilícitas ni vulnerar las políticas del Programa o utilizar el acceso remoto suministrado para obtener lucro comercial.
RECURSOS HUMANOS	a. Cuando el personal inicia la relación laboral se le asignan los permisos apropiados para desempeñar su trabajo, como: a.1. Permisos a las aplicaciones informáticas internas y/ externas a.2. Permisos a una cuenta de correo del Programa a.3. Permiso a una computadora con carpetas locales y una carpeta en red b. Cuando el personal termina su relación laboral b.1. Se remueven los permisos brindados, como: i) Permisos a las aplicaciones informáticas internas y/ externas: Se eliminan los accesos. ii) Permisos a una cuenta de correo del Programa: Se realizar una copia de seguridad del correo y después se elimina el correo. iii) Permiso a una computadora: Se eliminan los archivos locales y archivos de carpetas de red del usuario en mención. b.2. Dado que los archivos de la computadora en local y en red del usuario son eliminados, es responsabilidad del personal realizar una copia de seguridad sin violar las Políticas de Seguridad de la Información del Programa. b.3. Dado que la cuenta del correo del Programa es eliminada, es responsabilidad del personal realizar la copia de seguridad sin violar las Políticas de Seguridad de la Información del Programa. b.4. En el caso de la cuenta del correo del Programa, la persona podrá solicitar la entrega de los mensajes contenidos en su correo dado que antes de su desvinculación se ha realizado la copia de seguridad del mismo, esta solicitud siempre debe realizarse de la manera más específica posible para evitar violar las Políticas de Seguridad de la Información del Programa.
ACTIVOS	a. El uso de los activos de información debe ser para propósitos de las actividades del Programa de acuerdo con las políticas y procedimientos que se definan y considerando criterios de buen uso. b. No se debe divulgar información que haya sido clasificada como “Uso Interno”, salvo tenga una respuesta satisfacción de la consulta por parte de la Unidad de Asesoría Jurídica. c. Se deben cumplir con los requisitos legales, contractuales y normativos relativos al uso de activos de información, incluyendo las políticas de seguridad que deben mantenerse alineadas con las leyes vigentes.

	d. Se deben gestionar adecuadamente los elementos de control de acceso, como contraseñas (control lógico) así como llaves de cerradura (control físico). e. El personal que ponga en riesgo los activos de información, se le aplicará medidas disciplinarias de acuerdo con el Reglamento Interno de Trabajo. Esta sanción estará sujeta a la gravedad del incidente ocasionado y conforme a las normas establecidas.
CONTRASEÑAS SEGURAS	a. Se recomienda cambiar la contraseña en el primer momento de acceder a la cuenta, para que la nueva contraseña sea distinta a la que va en la solicitud. b. No comparta las cuentas y contraseñas con nadie, incluyendo administrativos, secretarias, etc. Todas las contraseñas deben ser tratadas como información sensible y confidencial. c. A continuación, se presenta una lista de cosas que NO se deben hacer: c.1. No utilice la misma contraseña. c.2. No revele su contraseña por teléfono a NADIE, incluso aunque le hablen en nombre del servicio de informática o de un superior suyo en la organización. c.3. Las claves generadas por el usuario no deben ser distribuidas por ningún medio (oral, escrito, electrónico, etc.); las claves deben ser cambiadas si existen indicios de que puedan estar en riesgo las mismas claves o el sistema (en ese caso, se debe informar un incidente de seguridad). c.4. Nunca escriba la contraseña en papel y lo guarde. Tampoco almacene contraseñas en ficheros de ordenador sin cifrar o proveerlo de algún mecanismo de seguridad. c.5. No revele su contraseña a sus superiores, ni a ninguna persona. c.6. No hable sobre una contraseña delante de otras personas. c.7. No revele su contraseña en ningún cuestionario o formulario, independientemente de la confianza que le inspire el mismo. c.8. No comparta la contraseña con familiares. c.9. No revele la contraseña a sus compañeros cuando se marche de vacaciones. c.10. No utilice la característica de “Recordar Contraseña” existente en algunas aplicaciones (Outlook, Netscape, Internet Explorer). c.11. No se debe llevar un registro de las claves, a menos que un método seguro haya sido aprobado por el responsable del sistema.
GESTIÓN DE ACCESOS	a. Todo el personal es responsable de la confidencialidad de la contraseña asignada, y de las consecuencias por las acciones que terceras personas puedan hacer con el uso de la misma. b. Está prohibido compartir las contraseñas asignadas. c. El personal debe de bloquear su estación de trabajo si por algún motivo se retira de su puesto de trabajo.
ESCRITORIOS Y PANTALLAS LIMPIAS	**Escritorios Limpios** a. Toda vez que un usuario se ausenta de su lugar de trabajo debe guardar en lugar seguro cualquier documento, medio magnético u óptico removible que contenga información.

	b. Al finalizar la jornada de trabajo, el usuario debe guardar en un lugar seguro los documentos y medios que contengan información de **USO INTERNO**. c. La información confidencial o sensible, cuando se imprima se debe retirar inmediatamente de las impresoras. **Pantallas Limpias** a. Las estaciones de trabajo y equipos portátiles tienen bloqueo automático en un lapso de 10 minutos. b. La pantalla de autenticación a la red debe requerir solamente la identificación de la cuenta y una clave y no entregar otra información. **c.** Toda vez que el usuario se ausente de su lugar de trabajo debe bloquear su estación de trabajo o laptop de forma de proteger el acceso a las aplicaciones y servicios del Programa.
GESTIÓN DE INCIDENTES	Todos los usuarios deben comunicar las debilidades, eventos o incidentes a UTI mediante los canales establecidos (APLICATIVO WEB GLPI o correo electrónico).
CONTINUIDAD DEL NEGOCIO	a. Participar en las pruebas del **PL-GTEC-02 PLAN DE CONTINGENCIA INFORMÁTICO**, ante eventuales caídas de los sistemas de información y aplicaciones informáticas.
CORREO ELECTRÓNICO	a. El personal y proveedores de servicio deben velar por el correcto uso de su cuenta de correo electrónico institucional siendo de carácter privado y de su propiedad exclusiva. b. La cuenta de correo electrónico institucional es personal e intransferible, no permitiéndose que terceras personas hagan uso de ella. c. Si un personal o proveedor de servicio recibe un mensaje por error, no debe revelar, copiar, distribuir o utilizar su contenido, inmediatamente debe enviar al emisor una notificación sobre el hecho y proceder a eliminar el mensaje de su buzón de correo electrónico institucional. d. Uso indebido o inapropiado del correo electrónico: d.1. El personal o proveedores de servicio no deben enviar correos a personas que estén fuera de las actividades laborales o mensajes considerados ofensivos. En caso de que el Programa reciba quejas, denuncias o reclamos por estas prácticas, se cancelará su cuenta y se informará ante el responsable de la Unidad, para las medidas pertinentes según corresponda. d.2. El personal o proveedores de servicio no deben abrir ningún archivo recibido por correo electrónico, de cuenta desconocida, sin previamente verificar el remitente y/o su contenido (se aplica especialmente a saludos, tarjetas, juegos u otros archivos). d.3. Es prohibida la difusión de contenido para fines ajenos al Programa, como la transferencia de música, videos, imágenes inapropiadas, o software pirata. e. Al terminar la relación laborar con el Programa: e.1. Dado que la cuenta del correo electrónico del Programa, es responsabilidad del personal realizar la copia de seguridad sin violar las Políticas de Seguridad de la Información del Programa.

	e.2.	En el caso de la cuenta del correo del Programa, la persona podrá solicitar la entrega de los mensajes contenidos en su correo dado que antes de su desvinculación se ha realizado la copia de seguridad del mismo, esta solicitud siempre debe realizarse de la manera más específica posible para evitar violar las Políticas de Seguridad de la Información del Programa.

Las acciones descritas a continuación están estrictamente prohibidas:

- Divulgar información confidencial o secreta a personas que pueda provocar daños o perjuicios a la entidad.
- No está permitido acceder a internet con fines comerciales o recreativos (juegos, chat, radio por internet, blogs de música y video para descargar o escuchar en línea, conversación en tiempo real, etc.).
- Está prohibido manipular comidas, bebidas o por fumar cerca de los equipos informáticos que puedan originar directa o indirectamente su mal funcionamiento siendo el usuario responsable por el deterioro del mismo.
- Intentar acceder a recursos sin autorización mediante la utilización de herramientas intrusivas (hacking), descifre de contraseñas, descubrimiento de vulnerabilidades o cualquier otro medio no permitido.
- Cargar archivos que contengan virus, troyanos, gusanos, archivos dañados o cualquier otro programa o software similar que pueda perjudicar el funcionamiento de los equipos de la red.

Firmo la presente declaración y me comprometo a cumplir los lineamientos establecidos.

_____
Firma del Trabajador
N° de DNI_____

Lima, …….. de…….. de 20…..

ANEXO 8
LINEAMIENTOS DE SEGURIDAD DE LA INFORMACIÓN PARA LOS PROVEEDORES DE SERVICIOS

Con el objetivo de garantizar la protección de los activos del Programa que son accesibles por los Proveedores/Terceros. Se han definido los siguientes lineamientos de seguridad de la información:

1. Todo Proveedor que tenga acceso a la información del Programa en ejecución de un contrato, deberá considerar que dicha información, es confidencial.
2. Ningún Proveedor podrá utilizar la información del Programa para beneficio propio o de terceros. La información a la que tenga acceso el Proveedor únicamente podrá ser utilizada para los fines específicamente indicados en el contrato. Toda información proporcionada por la Entidad seguirá siendo de propiedad de esta última.
3. El Proveedor garantiza que a la terminación del servicio o ante el pedido efectuado en cualquier momento por la Entidad, cesará inmediatamente el uso de toda información proporcionada, debiendo entregar, (cualquiera sea el soporte en que se encuentre) toda la información que obre en su poder y destruir toda copia que se haya realizado, entregando una confirmación por escrito de ello con la calidad de declaración jurada.
4. Todas las obligaciones de confidencialidad continuarán vigentes aún culminado el contrato de prestación de servicios por cualquier causa.
5. Cuando el Proveedor conozca de cualquier pérdida, uso no autorizado o revelación de la Información proporcionada o de propiedad del Programa, deberá comunicarlo inmediatamente, debiendo adoptar todos los pasos necesarios para ayudar a la Entidad a remediar tal uso no autorizado o revelación de la Información.
6. El proveedor debe garantizar el cumplimiento de las restricciones legales respecto del uso del material protegido por normas de propiedad intelectual.
7. El Proveedor y su personal únicamente podrá utilizar la información y activos tecnológicos autorizados por la Entidad para el desarrollo de los servicios contratados.
8. La distribución de la información ya sea en formato digital o papel, se realizará mediante los recursos determinados en el contrato de prestación de servicios y para la finalidad exclusiva de facilitar las funciones asociados a dicho contrato.
9. Los recursos que la Entidad pone a disposición del Proveedor, independientemente del tipo que sean, (informáticos, datos, software, redes, sistemas de comunicación, etc.) están exclusivamente destinados para cumplir con las obligaciones y propósito para los que fueron proporcionados. La Entidad se reserva el derecho de implementar mecanismos de control y auditoría que verifiquen el uso apropiado de estos recursos.
10. En el caso de correo electrónico, cuando se le asigne una cuenta es de uso exclusivo para el Programa y la labor para lo que fue contratado, y al finalizar la relación laboral este también se elimina sin guardar una copia de seguridad del mismo.
11. Se prohíbe expresamente:
    a. El uso de recursos proporcionados por la Entidad para actividades no relacionadas con el propósito de servicio.
    b. La conexión a la red del Programa de equipos y/o aplicaciones que no estén especificados como parte del Software propio o bajo supervisión del Programa.
    c. Intentar obtener sin autorización explícita otros derechos o accesos distintos a los que la Entidad haya asignado.
    d. Intentar acceder, sin autorización explícita, a áreas restringidas de los Sistemas de Información del Programa.
12. Cualquier persona con acceso a información del Programa deberá respetar al menos las siguientes políticas de escritorio limpio, con el fin de proteger los documentos en papel y dispositivos de almacenamiento removibles y reducir los riesgos de acceso no autorizado, pérdida y daño de la información, tanto durante el horario normal de trabajo como fuera del mismo:
    a. Almacenar bajo llave los documentos de papel y los medios informáticos con información del Programa en mobiliario seguro cuando no están siendo utilizados.
    b. No dejar desatendidos los equipos y bloquear su acceso cuando no estén siendo utilizados.
    c. Los listados con datos de carácter personal o información confidencial deberán almacenarse en un lugar seguro al que únicamente tengan acceso personas autorizadas.

13. Todos los servicios que impliquen accesos a la información o sistemas de información del Programa deberán cumplir con las siguientes políticas con respecto a su personal:
    a. El proveedor deberá verificar los antecedentes profesionales, penales y policiales del personal asignado al servicio, garantizando a la Entidad que en el pasado no haya tenido algún tipo de sanción.
    b. El proveedor deberá garantizar a la Entidad la posibilidad de la baja inmediata del personal asignado al servicio de cualquier persona en relación con la cual la Entidad le indique.
14. Todo proveedor deberá permitir que la Entidad lleve a cabo auditoría de seguridad del servicio en cuanto lo requiera, colaborando con el equipo auditor y facilitando todas las evidencias y registros que le sean requeridos.
15. El alcance y profundidad de la auditoría será establecido expresamente por la Entidad en cada caso.
16. La Entidad se reserva el derecho de realizar auditorías extraordinarias adicionales, siempre que se den las causas específicas que lo justifiquen.
17. El Proveedor deberá ponerse en contacto con el Oficial de Seguridad de la Información del Programa, o quien haga sus veces, en caso detecte cualquier incidencia relacionada con la información o los recursos del Programa.
18. Todo proveedor de servicios es responsable de transmitir y hacer cumplir las políticas de seguridad del Programa a terceros subcontratados, autorizados debidamente por la Entidad.

Firmo la presente declaración y me comprometo a cumplir los lineamientos establecidos.

_____
Firma del Proveedor

Lima, …….. de…….. de 20…..

POLITICA DEL SISTEMA DE GESTIÓN INTEGRAL

Entregamos una subvencion monetaria a las personas adultas mayores a partir de 65 años de edad en situación de probreza extrema según calificación del sistema de focalización de Hogares – SISFOH, y que no reciben una pensión proveniente del sector público o privado, con el objeto de asegurarles un ingreso periodico que contribuya a su bienestar y mejora en la economía de su hogar; dentro de un marco de **tolerancia cero al soborno**, para lo cual sus servidores se comprometen con la prohibición de recibir directa o indirectamente, ya sea a través de un tercero; cualquier ventaja financiera o de otra naturaleza, con la intención de ejercer una influencia indebida sobre un determinado proceso; asimismo, se comprometen con la **protección de la información** asegurando el cumplimiento de la confidencialidad, integridad y disponibilidad de la misma.

Hacemos todo nuestro esfuerzo para que la **entrega de la subvencion se realice oportunamente, cumpliendo las** normas legales y reglamentarias en materia antisoborno, seguridad de la información y otras aplicables, en las mejores condiciones posibles de acuerdo a la localización geografica del usuario(a).

Articulamos y coordinamos con otros sectores y entidades públicas y privadas, para promover el acceso a los servicios que brinda el Estado; a fin de que los usuarios(as) puedan acceder plenamente a sus derechos ciudadanos; asegurando la protección de sus datos personales y mejorando su calidad de vida a través de la revalorización social de su rol en la familia y en la comunidad.

Promovemos mecanismos de participación y vigilancia ciudadana para garantizar los fines del Programa, así como; las denuncias de buena fe, brindando protección al denunciante asegurando la debida autoridad e independencia de los organos responsables asignados para el cumplimiento del Sistema de Gestión Antisoborno, cuyo incumplimiento estará sujeto a investigación interna y a la aplicación de las medidas disciplinarias establecidas, independiente de las sanciones penales que corresponda de acuerdo a los resultados de cada investigación.

Nos comprometemos a cumplir con lo establecido en nuestro Sistema de Gestión Integral, proporcionando un marco de referencia para establecer y revisar los objetivos, gestionar los riesgos y oportunidades en los procesos, y mejorar continuamente la eficacia del sistema con el fin de satisfascer las necesidades de nuestros usuarios.

Dirección Ejecutiva

Rev.16/08/2022

CONTROL DE DOCUMENTOS Y REGISTROS DEL SISTEMA DE GESTION INTEGRAL

(Vs. 01)

Coordinador del SGI	Coordinador del SGI	Comité del SGI	31/08/2022
Elaborado por	Revisado por	Aprobado por	Fecha de aprobación
Resolución Directoral N°			

Matriz de Control de Cambios en Documentos

Versión	Ítem	Modificación respecto a la versión anterior	Sustento	Unidad que solicitó el cambio	Observaciones

PR-GCAL-01-F05 Vs.01

1.	**OBJETIVO**
1.1	Establecer los lineamientos generales para la elaboración, revisión, aprobación, emisión, distribución, retiro y modificación de los documentos del Sistema de Gestión Integral (SGI) del Programa Nacional de Asistencia Solidaria (PNAS) - Pensión 65; así como, la identificación, legibilidad, almacenamiento, protección, recuperación, tiempo de conservación y disposición de los registros del SGI.
2.	**ALCANCE**
2.1	Este procedimiento es aplicable a todos los documentos (política, objetivos, manuales, procedimientos, instructivos, entre otros) y registros generados por P65 como resultado de la implementación y operación de su Sistema de Gestión Integral (SGI).
3.	**RESPONSABLES**
3.1	Comité del Sistema de Gestión Integral
3.2	Coordinador de Calidad
3.3	Todo el personal del PNAS – Pensión 65
4.	**DEFINICIONES Y ABREVIATURAS**
4.1	**SGI**: Sistema de Gestión Integral, se considera los Sistemas de Gestión de Calidad, Antisoborno, Seguridad de la Información y posteriores sistemas que se vayan implementando de la familia ISO.
4.2	**PNAS-P65:** Programa Nacional de Asistencia Solidaria - Pensión 65
4.3	**Registro:** Documento que presenta resultados obtenidos o proporciona evidencia de actividades desempeñadas.
5.	**DOCUMENTOS DE REFERENCIA**
5.1	ISO 9001:2015 - Requisito 7.5 Información Documentada ISO 37001:2016 – Requisito 7.5 Información Documentada ISO 27001:2013 – Requisito 7.5 Información Documentada
6.	**DISPOSICIONES**
6.1	**Cambios de un Documento del SGI.** El control de los documentos del SGI se lleva a cabo de la siguiente manera: a) El número de versión (Vs) del documento se coloca inmediatamente debajo del Nombre del Documento en la carátula de este. Cuando el documento cambia de versión, el Coordinador del SGI procede a retirar la versión obsoleta. b) Los cambios que se realizan entre una versión y otra son registrados en el formato PR-GCAL-01-F05 Vs.01 "Matriz de Control de Cambios en Documentos" (Anexo Nº08), de cada documento. c) Aplicara el uso de la matriz de control de cambios y numero de versiones cuando se trate de actualizaciones puntuales que no involucren una reestructuración de todo el documento. d) Si los cambios son estructurales del contenido del documento o cambio del proceso mismo se tendrá que elaborar un nuevo documento con el cambio del código y nombre del título del documento.
6.2	**Identificación de cambios:** Cada uno de los cambios realizados, se pueden identificar: a) En la Matriz de Control de Cambios en Documentos (PR-GCAL-01-F05), donde se indica los cambios realizados en cada versión del documento. b) Por comparación con el documento anterior.

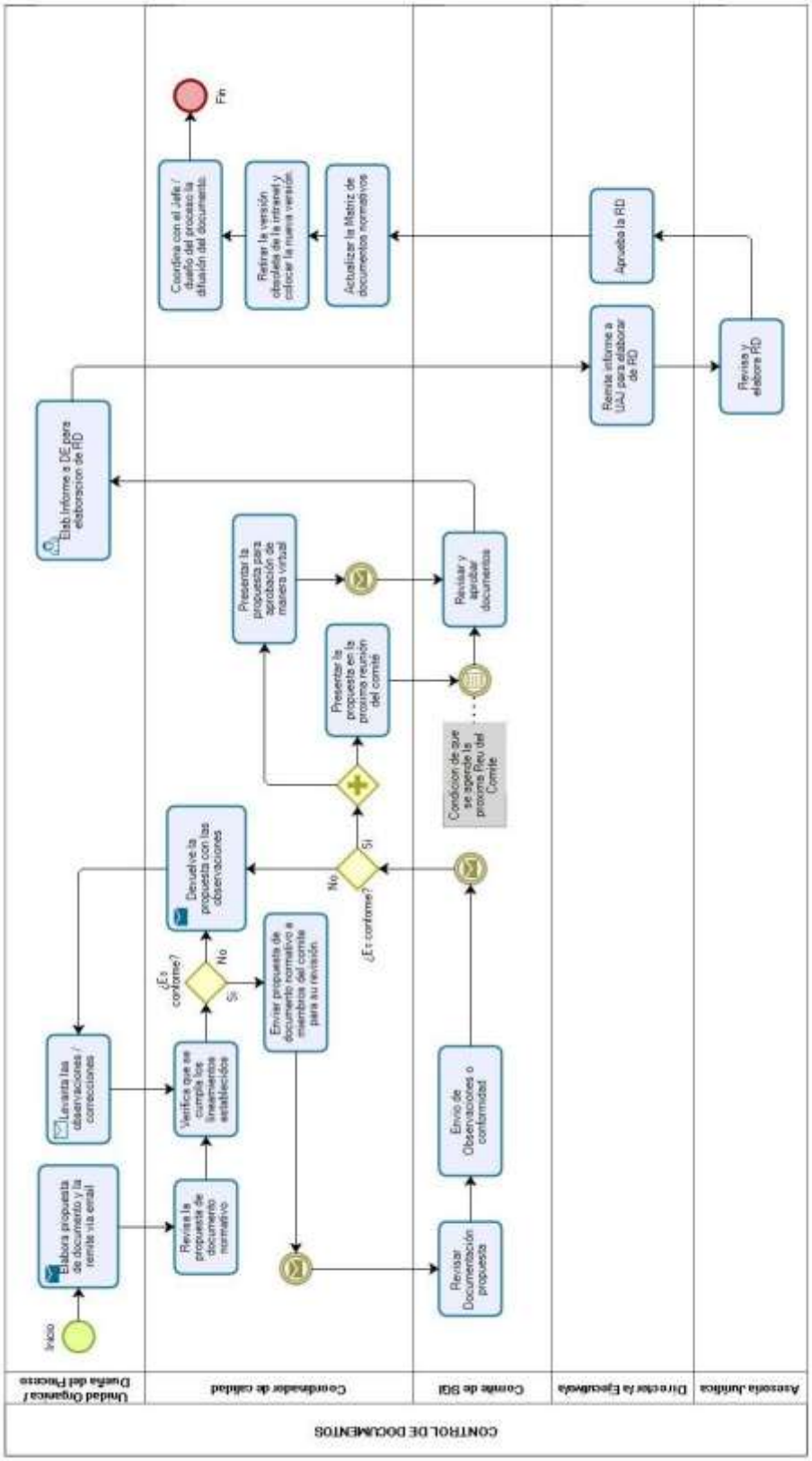
6.3	Los documentos y registros del Sistema de Gestión Integral, que se generen, son creados y conservados electrónicamente para conocimiento de los colaboradores en la intranet o drive (Google), y cuya finalidad es la reducción de uso del papel.	
6.4	Los archivos electrónicos son conservados de acuerdo a los lineamientos del respaldo de la información, establecidos por la Unidad de Tecnología de la Información.	
6.5	Para la representación gráfica de los procedimientos se recomienda utilizar los símbolos que se detallan en el Anexo N°6 del presente documento, no excluyendo el uso de otros símbolos como el usado en los programas BIZAGI MODELER, VISIO u otros.	
6.6	Disposición Final de las Versiones Físicas (Vigentes y Obsoletas): La Unidad de Asesoría Jurídica es la encargada de velar por el almacenamiento de las Resoluciones Directorales las cuales contienen los documentos normativos que son aprobados y las normas legales y reglamentarias aplicables.	
6.7	Ubicación de los documentos vigentes. Los documentos normativos vigentes se encuentran a disposición del personal en la intranet del programa, o el drive de Google, cuya dirección de enlace es la siguiente: https://drive.google.com/drive/u/1/folders/1iNGgeeC6UyXKnxiaO9Fv2CvAFdkriKgz La documentación digital correspondiente al Sistema de Gestión Integral se encuentra en custodia de la Coordinación de Calidad del Programa.	
6.8	Control y distribución de documentos externos controlados El control se realiza a través de la Matriz de Documentos Normativos del Programa PENSION 65 (Ver Anexo Nº04)	
7.	**DESARROLLO**	
	RESPONSABLE	**DESCRIPCIÓN DE LA ACTIVIDAD**
7.1	**CARÁTULA Y CODIFICACIÓN**	
	Coordinador de Calidad	Es responsable de asignar la carátula según el Anexo Nº03, y codificación a todos los documentos del Sistema de Gestión Integral, según lo descrito a continuación: **A. Directivas, Procedimientos, Manuales, Planes e Instructivos** Los documentos normativos utilizarán la siguiente codificación: **XX-YYYY-ZZ-VV** Donde: XX: identifica al tipo de documento normativo YYYY: identifica al proceso ZZ: correlativo del tipo de documento (comienza en 01) VV: versión del documento normativo (comienza en 01) **Tipo de Documento:** Puede ser Directiva (DI), Guía (GI), Instructivos (IN), Manual (MA), Plan (PL), Política (PO), Procedimiento (PR) y Reglamento (RE). **Siglas del Proceso:** GOPE: Gestión de Operaciones GADM: Gestión Administrativa GTEC: Gestión de Tecnologías de la Información GPPR: Gestión de Planeamiento y Presupuesto GCOM: Gestión de las Comunicaciones

