MODELO INTEGRADO DE PLANEACION Y GESTION - MIPG

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

OFICINA DE SISTEMAS

ENERO DE 2023

Tabla de contenido

1. INTRODUCCIÓN

EL INSTITUTO FINANCIERO PARA EL DESARROLLO DE SANTANDER (IDESAN) teniendo en cuenta y de acuerdo a los lineamientos para el cumplimiento de sus objetivos estratégicos de seguridad de la información y consiente de la obligación que tiene para asegurar la confidencialidad, integridad y disponibilidad de la misma, ha establecido como marco de gobierno la implementación del MSPI y los lineamientosde gestión relacionados en la ISO 27001.

Para IDESAN es importante que estas herramientas actúen integralmente y den respuesta al tratamiento de riesgos de seguridad de la información con el cierre efectivo de las brechas identificadas y minimizando el impacto a causa de la materialización de alguno de ellos.

1. DEFINICIONES

- **MSPI:** El Modelo de Seguridad y Privacidad de la Información - MSPI, imparte lineamientos a las entidades públicas de todo orden, en materia deimplementación y adopción de buenas prácticas, tomando como referencia estándares internacionales, con el objetivo de orientar la gestión e implementación adecuada del ciclo de vida de la seguridad de la información (Planeación, Implementación, Evaluación, Mejora Continua), permitiendo habilitar la implementación de la Política de Gobierno Digital.
- **Acceso a la Información Pública:** Derecho fundamental consistente en lafacultad que tienen todas las personas de conocer sobre la existencia y acceso a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4).
- **Activo:** En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de ésta (sistemas, software, hardware, soportes, edificios, personas) que tenga valor para la organización. (ISO/IEC 27000).
- **Activos de Información y recursos:** se refiere a elementos de hardware yde software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos asociados con elmanejo de los datos y la información misional, operativa y administrativa decada entidad, órgano u organismo.
- **Archivo:** Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o Entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3)

- **Auditoría:** Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoría. (ISO/IEC 27000).
- **Autorización:** Consentimiento previo, expreso e informado del Titular parallevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3)
- **Bases de Datos Personales:** Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3)
- **Ciberseguridad:** Protección de activos de información, mediante el tratamiento de las amenazas que ponen en riesgo la información que se procesa, almacena y transporta mediante los sistemas de información que se encuentran interconectados.
- **Ciberespacio:** Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).
- **Control:** Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definiciónmás simple, es una medida que modifica el riesgo.
- **Datos Abiertos**: Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de losmismos (Ley 1712 de 2014, art 6).
- **Datos Personales:** Cualquier información vinculada o que pueda asociarsea una o varias personas naturales determinadas o determinables. (Ley 1581de 2012, art 3).
- **Datos Personales Públicos:** Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos

pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3)

- **Datos Personales Privados:** Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h)
- **Datos Personales Mixtos**: Para efectos de esta guía es la información quecontiene datos personales públicos junto con datos privados o sensibles.
- **Datos Personales Sensibles**: Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen losderechos y garantías de partidos políticos de oposición, así como los datosrelativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377de 2013, art 3)
- **Declaración de aplicabilidad** Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI,de la organización tras el resultado de los procesos de evaluación ytratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001. (ISO/IEC 27000).
- **Derecho a la Intimidad**: Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural (Jurisprudencia Corte Constitucional).
- **Encargado del Tratamiento de Datos**: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento dedatos personales por cuenta del responsable del Tratamiento. (Ley 1581 de 2012, art 3)
- **Gestión de incidentes de seguridad de la información** Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de

seguridad de la información. (ISO/IEC 27000).

