PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
2022

INVIPASTO
POR UNA VIVIENDA DIGNA

INSTITUTO MUNICIPAL DE LA REFORMA URBANA Y VIVIENDA DE PASTO

SANDRA PATRICIA BRAVO LARRAÑAGA
Directora Ejecutiva

Historial de revisión

Fecha	Versión	Descripción	Autor
31/01/2022	1.0	Creación del documento	Ing. Fabio Vallejo

INTRODUCCIÓN

Con el fin de salvaguardar los activos de información del Instituto ante cualquier situación de amenaza, se establecerán diferentes mecanismos de seguridad y privacidad de la información, los cuales se comprenden a partir de un conjunto de medidas, procedimientos y controles establecidos. Para lo cual el MinTIC ha establecido diferentes lineamientos para aplicar el modelo de seguridad y privacidad a la información, esto garantiza que los activos de información mantengan su disponibilidad, integridad y confidencialidad. Para la implementación del Modelo de seguridad y Privacidad de la Información (MPSI) en INVIPASTO se presenta en el siguiente documento el plan de seguridad y privacidad de la información

1. OBJETIVO GENERAL

Definir la planificación de las actividades orientadas a fortalecer el tratamiento de la información que es generada, tratada y custodiada por el instituto en el presente plan; con el fin de hacer una identificación de riesgos y oportunidades para elevar el nivel de confianza con sus grupos de interés, mediante la preservación de su confidencialidad, integridad y disponibilidad, así como también la adopción de las buenas prácticas y el cumplimiento de la política de gobierno digital, el Modelo de Seguridad y Privacidad de la Información y el marco legal que le sea aplicable.

2. OBJETIVOS ESPECIFICOS

- Determinar las actividades necesarias para avanzar en la implementación y mejora de los controles de seguridad alineados con el Modelo de seguridad y privacidad de la información y la ISO 27001:2013.
- Contribuir a la disminución de incidentes y requerimientos relacionados con la seguridad de la información.
- Facilitar la implementación de los lineamientos del Marco de Referencia de Seguridad de la Información de Gobierno digital, relacionados con la seguridad de la información.
- Establecer un modelo aplicable y de mejoramiento continuo
- Definir y divulgar las políticas, lineamientos, procedimientos y buenas prácticas recomendaciones para establecer una cultura organizacional de Seguridad y Privacidad.

3. ALCANCE

El plan de Seguridad y Privacidad aplica a todos los procesos del instituto los cuales manejen, procesen o interactúen con información institucional.

Este plan está diseñado para cumplir la fase de determinar el estado actual de la gestión de seguridad y privacidad de la información al interior del instituto. Para realizar este paso los responsables del plan deben efectuar la recolección de la información con la ayuda de la guía de autoevaluación, guía de encuesta y guía metodológica de las pruebas de efectividad del MSPI.

4. DEFINICIONES

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

• **Activo:** En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC27000).

• **Activo de Información:** En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.

• **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)

• **Amenazas:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

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

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

• **Autorización:** Consentimiento previo, expreso e informado del Titular para llevar 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:** Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).

• **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 definición más 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 los mismos (Ley 1712 de 2014, art 6)

• **Datos Personales:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 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 que contiene 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 los

derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013, art 3)

• **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 y tratamiento 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 de datos 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 exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los

requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)

• **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 la Ley 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 acceso controlado, anonimización o cifrado.

• **Plan de continuidad del negocio:** Plan orientado a permitir la continuación de 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 entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL la correlativa obligación de proteger dicha información en observancia del marco legal vigente.

• **Registro Nacional de Bases de Datos:** Directorio público de las bases de datos 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 a 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. (ISO/IEC 27000).

• **Sistema de Gestión de Seguridad de la Información SGSI:** Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).

• **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 asociadas de 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).

• **Partes interesadas (Stakeholder):** Persona u organización que puede afectar a, ser afectada por no percibirse a sí misma como afectada por una decisión o actividad.