		GSGI: Gestión del Sistema de Gestión Integral GPDI: Gestión de Proyectos y Diseño de Intervenciones GRH: Gestión del Recurso Humano. GAJ: Gestión de Asesoría Jurídica GCAL: Gestión de Calidad. **Ejemplo:** PR-GOPE-01-01 → Versión 01 correspondiente al Procedimiento 01 de Gestión de Afiliación. → Procedimiento 01 de Gestión de Afiliación. → Proceso de Gestión de Operaciones → Procedimiento **B. Otros documentos** No se requiere establecer una codificación, debido a que el nombre del documento lo identifica.
7.2	**ESTRUCTURA DE LOS DOCUMENTOS**	
	Todo Personal de P65	Desarrollar el documento, según lo descrito a continuación: **A. Directivas, Procedimientos e Instructivos** 1. CARATULA 2. MATRIZ DE CONTROL DE CAMBIOS 3. OBJETIVO 4. ALCANCE 5. RESPONSABLES 6. DEFINICIONES Y ABREVIATURAS 7. DOCUMENTOS DE REFERENCIA 8. DISPOSICIONES 9. DESARROLLO 10. REGISTROS 11. ANEXOS **B. Otros Documentos** No se requiere establecer una estructura definida.
7.3	**IDENTIFICACIÓN DE VERSIÓN VIGENTE**	
	Coordinador de Calidad	Se consideran documentos vigentes los documentos del SGI que se encuentren a disposición en la intranet o drive (Google) del Programa P65, aprobados por el Comité del Sistema de Gestión Integral.
7.4	**CONTROL DE DOCUMENTOS**	

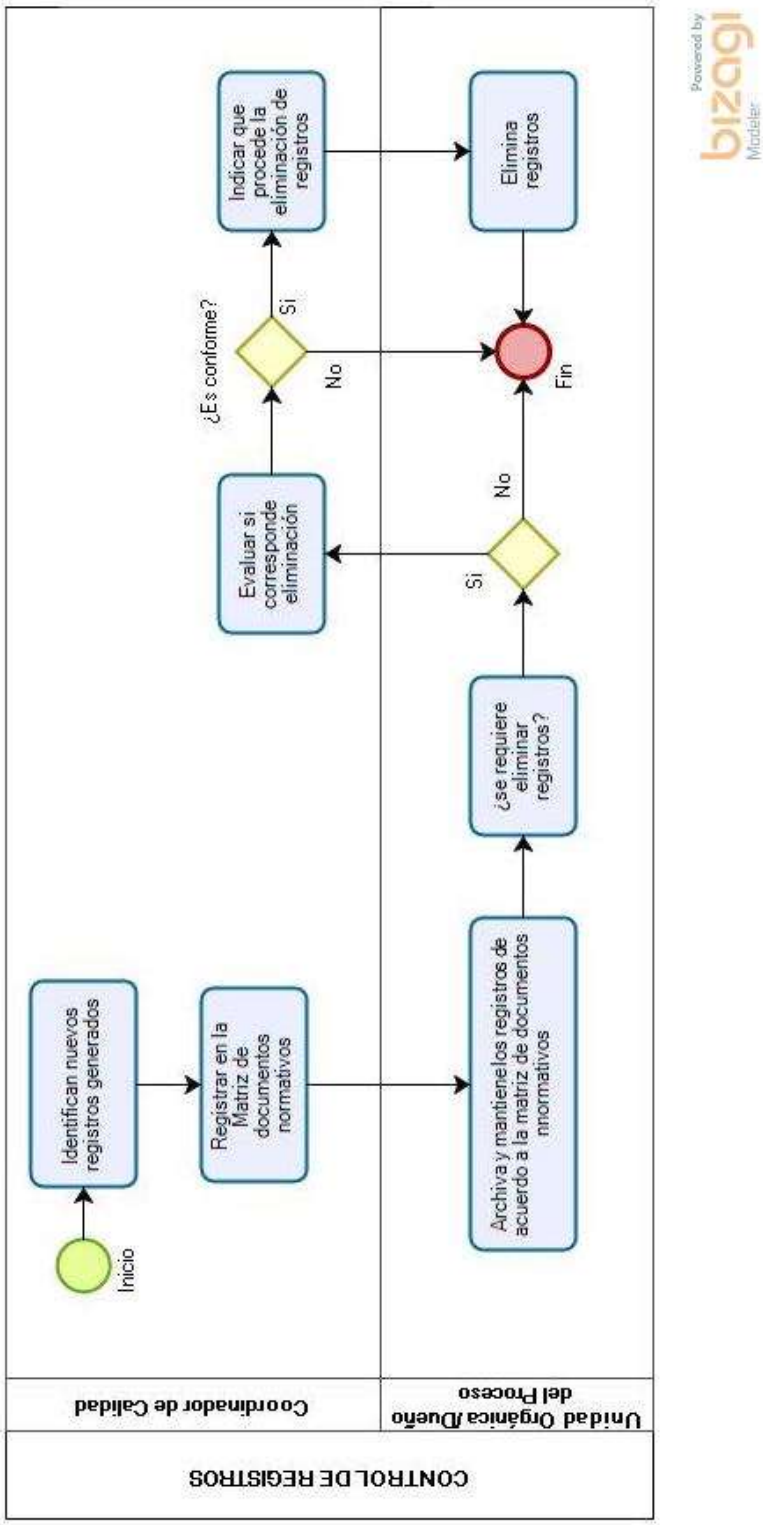
7.4.1	Unidad Orgánica / Dueño del Proceso	**Elaboración o Modificación/Revisión/Aprobación de Documentos** Elaborar la propuesta de documento normativo según el formato vigente, luego enviar dicha propuesta al coordinador de calidad vía email.
7.4.2	Coordinador de Calidad	Revisar la propuesta de documento normativo y verifica que este cumpla con las disposiciones establecidas. Si el documento no es conforme, se devuelve la propuesta con las observaciones para su levantamiento, finalizando el proceso. Si el documento es conforme, se envía la propuesta de documento normativo a los miembros del comité para su revisión, vía email.
7.4.3	Comité del Sistema de Gestión Integral	Los miembros del comité revisan la propuesta de documento normativo enviado sus observaciones y/o comentarios (vía email) al coordinador de calidad.
7.4.4	Coordinador de Calidad	Recibir y consolidar los comentarios u observaciones del documento revisado por los miembros del comité; si este resulta no conforme o presenta observaciones, se devolverá al dueño del proceso para que realice el levantamiento de las correcciones correspondientes. Si es conforme y no hay objeciones se realizará la aprobación bajo dos modalidades: Virtual: Presentación de la propuesta a los miembros del comité en la medida que no hubo objeciones y mediante un formulario proceder a realizar la aprobación virtual del documento. Reunión de Comité de SGI (Sistema de Gestión Integral): Presentación dentro de la agenda del Comité, lo cual tendrá una condicionante que dependerá de la fecha de la próxima reunión de este.
7.4.5	Comité del Sistema de Gestión Integral	Revisar el documento normativo propuesto y aprueba
7.4.6	Unidad Orgánica / Dueño del Proceso	Elaborar el informe a la Dirección Ejecutiva presentando las justificaciones de la propuesta del documento y solicitando en las recomendaciones la derivación a las unidades correspondientes para la elaboración de la Resolución Directoral.
7.4.7	Dirección Ejecutiva	Remitir el informe de propuesta de documento normativo a la unidad de asesoría jurídica para la elaboración de la Resolución Directoral.
7.4.8	Unidad de Asesoría Jurídica	Revisar y elaborar la Resolución Directoral y remitir a la Dirección Ejecutiva para la aprobación y firma / firma digital.
7.4.9	Dirección Ejecutiva	Firma / Firma Digital de la Resolución Directoral.
7.4.10	Coordinador de Calidad	Actualizar la Matriz de Documentos Normativos del Programa PENSION 65
7.4.11	Coordinador de Calidad	Retirar la versión electrónica obsoleta de la intranet o drive (Google) y publicar los documentos aprobados en la intranet o drive (Google) del Programa. (ver enlace en el ítem 6.7)
7.4.12	Coordinador de Calidad	Coordina la difusión del documento normativo a través de cada Jefe de Unidad (dueño del Proceso) y finaliza procedimiento.
7.5	**CONTROL DE REGISTROS**	

7.5.1	Coordinador de Calidad	**Identificación de Registros** Identifican los nuevos registros generados como evidencia de los resultados del Sistema de Gestión Integral. Registra en la matriz de documentos normativos, especificando en la columna de tipo de documento el nombre de "Registro".
7.5.2	Unidad Orgánica / Dueño del Proceso	**Conservación de Registros** El responsable de la unidad orgánica de la conservación del registro es el responsable del proceso, quien archiva y mantiene los registros de acuerdo con la matriz de documentos normativos. El responsable de la conservación del registro consultará con el coordinador de calidad sobre la eliminación de registros o su actualización.
7.5.3	Coordinador de Calidad	**Almacenamiento, identificación, protección y disposición de registros** Evaluar con el responsable de conservación del documento normativo, si corresponde la eliminación de los registros, comunicará al dueño del proceso para que proceda con la eliminación Archivar y mantener los registros digitales de acuerdo con la "Matriz de Documentos Normativos del Programa PENSION 65" (Ver Anexo Nº04).
8.	**REGISTROS**	
8.1	Matriz de Documentos Normativos del Programa PENSION 65 (PR-GCAL-01-F03 Vs.01)	
9.	**ANEXOS**	
9.1	Anexo 01: Flujograma Control de Documentos	
9.2	Anexo 02: Flujograma Control de Registros	
9.3	Anexo 03: Formato Primera Página de los Documentos	
9.4	Anexo 04: Matriz de Documentos Normativos del Programa PENSION 65	
9.5	Anexo 05: Matriz de Control de Cambios de Documentos	
9.6	Anexo 06: Símbolos a utilizar en los diagramas de flujo	
9.7	Anexo 07: Descripción de estructura documentaria.	

Anexo Nº01
Flujograma Control de Documentos



Anexo Nº02
Flujograma Control de Registros



Anexo Nº03
Formato Primera Página de los Documentos

pensión65 tranquilidad para más peruanos	**Tipo de Documento**	Código: Fecha: Páginas: de
	Nombre del documento	

NOMBRE DEL DOCUMENTO

(Vs.)

Elaborado por	Revisado por	Aprobado por	Fecha de aprobación
Resolución Directoral N° ……..			

Anexo Nº04
Matriz de Documentos Normativos del Programa PENSION 65

pensión65 tranquilidad para más peruanos	Matriz de Documentos Normativos del Programa PENSION 65											
N°	Clasificación	Tipo	Número	Denominación	Unidad / Área	Ubicación	Estado	Versión	Año	Fuente	Fecha de Publicación	Link

PR-GCAL-01-F03 Vs.02

Anexo Nº05
Matriz de Control de Cambios en Documentos

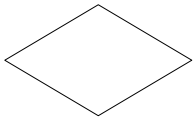
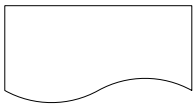
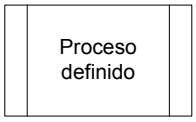
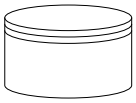
Versión	Item	Modificación respecto a la versión anterior	Sustento	Unidad que solicitó el cambio	Observaciones

PR-GCAL-01-F05 Vs.01

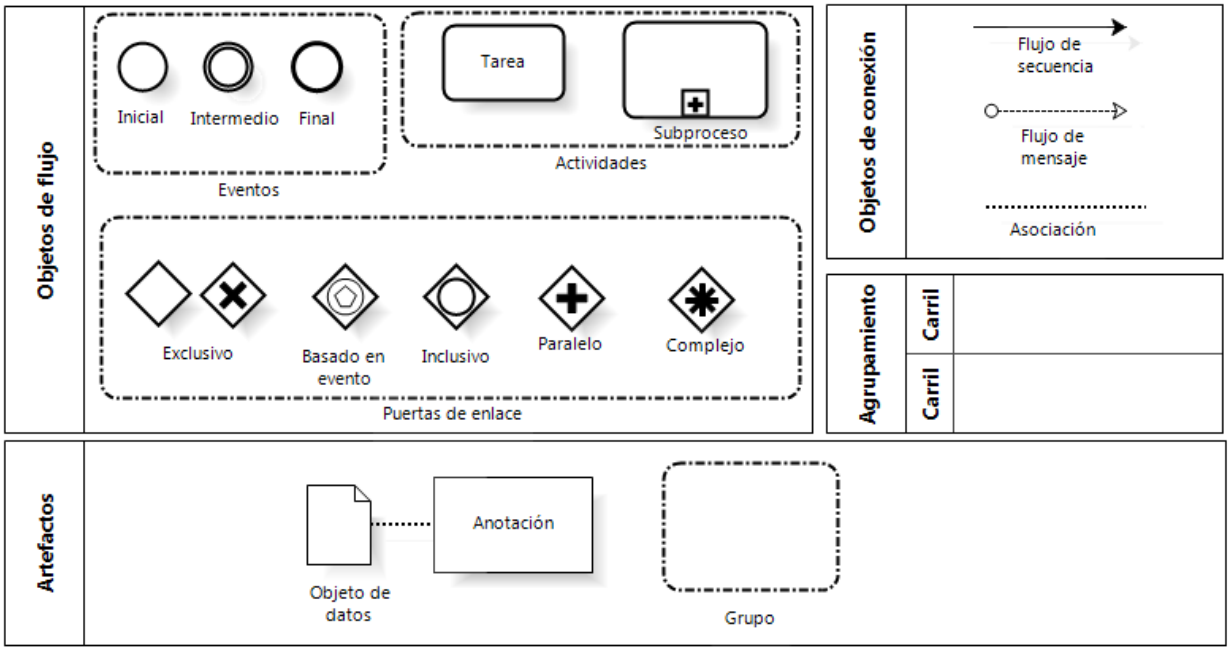
Anexo N°06

Símbolos básicos para utilizar en los diagramas de flujo

Notación ANSI:

Categoría	Descripción	Símbolo
De actividad	Representa la actividad que se realiza. De preferencia debe ser en voz activa. La descripción debe ser breve.	
De decisión	Designa un punto de decisión a partir del cual, el proceso tiene únicamente dos alternativas excluyentes. El camino a tomar depende de la respuesta a la decisión que aparece dentro del rombo	
De inicio	En el documento se puede utilizar mas de un símbolo de inicio.	
De registros	Se utiliza para representar un documento de entrada o salida.	
De líneas de flujo	Indica el flujo del proceso. En los casos que a un símbolo de actividad o documentación ingresen o salgan más de una línea, se considerarán actividades paralelas.	
De conexión	Indica la continuación de un diagrama de flujo hacia otra parte del diagrama a fin de continuar la secuencia. Se utiliza para abreviar el uso de líneas de flujo	
De documentación	Hace mención a un proceso distinto al analizado pero que se interrelaciona con el proceso que se está diagramando.	
De archivo	Símbolo que indica el archivo de un documento en medio físico o electrónico	
Fin	En el documento se puede utilizar mas de un símbolo de Fin	

Notación BPMN:



Nota: También se podrá hacer uso de los programas como BIZAGI MODELER, VISIO u otros

Anexo N°07

Descripción de estructura documentaria

CAMPO	DESCRIPCIÓN
Objetivo	Se deberá definir lo que se pretende alcanzar con la formulación del documento normativo
Alcance	Se deberá señalar la estructura organizacional o el personal que deberá cumplir con lo dispuesto en el documento
Responsables	Se deberá indicar que el órgano ó unidad orgánica que aprueba el documento normativo es responsable de velar por el cumplimiento de lo dispuesto en él.
Definiciones y abreviaturas	Se presentarán las definiciones, símbolos y abreviaturas que faciliten la comprensión de los términos a ser utilizados en el documento normativo.
Documentos de referencia	Se deberá precisar la normativa y documentación existente referida al documento normativo.
Disposiciones	Se señalarán las pautas que complementan la descripción del documento normativo que resulten necesarios para su aplicación.
Desarrollo	La descripción del documento normativo deberá señalar las actividades a desarrollar, los responsables, insumos y productos de cada una de ellas, de corresponder. En los casos que se requiera, deberá hacer referencia a otros documentos normativos que expliquen en mayor detalle las actividades mencionadas.
Registros	Se señalarán los registros que evidencien la ejecución de una actividad o tarea
Anexos	Formatos, diagramas, plantillas que se utilizan en la ejecución de las actividades detalladas en el documento normativo.

AUDITORÍAS INTERNAS AL SISTEMA DE GESTION INTEGRAL

(Vs. 01)

Coordinador de Calidad	Comité de Calidad	Alta Dirección	31/08/2022
Elaborado por	Revisado por	Aprobado por	Fecha de Aprobación
Resolución Directoral N° ……..			

Matriz de Control de Cambios en Documentos

Versión	Ítem	Modificación respecto a la versión anterior	Sustento	Unidad que solicitó el cambio	Observaciones

PR-GCAL-01-F05 Vs.01

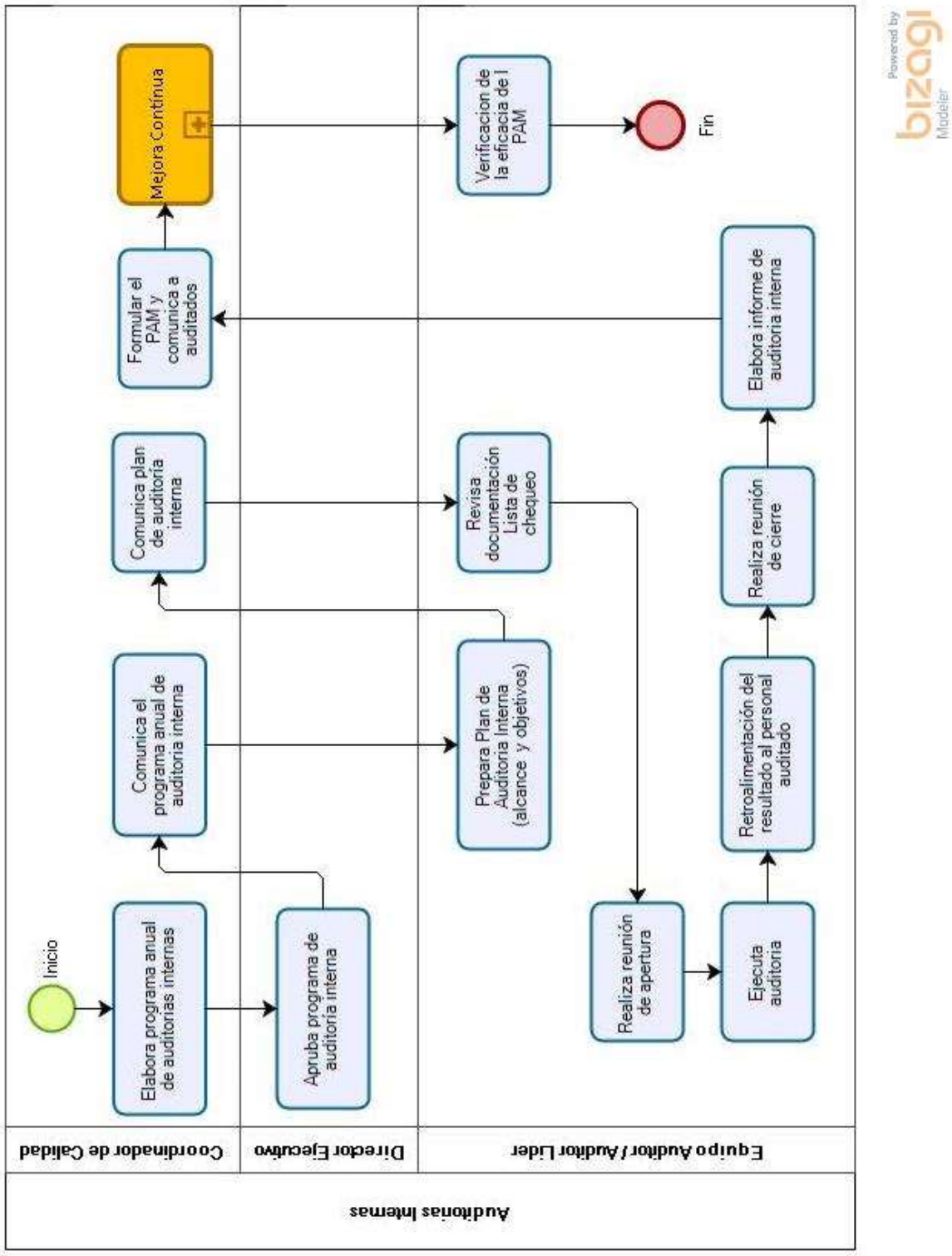
1.	**OBJETIVO**
	Establecer las actividades para la planificación, realización, documentación y seguimiento de las auditorías internas al sistema de gestión integral, con el objeto de verificar que las actividades de los procesos cumplen las disposiciones establecidas en los Sistemas de Calidad, Antisoborno y Sistemas de Seguridad de la Información en el Programa Nacional de Asistencia Solidaria Pensión 65.
2.	**ALCANCE**
	Este procedimiento es aplicable a todas las auditorías internas realizadas al Sistema de Gestión Integral (SGI) del Programa Nacional de Asistencia Solidaria Pensión 65, por los Auditores Internos o externos debidamente autorizados.
3.	**RESPONSABLES**
3.1	Coordinador de Calidad: Responsable de la planificación de las auditorías internas a nivel de Sede central y Unidades Territoriales.
3.2	Equipo Auditor: Programa y ejecuta a cabo las auditorías a los procesos seleccionados.
3.4	Auditor Líder: Integra el Equipo Auditor y tiene la responsabilidad de elaborar el plan de auditoría, la reunión de apertura y cierre del proceso de auditoria; así como, la elaboración consensuada con el equipo auditor del informe de auditoría.
3.3	Dirección Ejecutiva: Aprueba el Plan de Auditorías Internas del programa.
4.	**DEFINICIONES Y ABREVIATURAS**
4.1	**Auditoria:** Proceso sistemático, independiente y documentado para obtener evidencias de la auditoria y evaluarlas de manera objetiva con el fin de determinar la extensión en que se cumplen los criterios de auditoria.
4.2	**Auditor**: Persona calificada para llevar a cabo una auditoria. Puede ser un auditor interno calificado del Programa Social Pensión 65, o en caso se requiera, un auditor externo calificado.
4.3	**Criterios de auditoria**: Conjunto de políticas, normativas, procedimientos o requisitos de normas utilizados como referencia.
4.4	**Auditado**: organización o persona que es auditada.
4.5	**Evidencia**: Registros, declaraciones de hechos o cualquier otra información que son pertinentes para los criterios de auditoría y que son verificables.
4.6	**Hallazgos de la auditoria**: resultados de la evaluación de las evidencias de auditoría contra los criterios de auditoría.
4.7	**No Conformidad**: Incumplimiento de un requisito.
4.8	**Oportunidad de Mejora:** Conjunto de acciones tomadas para describir lo que puede ser aprovechable, que genera una oportunidad con un beneficio específico.
4.9	**Mejora Continua:** es la actividad de analizar los procesos que se usan dentro de una organización o administración, revisarlos y realizar adecuaciones para minimizar los errores de forma permanente.
4.10	**Rol**: Es el papel o función encargada (por designación) que alguien representa actividades específicas, que requieren dominio y carácter de interiorización de una postura emocional y afectiva para realizar acciones encomendadas.
5.	**DOCUMENTOS DE REFERENCIA**
5.1	ISO 9001 Sistema de Gestión de la Calidad - Requisitos
5.2	ISO 37001 Sistema de Gestión Antisoborno - Requisitos
5.3	ISO 27001 Sistema de Gestión de la Seguridad de la Información - Requisitos
6.	**DISPOSICIONES ESPECIFICAS**
6.1	Las personas en el rol de auditores internos deben cumplir los siguientes criterios: • Deben ser independientes del área auditada.