- **Información Pública Clasificada**: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)
- **Información Pública Reservada**: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuadade acceso a la ciudadanía por daño a intereses públicos y bajo cumplimientode la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712de 2014. (Ley 1712 de 2014, art 6)
- **Ley de Habeas Data**: Se refiere a la Ley Estatutaria 1266 de 2008.
- **Ley de Transparencia y Acceso a la Información Pública**: Se refiere a laLey Estatutaria 1712 de 2014.
- **Mecanismos de protección de datos personales**: Lo constituyen las distintas alternativas con que cuentan las entidades destinatarias para ofrecer protección a los datos personales de los titulares tales como accesocontrolado, anonimización o cifrado.
- **Plan de continuidad del negocio** Plan orientado a permitir la continuaciónde las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).
- **Plan de tratamiento de riesgos** Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).
- **Privacidad:** En el contexto de este documento, por privacidad se entiendeel derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de lasfunciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL la correlativa obligación de proteger dichainformación en observancia del marco legal vigente.
- **Registro Nacional de Bases de Datos**: Directorio público de las bases dedatos sujetas a Tratamiento que operan en el país. (Ley 1581 de 2012, art

25)

- **Responsabilidad Demostrada**: Conducta desplegada por los responsables o encargados del tratamiento de datos personales bajo la cual la petición de la Superintendencia de Industria y Comercio deben estar en capacidad de demostrarle a dicho organismo de control que han implementado medidas apropiadas y efectivas para cumplir lo establecido en la Ley 1581 de 2012 y sus normas reglamentarias.
- **Responsable del Tratamiento de Datos**: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos. (Ley 1581 de 2012, art 3).
- **Riesgo** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información.Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).
- **Seguridad de la información:** Preservación de la confidencialidad, integridad, y disponibilidad de la información en cualquier medio: impreso odigital. (ISO/IEC 27000).
- **Seguridad digital:** Preservación de la confidencialidad, integridad, y disponibilidad de la información que se encuentra en medios digitales.
- **Titulares de la información**: Personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3)
- **Tratamiento de Datos Personales**: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley 1581 de 2012, art 3).
- **Trazabilidad** Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadasde modo inequívoco a un individuo o entidad. (ISO/IEC 27000).
- **Vulnerabilidad** Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

2. OBJETIVOS

2.1. Objetivo general

Establecer un marco de operación para la gestión integral de los riesgos deseguridad de la información desde su identificación hasta el diseño de un planadecuado para su tratamiento, que le permita asegurar el cumplimiento de sus objetivos estratégicos y la conservación de la confidencialidad, integridady disponibilidad de la información.

2.2. Objetivos específicos

- Reducir el impacto que pudiese ocasionar la materialización de los riesgosde seguridad de la información a través de la aplicación de controles para su tratamiento.
- Implementar el Modelo de Seguridad y Privacidad de la información propuesto por el MINTIC en la entidad, con el fin de contribuir al incremento de la transparencia en la gestión pública.
- Generar en el Instituto un marco de gobierno que permita el fortalecimientoy apropiación del conocimiento bajo una cultura organizacional con pensamiento basado en riesgos de seguridad de la información.
- Responder a las necesidades y expectativas de las partes interesadasexternas e internas, requisitos legales y reglamentarios aplicables.
- Dar lineamientos para la implementación de mejores prácticas de seguridadque permita identificar infraestructuras críticas en la entidad.
- Orientar a la entidad en las mejores prácticas en seguridad y privacidad.
- Optimizar la labor de acceso de información pública al interior de la entidad

3. ALCANCE

La gestión de riesgos de seguridad de la información para IDESAN enmarca todoslos procesos estratégicos, misionales, de apoyo y soporte, de evaluación y seguimiento.

Así mismo, el tratamiento del riesgo tendrá en cuenta los riesgos que se encuentrenen los niveles alto y extremos acordes a los lineamientos establecidos en su Manual para el Tratamiento de Riesgos de Seguridad de la Información.

4. MARCO DE REFERENCIA

4.1. **Ley 1712 de 2014:** Para la Implementación de la Estrategia de Gobierno enLínea, entidades del orden nacional; Modelo de Seguridad de la Información para la Estrategia de Gobierno Digital.

4.2. **Ley estatutaria 1581 de 2012:** Por la cual se dictan disposiciones generalespara la protección de datos personales.

4.3. **Norma técnica colombiana NTC - ISO/IEC 27001:** Estándar para la seguridad de la información.

4.4. Modelo de privacidad y seguridad de la información (MSPI) - MINTIC.

4.5. **Decreto 1499 de 2017**: Integración de los sistemas de Gestión y Modificatorio del 1083 de 2015, decreto único reglamentario del sector de lafunción pública.