5. MARCO NORMATIVO

- Resolución 3564 de 2015 - Reglamenta aspectos relacionados con la Ley de Transparencia y Acceso a la Información Pública
- Decreto Reglamentario Único 1081 de 2015 - Reglamento sobre la gestión de la información pública
- Ley 1712 de 2014 - Ley de Transparencia y acceso a la información pública
- Ley 57 de 1985 -Publicidad de los actos y documentos oficiales
- Ley 594 de 2000 - Ley General de Archivos
- Ley Estatutaria 1757 de 2015 - Promoción y protección del derecho a la participación democrática
- Título 9 - Decreto 1078 de 2015 - Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones
- Ley estatutaria 1618 de 2013: Ejercicio pleno de las personas con discapacidad
- Ley 1437 de 2011: Código de Procedimiento Administrativo y de lo Contencioso Administrativo

- Acuerdo 03 de 2015 del Archivo General de la Nación Lineamientos generales sobre la gestión de documentos electrónicos

- Acuerdo 03 de 2015 del Archivo General de la Nación Lineamientos generales sobre la gestión de documentos electrónicos

- Decreto 019 de 2012 - Suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública

- Decreto 2364 de 2012 - Firma electrónica

- Ley 962 de 2005 - Racionalización de trámites y procedimientos administrativos procedimientos administrativos

- Decreto 1747 de 2000 - Entidades de certificación, los certificados y las firmas digitales

- Ley 527 de 1999 - Ley de Comercio Electrónico

- Decreto Ley 2150 de 1995 - Suprimen y reforman regulaciones, procedimientos o trámites innecesarios existentes en la Administración Pública

- Ley Estatutaria 1581 de 2012 - Protección de datos personales

- Ley 1266 de 2008 - Disposiciones generales de habeas data y se regula el manejo de la información.

6. REQUISITOS GENERALES

INVIPASTO, por medio de las políticas de gobierno digital y seguridad digital, impulsará la implementación del Modelo de Seguridad y Privacidad de la Información – MSPI propuesto por el MINTIC, en el contexto de las actividades globales de la entidad y de los riesgos que enfrenta. Para llevar a cabo este propósito, se basará en el modelo PHVA.

Planificar (Establecer el MSPI)	Establecer la política, los objetivos, procesos y procedimientos de seguridad pertinentes para gestionar los activos y el riesgo buscando mejorar la seguridad de la información, con el fin de entregar resultados acordes con las políticas y objetivos globales de una organización.
Hacer (Implementar y operar el MSPI)	Implementar y operar la política, los controles, procesos y procedimientos del MSPI.
Verificar (Hacer seguimiento y revisar el MSPI)	Evaluar, y, en donde sea aplicable, medir el desempeño del proceso contra la política y los objetivos de seguridad y la experiencia práctica, y reportar los resultados a la dirección, para su revisión.
Actuar (Mantener y mejorar el MSPI)	Emprender acciones correctivas preventivas con base en los resultados de la auditoría interna del MSPI y la revisión por la dirección, para lograr la mejora continua del MSPI.

7. ESTABLECIMIENTO Y GESTIÓN DEL MSPI

El alcance del MSPI en Instituto se establece para todos los procesos de la entidad. En concordancia con el ciclo de mejora continua, las actividades del modelo en cuestión, están distribuidas en cuatro (4) fases posteriores a la de Diagnostico.

A continuación, se describen las Fases del Modelo de Seguridad y Privacidad de la Información definido por los lineamientos del Gobierno Digital.

Fase de Diagnóstico:

Tiene el fin de identificar el estado actual de la organización con respecto al cumplimiento de los lineamientos de seguridad y privacidad de la información:

Las principales actividades de esta fase son:

- Identificar el Estado actual del instituto en cuanto a los lineamientos de Seguridad y privacidad de la información.
- Identificación del Nivel de Madurez del instituto con respecto al cumplimiento de los lineamientos de seguridad y la adopción del MSPI.
- Levantamiento de información referente a los principales activos de la organización.
- Identificación de las principales vulnerabilidades y amenazas a las que están expuestos los principales procesos y activos de información al igual que la efectividad de los controles implementados (si existen).
- El levantamiento de información y la identificación de fallos técnicos y administrativos de los procesos institucionales y de los activos de información, se realiza aplicando la Guia No. 1 metodología de pruebas de efectividad, definida por MinTIC como parte del modelo de seguridad.

Fase de Planificación:

Se procede con la definición de la estrategia referente a la planificación de la adopción del Modelo de Seguridad y privacidad de la Información que incluye:

- Se proyectara las políticas de seguridad y privacidad de la Información donde se definirán los objetivos, el alcance y se asignan los responsables de la gestión de la Seguridad y la privacidad de la información La política será sometida a aprobación y será divulgada al interior del instituto.
- Definir el plan de capacitación, comunicación y sensibilización
- Se construye la documentación requerida en cuanto a procedimientos. Formatos, instructivos y demás documentación requerida por el MSPI.
- Se realiza el inventario y la clasificación de activos de información.
- Se realiza el análisis de riesgos al que están expuestos los activos de información.