	• Educación: Grado académico universitario. • Formación: Cursos de Sistemas de Gestión ISO. • Taller: Formación de auditores internos. • Experiencia: Haber laborado al menos 06 meses en el programa (no requerido si se tratáse de un proveedor externo)
6.2	Para desempeñarse en el rol auditor líder debe contar con el siguiente perfil: • Educación: Grado académico universitario. • Formación: Curso de Auditor Interno en Sistemas de Gestión ISO y Curso de Interpretación de la Norma a auditar. • Experiencia mínima: haber participado en el rol de Auditor Líder en 3 oportunidades.
6.3	La participación de los auditores internos en las auditorías, es supervisada por un auditor líder, quien conformará un Equipo de Auditores Internos, el cual deberá ser formalizado y comunicado por la Dirección Ejecutiva a toda la organización, a través de una Resolución Directoral, cuya vigencia será de 1 año.
6.4	Para la realización de auditorías internas, se puede considerar la contratación de un proveedor externo, personal de otros programas o sectores que puedan acreditar sus competencias de acuerdo al ítem 6.1
6.5	Los Sistemas de Gestión Integral del PNAS-Pensión 65 son auditados por lo menos una vez al año.
6.6	El plan de auditoría y los temas relacionados se realiza en función a la importancia y el estado de las actividades o procesos a auditar, a los resultados del proceso de auditorías internas y externas anteriores, considerar las recomendaciones del órgano de control institucional, la matriz de riesgos y oportunidades y las propuestas que el Comité del Sistema de Gestión Integral pueda sugerir como temas auditables.
6.7	El plan de auditoría será elaborado por el Auditor Líder en consenso con el Coordinador de Calidad del Programa, quien comunicará a las jefaturas de unidades participantes, al equipo auditor, al Comité del Sistema de Gestión Integral y a las Unidades involucradas en dicho proceso.
6.8	El responsable de la unidad o área auditada: • Coopera y acompaña (presencialmente o virtualmente) al equipo auditor. • Facilita el acceso a las instalaciones físicas o virtuales, así como facilitar los documentos relevantes para la auditoría. • Propone las acciones correctivas necesarias para corregir las desviaciones (no conformidades) encontradas durante la auditoría. • Identifica de ser necesarios los riesgos y oportunidades como parte de las acciones a tomar.
6.9	En caso la auditoría interna sea realizada por un proveedor externo, se podrán utilizar los formatos de los auditores externos.
6.10	En caso sea necesaria una reprogramación, se deberá actualizar el formato del Programa Anual de Auditorías, en los campos correspondientes.
6.11	El Programa Anual de Auditorías Internas forma parte del Plan Anual de Desarrollo del Sistema de Gestión Integral, el cual es aprobado mediante Resolución Directoral.
7.	**DESARROLLO**

	RESPONSABLE	**DESCRIPCIÓN DE LA ACTIVIDAD**
7.1	Coordinador de Calidad	**Planificación de la auditoría**. Elabora el Programa Anual de Auditorías Internas (Ver Anexo Nº2).
7.2	Director Ejecutivo	Aprueba Programa Anual de Auditorías Internas para el SGI.
7.3	Coordinador de Calidad	Comparte el Programa Anual de Auditorías Internas para el SGI, a través de la intranet o drive de Google del programa y envío por correo electrónicos de ser necesario.
7.4	Equipo Auditor	**Preparación de la auditoría.** Prepara el Plan de Auditoría (Ver Anexo Nº3) definiendo alcances y objetivos.
7.5	Coordinador de Calidad	Comunica el Plan de Auditoría a las áreas a ser auditadas con la debida anticipación. De ser necesario reajusta el cronograma en coordinación con el auditado.

7.6	Equipo Auditor	Revisa la documentación relacionada con los objetivos y alcance de la auditoría, incluyendo informes de auditorías anteriores y no conformidades. Prepara listas de chequeo en base a los criterios de auditoría de los sistemas a auditar.
7.7	Auditor Líder	**Realización de la Reunión de Apertura.** Realiza una reunión de apertura, indicando el objetivo y alcance de la auditoría y la dinámica de su ejecución, entre otros puntos que crea necesario indicar.
7.8	Equipo Auditor	**Ejecución de la auditoría.** Realiza la auditoría buscando evidencias objetivas de la ejecución de los procesos. Concluida la auditoría, el auditor retroalimenta al auditado los hallazgos encontrados en base a los criterios de las normas ISO.
7.9	Equipo Auditor	**Retroalimentación de la Auditoría** Una vez terminada la auditoría, el equipo auditor se reúne para analizar las evidencias obtenidas y elaborar el informe preliminar.
7.10	Auditor Líder	**Realización de la Reunión de Cierre.** Comunicar los resultados del proceso de auditoría mediante un informe preliminar.
7.11	Auditor Líder	**Elaboración del Informe de Auditoría.** El auditor líder elabora el informe de auditoría interna (Ver Anexo Nº4), el cual es presentado al Coordinador de Calidad (representante del comité del SGI).
7.12	Coordinador de Calidad	Con el informe de auditoría se formulan los Planes de Acción de Mejora (PAM) los mismos que son tratados de acuerdo con lo establecido en el Procedimiento Mejora Continua. Comunicar y enviar a la Unidad o Área involucrada el PAM para su implementación, realizar el seguimiento de las acciones formuladas.
7.13	Equipo Auditor	**Actividades de Seguimiento de las Auditorías Internas** Las conclusiones de las auditorias pueden indicar no conformidades detectadas y la necesidad de acciones, correctivas, preventivas o de mejora según sea aplicable, tales acciones serán decididas y emprendidas por el auditado en un intervalo de tiempo acordado y no se considerará como parte de las auditorias posteriores. Las Unidades Orgánica del Programa debe asegurarse de que se tomen las acciones proactivamente, para eliminar las no conformidades detectadas y sus causas. El seguimiento incluye la verificación de la eficacia de las acciones tomadas y estas deben ser informadas al Coordinador de Calidad para el cierre o levantamiento de dicho PAM.
8.	**REGISTROS**	
8.1	Programa Anual de Auditorías Internas.	
8.2	Plan de Auditoría	
8.3	Informe de Auditoría Interna	
9.	**ANEXOS**	
9.1	Anexo 1: Flujograma	
9.2	Anexo 2: Formato Programa de Auditorías Internas	
9.3	Anexo 3: Formato Plan de Auditoría	
9.4	Anexo 4: Formato Informe de Auditoría Interna	

Anexo Nº 1
Flujograma



/

Anexo Nº 2
Formato de Programa Anual de Auditorías

N°	Proceso	Auditor	Responsable del proceso	Mes											
				E	F	M	A	M	J	J	A	S	O	N	D

Reprogramaciones

N°	Mes programado	Reprogramación	Motivo de reprogramación	Observaciones

Fecha: _____

PR-GCAL-02-F01 Vs.03

Anexo Nº 3

Formato de Plan de Auditoría

Nº AUDITORÍA:	**FECHAS DE AUDITORIA:**
TIPO DE AUDITORIA:	**Hora de Inicio: _____ / Hora de cierre: _____**
ALCANCE:	
OBJETIVOS:	
AUDITADOS:	
AUDITORES: **Auditor Líder: _____** **Apoyo: _____** **2do Auditor: _____** **3er Auditor: _____**	
CRITERIOS DE AUDITORIA: **Exclusión:**	

AGENDA

DIA	HORA	PROCESOS A AUDITAR	Personal a Auditar	Autoriza (Jefatura)	Requisito a auditar	AUDITOR

Fecha: ……..

VºBº Auditor Líder

PR-GCAL-02-F02 Vs.02

Anexo Nº 4

Formato de Informe de Auditoría

Nº de auditoria:	**Fecha**:
Objetivos:	
Alcance:	
Auditados:	
Equipo Auditor:	
Criterios de Auditoria:	

RESULTADOS DE LA AUDITORIA

Nº	Incumplimiento/Hallazgo	Genera			Criterio/ Requisito asociado
		No Conformidad	Oportunidad de Mejora	Observación	

CONCLUSIONES

RECOMENDACIONES

Firma del Auditor Líder: _____

Coordinador del SGI_____

Fecha: _____

PR-GCAL-02-F04 Vs.01

REVISIÓN POR LA DIRECCIÓN DEL SISTEMA DE GESTIÓN INTEGRAL

(Vs. 01)

Coordinador de Calidad	Comité de Sistema de Gestión Integral	Dirección Ejecutiva	20/11/2020
Elaborado por	Revisado por	Aprobado por	Fecha de Aprobación
Resolución Directoral:			

Matriz de Control de Cambios en Documentos

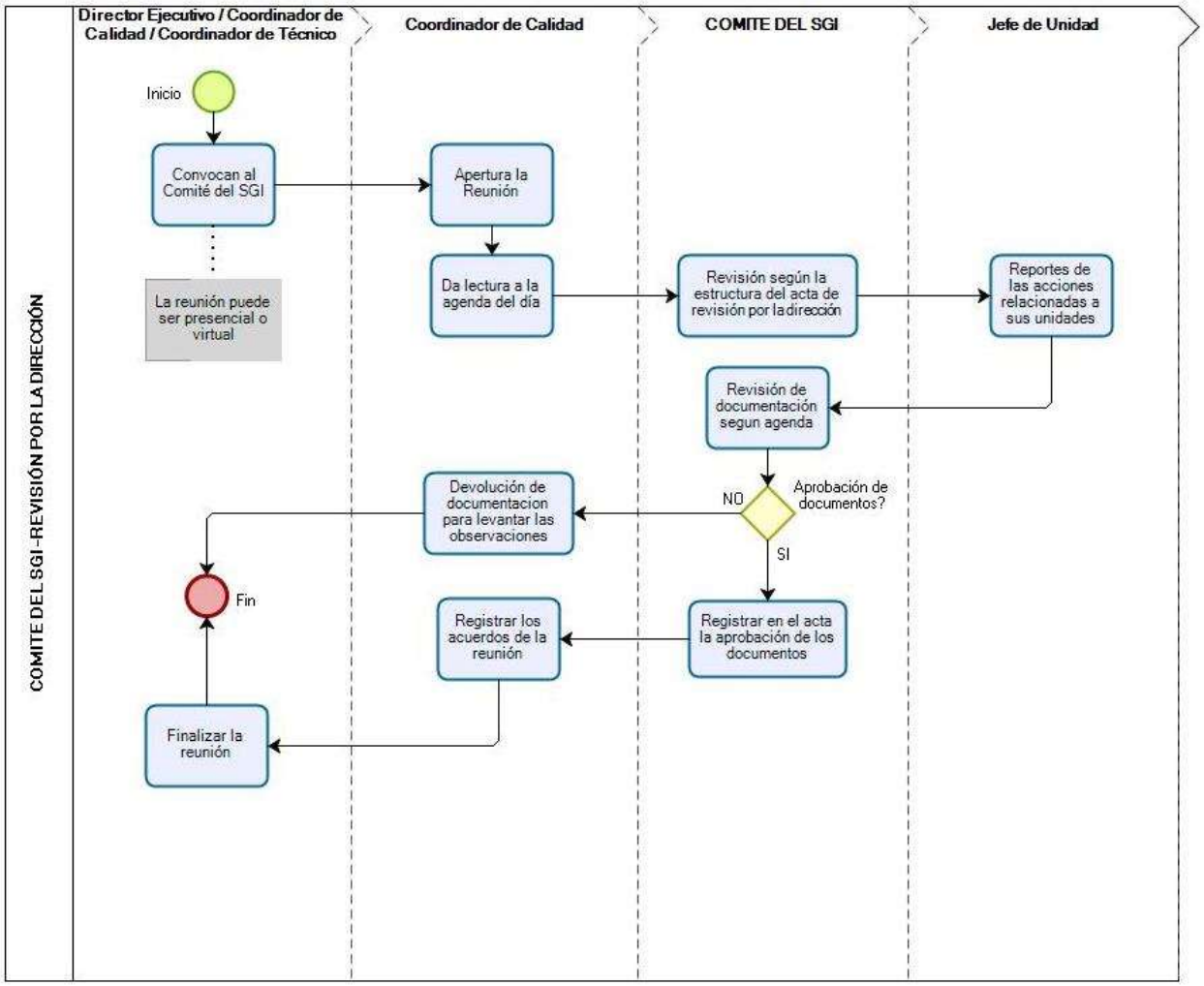
Versión	Ítem	Modificación respecto a la versión anterior	Sustento	Unidad que solicitó el cambio	Observaciones

PR-GCAL-01-F05 Vs.01

1.	**OBJETIVO**
	Establecer los lineamientos para mejorar continuamente la eficacia de los Sistemas de Gestión Integral mediante la Revisión por la Dirección con la finalidad de asegurar su conveniencia, adecuación y eficacia.
2.	**ALCANCE**
	Aplica a los procesos involucrados en los Sistemas de Gestión Integral del Programa Nacional de Asistencia Solidaría – Pensión 65.
3.	**RESPONSABLES**
3.1	Director/a Ejecutivo/a
3.2	Coordinador Técnico
3.3	Coordinador de Calidad
3.4	Comité del Sistema de Gestión Integrado (SGI)
4.	**DEFINICIONES Y ABREVIATURAS**
4.1	**SGI:** Sistema de Gestión Integrado.
4.2	**SGC: Sistema de Gestión de Calidad**
4.3	**SGA: Sistema de Gestión Antisoborno**
4.4	**SSI:** Sistema de Seguridad de la Información
5.	**DOCUMENTOS DE REFERENCIA**
5.1	ISO 9001:2015 – Requisitos
5.2	ISO 37001:2016 - Requisitos
5.3	ISO 27001:2013 - Requisitos
6.	**DISPOSICIONES ESPECIFICAS**
6.1	Preparación: La revisión por la Dirección se realiza en el marco de las reuniones del comité del SGI, y se debe realizar, como mínimo, una vez al año en donde se revisa: a) Políticas b) Estado de las acciones de las Revisiones por la Dirección previas c) Cambios en las cuestiones externas e internas que sean pertinentes para el SGI d) Información sobre el desempeño y la eficacia del Sistema de Gestión Integral: o Retroalimentación del Usuario o Grado de cumplimiento de los Objetivos del SGI o Desempeño de los procesos y conformidad de los servicios. o Estado de las no conformidades, acciones correctivas. o Resultados de seguimiento y medición. o Resultados de las Auditorías. o Desempeño de los Proveedores externos de servicios. o Reportes de los canales de denuncia por soborno, cuando aplique. o Reportes sobre el proceso de investigación de casos por Soborno. o Identificación, contención de los riesgos en materia de sobornos que enfrenta la organización, cuando aplique. e) Identificación de las partes interesadas del SGC y SGA f) Comentarios provenientes de las partes interesadas del SSI g) Adecuación de recursos h) Gestión de los riesgos y las oportunidades del SGI i) Oportunidades de Mejora del SGI Estos puntos pueden ser tratados en una revisión o en revisiones parciales, según su alcance.
6.2	La programación de las reuniones del comité del SGI para tratar temas de la Revisión por la Dirección, se hará una a comienzos del año (recomendable) y quedará registrada en el Plan Anual del Sistema de Gestión Integral, en el OE.04 - Evaluar el nivel de madurez de los procesos del programa (Comités del Sistema de Gestión Integral)

6.3	Las salidas de la revisión por la dirección son: a) Oportunidades de Mejora Continua. b) Cualquier necesidad de Cambio en el SGI. c) Las necesidades de recursos.	
7.	**DESARROLLO**	
	RESPONSABLE	**DESCRIPCION DE LA ACTIVIDAD**
7.1	Director/a Ejecutivo/a Coordinador de Calidad Coordinador Técnico	**Convocatoria:** El Coordinador de Calidad, en coordinación con la Dirección Ejecutiva (Alta Dirección), convoca vía correo electrónico a la reunión de Comité del SGI cuyos miembros son los jefes de las Unidades Orgánicas de la sede central. Esta convocatoria puede ser presencial o virtual.
7.2	Coordinador de Calidad	**Reunión de Apertura**: Apertura la reunión tomando lista de los presentes e indicando el objetivo y alcance de la reunión, los cuales quedan registrados en el Acta de correspondientes (PR-GCAL-06-F01 Vs.02).
7.3	Comité del SGI	Revisan temas según la estructura del acta de revisión, evalúan los reportes de las acciones relacionadas a sus unidades. De requerir se realizará la aprobación de documentos.
7.3	Coordinador de Calidad	Se realiza la devolución de documentos observados (cuando aplique) y se registra los resultados de la reunión en el acta, en donde se incluyen además todas las decisiones y acciones relacionadas con: - Las oportunidades de mejora. - Cualquier necesidad de cambio en el Sistemas de Gestión Integrado. - Las necesidades de recursos.
7.6	Director/a Ejecutivo/a o Coordinador Técnico	Luego de la revisión del SGI, da por concluida la reunión confirmando los acuerdos, decisiones y los plazos para ejecutar las acciones correctivas u oportunidades de mejora, en caso sea aplicable.
7.7	Coordinador de Calidad	Gestionar las acciones correctivas u oportunidades de mejora encontradas en la reunión de Revisión por la Dirección de acuerdo a lo establecido en el Procedimiento de Mejora Continua.
8.	**REGISTROS**	
8.1	Acta de Revisión por la Dirección.	
8.2	Plan Anual del Sistema de Gestión Integrado	
9.	**ANEXOS**	
9.1	Anexo 01: Flujograma	
9.2	Anexo 02: Formato de Registro: Acta de Revisión por la Dirección	

Anexo N°01
Flujograma



Anexo Nº 2
Acta de Revisión por la Dirección

No DE ACTA	LUGAR	FECHA Y Hora de Inicio
00#		dd/mm/aaaa – hh:mm am

AGENDA: LISTA DE CHEQUEO DE TEMAS A TRATAR	
☐	1. Políticas
☐	2. Estado de las acciones de las Revisiones por la Dirección previas
☐	3. Cambios en las cuestiones externas e internas que sean pertinentes para el SGI
☐	4. Información sobre el desempeño y la eficacia del Sistema de Gestión Integral:
☐	4.1. Retroalimentación del Usuario
☐	4.2. Grado de cumplimiento de los Objetivos del SGI
☐	4.3 Desempeño de los procesos y conformidad de los servicios.
☐	4.4 Estado de las no conformidades, acciones correctivas.
☐	4.5. Resultados de seguimiento y medición
☐	4.6. Resultados de las Auditorías
☐	4.7. Desempeño de los Proveedores externos de servicios.
☐	4.8. Reportes de los canales de denuncia por soborno, cuando aplique
☐	4.9. Reporte sobre el proceso de investigación de casos por soborno.
☐	4.10. Identificación, contención de los riesgos en materia de sobornos que enfrenta la organización.
☐	5. Identificación y comentarios (cuando aplique) de las partes interesadas del SGC y SGAS
☐	6. Comentarios provenientes de las partes interesadas del SSI
☐	7. Adecuación de recursos
☐	8. Gestión de los riesgos y las oportunidades del SGI
☐	9. Oportunidades de Mejora del SGI
☐	10. Resultados de la Revisión por la Dirección
☐	11. Cierre y Aprobación del Acta de Revisión por la Dirección.

DESARROLLO DE LA REUNION

1. POLÍTICAS

2. ESTADO DE LAS ACCIONES DE LAS REVISIONES POR LA DIRECCIÓN PREVIAS

3. CAMBIOS EN LAS CUESTIONES EXTERNAS E INTERNAS QUE SEAN PERTINENTES PARA EL SGI

4. INFORMACIÓN SOBRE EL DESEMPEÑO Y LA EFICACIA DEL SISTEMA DE GESTIÓN INTEGRADO:

4.1 RETROALIMENTACION DEL USUARIO

4.1.1 RESULTADOS DE ENCUESTA DE SATISFACCIÓN

4.1.2 QUEJAS Y RECLAMOS DE LOS USUARIOS

4.2 GRADO DE CUMPLIMIENTO DE LOS OBJETIVOS DEL SGI

4.3 DESEMPEÑO DE LOS PROCESOS Y CONFORMIDAD DEL SERVICIO.

4.4 ESTADO DE LAS NO CONFORMIDADES, ACCIONES CORRECTIVAS.

4.4.1 ACCIONES CORRECTIVAS

Tabla de no conformidades - Resumen

PROCESOS	NO CONFORMIDAD / Oportunidad de Mejora	ESTADO ACCION CORRECTIVA	
		ABIERTA	CERRADA
ESTRATEGICOS			
SISTEMAS DE GESTION			
OPERATIVOS			
SOPORTE-APOYO			

4.5 RESULTADOS DE SEGUIMIENTO Y MEDICIÓN

Procesos	Actividad	Responsable	Fecha de Revisión	Ejecución

4.6 RESULTADO DE LAS AUDITORIAS

No De Auditoria	Fecha	Proceso / Sistema de Gestión	Numero de no Conformidades

4.7 DESEMPEÑO DE LOS PROVEEDORES EXTERNOS DE SERVICIOS.

4.8 REPORTES DE LOS CANALES DE DENUNCIA POR SOBORNO, CUANDO APLIQUE

4.9 REPORTE SOBRE EL PROCESO DE INVESTIGACION DE CASOS POR SOBORNO, CUANDO APLIQUE

4.10 IDENTIFICACIÓN, CONTENCIÓN DE LOS RIESGOS EN MATERIA DE SOBORNOS QUE ENFRENTA LA ORGANIZACIÓN.

5. IDENTIFICACIÓN DE LAS PARTES INTERESADAS DEL SGC y SGA

6. COMENTARIOS PROVENIENTES DE LAS PARTES INTERESADAS DEL SSI

7. ADECUACIÓN DE RECURSOS

8. GESTIÓN DE LOS RIESGOS Y LAS OPORTUNIDADES DEL SGI

9. OPORTUNIDADES DE MEJORA DEL SGI

9.1 ACCIONES DE MEJORA DEL SGC-SGAS Y DE LOS PROCESOS.

Proceso	Actividad	Responsable	Fecha de Revisión

10. RESULTADOS DE LA REVISIÓN POR LA DIRECCIÓN

Oportunidades de Mejora Continua

Cualquier necesidad de Cambio en el SGI

Las necesidades de recursos

11. CIERRE Y APROBACION DEL ACTA DE REVISION POR LA DIRECCION

Siendo las _____ horas se dio por finalizada la reunión.
En constancia firman.