4.6. **Decreto 612 de 2018**: Por el cual se fijan directrices para la integración de los panes institucionales de entidades estatales.

5. METODOLOGÍA PARA LA IMPLEMENTACIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (MSPI)

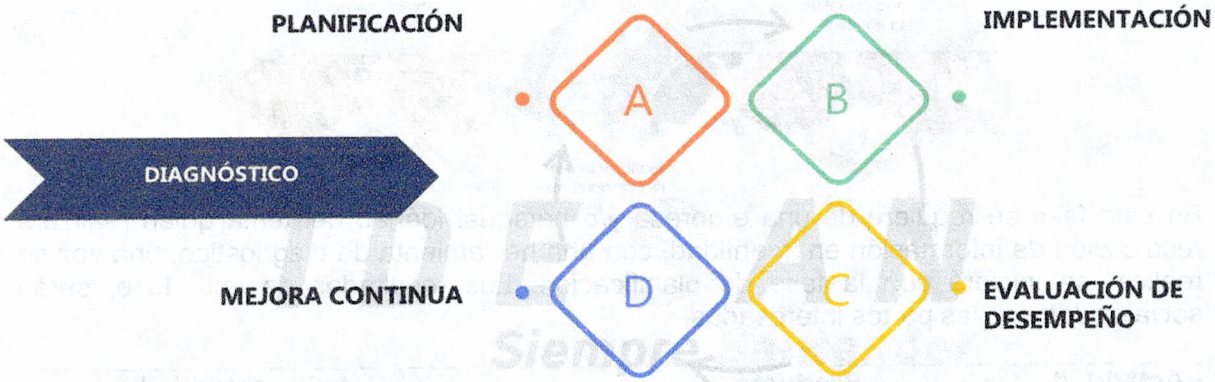
El Modelo de Seguridad y Privacidad de la información, contiene un ciclo de operación para la implementación, que consta de cinco (5) fases, las cualespermitirá que la entidad gestione adecuadamente de los activos de información en términos de seguridad y privacidad, siguiendo las directrices incluidas en el Modelo (MSPI) del Ministerio TIC, teniendo en cuenta que la Seguridad digital se constituyecomo un habilitador transversal de la Política de Gobierno Digital, y que se enfoca

en garantizar y preservar la confidencialidad, integridad y disponibilidad de la información de la entidad.

CICLO DE OPERACIÓN

En este capítulo se describe el modelo operación y cada una de las cinco (5) fasesque lo integran. Los objetivos, metas y herramientas que conllevan a crean un sistema de gestión sostenible para la seguridad y privacidad de la información. Como se he descrito anteriormente, este ciclo, corresponde a lo contemplado en elModelo de Seguridad y Privacidad de la Información del Mintic.

Figura 1. Ciclo de operación del MSPI



Diagnóstico: En esta etapa se identifica el estado actual de la entidad respecto a los lineamientos y requerimientos del MSPI.

Planificación: Con los resultados obtenidos de la etapa anterior, en esta etapa, se elabora el plan de seguridad y privacidad de la información, alineado con el objetivo misional, se definen metas, políticas relacionadas, indicadores y las actividades del proceso.

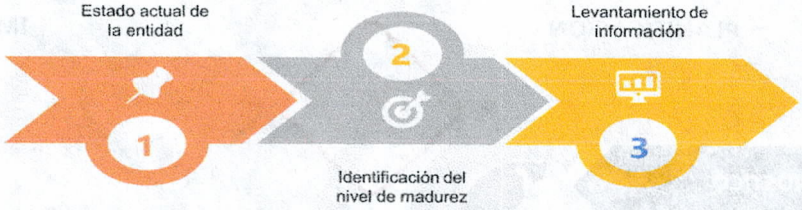
Implementación: En esta fase, se realizará la ejecución de las actividades relacionadas en la planificación realizada para lograr el cumplimiento de la política definida.