Fase de Implementación:

En esta fase se procede izar los lineamientos definidos en la planificación al igual que las políticas, procedimientos y demás instrumentos construidos en la fase anterior. A continuación, se relacionan las principales actividades referentes a la Implementación del MSPI:

- Implementación de los planes, procedimientos, políticas e instructivos.
- Definir los indicadores de gestión que permitan medir el cumplimiento de los lineamientos implementados en seguridad de la información, tales como: La efectividad de los controles, la Eficiencia del MSPI al interior del instituto, proveer los estados de seguridad de los principales componentes del sistema.

Fase de Evaluación de Desempeño:

El proceso de seguimiento y monitoreo del MSPI se hace con base a los resultados que arrojan los indicadores de la seguridad de la información propuestos para verificación de la efectividad, la eficiencia y la eficacia de las acciones implementadas. Las principales actividades de esta fase se relacionan a continuación:

- Monitoreo, medición, análisis y evaluación del plan de tratamiento de riesgos

a partir de la medición de la efectividad de los controles técnicos y demás contramedidas administrativas adoptadas por la organización.

- Revisión de la efectividad del sistema de gestión de seguridad de la información por parte de la alta dirección

Fase de Mejora Continua:

En esta fase, se toman los resultados obtenidos de la monitorización, medición y evaluación como parámetros de entrada para diseñar un plan para el mejoramiento continuo de la postura de seguridad y privacidad de la información tomando las Acciones para mitigar las debilidades identificadas.

8. REQUISITOS DE DOCUMENTACION

8.1 GENERALIDADES

Los documentos del MSPI se crearan en el sistema de gestión de calidad en el proceso de Gestión de Tecnologías de la Información.

8.2 CONTROL DE DOCUMENTOS

La creación de documentos del MSPI se acoge a los procedimientos que establezcan en el sistema de gestión de calidad del instituto dentro del proceso de mejora continua.

8.3 CONTROL DE REGISTROS

Los empleados del instituto pueden acceder a registros archivados solamente después de obtener un permiso de la persona designada como responsable del archivo de registros individuales. Se determinará la ubicación de los registros según el tipo de documento del MSPI, cuando los documentos deban ser custodiados por las dependencias igual mente se determinará el manejo que se le debe dar a los mismos.

9. RESPONSABILIDAD DE LA INFORMACION

9.1 RESPONSABILIDAD DE LA DIRECCION

INVIPASTO a través de un Comité Institucional de seguridad digital, será la responsable de definir la política de seguridad de la información de primer y segundo nivel, sin embargo para dar fundamento a estas políticas se deberán aprobar mediante decreto.

9.2 GESTION DE RECURSOS

9.2.1 PROVICION DE RECURSOS

Cada dependencia será responsable de apropiar los recursos financieros necesarios para la implementación de los controles necesarios para mitigar los riesgos de seguridad de la información.

De igual manera cada dependencia en cabeza del funcionario de nivel directivo que tenga a su cargo es responsable de la ejecución de las actividades necesarias para garantizar la seguridad de los activos de información y de la implementación de los controles necesarios para mitigar los riesgos de seguridad de lo información.

9.2.2 FORMACION TOMA DE CONSIENCIA Y COMPETENCIA

INVIPASTO a través de la subdirección administrativa y financiera dentro del plan institucional de capacitaciones deberá incluir un componente relacionado con seguridad de la información.

10. AUDITORIAS INTERNAS DEL MSPI

Las auditorías del sistema MSPI están en una fase inicial de implementación se deberán desarrollar en un momento donde la entidad tenga mayor madurez del mismo. La entidad deberá determinar la competencia para la realización de estas auditorías.

11. REVISION DEL MSPI POR LA DIRECCION

AI menos una vez al año mediante el Comité Institucional en la Política de Seguridad Digital realizará una revisión del MSPI para asegurar su conveniencia, suficiencia y eficacia. Esta revisión debe incluir la evaluación de las oportunidades de mejora y la necesidad de cambios del MSPI, incluidos la política de seguridad y los objetivos de seguridad.

Las entradas que se consideraron para la revisión del MSPI por la dirección son:

- Retroalimentación de las partes interesadas.
- Técnicas, productos o procedimiento que se pueden usar en la organización para mejorar el desempeño y eficacia del MSPI.
- Estado de las acciones correctivas y preventivas.
- Informes de seguimiento al plan de tratamiento de riesgos.
- Documentos relacionados con incidentes de seguridad de la información.