ASISTENTES		
NOMBRE	**CARGO**	**FIRMA**

MEJORA CONTINUA DEL SISTEMA DE GESTION INTEGRAL

(Vs. 01)

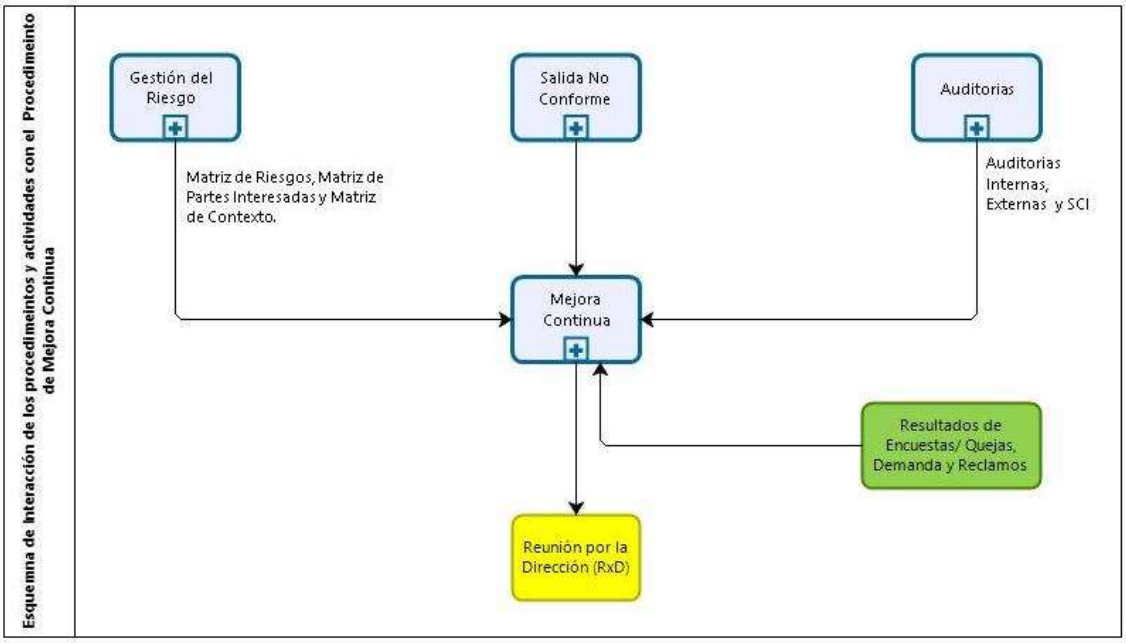
Coordinador de Calidad	Comité del Sistema de Gestión Integral	Dirección Ejecutiva	31/08/2022
Elaborado por	Revisado por	Aprobado por	Fecha de Aprobación
Resolución Directoral N°			

Matriz de Control de Cambios en Documentos

Versión	Ítem	Modificación respecto a la versión anterior	Sustento	Unidad que solicitó el cambio	Observaciones

PR-GCAL-01-F05 Vs.01

1.	**OBJETIVO**
	Establecer los lineamientos necesarios para la toma de acciones de mejora que pueden ser del tipo correctivo y/o preventivo, con la finalidad de identificar y/o eliminar las causas que originan las no conformidades del tipo reales o potencial, tratando de prevenir su repetición; mejorando para ello los procesos de los sistemas de gestión de la organización.
2.	**ALCANCE**
	El presente procedimiento aplica a las acciones correctivas, oportunidades de mejoras y salidas no conformes; orientadas a minimizar o eliminar las causas que lo originan, sean reales o potenciales, Esta se inicia desde la identificación de la desviación o hallazgo (no conformidad) hasta el seguimiento y cierre de los Planes de Acción de Mejora (PAM).
3.	**RESPONSABLES**
3.1	Coordinador de Calidad: Responsable de gestionar la ejecución de los Planes de Acción de Mejora.
3.2	Personal del programa: Responsable de identificar y reportar las salidas No Conformes de sus respectivos procesos.
4.	**DEFINICIONES Y ABREVIATURAS**
4.1	**No Conformidad (NC):** Incumplimiento a una Normativa, Reglamento, Ley, Directiva, Cláusula de Contrato y/o Convenio etc.
4.2	**No Conformidad Menor (NCm):** Incumplimiento que solo afecta parcialmente a un punto de la norma de los sistemas de gestión implementados en el Programa.
4.3	**No Conformidad Mayor (NCM):** Incumplimiento que afecta a un punto completo de la norma de los sistemas de gestión implementados en el Programa.
4.4	**Salidas No Conforme (SNC)**: Es el resultado de un proceso que no cumple requisitos, pautas, estándares de calidad o lineamientos específicos; que origina una No conformidad o desviación de los parámetros convencionalmente establecidos.
4.5	**Plan de Acción de Mejora (PAM):** Se utiliza cuando: a) Apertura una mejora de un proceso, producto de hallazgos en las auditorías internas y/o externas; u otra actividad de similar criterio. b) Como producto de la identificación de las salidas de “No Conformes”; resultado de actividades que requieren corrección inmediata, u oportunidades de mejora que son identificadas en los procesos de la organización. c) También generan los PAM las consideradas “fallas” o “errores” producidos por los sistemas informáticos, los servicios que presta el programa, procesos en general. d) Las DQR (Denuncias, Quejas y Reclamos). e) Los resultados de las encuestas también suelen ser una fuente de oportunidades de mejora para desarrollar un PAM.
4.6	**Potencial No Conformidad (PNC):** Incumplimiento que no ha ocurrido aún; pero, si no se toman las acciones correspondientes terminará ocurriendo, convirtiéndose en un incumplimiento real.
4.7	**Acción Correctiva:** Es aquella que busca eliminar la causa raíz de una no conformidad o salida no conforme presentada, de un defecto o de cualquier otra situación indeseable existente para evitar que vuelva a ocurrir.
4.8	**Acción Preventiva**: Es aquella que busca eliminar la causa de una no conformidad presentada, de un defecto o de cualquier otra situación indeseable potencial existente para evitar que ocurra.
4.9	**Oportunidad de Mejora (OM):** Es aquella que se implementa sin de que por medio exista una no conformidad y se origina por una iniciativa de mejora
4.10	**Efectos o consecuencia**: Son aquellas situaciones originadas por las desviaciones identificadas.
4.11	**Mejora Contínua:** Es un conjunto de actividades coordinadas y controladas llevadas a cabo para lograr un objetivo que permita la mejora permanente del Sistema de Gestión en el PNAS-Pensión 65.
4.12	**Plan de Mejoramiento**: conjunto de actividades coordinadas y controladas llevadas a cabo para lograr un objetivo que permita la mejora continua.
4.13	**5 ¿Por qué?:** Técnica básica para analizar las causas que originan un problema. Consiste en realizar preguntas repetitivas, para explorar las relaciones de causa y efecto subyacentes a un problema particular.[1] El objetivo principal de la técnica es determinar la causa raíz de un defecto o problema repitiendo la pregunta "¿Por qué?". Cada respuesta forma la base de la siguiente pregunta. El "5" en el

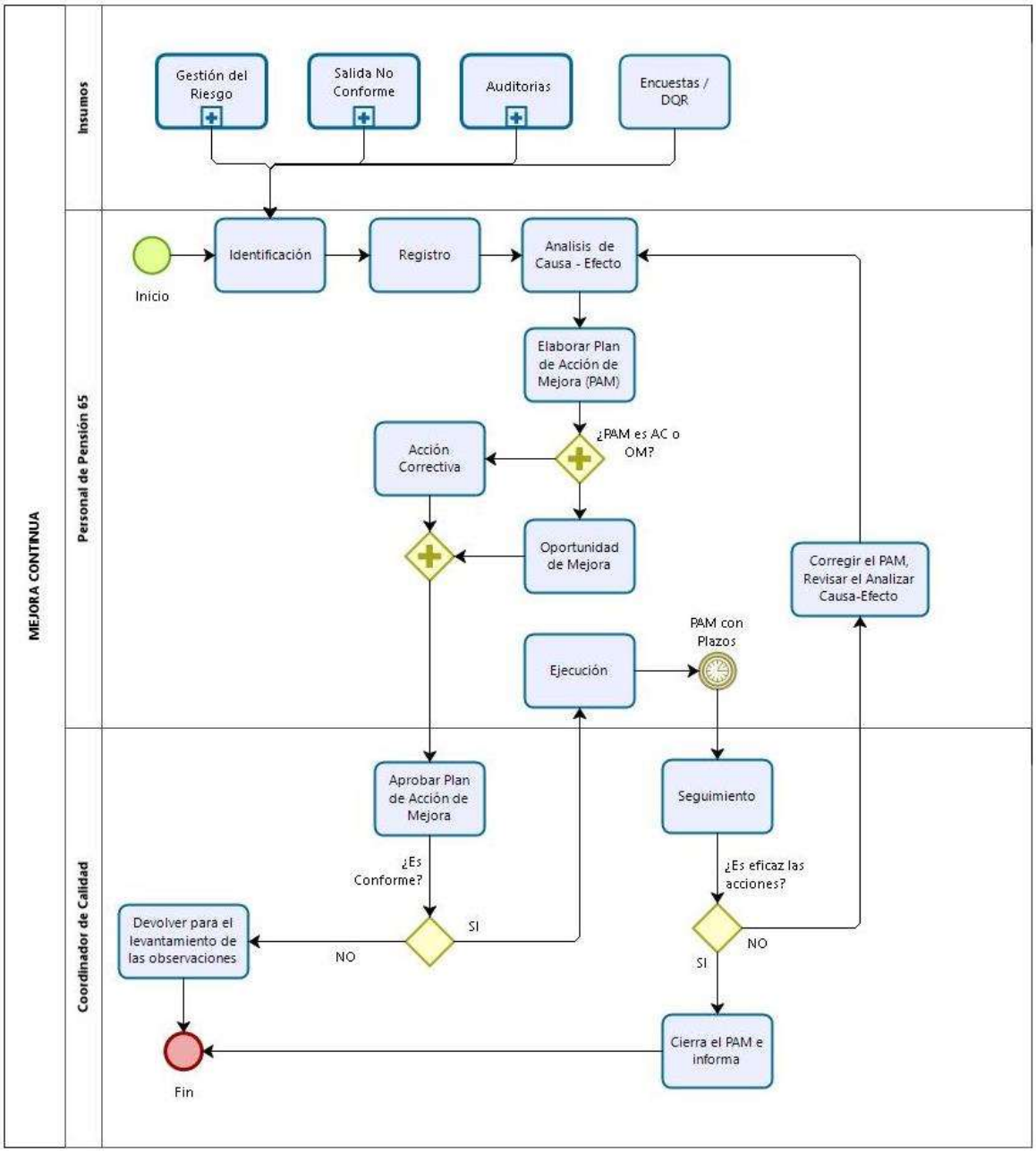
	nombre se deriva de la observación empírica en el número de iteraciones típicamente requeridas para resolver el problema.
4.14	**Diagrama de Ishikawa:** Diagrama de causa y efecto representado de manera gráfica, que ayuda a levantar las causas-raíces de un problema, analizando todos los factores que involucran la ejecución del proceso. Comúnmente conocida como espina de pescado, es una herramienta que complementa el análisis, logrando que las alternativas de soluciones sean más precisas.
5.	**DOCUMENTOS DE REFERENCIA**
5.1	Norma ISO 9001:2015
5.2	Norma ISO 37001:2016
5.3	Norma ISO 27001:2013
5.4	Procedimiento de Auditorías Internas en el SGI
5.5	Procedimiento de Salidas No Conforme.
5.6	Procedimiento de Gestión de Riesgos y Oportunidades
6.	**DISPOSICIONES ESPECIFICAS**
6.1	Una acción correctiva y/o de mejora es eficaz si cumple el objetivo planteado.
6.2	En el caso que las acciones correctivas no sean efectivas o exitosas, se procederá a generar una actualización del PAM o de ser el caso un nuevo Plan de Acción de Mejora.
6.3	Las no conformidades reales o potenciales pueden detectarse después de llevarse a cabo la acción o de ocurrir alguno de los eventos que se indican a continuación: a) Actividades de rutina en cualquiera de las áreas de Pensión 65. b) Como consecuencia de una Salida No Conforme. c) Revisión del Sistema de gestión Integral (SGI) por parte de la Dirección. d) Auditorías internas y/o Auditorías externas. e) Resultados de los registros de denuncias, quejas y reclamos. f) Resultados de las mediciones de la satisfacción del cliente (encuestas) g) Otros
6.4	Interacción del Procedimiento de Mejora Contínua con los otros documentos normativos como el de Gestión de Riesgos, Salidas No Conformes y Auditorías internas y externas, entre otros. 

7.	DESARROLLO	
	RESPONSABLE	**DESCRIPCIÓN DE LA ACTIVIDAD**
7.1	Personal de P65	**Identificación de las Salidas No Conformes, Acciones Correctivas u Oportunidades de Mejora.** Analizar información proveniente de: – Actividades de rutina en cualquiera de las unidades de Pensión 65 (Salida No Conforme) – Matriz de Monitoreo del Plan de Acción de Mejora (PAM). – Desempeño de los indicadores de gestión. – Denuncias, Quejas y/o Reclamos (DQR). – Incumplimiento de requisitos legales o normativos. – Sistema de Control Interno – Gestión de los riesgos y oportunidades – Análisis del contexto de la organización. – Revisión por la Dirección. – Auditorías internas o externas. – Resultados de las encuestas a los usuarios – Determinación de los requisitos de las partes interesadas.
7.2	Personal de P65	**Registro de las Salidas No Conformes, Acciones Correctivas u Oportunidades de Mejora** De acuerdo a la información analizada, definir si se genera: – Acción Correctiva – Oportunidad de Mejora
7.3	Personal de P65	**Análisis de Causa** Identifica y analiza la causa raíz de la No Conformidad y registrar en el formato Plan de Acción de Mejora, pudiendo emplear la metodología de los 5 por qué o del diagrama de Ishikawa. En caso de Oportunidad de Mejora describir el objetivo
7.4	Personal de P65	**Plan de Acción de Mejora (PAM)** Registra en el formato Plan de Mejora (Anexo N°02) el plan de acción considerando las actividades a desarrollar, responsables, fechas de inicio-fin y los recursos orientado a: - Erradicar la(s) causa(s) raíz (ces) de la No Conformidad - Lograr el objetivo de mejora Envía la acción correctiva y/o de mejora al Jefe de Área para su revisión.
7.5	Personal de P65	**Acción Correctiva** Plantear la acción inmediata a fin de corregir desviaciones de las No Conformidades.
7.6	Personal de P65	**Oportunidad de Mejora** Plantear las acciones que correspondan con la finalidad de evitar la el riesgo de materialización de una no conformidad o de mejorar la eficacia de los procesos.
7.7	Coordinador de Calidad	**Aprobación del Plan de Acción de Mejora** Evalúa y aprueba el registro Plan de Acción de Mejora, caso contrario señalar las observaciones para las correcciones necesarias.
7.8	Personal de P65	**Ejecución del Plan de Acción de Mejora** Ejecuta lo establecido en el registro Plan de Acción de Mejora, registrar el avance y cumplir los plazos establecidos.
7.9	Coordinador de Calidad / Auditores Internos	**Seguimiento y Verificación de la Eficacia:** Realiza el seguimiento de los Planes de Acción de Mejora (PAM) y verifica la eficacia de las acciones tomadas. Registra en el formato seguimiento a los Planes de Acción de Mejora (Anexo 03), finalizando la implementación y dar por cerrado el PAM.

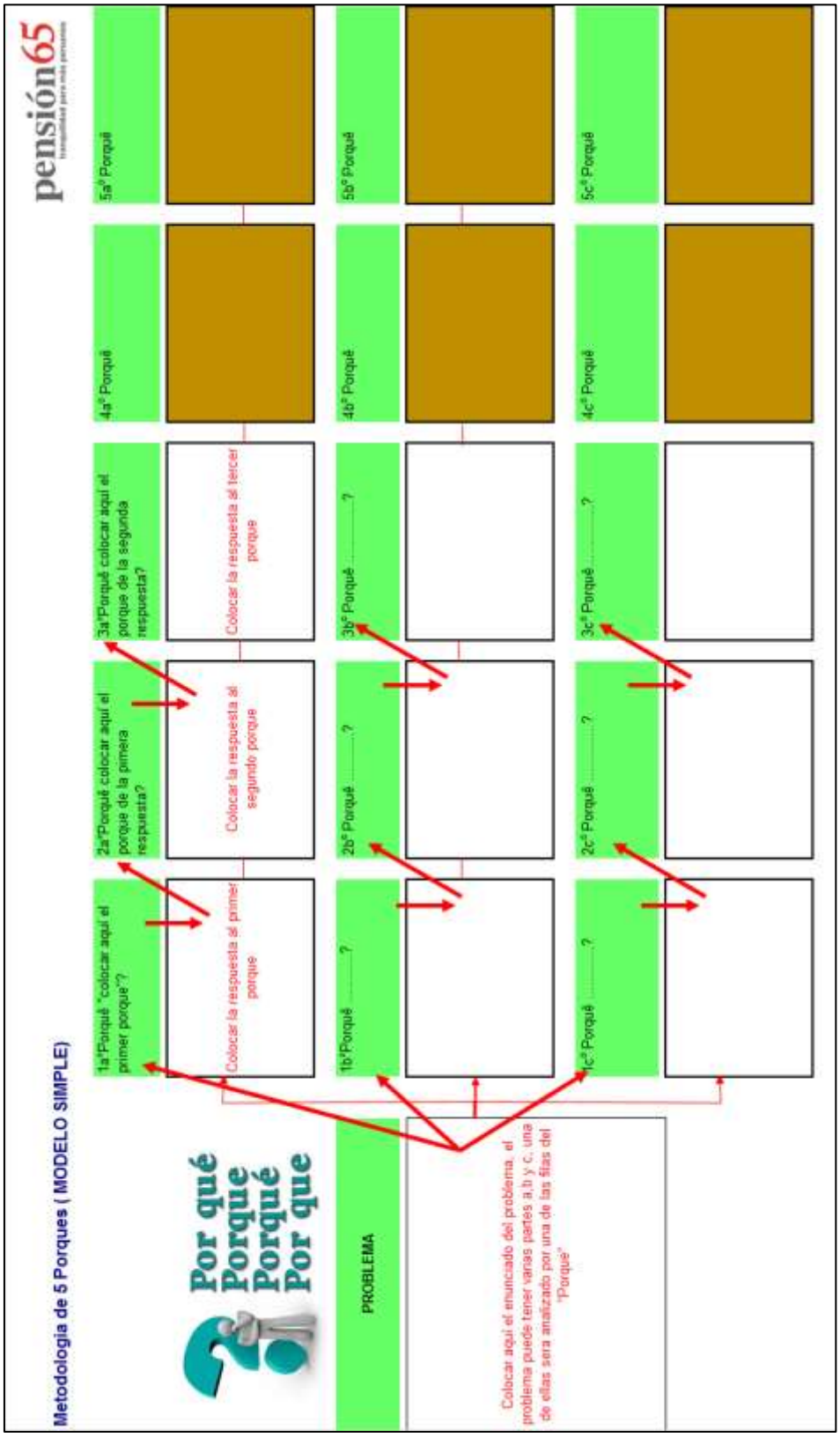
8.	**REGISTROS**
8.1	Plan de Acción de Mejora (PAM)
9.	**ANEXOS**
9.1	Anexo 1: Flujograma de Mejora Continua
9.2	Anexo 2: Metodología de los 5 ¿Porqués?
9.3	Anexo 3: Formato de Plan de Acción de Mejora
9.4	Anexo 4: Matriz de Seguimiento a los Planes de Mejora
9.5	Anexo 5: Matriz de Identificación y Tratamiento de Salidas No Conformes

Anexo Nº 01

Flujograma: Mejora Continua



Anexo N°02



Anexo Nº 03

PENSIÓN65 — **PLAN DE ACCION DE MEJORA**

Unidad / Proceso: | N°:
Plazo: | Fecha de Emisión:

Tipos de Hallazgos
Salida No Conforme: ☐
No Conformidad: ☐
Oport. de Mejora: ☐

Fallo Identificado en:
SISTEMA INFORMATICO: ☐
SERVICIO: ☐
PROCESO: ☐
DQR: ☐

1. DESCRIPCIÓN DEL HALLAZGO IDENTIFICADO

Identificado por: | fecha
Proceso / Unidad:

2. OBJETIVO O FINALIDAD (Para el caso de Oportunidades de Mejora)

Elaborado por: | fecha

3. CORRECCIÓN (Para los casos de Salidad NC y No Conformidades.)

Verificado por: | fecha ___/___/___

4. ANALISIS DE CAUSA (para el caso de acciones correctivas).

Responsable: | fecha ___/___/___

5. PLAN DE ACCION PARA LA MEJORA CONTINUA

Actividades	Responsables	Programado	Real	Observaciones
		___/___/___	___/___/___	
		___/___/___	___/___/___	
		___/___/___	___/___/___	
		___/___/___	___/___/___	
		___/___/___	___/___/___	

6. EFICACIA DE LAS ACCIONES PROPUESTAS

Fecha Programada ___/___/___ | Fecha Ejecutada ___/___/___

Conforme: ☐
No Conforme: ☐

Observaciones:

Responsable de la Unidad /Area | Aprobado por

Anexo N° 04

MATRIZ DE BASE DE DATOS PARA EL MONITOREO DE PLANES DE ACCION Y MEJORA CONTINUA (nombre de columnas)

MATRIZ DE BASE DE DATOS PARA EL MONITOREO DE PLANES DE ACCION Y MEJORA CONTINUA pensión65

N°	Fecha1 de Registro	Sis.Ges	Tipo Tratamiento	Tipo Hallazgo	Origen	Descrip_1	Identificado por	Ubicado en	Accion Inmediata	Unidad /Area

Unidad / Area Responsable	Fecha2 de realizada la accion	Analisis de Causa_Efecto	Elaborado por	Fecha3 de elaboracion	Tipo de Accion	Descrip_2	N°Plan. Acc	Actividades	Responsable2	F4.Program

F5.Ejecuc	Tipo de Mejora	Obs.1	Responsables	Aprobado	Verificado por	Fecha6 programada para la Verificació	Verificación de la Efectividad de la Implementaci	Descrip_3	Calificación	Resp.Verif/ Auditor

Fecha/ Cierre	Fecha8 de Prox.Plazo	ESTADO	Archivo	Observaciones	Evidencias

Anexo Nº 05

Matriz de Identificación y Tratamiento de Salidas No Conformes

N°	Salida No Conforme	Descripción del Tratamiento
1	Afiliación de un Usuario que no cumple los requisitos establecidos en el DS 081-2011.	1. Revisión y/o actualización del padrón de usuarios en el proceso Afiliaciones. 2. Solicitud de la actualización de datos a RENIEC 3. Retiro del usuario de la RBU y activación del proceso de recupero (cuando aplique) 4. Generar un plan de acción de mejora en casos de repetitividad
2	Transferencia de un monto mayor o menor a la emitida en la carta orden	1. Revisión de la Transferencia emitida en el proceso de subvenciones monetarias. 2. Solicitud del monto recibido por el Banco de la Nación. 3. Solicitud de la devolución del monto excedido (monto mayor). 4. Generación de la nueva carta orden por el monto faltante (monto menor). 5. Generar un plan de acción de mejora en casos de repetitividad.
3	Transferencia Monetaria a Usuario (por (desfase en el reporte de fallecidos por RENIEC)	1. Actualización de la data enviada por RENIEC 2. Solicitud de extorno del dinero al Banco de la Nación 3. Activación del proceso de recuperos (cuando aplique) 4. Generar un plan de acción de mejora en casos de repetitividad.
4	Incumplimiento de un requisito determinado en las Actas de Acuerdos u Ordenanzas Municipales para la implementación de los Saberes Productivos.	1. Identificar a las partes involucradas en la implementación de la intervención. 2. Revisión de la última asistencia técnica brindada por Pensión 65. 3. Revisión de las últimas actas de acuerdos. 4. Visita técnica extraordinaria (cuando aplique) 5. Generar un Plan de Mejora en casos de repetitividad.
5	Usuario no incorporado en la RBU, por fallas en actualización de los cotejos que determinan cambios en su CSE (SISFOH), la actualización de datos (RENIEC) o por cobro de pensiones públicas o privadas.	1. Identificar a los usuarios afectados por este tipo de fallo. 2. Solicitar la confirmación o revalidación con las entidades (SISFOH, RENIEC u otras), que han afectado a los usuarios en el proceso de su cotejo. 3. Confirmar con la Unidad de Planeamiento, Presupuesto y Modernización, la habilitación de la partida presupuestal para poder emitir una RUA[1]