Evaluación de Desempeño: En el Modelo diseñado por MINTIC, esta etapaestá definida como: "un proceso de seguimiento y monitoreo del MSPI se hace conbase a los resultados que arrojan los indicadores de la seguridad de la informaciónpropuestos para verificación de la efectividad, la eficiencia y la eficacia de las acciones implementadas"[1].

Mejora Continua: En esta etapa se analizan en termino de mejoramiento, los resultados de las políticas implementadas y los niveles de incumplimiento de losobjetivos, con esto se diseña un plan de mejoramiento continuo de seguridad y privacidad de la información.

5.1. FASE 1. DIAGNOSTICO

El objetivo de esta fase es identificar el estado actual del IDESAN, con respecto a los requerimientos del MSPI.



En esta fase se requiere de una empresa y/o personal idóneo del tema quien realizará recolección de información en la entidad, con una herramienta de diagnóstico, una vez se realice, se iniciará con la fase de planificación. Los resultados de esta fase, serán socializados con las partes interesadas.

Actividad	Producto	Detalles actividades
Determinar el estado inicial	* **Estado actual del instituto**: Evaluación de efectividad de controles ISO27001:2013 * **Identificación nivel de madurez**: Nivel de madurez MSPI ***Identificación nivel de cumplimiento NIST**: Nivel de cumplimiento frente a las	Pruebas de vulnerabilidades internas de servidores
		Pruebas de vulnerabilidades internas de equipos
		Pruebas de vulnerabilidades externas

[1] https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

	mejores prácticas de Ciberseguridad. *Identificación vulnerabilidades: Identificar vulnerabilidades mediante pruebas de intrusióny hacking ético.	Presentación de informe con resultados

5.2. FASE DE PLANIFICACIÓN

Con los resultados de la fase anterior, se elabora el plan de seguridad digital y privacidad de la información, se define la metodología, alcance, objetivos, procesos,procedimientos en cumplimiento de la política de seguridad digital y privacidad de la información.

Actividad	Producto	Detalles actividades
Establecer un plan de seguridad y privacidad de la información basado en las necesidades y objetivos estratégicos del Instituto, priorizandoprocesos, sistemas de información, ubicaciones físicas.	* **Contexto del instituto:** Definir alcance del MSPI con base en las necesidades y expectativas de sus partes interesadas.	Identificación de partes interesadas y documentación del alcancedel MSPI alineado al actual SIG, PEI y necesidades del Instituto.
	* **Actualización inventario de activos de información:** Cronograma de aplicación de metodología para la actualización del inventario de activos de información	Mesa de trabajo para establecer Procesos críticos y pendientes a intervenirpara la actualización del inventario de los activos de información. Cronograma de aplicaciónpara el inventario de activos de información
	Manual y Política deseguridad y privacidad de la información debidamente aprobado por la Gerencia ysocializado a todas laspartes	Solicitud de ajustes documentales y de proceso. Mesas de trabajo para Seguimiento.

	interesadas	Socialización de resultados
	Procesos y procedimientos de SINORMALIZADOS	

NIT: 890.205.565-1	PBX: (7) 6430301 Telefax: (7) 6473850	CALLE 48 No. 27A – 48 C.P. 680003 BUCARAMANGA, SANTANDER	www.idesan.gov.co	Facebook: @idesansiempresantander	Twitter: @idesansiempres1

	Roles y Responsabilidades de SI: Designación del responsable de SI y asignación de funciones de SI	
	Integración del MSPI con el de Gestión Documental	
	Plan de comunicaciones y capacitación	Identificación de necesidades de capacitación
		Diseño de plan de comunicaciones
		Seguimiento a la implementación
	Mitigación de riesgos de perdida de información	Instructivo de copias de seguridad actualizado.

5.3. FASE DE IMPLEMENTACIÓN

Esta fase le permitirá a la entidad, llevar a cabo la implementación de la planificaciónrealizada en la fase anterior del MSPI.