Los resultados de la revisión por la dirección deben incluir cualquier decisión y acción relacionada con:

- La mejora de la eficacia del MSPI.
- La modificación de los procedimientos y controles que afecten la seguridad de la información, para responder a eventos internos o externos que puedan tener impacto en el MSPI.
- Evaluación del plan de tratamiento de riesgos de seguridad de la información.

12. MEJORA DEL MSPI

12.1 MEJORA CONTINUA El MSPI

Al integrar el MSPI con el Sistema de Gestión de la Calidad, se acogera a los procedimientos de mejora continua que se aplican en este sistema.

La entidad debe mejorar continuamente la eficacia del MSPI mediante:

- El uso de la política de seguridad de la información.
- Los objetivos de seguridad de la información.
- Las acciones correctivas y preventivas y la revisión por la dirección.

13. PLAN DE ACCIÓN

Las actividades necesarias para avanzar en la implementación del sistema de seguridad de la información son:

Actividad	Producto	Meta	Responsable	Inicio	Fin
Elaborar diagnóstico de seguridad de la información	Diagnóstico de seguridad de la información elaborado	Un (1) diagnóstico deseguridad de la información	Sistemas	.Feb – 2022	Jun - 2022
Definir las políticas de uso de correos electrónicos, política de uso de redes sociales, política de uso de internet, política de gestión de medios de almacenamiento, política de escritorio despejado y pantalla despejada, política de copias de seguridad	Políticas de uso de correos electrónicos, política de uso de redes sociales, política deuso de internet, política de gestión de medios de almacenamiento, política de escritorio despejado y pantalla despejada,política de copias de seguridad definidas	Seis (6) políticas deseguridad de la información	Sistemas	Feb – 2022	Abr - 2022
Implementar las políticas de uso de correos electrónicos, política de uso de redes sociales, política de uso de internet, política de gestión de medios de almacenamiento, política de escritorio despejado y pantalla despejada, política de copias deseguridad	Políticas de uso de correos electrónicos, política de uso de redes sociales, política deuso de internet, política de gestión de medios de almacenamiento, política de escritorio despejado y pantalla despejada, política de copias de seguridad implementadas	Seis (6) políticas deseguridad de la información	Sistemas	Abr – 2022	Jun – 2022
Sensibilizar las temáticas de seguridad y privacidad de la información acorde al plan institucional de capacitaciones	Temáticas de seguridad y privacidad de la información acorde al plan institucional de capacitaciones socializadas	Una (1) socializaciones en temas de seguridad y privacidad de la información	Sistemas	Feb – 2022	Dic - 2022
Adecuar cableado estructurado casa china INVIPASTO	cableado estructurado casa china INVIPASTO	Un (1) cableado estructurado casa china INVIPASTO	Sistemas	Feb - 2022	Dic - 2022
Inicio fase 1 levantamiento de información documentación Migrar del protocolo de red IPv4 a IPv6	Protocolo de red IPv4 a IPv6 migrado	Un (1) protocolo de redIPv6	Sistemas	Feb – 2022	Dic - 2022
Definir e implementar la política deprotección de datos personales	Definir e Implementar la política deprotección de datos personales	Dos (1) Definir e Implementar la política de protección de datos personales	Sistemas	Feb – 2022	Dic - 2022

Actividad	Producto	Meta	Responsable	Inicio	Fin
Evaluar el estado actual de licenciamiento de software	Estado actual de licenciamiento de software evaluado	Un (1) informe de estado actual de licenciamiento de software	Sistemas	Feb – 2022	Jun -2022
Implementar procedimiento para realizar copias de seguridadde información digital institucional	Procedimientos y mecanismos para realizarcopias de seguridad de información digital institucional implementados	Un (1) procedimiento para realizar copias de seguridad	Sistemas	Mar – 2022	Jul - 2022
Programar el plan de mantenimiento de servicios tecnológicos	plan de mantenimiento deinfraestructura tecnológica programado	Un (1) plan de mantenimiento de infraestructura tecnológica	Sistemas	Feb – 2022	Mar - 2022
Ejecutar el plan de mantenimiento de servicios tecnológicos	Ejecutar el plan de mantenimiento de infraestructura tecnológica ejecutado	Un (1) plan de mantenimiento de infraestructura tecnológica	Sistemas	Feb – 2022	Dic - 2022
Implementar sistema Orfeo para la gestión documental	sistema Orfeo para la gestión documental	Un (1) sistema Orfeo para la gestión documental	Sistemas	Feb – 2022	Dic - 2022
Implementar sistema para regular y resguardar el fluido electrico	sistema para regular y resguardar el fluido electrico	Un (1) sistema para regular y resguardar el fluido electrico	Sistemas	Feb – 2022	Dic - 2022