[1] Modificación de la Directiva de gestión de la entrega de la subvención monetaria, RD N°162-2019-MIDIS/P65-DE, del 20/12/2019, numeral 5.11 y 6.2

SALIDAS NO CONFORME DEL SISTEMA DE GESTION INTEGRAL

(Vs. 01)

Coordinador de Calidad	Comité del Sistema de Gestión Integral	Director Ejecutivo	31/08/2022
Elaborado por	Revisado por	Aprobado por	Fecha de Aprobación
Resolución Directoral N° ……			

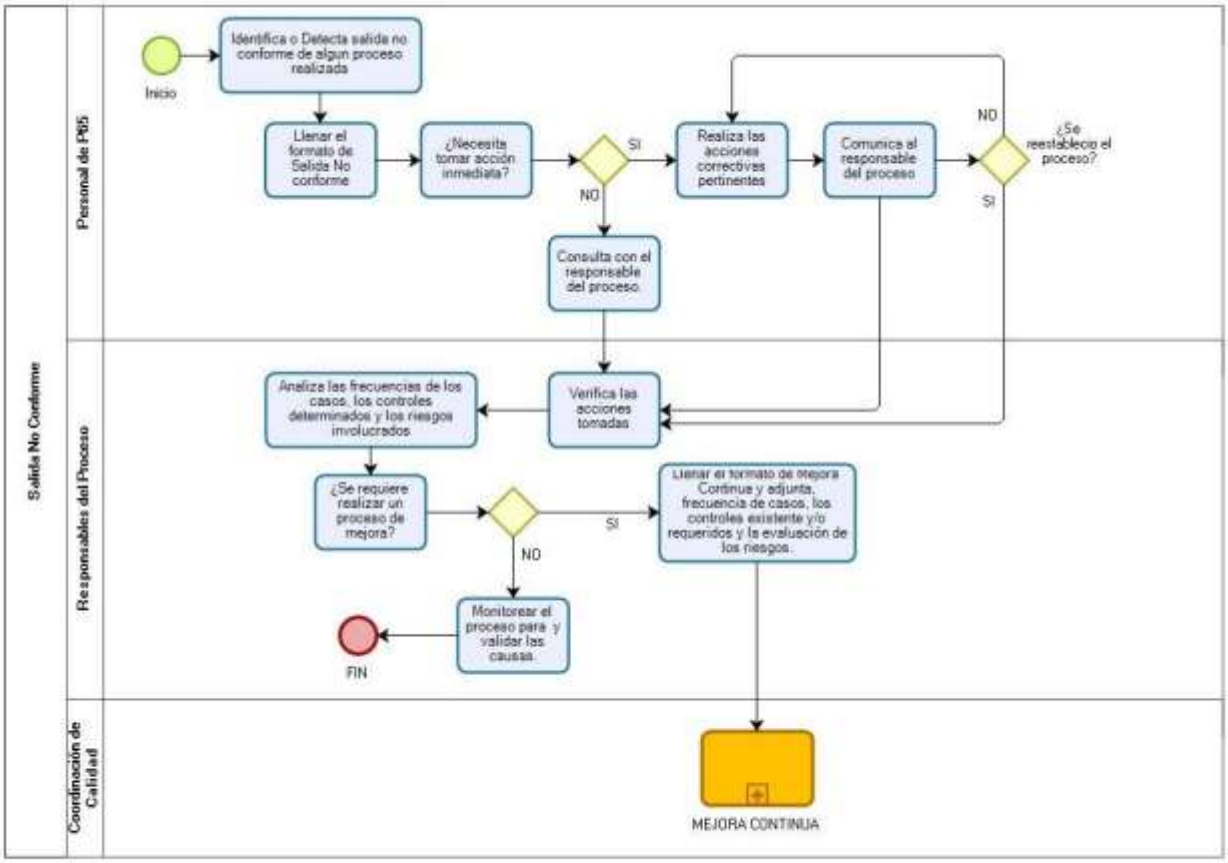
Matriz de Control de Cambios en Documentos

Versión	Ítem	Modificación respecto a la versión anterior	Sustento	Unidad que solicitó el cambio	Observaciones

1.	**OBJETIVO**	
	Establecer los lineamientos para identificar y controlar las salidas no conformes de los procesos ejecutados en la organización, a fin de implementar planes de acción que instruyan su corrección o mejora de dichos procesos.	
2.	**ALCANCE**	
	Todos los procesos que por su naturaleza tengan probabilidades de identificar salida no conforme, durante el desarrollo de los procesos del Programa Pensión 65.	
3.	**RESPONSABLES**	
3.1	Jefe de la Unidad Orgánica (sede central)	
3.2	Jefe de la Unidad Territorial.	
3.2	Coordinador de Calidad	
3.3	Personal del Programa	
4.	**DEFINICIONES Y ABREVIATURAS**	
4.1	**Servicio:** Resultado de un proceso (puede ser un bien o servicio).	
4.2	**Salida No Conforme (SNC)**: Actividad, servicio o producto, que después de haber pasado por un proceso o procesos de transformación, sus criterios de conformidad registran el no cumplimiento con los requisitos convencionalmente establecidos.	
5.	**DOCUMENTOS DE REFERENCIA**	
5.1	Norma ISO 9001:2015	
5.2	Norma ISO 27001:2013	
5.3	NTP ISO 31000:2018 – Gestión del Riesgo	
5.4	Resolución de Contraloría General N°458-2008-CG “Guía para la implementación del Sistema de Control Interno en las entidades del Estado”	
5.5	Procedimiento de Mejora Contínua	
6.	**DISPOSICIONES ESPECIFICAS**	
	No Aplica	
7.	**DESARROLLO**	
	RESPONSABLE	**DESCRIPCION DE LA ACTIVIDAD**
7.1	Personal de P65	Identifica o detecta de Salida No Conforme, después de verificar los requisitos de conformidad del proceso, estos pueden ser estandarizados como requisitos convencionalmente adoptados por quien recibe y por quien entrega el producto, servicio o bien.
7.2	Personal de P65	Llenar el formato de Salida No Conforme (SNC), es importante anotar la descripción de la SNC y que requisitos incumple si corresponde, así como los tratamientos inmediatos que se hubiere aplicado.
7.3	Personal de P65	Toma acciones inmediatas necesarias para el control del SNC, de acuerdo a la responsabilidad y autoridad asignada. De no estar seguro de las acciones a tomar, es necesario que haga las consultas correspondientes al responsable del proceso (Coordinador o jefe inmediato).
	Personal de P65	De no reestablecerse el proceso, realizar un análisis de causas y consultar con el responsable del proceso para su implementación y monitoreo.
7.3	Responsable del Proceso	Verifica que las acciones tomadas y/o implementadas aseguren el levantamiento del SNC y reestablezcan las condiciones satisfactorias del proceso.
7.4	Responsable del Proceso	Analizar las frecuencias de los casos de SNC identificados, los controles determinados en cada caso y los riesgos involucrados. Con la información recabada, validar si se requiere realizar un proceso de mejora contínua; de no ser necesario, solicitar el monitoreo del proceso para validar las causas.

7.5	Responsable del Proceso	De requerir el proceso una mejora, llenar el formato indicado según el procedimiento de Mejora Continua y adjuntar, las frecuencias de casos reportados, los controles existentes y/o requeridos y la evaluación de los riesgos.
7.6	Coordinador de Calidad	Recibirá la propuesta de mejora contínua del proceso, y procederá según el procedimiento de Mejora Continua.
8.	**REGISTROS**	
8.1	Registro de Servicio No Conforme. Plan de Acción de Mejora (PAM)	
9.	**ANEXOS**	
9.1	Anexo 1: Flujograma de Salida No Conforme	
9.2	Anexo 2: Formato de Registro de Salida No Conforme	
9.3	Anexo 3: Formato de Plan de Acción de Mejora.	
9.4	Anexo 4: Matriz de Identificación y Tratamiento de Salidas No Conformes	

Anexo Nº01 Flujograma



Anexo Nº02

pensión65 tranquilidad para más peruanos

REGISTRO DE SALIDA NO CONFORME

N° ____

1. IDENTIFICACION

Fecha:	___/___/___	Unidad / Area:	
Identificado por:		Proceso:	

2. DESCRIPCION DE LA SALIDA NO CONFORME

3. TRATAMIENTO DE LA SALIDA NO CONFORME

Responsable:		fecha	___/___/___

4. SEGUIMIENTO A LA SALIDA NO CONFORME

Item	Fechas	Acciones	Responsables	Observaciones
	___/___/___			
	___/___/___			
	___/___/___			
	___/___/___			
	___/___/___			
	___/___/___			
	___/___/___			

Anexo Nº03

pensión65

PLAN DE ACCION DE MEJORA

N° _____

Unidad Orgánica /UT: _____ Fecha Emisión: __/__/____ Plazo: ____

Tipo de Acción:

Salidas No Conforme ☐ Acción Correctiva ☐ Oportunidad de Mejora ☐

Identificado / originado por:

No Conformidad (menor) ☐	Sist.Informatico: ☐	Gestión de Riesgo: ☐
Auditoría Interna: ☐	Proceso: ☐	Encuestas: ☐
Auditoría Externa: ☐	DQR: ☐	Otros: ☐

DESCRIPCIÓN

Identificado por: _____ fecha __/__/__

ANALISIS DE CAUSA Y EFECTO (para acciones correctivas)

OBJETIVO (Para Oportunidades de Mejora)

CORRECCIÓN (Para Salidas No Conformes y Acciones Correctivas)

PLAN DE ACCION DE MEJORA

Actividades	Responsables	Programado	Real	Observaciones

Responsable: _____

Puesto: _____ Aprobado: _____

EFECTIVIDAD DE LAS ACCIONES DE MEJORA

Conforme: ☐ Fecha programada: __/__/__

No Conforme: ☐ Fecha ejecutada: __/__/__

Verificado por:

Observaciones:

Nuevo plazo de Verificacion: __/__/__

Fecha de cierre: __/__/__

V°B° Coordinador de Calidad

Anexo Nº04
Matriz de Identificación y Tratamiento de Salidas No Conformes

N°	Salida No Conforme	Descripción del Tratamiento
1	Afiliación de un Usuario que no cumple los requisitos establecidos en el DS 081-2011.	1. Revisión y/o actualización del padrón de usuarios en el proceso Afiliaciones. 2. Solicitud de la actualización de datos a RENIEC 3. Retiro del usuario de la RBU y activación del proceso de recupero (cuando aplique) 4. Generar un plan de acción de mejora en casos de repetitividad
2	Transferencia de un monto mayor o menor a la emitida en la carta orden	1. Revisión de la Transferencia emitida en el proceso de subvenciones monetarias. 2. Solicitud del monto recibido por el Banco de la Nación. 3. Solicitud de la devolución del monto excedido (monto mayor). 4. Generación de la nueva carta orden por el monto faltante (monto menor). 5. Generar un plan de acción de mejora en casos de repetitividad.
3	Transferencia Monetaria a Usuario (por (desfase en el reporte de fallecidos por RENIEC)	1. Actualización de la data enviada por RENIEC 2. Solicitud de extorno del dinero al Banco de la Nación 3. Activación del proceso de recuperos (cuando aplique) 4. Generar un plan de acción de mejora en casos de repetitividad.
4	Incumplimiento de un requisito determinado en las Actas de Acuerdos u Ordenanzas Municipales para la implementación de los Saberes Productivos.	1. Identificar a las partes involucradas en la implementación de la intervención. 2. Revisión de la última asistencia técnica brindada por Pensión 65. 3. Revisión de las últimas actas de acuerdos. 4. Visita técnica extraordinaria (cuando aplique) 5. Generar un Plan de Mejora en casos de repetitividad.
5	Usuario no incorporado en la RBU, por fallas en actualización de los cotejos que determinan cambios en su CSE (SISFOH), la actualización de datos (RENIEC) o por cobro de pensiones públicas o privadas.	1. Identificar a los usuarios afectados por este tipo de fallo. 2. Solicitar la confirmación o revalidación con las entidades (SISFOH, RENIEC u otras), que han afectado a los usuarios en el proceso de su cotejo. 3. Confirmar con la Unidad de Planeamiento, Presupuesto y Modernización, la habilitación de la partida presupuestal para poder emitir una RUA[1]

[1] Modificación de la Directiva de gestión de la entrega de la subvención monetaria, RD N°162-2019-MIDIS/P65-DE, del 20/12/2019, numeral 5.11 y 6.2

GESTIÓN DE RIESGOS Y OPORTUNIDADES DEL SISTEMA DE GESTION INTEGRAL

(Vs.01)

Coordinador de Calidad	**Comité del Sistema de Gestión Integral**	**Director Ejecutivo**	31/08/2022
Elaborado por	Revisado por	Aprobado por	Fecha de aprobación

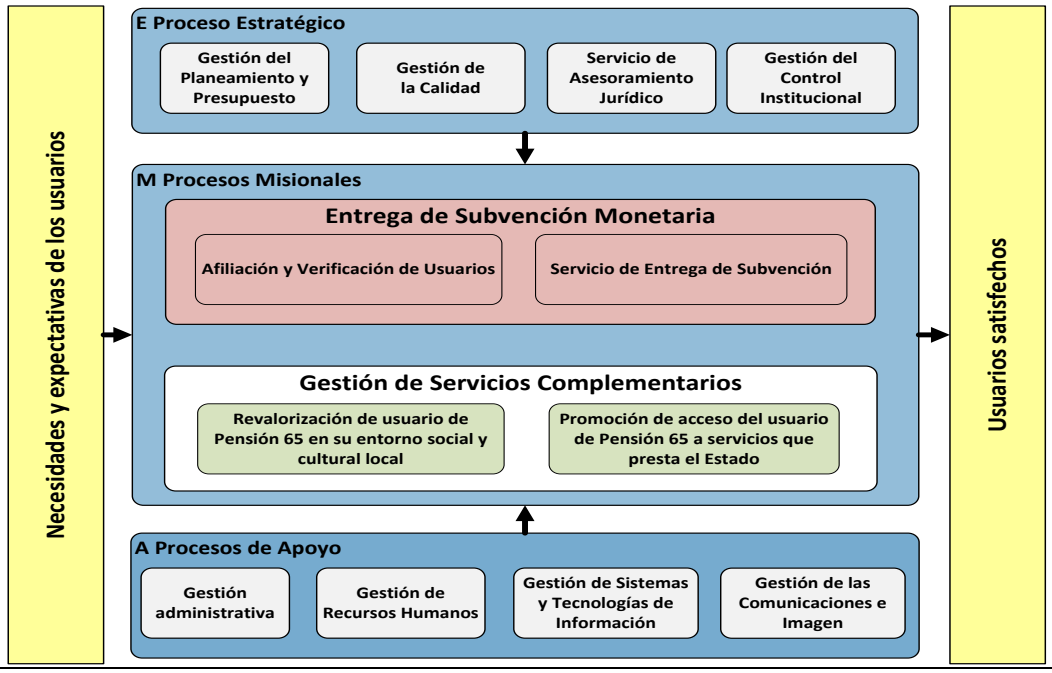
Resolución Directoral N° ……

Matriz de Control de Cambios en Documentos

Versión	Ítem	Modificación respecto a la versión anterior	Sustento	Unidad que solicitó el cambio	Observaciones

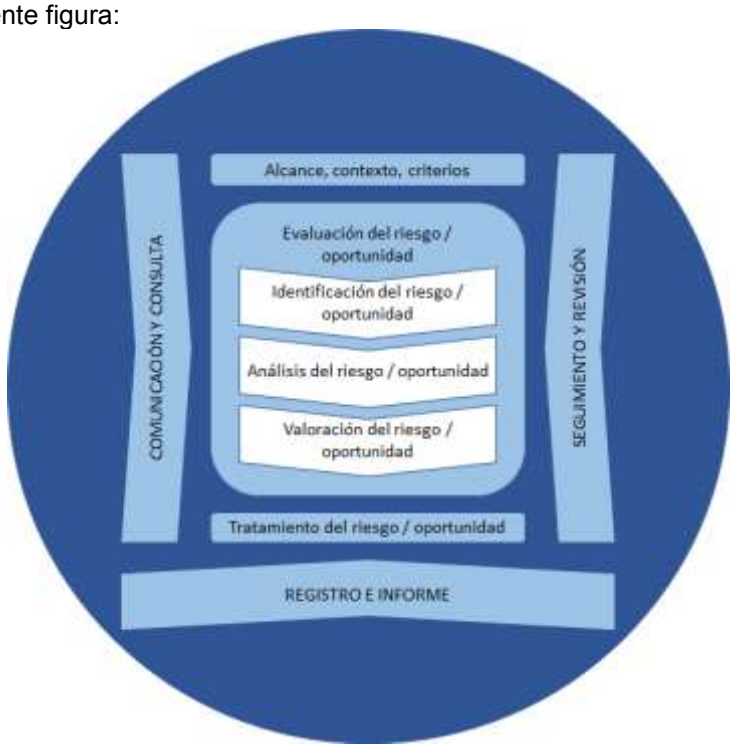
1.	**OBJETIVO**
	Estandarizar la metodología para planificar la gestión de riesgos y oportunidades del sistema de gestión integral del programa, desde la identificación, análisis, evaluación hasta el tratamiento de estos en el PNAS-Pensión 65.
2.	**ALCANCE**
	Todos los procesos del Programa Nacional de Asistencia Solidaria Pensión 65.
3.	**RESPONSABLES**
3.1	Jefes de Unidades
3.2	Personal del PNAS-Pensión 65
3.3	Coordinador de Calidad
4.	**DEFINICIONES**
4.1	**Riesgo**: Efecto de la incertidumbre sobre la ocurrencia de un evento que podría afectar el logro de los objetivos institucionales. El riesgo es medido en términos de sus consecuencias (impacto) y posibilidades (probabilidad de ocurrencia). Nota: El término riesgo, involucra tanto riesgo (negativo) como oportunidad (riesgos positivos), por lo que se podrá utilizar dicho término incluyendo ambas definiciones.
4.2	**Oportunidades**: Efecto de la incertidumbre sobre la ocurrencia de un evento que podría afectar el logro de los objetivos institucionales de manera positiva. La oportunidad es medida en términos de sus consecuencias (impacto) y posibilidades (probabilidad de ocurrencia). También conocida como riesgo positivo.
4.3	**Gestión del Riesgo y Oportunidades:** Actividades coordinadas para dirigir y controlar la organización con relación al riesgo y la oportunidad.
4.4	**Fuente de Riesgo/Oportunidad:** Elemento que, por si solo o en combinación con otros, tiene el potencial de generar riesgo u oportunidad.
4.5	**Parte Interesada:** Persona u organización que puede afectar, verse afectada, o percibirse como afectada por una decisión o actividad.
4.6	**Contexto de la Organización:** es un nuevo requerimiento en ISO 9001, y básicamente indica que una organización debe considerar las cuestiones internas y externas que pueden impactar a sus objetivos estratégicos y a la planificación del sistema de gestión de la calidad.
4.7	**Evento:** ocurrencia o cambio de un conjunto articular de circunstancias.
4.8	**Consecuencia:** Es el resultado de un evento que afecta a los objetivos. Esta puede ser cierta o incierta, teniendo efectos positivos o negativos, directos o indirectos sobre los objetivos definidos. Las expresiones pueden ser cualitativas o cuantitativas, pudiéndose incrementar sus efectos de manera de cascadas o acumulativamente.
4.9	**Probabilidad:** Es la posibilidad que suceda algo.
4.10	**Control:** Medida que mantiene o modifica el riesgo u oportunidad.
4.11	**Impacto**: Es el resultado de un evento expresado cualitativa o cuantitativamente
4.11	**Viabilidad**: es un análisis que tiene por finalidad conocer la probabilidad que existe de poder llevar a cabo una actividad con éxito o materializar el hecho propuesto.
4.12	**Rentabilidad**: hace referencia a los beneficios que puede obtener una comunidad (personal, trabajadores, cliente o usuarios) de una actividad o inversión realizada por una organización. Esta rentabilidad puede ser social, económica, financiera, cultural, tecnológica, entre otras.
4.13	**Amenaza**: Situación de origen humano o natural que puede afectar en forma negativa a la institución mediante la destrucción total o parcial de sus activos, y por consiguiente afectando la posibilidad de cumplir con sus objetivos
4.14	**Identificación de riesgos/oportunidad**: es el proceso de detectar las fuentes principales de riesgos u oportunidades y determinar que puede suceder, por qué y cómo en una situación determinada y en un período de tiempo definido.
4.15	**Evaluación de riesgos/oportunidad**: determinar la probabilidad de ocurrencia del riesgo u oportunidad y su impacto en el logro de objetivos

4.16	**Nivel del riesgo/oportunidad**: Valor obtenido por el producto entre la probabilidad e impacto asignados a un riesgo u oportunidad.
4.17	**Análisis FODA**: Se analizan las fortalezas, las oportunidades, las debilidades y las amenazas de la organización para identificar los riesgos u oportunidades.
4.18	**Técnica Delphi**: Se busca llegar a un consenso basándose en la información proporcionada de manera anónima por expertos mediante cuestionarios. Las conclusiones se forman a partir de las estadísticas de los datos obtenidos.
4.19	**Confidencialidad:** en informática, es un principio fundamental de la seguridad de la información que garantiza el necesario nivel de secreto de la información y de su tratamiento, para prevenir su divulgación no autorizada cuando está almacenada o en tránsito.
4.20	**Disponibilidad:** en informática, implica la adopción de sistemas que puedan garantizar el ingreso a las personas que cuenten con las credenciales requeridas, así como a procesos, servicios y datos que la empresa posee en su haber.
4.21	**Integridad:** en informática, implica la confiabilidad y garantía de la exactitud de los datos transportados o almacenados, asegurando que no se ha producido su alteración, pérdida o destrucción, ya sea de forma accidental o intencionada.
5.	**DOCUMENTOS DE REFERENCIA**
5.1	Manual de Operaciones del programa aprobado mediante Resolución Ministerial N°273-2017-MIDIS.
5.2	Directiva N°006-2019-CG/INTEG, del 15/05/2019 – "Implementación del Sistema de Control Interno en las Entidades del Estado" – Anexos: 5, 6, 7, 8 y 9 y sus correspondientes modificatorias.
5.3	Directrices para la Gestión del Riesgo ISO 31000:2018 – UNE
5.4	Norma ISO 37001:2016
5.5	Norma ISO 9001:2015
5.6	NTP ISO 31000:2018 – Gestión del Riesgo
5.7	Norma ISO 27001:2013
6.	**DISPOSICIONES ESPECÍFICAS**
6.1	La aprobación de la Matriz de Riesgos y Oportunidades se realiza con una frecuencia anual, sin embargo, su revisión puede darse según la necesidad de la organización. Esta revisión incluye observar los valores de probabilidad, viabilidad, impacto, rentabilidad, confiabilidad, disponibilidad e integridad; así como, nivel, evaluación y significancia de los riesgos u oportunidades identificados en los procesos misionales del programa de acuerdo con el Mapa de Procesos aprobado en el Manual de Operaciones.