Actividad	Producto	Detalles actividades
Identificación de activos de	Inventario con el listado de los activos de información de	Aplicación de actividades para el inventario de activos

información: de acuerdo a la priorización de los procesos se levanta el listado de activos de información primarios y secundario siguiendo la metodología establecida por la Organización alineada a estándares normativos del MinTic y la DAFP	IDESAN para los procesos misionales y de apoyo clasificados como críticos para la Organización	de Información. Consolidación de resultados Entrega producto final - Inventario de activos de información
Definición de los controles de seguridad: De acuerdo al plan parael tratamiento de los riesgos, seleccionar los controles mediante una declaración de aplicabilidad basados en el Anexo A ISO27001	Declaración de aplicabilidad	Mesas de trabajo para la elaboración de la declaración de aplicabilidad con base en las necesidades identificadas deseguridad de la información establecidas por la Organización
Definición de indicadores de gestión: Establecer indicadores que permitan medir la eficiencia de los controles y el nivel de implementación del MSPI	Hoja de vida de Indicadores de gestión de seguridad de la información	Diseño de indicadores de gestión para el seguimientoa la implementación demodelo de seguridad y privacidad de la información, adicionalmente de la eficacia de los controles establecidos

5.4. FASE DE EVALUACIÓN Y DESEMPEÑO

En esta fase, se realiza el proceso de seguimiento y monitoreo del MSPI, conformea los resultados de los indicadores de desempeño. (eficacia, efectividad, eficiencia) de la implementación de la política de SDPI.

Actividad	Producto	Detalles actividades
Plan de auditorías: Establecer una serie de auditorías internas/externas que permitan hacer monitoreo y seguimiento al MSPI junto con las acciones de mejora definidas en búsqueda de la Certificación	Plan de auditorías Informe evaluación de desempeño	Implementación de auditoríasy apoyo para el cierre de hallazgos

5.5. FASE DE MEJORA CONTINUA

En esta etapa se analizan en termino de mejoramiento, los resultados de las políticas implementadas y los niveles de incumplimiento de los objetivos, con esto se diseña un plan de mejoramiento continuo de seguridad y privacidad de la información.

Actividad	Producto	Detalles actividades
Planes de mejora continua	Planes de mejora	Documento con el plan de mejoramiento. Documento con el plan de comunicación de resultados.

6. CRONOGRAMA DE PLAN DE IMPLEMENTACIÓN DE SEGURIDAD DIGITAL Y PRIVACIDAD DE LA INFORMACIÓN

Actividad	Fecha de inicio	Fecha Final
FASE 1: DIAGNÓSTICO		
Determinar el estado inicial	**Marzo de 2023**	**Marzo de 2023**
FASE 2: PLANIFICACIÓN		
Establecer un plan de seguridad y privacidad de la información basadoen las necesidades y objetivosestratégicos del Instituto, priorizando procesos, sistemas de información, ubicaciones físicas.	**Abril de 2023**	**Mayo de 2023**
FASE 3: IMPLEMENTACIÓN		
Identificación de activos de información: de acuerdo a la priorización de los procesos se levanta el listado de activos de información primarios y secundario siguiendo la metodología establecida por la Organización alineada a estándares normativos del MinTic y la DAFP	**Junio de 2023**	**Julio de 2023**
Definición de los controles de seguridad: De acuerdo al plan parael tratamiento de los riesgos, seleccionar los controles mediante una declaración de aplicabilidad basados en el Anexo A ISO27001	**Agosto de 2023**	**Septiembre de 2023**
Definición de indicadores de gestión: Establecer indicadores quepermitan medir la eficiencia de los controles y el nivel de implementación del MSPI	**Octubre de 2023**	**Noviembre de 2023**
FASE 4: EVALUACIÓN DE DESEMPEÑO		
Plan de auditorías: Establecer una serie de auditorías internas/externas que permitan	**Diciembre de 2023**	**Diciembre de 2023**

hacer monitoreo y seguimiento al MSPI junto con las acciones de mejora definidas en búsqueda de la Certificación		
FASE 5: MEJORA CONTINUA		
Planes de mejora continua		

Elaboró: ***Ing Edwin O. Correa*** -Ingeniero de sistemas
Contratista Idesan 2022

Reviso: Dra. **Ana Milena Tristancho Ballesteros**
Coordinadora Grupo Financiero y Administrativo