6.2	Los insumos para identificar los riesgos u oportunidades pueden ser los siguientes: • Flujogramas. • Procedimientos. • Cronogramas de trabajo. • Factores internos: son los relacionados con la organización y sus actitudes respecto del riesgo/oportunidad y la tolerancia al riesgo/oportunidad. • Factores externos: son los relacionados con el entorno externo de la organización: Gobierno Central, Sector Ministerial, Proveedores, Partes Interesadas, Marco Legal, entre otras. • Objetivos de Calidad • Interacción con entre los procesos de la organización.
6.3	**Tipos de riesgo u oportunidad** • Estratégico: Se asocia con la forma en que se administra la entidad. El manejo del riesgo u oportunidad estratégica 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 • Operativo: Comprende los riesgos u oportunidades relacionados tanto con la parte operativa como técnica de la entidad, incluye riesgos u oportunidades 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 e incumplimiento de los compromisos institucionales. • Financiero: Se relacionan con el manejo de los recursos de la entidad e incluye, la ejecución presupuestal, la elaboración de los estados financieros, los pagos, manejos de excedentes de tesorería y el 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 toda entidad. • 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. • Desastres: Aquellos asociados a eventos de origen externo que podría abrir ventanas de identificar nuevos riesgos o abrir nuevas oportunidades de servicios o productos. • Informáticos: Desde el punto de vista del riesgo puede considerarse como una debilidad del sistema informático que puede ser utilizada para causar un daño. Las debilidades pueden aparecer en cualquiera de los elementos de un computador, tanto en el hardware, el sistema operativo, cómo en el software. Por otro lado, puede verse como una oportunidad si esta se mejora para aumentando su capacidad o alcance que permita brindar el soporte para servicios futuros o permitir que otro público objetivo acceda a tales servicios. • Riesgos 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. • Riesgos de Corrupción: Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado. • Riesgo de Disponibilidad, es la posibilidad de que, al acceder a la información solicitada, esta no se halle o se encuentre habilitada y no tenga un respaldo oportuno. • Riesgo de Confidencialidad, es la posibilidad de que, la información tenga un fácil acceso, pudiendo ser vulnerada. • Riesgo de Integridad, es la posibilidad de que, la información no se halle completa o parcialmente completa, o se encuentre fragmento con pérdida de información, resultado información no confiable.
6.4	**Comprensión de la Organización y de su contexto:** Elaborar la matriz de contexto del programa (ver anexo 14) que servirá de marco referencial para la Matriz de Riesgos y Oportunidades. Este puede incluir, pero no limitarse: Contexto Externo: • Factores sociales, culturales, políticos, legales, reglamentarios, financieros, tecnológicos.

	• Impulsores claves y las tendencias que puedan afectar a los objetivos de la organización. • Valores, necesidades y expectativas de las partes interesadas. • Relaciones contractuales y compromisos. • Complejidad de las redes y dependencia. Contexto Interno: • Revisión de la misión, visión y valores. • Gobernanza, roles y rendición de cuentas. • Cultura Organizacional, Objetivos y/o Políticas, Directrices, Capacidades, Recursos, Datos, sistemas de información, flujos de información, encuesta de clima laboral, Interdependencia e interconexiones. Otra forma de análisis del contexto del programa es a través de Factores, en los cuales se identifica las condiciones y los efectos potenciales que involucran a la organización. Entre estos factores tenemos al tamaño de la organización, la estructura de la organización, el alcance del programa, el crecimiento de su servicio, el modelo de intervención empleado, las entidades con las cuales entrega el servicio, articulación con aliados estratégicos, entidades, aliados, Gobierno y los temas normativos y de control interno. También se puede emplear los criterios del análisis FODA de la organización. Los criterios para la Actualización de la Matriz de Contexto (ver anexo 14) son: - Frecuencia Anual (como mínimo). - Cambio de Alcance de los Sistemas de gestión - Cambios Políticos y estratégicos del sector MIDIS
6.5	**Partes Interesadas:** La identificación de las necesidades y expectativas de las Partes Interesadas, se considera un punto fundamental dentro de la evaluación del Contexto de la organización, y clave para definir una estrategia adecuada. Una vez identificada las necesidades, cada organización en base a sus intereses en cada momento deberá determinar cuáles de ellas pasan a formar parte de nuestro Sistema de Gestión Integral, y cuáles no. Es importante diferenciar entre lo que son necesidades de las Partes Interesadas de lo que son expectativas y deseos, ya que la prioridad debería ser distinta en cada caso (ver anexo 15) Los grupos para analizar y/o considerados como partes interesadas, son los siguientes: • **Usuarios:** Los receptores directos y que utilizan su producto o servicio afectan directamente su capacidad para satisfacer sus necesidades. Es necesario comprender las necesidades, las expectativas y los requisitos de las partes interesadas. Es importante conocer que se va a utilizar su producto o servicio que determina como deben hacerse llegar. Estas pueden ser algunas de sus partes interesadas más importantes. • **Entidades del Gobierno y Organizaciones no gubernamentales.** Como Programa Social perteneciente al Sector Publico, tienen requisitos legales que sus productos y servicios deben cumplir y puede que exista un gran costo social en caso de no cumplir, por lo tanto, es importante entender las expectativas del sector al cual pertenece el programa, como el monitoreo de las condiciones de los usuarios, los servicios complementarios que se ofrece, entre otros aspectos relevantes para el sector público. Dentro de este grupo podemos encontrar a los Gobiernos Locales, Gobiernos Regionales, entidades como: MINSA, MINEDU, MIMPV, Congreso de la República, MINPUB, Contraloría, CTVC, entre otros. • **El Personal**: Colaboradores que trabajan en la organización y viene a ser la parte fundamental del Programa, son responsables en gran medida del éxito a largo plazo, por lo tanto; conocer sus necesidades, expectativas y preocupaciones, nos ayudará a realizar acciones efectivas, que posiblemente no supongan un elevado gasto, sino que repercuta en un fuerte compromiso con los objetivos de la organización. • **Autoridades del Sector**: Como Programa Social, pertenecemos al Ministerio de Desarrollo e Inclusión Social (MIDIS), al cual se rinde cuentas a través de informes permanentes que indican el balance presupuestal, el cumplimiento de metas, entre otros aspectos de interés relacionado a ese

	nivel del sector. Los aspectos del desempeño del Sistema de Gestión Integral y las expectativas en cuanto a la mejora continua, no están ajenos al interés de las autoridades del sector y puede ser muy importante para este grupo de partes interesadas su monitoreo y evaluación permanente. • **Proveedores de Información, de servicios y aliados estratégicos:** Muchas empresas pasan por alto los beneficios que supone la relación ganar-ganar y el beneficio mutuo. Con respecto a los proveedores de servicio, tenemos al Banco de la Nación, y los proveedores logísticos y administrativos. Así mismo, los proveedores de información tales como: SISFOH, RENIEC, SBS, SUNAT, entre otros entes con los cuales se coteja el registro bimensual de usuarios (RBU). En cuanto a los temas de articulación contamos con los aliados estratégicos, entidades con las cuales la colaboración es sumamente importante para el desarrollo de las actividades complementarias al servicio de la subvención monetaria. Los criterios para la Actualización de las Partes Interesadas (ver anexo 15) son: - Frecuencia Anual (como mínimo). - Cambio de Alcance de los Sistemas de gestión - Cambios Políticos y estratégicos del sector MIDIS
6.6	**Proceso de la Gestión del Riesgo / Oportunidad:** Esta implica la aplicación sistemática como se muestra en la siguiente figura: 
6.7	**Identificación del riesgo / oportunidad:** El propósito es encontrar, reconocer y describir los riesgos u oportunidades dentro de los procesos que pueden ayudar o impedir a una organización lograr sus objetivos. Se debería considerar los factores siguientes y la relación de los riesgos u oportunidades; para ello, es importante contar con información pertinente, apropiada y actualizada. (ver anexo n°13). • Fuente de riesgos u oportunidades tangibles e intangibles. • Las causas y los eventos. • Los cambios en los contextos externo e interno. • Los indicadores de riesgos u oportunidades emergentes. • La naturaleza y el valor de los activos y los recursos. • Las consecuencias y los impactos en los objetivos. • Las limitaciones de conocimiento y confiabilidad de la información.

	• Los factores relacionados con el tiempo. • Los sesgos, los supuestos y las creencias de las personas involucradas. • El activo o grupo de activos de información involucrado. • La afectación a la confidencialidad, integridad o disponibilidad de la información En el caso del Sistema de Gestión de Seguridad de la Información (SGSI) se considerarán los niveles confidencialidad, integridad o disponibilidad de los activos de información, por lo que la gestión de riesgos de seguridad de la información será para aquellos valorados como Altos o Muy Altos principalmente. Para la valoración de los activos de la información se utilizarán: • Anexo Nº16: Lista de Activos de la Información • Anexo Nº17: Escala CID para Activos de la Información • Anexo Nº18: Criterios de Evaluación para Activos de la Información
6.8	**Análisis del Riesgo / Oportunidad:** El propósito es comprender la naturaleza del riesgo u oportunidad y sus características, incluyendo cuando sea apropiado, el nivel de riesgo u oportunidad. Para este análisis se debe considerar los siguientes factores: • La probabilidad de los eventos y las consecuencias. • La viabilidad de concretar las oportunidades y su rentabilidad. • Las probabilidades y los impactos (para la evaluación del riesgo) • Las viabilidades y rentabilidades (para la evaluación de la oportunidad) • Para la evaluación de vulnerabilidad de los sistemas de información, se considera el "riesgo asociado a la Disponibilidad, Confiabilidad e Integridad como parte del impacto o rentabilidad del evento. • La Naturaleza y la magnitud de la consecuencia. • La complejidad y la interconexión. • Los factores relacionados con el tiempo y la volatilidad. • La eficacia de los controles existentes, madurez del control (ver anexo n°13). • Los niveles de sensibilidad y de confianza. • El impacto confidencialidad, integridad o disponibilidad de la información
6.9	**Valoración de los Riesgos:** Proceso que consiste en priorizar los riesgos para realizar otros análisis o acciones posteriores, evaluando y combinando la probabilidad de ocurrencia y el impacto de dichos riesgos. En este proceso, se evalúa la prioridad de los riesgos identificados usando la probabilidad relativa de ocurrencia, el impacto correspondiente sobre los objetivos del proyecto si los riesgos se presentan, así como otros factores, tales como el plazo de respuesta y la tolerancia al riesgo u oportunidad por parte de los encargados de los procesos. Las técnicas utilizadas para realizar este análisis incluyen: • Evaluación de probabilidad e impacto: La evaluación de la probabilidad de los riesgos estudia la probabilidad de ocurrencia de cada riesgo específico. Por otro lado, la evaluación del impacto de los riesgos investiga el efecto potencial de los mismos sobre un objetivo del proyecto. Como pueden ser, el cronograma, el costo, la calidad o el desempeño. Incluidos tanto los efectos negativos en el caso de las amenazas, como positivos, en el caso de las oportunidades. • Los valores para determinar la probabilidad y el impacto del riesgo: Valores para determinar la probabilidad del riesgo **NIVEL** / **VALOR** Baja: 4 Media: 6 Alta: 8 Muy Alta: 10 Valores para determinar el impacto del riesgo

NIVEL	VALOR
Baja	4
Media	6
Alta	8
Muy Alta	10

- Fórmula para determinar el valor del riesgo:

Valor del riesgo (Vr) = Probabilidad x Impacto

- Matriz de probabilidad e impacto: Tabla de doble entrada que combina la probabilidad de que ocurra un evento, con el impacto que éste puede causar en el proceso. De esta manera, conseguimos establecer una priorización de los riesgos.

			Impacto			
Probabilidad			Bajo	Medio	Alto	Muy Alto
			4	6	8	10
	Muy Alta	10	40	60	80	100
	Alta	8	32	48	64	80
	Media	6	24	36	48	60
	Baja	4	16	24	32	40

- Valores y Niveles de riesgo por intervalos:

RB (Riesgo Bajo)	RM (Riesgo Medio)	RA (Riesgo Alto)	RMA (riesgo Muy Alto)
16 - 24	32 - 40	48 - 64	80 - 100

- Se adoptarán medidas de tratamiento de control para aquellos riesgos que se encuentren en los niveles de medio, alto y muy alto.
- De acuerdo con los riesgos identificados estos pueden conducir a una toma de decisión de:
  - No hacer nada más.
  - Considerar opciones para el tratamiento de riesgo.
  - Realizar un análisis adicional para comprender mejor el riesgo.
  - Mantener controles existentes.
  - Reconsiderar los objetivos.
- Los resultados de las valoraciones se validarán en los grupos de trabajos, comités u otro similar dentro de la organización.

Nota: Sólo en el caso del Sistema de Seguridad de la información (SSI), la asignación del impacto de riesgo o rentabilidad de la oportunidad, se realiza a partir del siguiente criterio:

- Impacto resultante es la suma del valor indicado en la Confidencialidad (C.), Integridad (I) y Disponibilidad (D)
- Los niveles de impacto de los criterios de Confidencialidad (C.), Integridad (I) o Disponibilidad (D) son Baja, Media, Alta, Muy Alta.

DISPONIBILIDAD. Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.	
Bajo	Su indisponibilidad supone un daño menor a la organización, la disponibilidad requerida de ese activo es de 1 a 6 meses.

Medio	Su indisponibilidad supone un daño considerable a la organización, la disponibilidad requerida de ese activo es de 1 semana a 1 mes.
Alto	Su indisponibilidad supone un daño importante a la organización, la disponibilidad requerida de ese activo es de 1 día a 1 semana.
Muy Alto	Su indisponibilidad supone un daño muy grave o la no recuperación de la organización, la disponibilidad requerida de ese activo es menor de 1 día.

INTEGRIDAD. Propiedad de la información relativa a su exactitud y completitud.	
Bajo	Su alteración o modificación supone un daño menor a la organización, puede modificarse por personal de la organización sin requerir autorización.
Medio	Su alteración o modificación supone un daño considerable a la organización, puede modificarse con solo permiso del responsable de la Unidad o del Propietario del Activo.
Alto	Su alteración o modificación supone un daño importante a la organización, puede modificarse solo con permiso del Oficial de Seguridad de Información.
Muy Alto	Su alteración supone un daño muy grave o la no recuperación de la organización, puede modificarse solo con permiso de Dirección Ejecutiva y bajo supervisión del Oficial de Seguridad de Información.

CONFIDENCIALIDAD. Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.	
Bajo (Nivel Interno-Publico/Organización)	Su revelación supone un daño poco preocupante a la organización, es de carácter público o conocido por personal de la organización.
Medio (Nivel Interno-Unidad)	Su revelación causaría un daño considerable a la organización, solo debe ser conocido por ciertos grupos dentro de la organización como unidades.
Alto (Nivel Interno-Persona)	Su revelación causaría un daño importante a la organización, solo debe conocerla determinadas personas de la organización.
Muy Alto (Nivel Confidencial)	Su revelación no autorizada supone un daño muy grave o un incumplimiento legal, solo debe conocerla Dirección Ejecutiva.

Valoración combinada de la Confidencialidad, Integridad y Disponibilidad
Donde la combinación de los valores de C+I+D es el resultado de los intervalos
Baja [24 – 28]; Media [32 – 44]; Alta [48 – 64] y Muy Alta [70-78]

MAPA DE COMBINACIONES D+C+I						
Confidencialidad	26	60	64	70	78	26
	18	44	48	54	62	18
	12	32	36	42	50	12
	8	24	28	34	42	8
		8	12	18	26	
		DIPONIBILIDAD				

Integridad

Donde los valores de los niveles se registran en la siguiente tabla:

Niveles	Disponibilidad	Confidencialidad	Integridad	Valor
Muy Alta	Muy Alta	Muy Alta	Muy Alta	26
Alta	Alta	Alta	Alta	18
Media	Media	Media	Media	12
Baja	Baja	Baja	Baja	**8**

6.10 **Valoración de las Oportunidades:**

Por la parte de las oportunidades el razonamiento es similar al de los riesgos, pero pensando en sentido positivo, lo que se conoce como "riesgo positivo". En este caso se utiliza un criterio basado en el binomio viabilidad - rentabilidad; es decir, abordar aquella oportunidad que tenga la relación más alta entre la viabilidad de lo que se ha identificado como oportunidad, frente a aquella oportunidad que tenga mejor rentabilidad y por tanto aumentar la eficacia de la organización.

Al igual que con los riesgos, lo primero que se realiza es clasificar la viabilidad - rentabilidad en ALTO, MEDIO y BAJO. Según el criterio desarrollado, estas son tres categorías:

Viabilidad: Es la probabilidad de que se materialice la oportunidad

ALTA	Podría materializarse con pocos recursos, como elaboración de una Resolución Directoral, documentos normativos, disposiciones específicas, que pueden darse dentro los próximos 6 meses o cuya inversión económica no supere las 4 UTI
MEDIA	Podría materializarse con la elaboración de una Resolución Ministerial, o con una pequeña inversión mayor a las 4 UIT, o que necesite ser gestionada dentro los próximos 12 meses.
BAJA	Podría materializarse con la elaboración de un Decreto Supremo o Ley, o con una inversión no mayor del 10% de nuestro presupuesto, o que necesite ser gestionada dentro los próximos 24 meses.

Rentabilidad: Es el impacto que tendrá en los usuarios o personal del programa de materializarse la oportunidad.

ALTA	De materializarse, podría impactar con el aumento no mayor del 10% en cualquiera de los siguientes aspectos: a) Aumento en la percepción de la satisfacción de nuestros usuarios. b) Aumento de los puntos de pagos a nuestros usuarios c) Aumento de la capacidad tecnológica del programa.

	d) Aumento en el porcentaje de colaboradores encuestados que perciben una cultura de ética e integridad en el programa De materializarse, podría impactar en la reducción no mayor del 1% en los siguientes aspectos: a) Reducción del porcentaje de no cobros oportuno de nuestros usuarios.
MEDIA	De materializarse, podría impactar con el aumento no menor del 10% en cualquiera de los siguientes aspectos: a) Aumento en la percepción de la satisfacción de nuestros usuarios. b) Aumento de los puntos de pagos a nuestros usuarios c) Aumento de la capacidad tecnológica del programa. d) Aumento en el porcentaje de colaboradores encuestados que perciben una cultura de ética e integridad en el programa De materializarse, podría impactar en la reducción no mayor del 0.5% en los siguientes aspectos: Reducción del porcentaje de no cobros oportuno de nuestros usuarios.
BAJA	De materializarse, podría impactar con el aumento mayor del 25% en cualquiera de los siguientes aspectos: a) Aumento en la percepción de la satisfacción de nuestros usuarios. b) Aumento de los puntos de pagos a nuestros usuarios. c) Aumento de la capacidad tecnológica del programa. d) Aumento en el porcentaje de colaboradores encuestados que perciben una cultura de ética e integridad en el programa De materializarse, podría impactar en la reducción no mayor del 0.25% en los siguientes aspectos: a) Reducción del porcentaje de no cobros oportuno de nuestros usuarios.

Identificada, como la oportunidad podría verse materializada mediante la determinación de la viabilidad y cómo esta se podría generar una rentabilidad, como por ejemplo del tipo social.
A continuación, se definirá la relación entre Viabilidad-Rentabilidad para establecer las prioridades a la hora de abordar las oportunidades.
Como se podrá observar las oportunidades con puntuación más alta serán aquellas que tengan una viabilidad alta para poder abordarse y una rentabilidad económica también alta en caso de materializarse con el menor esfuerzo posible.

A continuación, la tabla que define como establecer las prioridades de este binomio viabilidad - rentabilidad y priorizar así las distintas situaciones de oportunidades identificadas. Las denominaciones como se observa en la tabla son las categorías de cada oportunidad:

VIABILIDAD	RENTABILIDAD		
	BAJA (4)	MEDIA (6)	ALTA (8)
BAJA (4)	Factible (16)	Factible (24)	Adecuada (32)
MEDIA (6)	Factible (24)	Adecuada (36)	Destacada (48)
ALTA (8)	Adecuada (32)	Destacada (48)	Prioridad (64)

Tenemos por tanto los siguientes tipos de oportunidades:

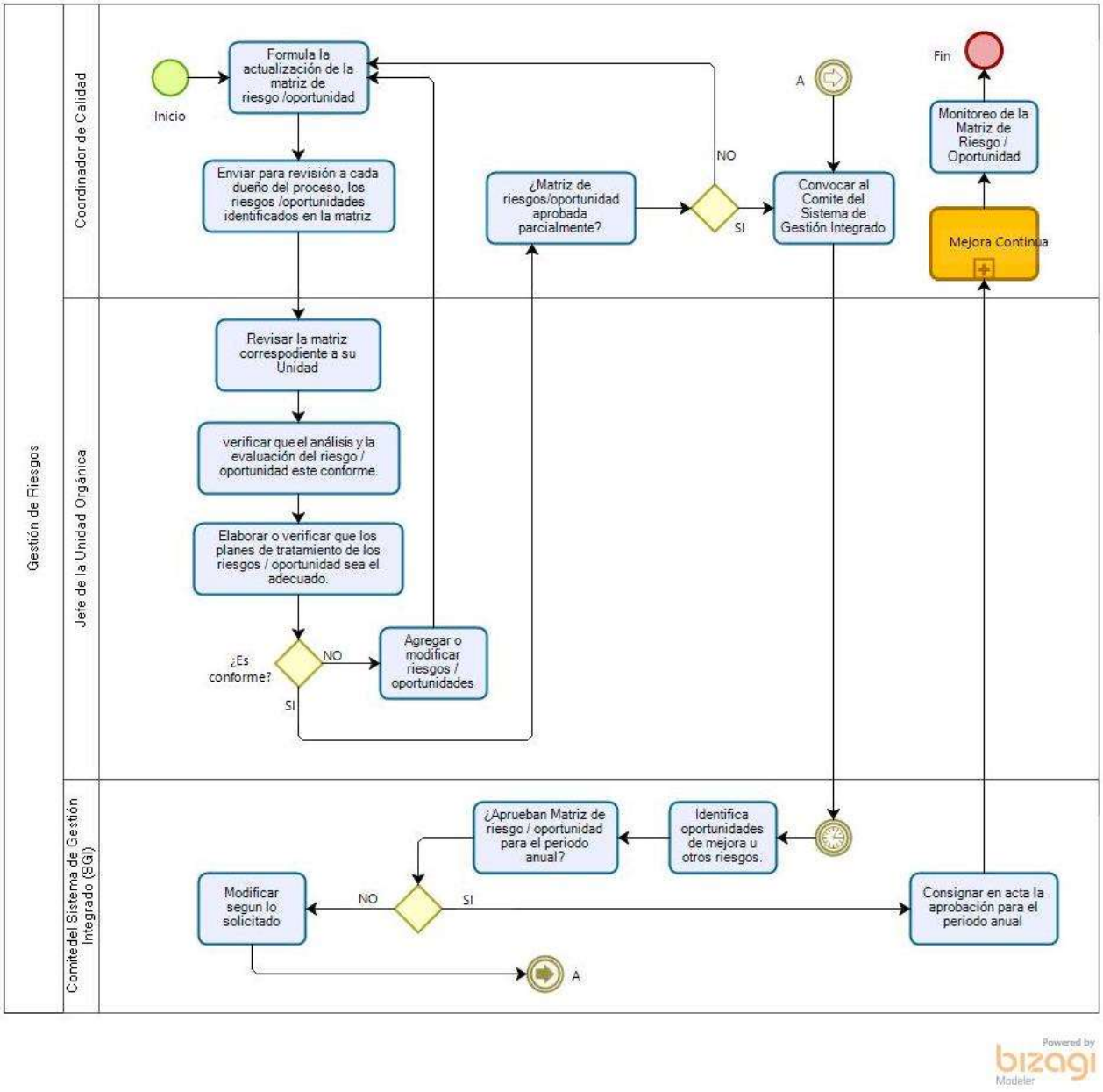
FACTIBLE (16 a 24)	La cual no requiere que se tomen medidas para abordarlas, sin embargo, pueden tomarse medidas para abordarlas, realizando comprobaciones periódicas para detectar posibles cambios en la rentabilidad-viabilidad.

	<table><tr><td>ADECUADA (32 – 36)</td><td>La cual se puede abordar si los beneficios esperados superan los recursos asignados (Beneficios > Recursos asignados). Es decir, si el beneficio o el resultado de aplicar estas medidas es mayor al tiempo-coste que te llevará implementar estas medidas. Esta decisión estará en manos de la Alta Dirección si se aborda o no una oportunidad clasificada como adecuada.</td></tr><tr><td>DESTACADA (48)</td><td>La cual se debe abordar para aprovechar la oportunidad detectada con un seguimiento acorde a los objetivos planteados.</td></tr><tr><td>PRIORITARIA (64)</td><td>La cual se debe abordar de forma inmediata para aprovechar la oportunidad detectada con un seguimiento acorde a los objetivos planteados.</td></tr></table>
6.11	**Tratamiento de Riesgos / Oportunidad**: Es el proceso por el cual se desarrollan opciones y acciones para mejorar las oportunidades y reducir las amenazas a los objetivos del programa. Incluye la identificación y asignación del propietario del riesgo/oportunidad, para que asuma la responsabilidad de la ejecución de la respuesta al riesgo u oportunidad. Consiste en determinar la respuesta a los riesgos u oportunidades de acuerdo con el Anexo N°07 y Anexo N°08. Esto involucra identificar el rango de opciones para tratar cada uno de los riesgos u oportunidades identificados, la evaluación de las opciones y la preparación de planes para su implementación. Las opciones de tratamiento pueden ser evaluadas sobre la base del alcance, la reducción del riesgo/oportunidad y el alcance de los beneficios creados. La selección de la opción más apropiada involucra balancear costos, contra los beneficios derivados de la misma. El abordar el riesgo u oportunidad mediante un tratamiento implica un proceso iterativo de: • Formular y seleccionar opciones para el tratamiento del riesgo u oportunidad. • Planificar e implementar el tratamiento del riesgo u oportunidad. • Evaluar la eficacia de ese tratamiento. • Decidir si el riesgo u oportunidad residual es aceptable. • De no ser aceptable iniciar un tratamiento adicional • Aceptar o aumentar el riesgo en busca de una oportunidad. • Eliminar la fuente de riesgo. • Modificar la Probabilidad o Viabilidad • Modificar las consecuencias o mitigar los impactos o rentabilidades. • Compartir el riesgo u oportunidad (por ejemplo: a través de contratos, compra de seguros) • Trasladar el riesgo. • Retener el riesgo u oportunidad con base a una decisión informada.
6.12	**Monitoreo y control:** Es el proceso por el cual se implementan planes de respuesta a los riesgos u oportunidades, se rastrean los riesgos u oportunidades identificados, se monitorean los riesgos u oportunidades residuales, se identifican nuevos riesgos o nuevas oportunidades y se evalúa la eficacia de la gestión riesgos y oportunidades. Las respuestas a los riesgos u oportunidades planificados que se incluyen en el plan de acción de mejora (PAM) para el proceso, se ejecutan durante un ciclo de duración del plan, monitoreando continuamente, para detectar riesgos u oportunidades nuevas, que cambian o que se vuelven obsoletos. La actividad de Monitorear y Controlar los Riesgos y las Oportunidades requiere de la aplicación de técnicas, tales como el análisis de variación y de tendencias, que requieren el uso de información del desempeño generada durante el desarrollo de los procesos. Otras finalidades es determinar si: ○ Los supuestos del proceso siguen siendo válidos. ○ Los análisis muestran que un riesgo u oportunidad evaluado ha cambiado o puede descartarse. ○ Se respetan las políticas y los procedimientos de gestión de riesgos.

	○ Las reservas para contingencias de costo o cronograma deben modificarse para alinearlas con la evaluación actual de los riesgos. También implica la selección de estrategias alternativas, la ejecución de un plan de contingencia o de reserva, la implementación de acciones correctivas y la modificación del PAM para la mejora del proceso. Esto puede significar también una actualización a los activos de los procesos de la organización, incluidas las bases de datos de las lecciones aprendidas y las plantillas de gestión de riesgos. Los riesgos u oportunidades y la eficacia de las medidas de control necesitan ser monitoreadas para asegurar que las circunstancias cambiantes no alteren las prioridades de los riesgos u oportunidades y para identificar amenazas no previstas originalmente.	
7.	**DESARROLLO**	
	Responsable	**Actividad**
7.1	Coordinador de Calidad	Formula la actualización de la Matriz de Riesgos y Oportunidades, de manera anual o según los cambios que se suscitan en los procesos, en la organización, producto de las salidas no conformes, y planes de acción de mejora que permiten identificar nuevos riesgos/oportunidades durante el periodo.
7.2	Coordinador de Calidad	Enviar a cada dueño del proceso, la parte correspondiente a los riesgos/oportunidades identificados en la matriz para su revisión.
7.3	Jefe de la Unidad Orgánica	Revisar la matriz correspondiente a su unidad, realiza el Monitoreo y Control de los Riesgos identificados. Genera lista de eventos que han logrado un impacto positivo (oportunidad) o negativo (amenaza) en el cumplimiento de los objetivos de calidad. Evalúa los riesgos u oportunidades identificados inicialmente e identifica nuevos riesgos.
7.4	Jefe de la Unidad Orgánica	Verificar que el análisis y la evaluación del riesgo/oportunidad este conforme.
7.5	Jefe de la Unidad Orgánica	Elaborar o verificar que los planes y tratamientos de los riesgos/oportunidades sea el adecuado.
7.6	Jefe de la Unidad Orgánica	Si todo está conforme enviar al Coordinador de Calidad. Si no es conforme y agregar o modificar los riesgos/oportunidades y planes de tratamiento correspondientes, y enviárselo al Coordinador de Calidad.
7.7	Coordinador de Calidad	Si la matriz ha sido aprobada parcialmente por cada una de las unidades orgánicas, se coordina la convocatoria del comité de calidad para una fecha programada.
7.8	Comité de Calidad	Identifica de las oportunidades de mejora que puedan suscitarse de la evaluación de los riesgos u oportunidades o identifican nuevos.
7.9	Comité de Calidad	El comité aprueba la Matriz de Riesgos u Oportunidades para el periodo anual correspondiente, consignándolo en un acta de sesión del Comité de Calidad.
7.10	Comité de Calidad	Caso contrario, se realizarán las modificaciones o ajustes necesarios según lo solicitado por el Comité.
7.11	Coordinador de Calidad	Aprobada la Matriz de Riesgos y Oportunidades, se procede a realizar el monitoreo y actualización de los planes de tratamiento, Identificando las oportunidades de mejora en los controles, midiendo la eficacia de los mismos, a través de los niveles de valoración de riesgos.
8.	**REGISTROS**	
8.1	Matriz de Gestión de Riesgos y Oportunidades	
8.2	Matriz de Tratamiento de Riesgos y Oportunidades	

9.	ANEXOS
9.1	Anexo N° 01: Flujograma
9.2	Anexo N° 02: Escala de Madurez de los controles
9.3	Anexo N° 03: Escala de Probabilidades
9.4	Anexo N° 04: Escala de Viabilidad
9.5	Anexo N° 05: Escala de Impactos
9.6	Anexo N° 06: Escala de Rentabilidad
9.7	Anexo N° 07: Escala de Nivel de Riesgo por intervalos
9.8	Anexo N° 08: Escala de Nivel de Oportunidades por intervalos
9.9	Anexo N° 09: Criterios de Evaluación de Riesgo / Oportunidades
9.10	Anexo N° 10: Significancia del Riesgo / Oportunidades
9.11	Anexo N° 11: Tratamiento de Riesgos.
9.12	Anexo N° 12: Tratamiento de Oportunidades.
9.13	Anexo N° 13 : Estructura de la Matriz de Gestión de Riesgos / Oportunidades y Tratamientos
9.14	Anexo N° 14 : Estructura de la Matriz de Contexto.
9.15	Anexo N° 15 : Estructura de la Matriz de Partes Interesadas.
9.16	Anexo Nº 16 : Lista de Activos de la Información
9.17	Anexo Nº 17 : Escala CID para Activos de la Información
9.18	Anexo Nº 18 : Criterios de Evaluación para Activos de la Información

Anexo N°01
Flujograma



Anexo N° 02
Escala de Madurez de los controles

Clasificación	Descripción
Débil	No existe ningún control planificado o implementado. Existe el control, sin embargo, éste no cumple con el fin establecido.
Moderado	Control implantado sin documentar (ya está hecho, pero falta documentarlo), Control implantado documentado, sin embargo, cumple en forma parcial.
Fuerte	Control implementado y documentado, cumple en forma eficaz

Anexo N° 03
Escala de Probabilidades

Clasificación	Valor	Probabilidad
Baja	**4**	**Podría realizarse** Existen condiciones que hacen que su probabilidad de realización sea a largo plazo o nula
Media	**6**	**Puede ocurrir su realización.** Existen condiciones que hacen poco probable la realización en el corto plazo (1 año) pero que no son suficientes para evitarlo en el largo plazo.
Alta	**8**	**Probablemente se realice.** Se puede dar en el corto plazo y no existen condiciones que impidan la ocurrencia (más de 2 veces al año)
Muy Alta	**10**	Se puede realizar en la mayoría de las circunstancias. La ocurrencia es inminente.

Anexo N° 04
Escala de Viabilidad

Clasificación	Valor	Viabilidad
BAJA	**4**	Podría materializarse con la elaboración de un Decreto Supremo o Ley, o con una inversión no mayor del 10% de nuestro presupuesto, o que necesite ser gestionada dentro los próximos 24 meses.
MEDIA	**6**	Podría materializarse con la elaboración de una Resolución Ministerial, o con una pequeña inversión mayor a las 4 UIT, o que necesite ser gestionada dentro los próximos 12 meses.
ALTA	**8**	Podría materializarse con pocos recursos, como elaboración de una Resolución Directoral, documentos normativos, disposiciones específicas, que pueden darse dentro los próximos 6 meses o cuya inversión económica no supere las 4 UTI

Anexo N°05
Escala de Impactos

Clasificación	Valor	Descripción
Bajo	**4**	Impacto no significativo, afectaría una actividad o proceso no críticos de la organización o terceros.
Moderado	**6**	Impacto que podría ocasionar un perjuicio/beneficio en una actividad o proceso crítico o más de una actividad o proceso no crítico de la organización o terceros.
Alto	**8**	Impacto que podría ocasionar un perjuicio/beneficio significativo para la organización o terceros y que podría impedir/promover la ejecución de las actividades de la organización.
Muy Alto	**10**	Impacto que podría ocasionar un perjuicio/beneficio significativo para la organización o terceros y que podría impedir/promover la ejecución de las actividades de la organización, incumplimientos legales, regulatorios, normativos, hay multas y/o sanciones.

Anexo N°06
Escala de Rentabilidad

Clasificación	Valor	Descripción
BAJA	**4**	De materializarse, podría impactar con el aumento mayor del 25% en cualquiera de los siguientes aspectos: a) Aumento en la percepción de la satisfacción de nuestros usuarios. b) Aumento de los puntos de pagos a nuestros usuarios. c) Aumento de la capacidad tecnológica del programa. d) Aumento en el porcentaje de colaboradores encuestados que perciben una cultura de ética e integridad en el programa De materializarse, podría impactar en la reducción no mayor del 0.25% en los siguientes aspectos: Reducción del porcentaje de no cobros oportuno de nuestros usuarios.
MEDIA	**6**	De materializarse, podría impactar con el aumento no menor del 10% en cualquiera de los siguientes aspectos: a) Aumento en la percepción de la satisfacción de nuestros usuarios. b) Aumento de los puntos de pagos a nuestros usuarios c) Aumento de la capacidad tecnológica del programa. d) Aumento en el porcentaje de colaboradores encuestados que perciben una cultura de ética e integridad en el programa De materializarse, podría impactar en la reducción no mayor del 0.5% en los siguientes aspectos: Reducción del porcentaje de no cobros oportuno de nuestros usuarios.
ALTA	**8**	De materializarse, podría impactar con el aumento no mayor del 10% en cualquiera de los siguientes aspectos: a) Aumento en la percepción de la satisfacción de nuestros usuarios. b) Aumento de los puntos de pagos a nuestros usuarios c) Aumento de la capacidad tecnológica del programa. d) Aumento en el porcentaje de colaboradores encuestados que perciben una cultura de ética e integridad en el programa De materializarse, podría impactar en la reducción no mayor del 1% en los siguientes aspectos: a) Reducción del porcentaje de no cobros oportuno de nuestros usuarios.

Anexo N° 07
Escala de Nivel de Riesgo por intervalos

Clasificación	P° x I	Descripción
Riesgo Bajo	**16 a 24**	**Riesgo Bajo**, con probabilidad baja, impacto bajo o moderado en la consecución de los objetivos del proceso. No afecta las operaciones ni la productividad. No hay consecuencias.
Riesgo Medio	**32 a 40**	**Riesgo medio**, con **probabilidad de ocurrencia media o alta e impacto leve o moderado** en la consecución de los objetivos del proceso. Hay una posibilidad de que las operaciones y la productividad se vean afectados negativamente/positivamente.
Riesgo Alto	**48 a 64**	Riesgo **alto, con probabilidad de ocurrencia media o alta e impacto alto en la consecución de los objetivos del proceso**. Lo que conlleva a una pérdida/ganancia alta o afectar parcialmente las operaciones y la productividad de los procesos.
Riesgo Muy Alto	**80 a 100**	Riesgo con **impacto muy alto, con probabilidad de ocurrencia alta e impacto muy alto** en la consecución de los objetivos del proceso. Lo que conlleva a una pérdida/ganancia muy alta o afectar totalmente las operaciones y la productividad de los procesos.

Anexo N° 08
Escala de Nivel de Oportunidades por intervalos

Clasificación	V° x R	Descripción
FACTIBLE	**16 a 24**	La cual no requiere que se tomen medidas para abordarlas, tan solo se recomienda que se realices comprobaciones periódicas para detectar posibles cambios en la rentabilidad-viabilidad.
ADECUADA	**32 a 36**	La cual se puede abordar si los beneficios esperados superan los recursos asignados (Beneficios > Recursos asignados). Es decir, si el beneficio o el resultado de aplicar estas medidas es mayor al tiempo-coste que te llevará implementar estas medidas. Esta decisión estará en manos de la Alta Dirección si se aborda o no una oportunidad clasificada como adecuada.
DESTACADA	**48**	La cual se debe abordar para aprovechar la oportunidad detectada con un seguimiento acorde a los objetivos planteados.
PRIORITARIA	**64**	La cual se debe abordar de forma inmediata para aprovechar la oportunidad detectada con un seguimiento acorde a los objetivos planteados.

Nota: Impacto o Rentabilidad puede ser negativa (Riesgo) o positiva (Oportunidad) respectivamente.

Anexo N° 09
Criterios de Evaluación de Riesgo / Oportunidad

Tipo de Evaluación	Clasificación	Nivel	Valor Estratégico (Riesgos/ Oportunidades)	Multa / Sanciones/ Incumplimientos (Sólo Riesgos)	Cliente Interno/Externo (Riesgos/ Oportunidades)	Operacional (Riesgos/ Oportunidades)
Riesgo	**Bajo**	**16 a 24**	**El impacto sobre la estrategia de la organización es indirecto**, pero bajo / factible.	No existe posibilidad de multa o sanción, pero si de una recomendación. La(s) actividad(es) afectada(s) no está(n) sujeta(s) a supervisión por parte de otra Organización.	La materialización del impacto es leve y es percibida por el cliente interno, pero no es percibida por el cliente externo.	Impacto puede ser asimilado por la organización en un tiempo no muy prolongado. Los costos son bajos.
Oportunidad	**FACTIBLE**	**16 a 24**				
Riesgo	**Medio**	**32 a 40**	**El impacto sobre la estrategia de la organización es directo**, pero el efecto es moderado / adecuada	Posibilidad de multa o sanción. La(s) actividad(es) afectada(s) está(n) sujeta(s) a supervisión por parte de otra Organización.	La materialización del **impacto es moderada** y es percibida por el cliente interno y externo.	Impacto afecta la productividad del negocio en un horizonte de **1 día**. Los costos son moderados.
Oportunidad	**ADECUADA**	**32 a 36**				
Riesgo	**Alto**	**48 a 64**	**El impacto sobre la estrategia de la organización es directo,** y el efecto es alto / destacada.	Posibilidad de multa o sanción por falta(s) grave(s). Posibilidad de hallazgos de incumplimiento en auditorías.	La materialización del **impacto es alta** y puede originar sanciones.	Impacto potencial en el negocio y productividad; en un horizonte mayor a 2 días. El costo de interrupción es alto. Se requerirá de personal adicional.
Oportunidad	**DESTACADA**	**48**				
Riesgo	**Muy Alto**	**80 a 100**	El **impacto sobre la estrategia de la organización es** catastrófico / prioritario**.**	Posibilidad de multa o sanción, cierre de las instalaciones. Posibilidad de hallazgos de incumplimiento en auditorías.	**Impacto elevado** en el cliente interno y externo, **lo que puede originar multa y/o sanciones** graves.	Interrupción total de las actividades (operaciones) de la compañía. El costo de interrupción es muy alto.
Oportunidad	**PRIORITARIA**	**64**				

Nota: Impacto o afectación puede ser positiva (Oportunidad) o negativa (Riesgo)

Anexo N°10
Significancia del Riesgo / Oportunidad

TIPO	Valor de Evaluación de Riesgos / Oportunidad	Calificación del Riesgo / Oportunidad	Descripción
RIESGO	16 a 24	Bajo	Es un riesgo aceptable, no genera riesgos u oportunidades en los procesos, en las operaciones, no afecta las estrategias organizacionales, no hay impactos legales, no afecta la imagen, los controles actuales son suficientes.
	32 a 40	Medio	Es un riesgo/oportunidad aceptable. Podría generar riesgos u oportunidades en los procesos, pero no en las operaciones, no afecta las estrategias organizacionales, no hay impactos legales, no afecta la imagen, los controles actuales podrían ser no suficientes, por lo que se requerirá adoptar medidas de tratamiento.
	48 a 64	Alto	Es un riesgo/oportunidad que amerita tratamiento para evitar que afecte/mejore la reputación, ocasionar pérdidas/ganancias financieras, incurrir en investigación/felicitación del regulador o causar interrupción/fortalecimiento parcial de los procesos
	80 a 100	Muy Alto	Cuando la organización se encuentra expuesta a riesgos/oportunidades muy altas que ameritan ser tratados de manera inmediata porque afecta los procesos causando interrupción/fortalecimiento del negocio, dañará/mejorará la reputación, ocasionará pérdidas/ganancias financieras, se incurrirá en multas/beneficios legales.
OPORTUNIDAD	16 a 24	Factible	Es una oportunidad factible, la cual no requiere que se tomen medidas para abordarlas, tan solo se recomienda que se realices comprobaciones periódicas para detectar posibles cambios en la rentabilidad-viabilidad.
	32 a 36	Adecuada	La cual se puede abordar si los beneficios esperados superan los recursos asignados (Beneficios > Recursos asignados). Es decir, si el beneficio o el resultado de aplicar estas medidas es mayor al tiempo-coste que te llevará implementar estas medidas. Esta decisión estará en manos de la Alta Dirección si se aborda o no una oportunidad clasificada como adecuada.
	48	Destacada	La cual se debe abordar para aprovechar la oportunidad detectada con un seguimiento acorde a los objetivos planteados.
	64	Prioritaria	La cual se debe abordar de forma inmediata para aprovechar la oportunidad detectada con un seguimiento acorde a los objetivos planteados.

Nota: Impacto o afectación puede ser positiva (Oportunidad) o negativa (Riesgo)

Anexo N° 11
Tratamiento de Riesgos

Estrategia	Descripción
Evitar	Realizar cambios en el plan para eliminar el riesgo. Esto puede implicar cambios en el cronograma o el alcance del proceso para eliminar la amenaza.
Transferir	Trasladar el impacto de una amenaza a un tercero junto con la responsabilidad de la respuesta.
Mitigar	Disminuir la probabilidad y/o impacto de que se produzca el riesgo.
Aceptar	No tomar ninguna medida a menos de que el riesgo u oportunidad suceda. Esta estrategia se da cuando no es viable o rentable abordar el riesgo u oportunidad de otra manera. Hay dos tipos de aceptación de una amenaza: pasiva, no hacer nada, y activa, establecer una reserva de contingencia en tiempo o dinero.

Anexo N°12
Tratamiento de Oportunidades

Estrategia	Descripción
Apalancar	Utilizar los recursos necesarios para hacer realidad la oportunidad.
Mejorar	Aumentar la viabilidad y/o la rentabilidad de una oportunidad.
Compartir	Pasarle la oportunidad a un tercero para que el beneficio del proceso tenga una rentabilidad social.
Aceptar	Aprovechar la oportunidad cuando esta se presente sin haber hecho algo para que sucediera.

Anexo N°13
Estructura de la Matriz de Gestión de Riesgos / Oportunidades y Tratamientos

Cabecera de la Sección de Identificación

Cabecera de la Sección de Tratamiento

Anexo N°14
Estructura de la Matriz de Contexto

MATRIZ DE CONTEXTO DEL PROGRAMA PENSION 65		
Entorno del Programa, factores externos e internos que pueden afectar el enfoque del programa, sus productos, sus servicios complementarios y las partes interesadas.		
Factores	**Condiciones**	**Efectos Potenciales**
Tamaño		
Organización		
Alcance		
Crecimiento		
Modelo		
Entidades		
Aliados		
Gobierno		
Normativas		

Anexo N°15
Estructura de la Matriz de Partes Interesadas

pensión65	MATRIZ DE PARTES INTERESADAS				PR-GCAL-13-01	Fecha de Elaboración/ Actualización	
						Versión	2022
N°	PARTE INTERESADA	REQUISITOS DE SUBVENCIÓN MONETARIA			REQUISITOS DE SERVICIOS COMPLEMENTARIOS (SABERES PRODUCTIVOS)		
		Sistema de Gestion			Sistema de Gestion		

Anexo Nº16
Lista de Activos de la Información

TIPO	CATEGORIA	DESCRIPCION	Confidencialidad	Integridad	Disponibilidad	Valor del Grupo de Activo

Anexo Nº 17 : Escala CID para Activos de la Información

Niveles	CONFIDENCIALIDAD
(3) Alta	Su distribución debe estar restringida a un pequeño grupo de personas, pues revelarla sin permiso puede tener un impacto negativo de grandes alcances para la organización empleados y/o terceros. Su acceso debe ser expresamente autorizado por el Propietario de la Información y restringido a un grupo reducido de usuarios que la necesite para el desarrollo de sus tareas habituales. Revelarla sin autorización puede repercutir negativamente, originando un impacto mayor en las operaciones.
(2) Media	La clasificación interna es la más común que se maneja en la organización. Su distribución está generalmente restringida a un grupo más grande de personas. Revelarla sin autorización puede repercutir negativamente, originando un impacto moderado en las operaciones, pero es posible remediar la situación en el corto plazo. La información de uso interno se convertirá en pública solo con la autorización del propietario de la información, quién deberá autorizar cualquier difusión de la misma. Los activos no requieren de medidas complejas de seguridad.
(1) Baja	La información pública no es confidencial y está enfocada al uso general tanto dentro como fuera de la organización. Podrá ser revelada por el dueño o responsable de la misma que tenga dentro de sus funciones la autorización para revelarla al público. No se afecta la organización si la información se divulga incluso al exterior de la misma.

Niveles	INTEGRIDAD
(3) Alta	Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo, retrasar sus funciones, o generar pérdidas de imagen severas a la organización, impacta a terceros.
(2) Media	Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo, retrasar sus funciones, o generar pérdida de imagen moderado a la organización.
(1) Baja	Información cuya pérdida de exactitud y completitud conlleva un impacto no significativo para la organización o externos.

Niveles	DISPONIBILIDAD
(3) Alta	No se puede disponer libremente del activo. La información requerida para la toma de decisiones debe estar disponible a la brevedad posible. Se generan costos, multas, se incumplen políticas, se retienen o impactan los valores o resultados de los procesos de la Entidad si la información no está disponible.
(2) Media	La no disponibilidad de la información puede conllevar un impacto negativo, retrasar sus funciones, o generar pérdida de imagen moderado a la organización, puede afectar a terceros.
(1) Baja	Se puede disponer libremente del activo y no habrá interrupciones del servicio. La organización no se afecta si el activo no está disponible pues no es vital para la toma de decisiones y, los esfuerzos por recuperarla no afectan la operación normal, inclusive si la información se pierde definitivamente.

Anexo Nº 18 : Criterios de Evaluación para Activos de la Información

Considerando un valor de ponderancia (pesos) igual a 1 para los criterios de confidencialidad, integridad y disponibilidad, la suma de sus valore combinados resulta la siguiente tabla, donde su sumatoria total de las combinaciones es 54.

PESO 1		RESULTADO DE VALORES C+I+D			1 PESO	
C	3	7	8	9	3	I
	2	5	6	7	2	
	1	3	4	5	1	
PESO 1		1	2	3	54	
		D				

Según la suma combinatoria se establece los rangos de criticidad, de acuerdo a la siguiente tabla: Rango de 8 a 9 = Crítico; Rango de 6 a 7 = Alto; Rango de 5 = Moderado; Rango de 4 = Menor y Rango de 3 = No Critico

CUANDO EL PESO DE C+I+D es = 1						
C	3	Alto	Critico	Critico	3	I
	2	Moderado	Alto	Alto	2	
	1	No Critico	Menor	Moderado	1	
		1	2	3		
		D				

La siguiente tabla es un resultado de combinaciones con sus respectivos valores críticos, considerando el peso de C+I+D por igual a 1

Aspecto de Seguridad afectado por el riesgo				
C	I	D	Suma combinada	VALOR CID
1	1	1	3	No Critico
1	1	2	4	Menor
1	2	1	4	Menor
2	1	1	4	Menor
1	1	3	5	Moderado
1	2	2	5	Moderado
1	3	1	5	Moderado
2	1	2	5	Moderado
2	2	1	5	Moderado
3	1	1	5	Moderado
1	2	3	6	Alto
1	3	2	6	Alto
2	1	3	6	Alto

2	2	2	6	Alto
2	3	1	6	Alto
3	1	2	6	Alto
3	2	1	6	Alto
1	3	3	7	Alto
2	2	3	7	Alto
2	3	2	7	Alto
3	1	3	7	Alto
3	2	2	7	Alto
3	3	1	7	Alto
2	3	3	8	Critico
3	2	3	8	Critico
3	3	2	8	Critico
3	3	3	9	Critico

pensión65
tranquilidad para más peruanos

MATRIZ DE CONTEXTO DE LA ORGANIZACIÓN

Entorno del Programa, factores externos e internos que pueden afectar el enfoque del programa, sus productos, sus servicios complementarios y las partes interesadas.

Factores	Condiciones	Efectos Potenciales ISO 37001:2016	Efectos Potenciales ISO 9001:2015	Efectos Potenciales ISO 27001:2013
Tamaño	Empleados con estructura de sueldos no estandarizada.	El tener empleados con el mismo cargo y responsabilidad, con diferencias de sueldos, motiva a que pierdan integridad y sean vulnerables a ser sobornados.		
Tamaño	La Gestion Operativa de las UT, no cuenta con documentos procedimentales.		Genera alto riesgo de fallos o errores en la identificacion, atención y servicio oportuno al Adulto Mayor.	
Tamaño	Contar con Unidades Territoriales en todas las regiones del Perú, siendo Lima la sede Central.			Evaluar el alcance inicial apropiado de la implementación de la norma ISO 27001 en el Programa.
Tamaño	Plataforma TiCS y mesa de ayuda insuficiente.			Ampliar el alcance a nivel nacional, de acuerdo con la accesibilidad y versatibilidad de la mesa de ayuda tecnologica.
Organización	La Pandemia COVI-19, y sus respectivas variantes, limitan reestablecer las actividades presenciales, relentizado los ciclos de reemplazo de personal por temas de contagío u/o enfermedades.		Genera el riesgo de fallos de errores por la sobrecarga de trabajo asumida por el personal en los puestos de reemplazos o vacantes.	
Organización	La coyuntura actual evidencia la necesidad de actualizar la organización del programa con la finalidad de brindar un servicio oportuno a nuestros usuarios.	Los usuarios requieren de nuevas modalidades de pago de sus subvenciones para evitar los riesgos de suplantaciones, sobornos, estafas, cobros indebidos, entre otros.	Los usuarios requieren de nuevas modalidades de pago de sus subvenciones generando más oportunidades de acceder al cobro de la subvencion.	
Organización	La coyuntura actual evidencia la necesidad de actualizar la organización del programa		El programa requiere una reestructuración organizacional acorde a la situación actual, que le permita realizar las mejoras oportunas garantizando la calidad del servicio al usuario.	
Organización	La coyuntura actual, evidencia la necesidad de actualizar tecnologicamente al Programa, contando para ello con el apoyo y gran interes de la Alta Dirección por implementar un sistema de gestión de seguridad de la información.			Infraestructura tecnologica se ha visto incrementada, teniendo una mejor capacidad para futuros crecimientos en el desarrollo de programas.
Organización	Estar Certificados en las Normas ISO 9001 e ISO 37001.			Disminuir el grado de complejidad del proceso de implementación de otros sistemas como el de la Norma ISO 27001
Alcance	Contar con unidades territoriales en las 24 regiones del Perú.	No tener un monitoreo remoto, presencial y permanente en las UT implicaría que se pueda materializar el riesgo de soborno.	No tener un Sistema de Información eficaz aumenta el riesgo de toma de decisiones erradas o no oportunas por parte de la Alta Dirección.	Plantear y evaluar las estrategias de implementación de la norma ISO 27001, empezando por la sede central y diversificando por etapas en las otras regiones.

pensión65
tranquilidad para más peruanos

MATRIZ DE CONTEXTO DE LA ORGANIZACIÓN

Entorno del Programa, factores externos e internos que pueden afectar el enfoque del programa, sus productos, sus servicios complementarios y las partes interesadas.

Factores	Condiciones	Efectos Potenciales ISO 37001:2016	Efectos Potenciales ISO 9001:2015	Efectos Potenciales ISO 27001:2013
Crecimiento	Capacitacion del Personal de Campo (Promotores)	No tener Capacitado a los Promotores en el Sistema de Gestión Antisoborno, implicaría un riesgo de vulnerabilidad al Programa.	No tener Capacitado a los Promotores en el Sistemas Integrado de Gestion, implicaría un riesgo de fallo en la atencion al usuario.	Falta de concientización del personal de la organización en el buen uso y cuidado de los equipos asignados y activos de información.
Crecimiento	Poseer poca difusión en seguridad de la información al personal.			Posible incumplimiento del personal de la organización en el buen uso de activos de información asignados.
Modelo	El modelo de acercamiento al AM, a través de la subvencion bimensual + servicios complementarios, cuyas entidades aliadas corresponden al Banco de la Nación y Otras Entidades del Estado como las DIRESAS, Gob. Regionales y Municipales.	El acercamiento y el acompañamiento en la prestacion de servicios complementarios, incrementa la vulnerabilidad del programa, al articular con mayor frecuencia con Entidades aliadas que desconocen nuestro sistema de gestion antisoborno.	Vulnerabilidad del Programa, al articular con entidades aliadas, que desconocen nuestro Sistema Integrado de Gestión, aumentando el riesgo que nos provean informacion errada, incompleta o no confiable, que pueda afectar las atenciones al Adulto Mayor.	Gestionar e incrementar la Proteccion de la información de los usuarios del Programa.
Modelo	Entrega de Subsidios Monetarios a través de BONOS, de acuerdo al Padrón entregado por el SISFOH.		Aumento de la capacidad de procesamiento de información, monitoreo y reprocesamiento de datos para la coordinación de la entrega del subsidio monetario - BONO a la población identificada en padrones.	Gestionar de manera adecuada el intercambio de información con las Entidades relacionadas a la subvención monetaria y subsidio (bonos).
Entidades	Articulacion con Entidades prestadoras de servicios complementarios ligados a la subvencion bimensual.	Programa tiene un riesgo de exposición mediático si se ve involucrado, en ser parte de la cadena de corrupcion de estas entidades aliadas sino difunde oportunamente el SGAS.	Programa se expone a ser afectado mediaticamente, por ser parte de la cadena de fallos que otras Entidades puedan tener, por no haberla corregido o por ser parte tambien de una gran cadena de fallo gubernamental.	Gestionar de manera adecuada el intercambio de información, considerando en los convenios u otro documentos de Acuerdos, artículos relacionados a los temas de seguridad de la información.
Aliados	Articulacion con Entidades financieras, Gobiernos Locales, Municipalidades, Prefecturas o Suprefecturas, ONG, etc.	Programa tiene un riesgo de exposición mediático si se ve involucrado, en ser parte de la cadena de corrupcion de estas entidades aliadas sino difunde oportunamente el SGAS.	Programa se expone mediáticamente a ser parte de una secuencia sistemática de fallos, que originan estas Entidades Aliadas; sino se reducen los riesgos con controles de monitoreo a la informacion y/o servicios prestados, que permitan realizar detecciones con la debida anticipación	Gestionar de manera adecuada el intercambio de información, considerando en los convenios u otro documentos de Acuerdos, artículos relacionados a los temas de seguridad de la información.
Gobierno	Cambios de Presidente / Gabinete. Cambios de Ministro/a del sector. Cambio de Director del Programa	Relentización de Procesos y/o actividades que hacen que los controles establecidos pierdan efectividad haciendo vulnerable las acciones de soborno.	Relentización de Procesos administrativos y/o actividades que hacen que los controles establecidos, tengan el riesgo de perdida de efectividad, haciendo vulnerable nuestro servicio oportuno al Adulto Mayor.	Gestionar las politicas de seguridad de la información en el programa para mantener la continuidad de los sistemas de gestión.
Gobierno	Cambios de Presidente / Gabinete. Cambios de Ministro/a del sector. Cambio de Director del Programa			Manejar adecuadamente cambios dirección politica, evaluando el impacto técnico en el sistema de gestión de seguridad de la información.
Normativas	Vacios normativos / legales en actividades que regulan relaciones economicas, politicas y sociales.	Incrementa el riesgo de vulnerabilidad de las personas en verse involucrados en actos de soborno, al no contar con un sistema antisoborno permanente.	Incrementa el riesgo de vulnerabilidad de las personas que estan, en estas actividades; elevando el riesgo de cometer errores que determinen una mala decision de la alta dirección o un mal servicio a un usuario.	Gestionar e incrementar la revisón de documentación relevantes e incluir en sus contenidos, aspectos relacionados a la seguridad de la información.

MATRIZ DE PARTES INTERESADAS

CODIGO: PR-GSGI-03-01	Fecha de Elaboración/ Actualización	ago/2022
	Versión	2022

N°	PARTE INTERESADA	REQUISITOS DE SUBVENCIÓN MONETARIA			REQUISITOS DE SERVICIOS COMPLEMENTARIOS (SABERES PRODUCTIVOS)		
		ISO 9001	ISO 37001	ISO 27001	ISO 9001	ISO 37001	ISO 27001
1	Gobierno Central	C1.1 Que se cumpla oportunamente con el gasto del Presupuesto Institucional asignado.	D1.1 Que se cumpla la aplicación de las sanciones que correspondan en el marco del Sistema de Gestión Antisoborno.	E.1.1 Que las entidades del Estado tengan implementado el Gobierno Digital y la ISO 27001	A1.1 Que se cumplan las leyes y normas brindadas por el Estado para la gestión del Programa.	B1.1 Que se cumpla el DS 092-2017-PCM que aprueba la Politica Nacional de Integridad y lucha contra la corrupción.	F1.1 Que el Programa tenga implementado el Gobierno Digital y la ISO 27001
2	Ministerio de Economía y Finanza (MEF)	C2.1 Cumplir con la asignación de presupuesto otorgada para el cierre de brechas de Potenciales Usuarios.	D2.1 Que se cumpla con la debida diligencia de la ejecución de los gastos presupuestados para el programa Pensión 65	E.2.1 Que las entidades del Estado cuenten con SSI para asegurar la información de los aplicativos de gastos presupuestales y de planeamiento.	A2.1 Que se cumplan con las metas presupuestarias otorgadas.	B2.1 Que las Entidades del Estado sean Transparentes en la ejecución del presupuesto institucional.	F2.1 Que el Programa cuente con un SSI para asegurar la información de los aplicativos de gastos presupuestales y de planeamiento.
3	Gobierno Locales (Municipalidades)	C3.1 Atención oportuna y eficiente de las solicitudes de afiliación enviadas por los GL. C3.2 Envio oportuno de los cronogramas de Pago. C3.3 Se realicen las coordinaciones previas para la realización de los pagos de la subvención monetaria	D3.1 Realizar el proceso de afiliación de usuarios, de manera transparente. D3.2 Garantizar la transparencia de la gestión del programa, difundiendo su politica gestión integral.	E.3.1 Que los aplicativos informaticos para registro de las Declaraciones Juradas para el proceso de afiliación sean confiables.	A3.1 Realizar la asistencia técnica para la implementación de Saberes Productivos a usuarios AM que son parte del CIAM A3.2 Asignar los recursos a los CIAM e implementar las acciones de intervención de Saberes en los plazos establecidos.	B3.1 Que se cumpla con la debida diligencia en la elaboracion de acuerdos o convenios para garantizar procesos transparentes entre las entidades del Estado.	F.3.1 Que se desarrollen aplicativos informaticos para el registro de desarrollo de Saberes Productivos
4	Personal del Programa	C4.1 Contar con los procesos normativos adecuados para brindar una mejor atención a los usuarios. C4.2 Capacitarse en temas de Gestión del Servicio de calidad a nuestros usuarios. C4.3 Pago oportuno de salarios.	D4.1 Trabajar con honestidad, integridad y transparencia. D4.2 Cumplimiento del código de conducta. D4.3 Cumplimiento del sistema de gestión antisoborno. D4.4 Conocimiento y utilizacion diligente de los canales de denuncia.	E4.1 Contar con activos de información que mantengan segura la información que se va generando en el puesto de trabajo. E4.2 Capacitarse en temas de Seguridad de la Información E4.3 Conocimiento en cuanto el proceso de Subvención Económica	A4.1 Buen Clima Laboral. A4.2 Instalaciones adecuadas para la ejecución de sus servicios. A4.3 Contar con los recursos oportunamente para el eficaz desempeño de la labor encomendada. A4.4 Capacitar al personal en temas de Cuidados y Asistencias al Adulto Mayor.	B4.1 Liderazgo y compromiso en el cumplimiento del Sistema de Gestión Antisoborno. B4.2 Procesos de Selección Transparentes. B4.3 Capacitar al promotor de las UTs en el SGAS para identificar riesgos potenciales.	F4.1 Contar con activos de información que mantengan segura la información que se va generando en el puesto de trabajo. F4.2 Capacitarse en temas de Seguridad de la Información F4.3 Conocimiento en cuanto el proceso de Saberes Productivos
5	Usuarios	C5.1 Cumplir los requisitos establecidos en la Ley de creación del Programa. C5.2 Pagar la Subvención monetaria de manera oportuna y exacta. C5.3 Facilitar la entrega de los subsidios monetarios (bonos) a traves de los diversos canales que ofrecen las entidades financieras. C5.4 Mejorar Contínuamente los modelos de entrega de la subvención.	D5.1 Velar por la honestidad en las Declaraciones Juradas, principalmente en temas referidos a su condición socioeconómica. D5.2 Facilitar el acceso y transparencia para realizar las denuncias de buena fe y su atencion respectiva, con la disponibilidad de la proteccion al denunciante.	E5.1. Que el Programa mantenga controles de seguridad de información para sus datos personales, así como los registros que han generado para la subvención monetaria	A5.1 Brindar asistencia técnica correspondiente para la implementación de Saberes Productivos y lograr la participación activa de nuestros usuarios.	B5.1 Transparencia en el proceso de integrar a nuestros usuarios en los temas de saberes productivos. B5.2 Difundir a los usuarios sobre la politica de gestión integral del Programa Pensión 65.	F5.1. Que el Programa mantenga controles de seguridad de información para sus datos personales, así como los registros de saberes productivos que han reazlizado.
6	Proveedores	C6.1 Cumplimiento de los terminos de referencia que correspondan a cada contrato. C6.2 Estar registrado en el OSCE. C6.3 Pago oportuno y completo de los servicios prestados.	D6.1 No ofrecer un beneficio al funcionario público para la asignación de la buena pro. D6.2 Comunicar el otorgamiento de un puntaje adicional a las empresas que presenten el certificado ISO 37001, anti soborno	E6.1 Que el programa comunique oportunamente los controles de seguridad de información para los proveedores.	A6.1 Difundir la Politica del Sistema de Gestión Integral del Programa Pensión 65 através de los canales de comunicación que se tenga con el proveedor de servicios.	B6.1 No supeditar los servicios prestados al pago de beneficios económicos.	F6.1 Que el programa comunique oportunamente los controles de seguridad de información para los proveedores.

pensión65
tranquilidad para más peruanos

MATRIZ DE PARTES INTERESADAS

CODIGO: PR-GSGI-03-01	Fecha de Elaboración/ Actualización	ago/2022
	Versión	2022

N°	PARTE INTERESADA	REQUISITOS DE SUBVENCIÓN MONETARIA			REQUISITOS DE SERVICIOS COMPLEMENTARIOS (SABERES PRODUCTIVOS)		
		ISO 9001	ISO 37001	ISO 27001	ISO 9001	ISO 37001	ISO 27001
7	Banco de la Nacion	C7.1 Cumplir con el Cronograma de Pagos. C7.2 Brindar la lista de usuarios que integran el RBU de manera oportuna. C7.3 Planificar oportunamente la articulación de los pagos de la subvención monetaria en sus distintas modalidades. C7.4 Coordinar y monitorear las diversas modalidades de pagos y solucionar oportunamente las incidencias que se presenten.	D7.1 Honestidad y transparencia en las transacciones de recursos financieros a los usuarios del programa. D7.2 Difundir la politica del sistema de gestión integral al personal del banco. D7.1 Informar sobre la transparencia del servicio durante el pago a los usuarios. D7.4 Gestionar y mejorar continuamente el servicio atención preferencial del banco bajo cualquier modalidad de pago al AM.	E7.1 Que el programa implemente los respaldos y mantenga la confidencialidad de toda la información proporcionado por el BN.	A7.1 Gestionar con las área de Responsabilidad Social de las Entidades publicas o privadas, el apoyo para incentivar el crecimiento de los servicios de educación financiera, tarjetización y Saberes Productivos.	No aplica	No aplica
8	RENIEC	C8.1 Gestionar la articulación oportuna de la información de usuarios fallecidos o con restricciones. C8.2 Gestionar la articulación oportuna para el registro de actualización de huellas y otorgamiento de DNI a los AM, evitando asi la restriccion del pago por la entidad bancaria.	D8.1 Difundir la politica del sistema de gestión integral al personal de RENIEC. D8.2 Gestionar y mejorar la calidad del trato preferencial al AM, durante los procesos de actualización de huellas o al gestionar un nuevo DNI.	E8.1 Que el programa implemente confidencialidad y respaldos a toda la información proporcionado por la RENIEC.	No aplica	No aplica	No aplica
9	SISFOH	C9.1 Gestionar la articulación para el traslado oportuno de los reportes de actualización de las CSE de usuarios, producto de las observaciones de las visitas domiciliarias.	D9.1 Difundir la politica del sistema de gestión integral a las autoriades de las Entidades Proveedoras de Informacion. D9.1 Gestionar y mejorar la calidad del trato peferencial del AM, durante los procesos de actualización de la CSE o gestion de renovación de la misma, ya que la demora o falta de la misma genera la desafiliacion automatica del usuario.	E.9.1 Que el programa implemente controles de seguridad a toda la información proporcionada	No aplica	No aplica	No aplica
10	Comité de Transparencia y Vigilancia Ciudadana (CTVC)	C10.1 Getionar la articulación para la oportuna atención de las respuestas a usuarios, producto de las Denuncias, Quejas y Reclamos (DQR) recibidas.	D10.1 Difundir la politica del sistema de gestión integral a las autoridades y personal de la CTVC que solicitan Informacion de manera recurrente sobre la transparencia de nuestros procesos.	E10.1 Que el Programa difunda su Política de Seguridad de la Información	No aplica	No aplica	No aplica
11	Ministerio de Salud	C11.1 Gestionar la articulación para las campañas de salud, en los puntos de pago a nuestros usuarios.	No aplica	No aplica	A11.1 Articular con la entidad para promover el desarrollo del Saber relacionado a la Medicina Tradicional Ancestral. A11.2 Articular con la entidad para la programación de campañas de salud para el AM	B11.1 Difundir la politica del sistema de gestión integral a las autoridades del MINSA, durante las campañas y/o promociones de salud al AM.	F11.1 Que el Programa difunda su Política de Seguridad de la Información

pensión65
tranquilidad para más peruanos

MATRIZ DE PARTES INTERESADAS

CODIGO: PR-GSGI-03-01

Fecha de Elaboración/ Actualización	ago/2022
Versión	2022

N°	PARTE INTERESADA	REQUISITOS DE SUBVENCIÓN MONETARIA			REQUISITOS DE SERVICIOS COMPLEMENTARIOS (SABERES PRODUCTIVOS)		
		ISO 9001	ISO 37001	ISO 27001	ISO 9001	ISO 37001	ISO 27001
12	Ministerio de la Mujer y Poblaciones Vulnerables.	C12.1 Gestionar y articular con la entidad competente para la visibilidad del AM en el Estado. C12.2 Gestionar la priorizacion de AM en la condición de su vulnerabilidad cuando presenta estado de abandono.	No aplica	No aplica	A12.1 Gestionar con la entidad, la promocion de los temas relacionados a la "violencia familiar" y "derechos del adulto mayor".	B12.1 Difundir la politica del sistema de gestión integral a las autoridades del MIMPV, durante las campañas contra la violencia familiar y promociones de los derechos del AM.	F12.1 Que el Programa difunda su Política de Seguridad de la Información
13	Ministerio de Educación	No aplica	No aplica	No aplica	A13.1 Articular con la entidad en la promoción de Servicios Complementarios, relacionados a la Alfabetización del AM.	B11.1 Difundir la politica del sistema de gestión integral a las autoriades del MINEDU, durante las campañas y/o promociones de alfabetización al AM.	F13.1 Que el Programa difunda su Política de Seguridad de la Información
14	Ministerio de Cultura	No aplica	No aplica	No aplica	A14.1 Articular con la entidad los Servicios Complementarios relacionados a la promoción de Saberes de Lenguas Ancentrales del AM.	B11.1 Difundir la politica del sistema de gestión integral a las autoriades del MINCU, durante las campañas y/o promociones al AM de las comunidades amazonicas.	F14.1 Que el Programa difunda su Política de Seguridad de la Información
15	Universidades e Institutos	C15.1 Gestionar y articular con la Entidad para promover el voluntariado para los servicios de corte de pelo, masajes, podologia, gestion de colas, acompañamiento y asistencia durante las campañas de pago.	D15.1 Difundir la politica del sistema de gestión integral a las autoriades y personal voluntariado de las universidades e institutos que participa durante la programación de pagos de la subvencion al AM	E15.1 Que el Programa difunda su Política de Seguridad de la Información	A15.1 Gestionar y articular con la entidad los Servicios Complementarios relacionados a la promocion del voluntariado y apoyo social en el acompañamiento al AM.	B12.1 Difundir la politica del sistema de gestión integral al personal que participa como voluntariado en los acompañamientos al AM en los diferentes servicios complementarios articulados por el programa.	F15.1 Que el Programa difunda su Política de Seguridad de la Información
16	Ministerio de Defensa / FFAA	C16.1 Gestionar y articular con la Entidad para facilitar el acceso y/o traslado del AM a los Puntos de pagos.	D16.1 Difundir la politica del sistema de gestión integral a las autoriades y personal del MINDEF y las Fuerzas Armadas, en las campañas de presencia del ESTADO en lugares de dificil acceso, durante el desarrollo de los procesos de pagos.	E16.1 Que el Programa difunda su Política de Seguridad de la Información	A16.1 Gestionar y articular con la entidad en el apoyo logistico de los Servicios Complementarios, relacionados a Campañas de Salud al AM en zonas alejadas o de dificil acceso.	B16.1 Difundir la politica del sistema de gestión integral a las autoriades y personal del MINDEF y las Fuerzas Armadas, en las campañas de presencia del ESTADO en lugares de dificil acceso, durante el desarrollo de los servicios complementarios	F16.1 Que el Programa difunda su Política de Seguridad de la Información
17	Ministerio de Desarrollo e Inclusión Social (MIDIS)	C17.1 Gestionar y articular con la Entidad el monitoreo del Plan de Desarrollo de la Calidad, asi como recoger las recomendaciones correspondientes en materia de estos temas. C17.2 Apoyo y facilidades en la asesoria en materia de evaluación y seguimiento de encuestas de percepción.	D17.1 Difundir la politica del sistema de gestión integral a las autoriades y personal del MIDIS. D17.2 Apoyo y facilidades en la asesoría en materia de evaluación y seguimiento enlos temas de Antisoborno y en los temas de Etíca e Integridad	E17.1 Que el Programa difunda su Política de Seguridad de la Información	A17.1 Gestionar y articular con la entidad en el apoyo con la información estadistica de las poblaciones vulnerables, de brechas y niveles de pobreza en el país.	No aplica	No aplica