PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN

2020 – 2023

GOBERNACIÓN DE ANTIOQUIA
SECRETARÍA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

UNIDOS

Andrés Orlando López Lujan

Secretario de Tecnologías de Información y las comunicaciones

Patricia Restrepo Vélez

Directora de Tecnología e Información

Secretaría de Tecnologías de Información y las Comunicaciones

2021

GOBERNACIÓN DE ANTIOQUIA

SECRETARÍA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

UNIDOS

Contenido

Equipo que trabajo y apoyó en la construcción del PESI

Nombre	Rol
Andrés Orlando López Luján	Secretario de Tecnologías de Información y las Comunicaciones
Patricia Restrepo Vélez	Directora de Tecnología e Información
Sergio Andrés Cadavid Echeverry Pablo Andrés Hidalgo Lara John Fredy Borja Carvajal Alejandro Ospina Gil Iván Yesid Espinoza Guzmán	Construcción del PESI desde el enfoque de la MSPI y la guía propuesta por MINTIC

Tabla 1 - Equipo Que Trabajo Y Apoyó En La Construcción Del PESI

INTRODUCCIÓN

La Gobernación de Antioquia como Entidad Gubernamental está en la obligación de cumplir con la política de gobierno digital impuesta en el decreto No. 1008 del 14 de junio 2018, por la cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de las Tecnologías de Información y Comunicaciones.

Que en la política de gobierno digital en su artículo 2.2.9.1.1.3. – Principios; tiene como prioridad la seguridad de la información, el cual dice textualmente: "Este principio busca crear condiciones de uso confiable en el entorno digital, mediante un enfoque basado en la gestión de riesgos, preservando la confidencialidad, integridad y disponibilidad de la información de las entidades estatales, y de los servicios que prestan al ciudadano".

Para la realización del documento se tomará como base los lineamientos de seguridad de la información establecidos por la política de seguridad digital de junio de 2018. La Gobernación de Antioquia se guiará bajo los lineamientos normativos de la NTC/ISO 27001:2013, la cual establece los requisitos de la implementación del SGSI, la NTC/ISO 31000:2018; que proporciona un esquema para la gestión de riesgos y las mejores prácticas, tales como la 27002:2015, ISO 27005:2009, entre otras; buscando mejorar el desempeño y la capacidad de prestar un servicio que responsa a las necesidades y expectativas de las partes interesadas.

Por otra parte, el Plan Estratégico de Tecnologías de la Información y Comunicaciones (PETI), es un documento que expresa las intenciones de la organización, en la implementación de iniciativas y acciones que promuevan el uso de las Tecnologías de la Información y las Comunicaciones – TIC's como contribución al logro de los Objetivos y Lineamientos Estratégicos enmarcados en el Plan Estratégico Institucional, Plan Diamante 2016-2022. El PESI descrito en este documento está alineado completamente con el PETI.

El documento PETI define lineamientos para el mejoramiento del nivel de madurez institucional en la implementación de soluciones tecnológicas que generen valor y promuevan el cumplimiento de la misión con sostenibilidad tecnológica. El fortalecimiento y mejoramiento de la infraestructura tecnológica, el fortalecimiento de una mesa de ayuda, la implementación de los sistemas de seguridad de la información y la continuidad de negocio, la optimización en el procesamiento y análisis de información, el fortalecimiento y mejora de los procesos institucionales (Estratégicos, Misionales y de Apoyo) y de gestión de la información y gobernabilidad de TI, de acuerdo con la Estrategia Gobierno en Línea - GEL del Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC (Para mayor información ver PETI).

Finalmente, los lineamientos y proyectos para el desarrollo, optimización e implementación efectiva de los Sistemas de Información, así como las iniciativas que permitirán una adecuada gestión de la Infraestructura de Hardware/Software, basados en el Modelo de Seguridad y Privacidad de la Información – MSPI y en las mejores prácticas de Gestión de Servicios y Proyectos de TI, contribuirán no solo con el logro de los objetivos institucionales, sino en la generación de confianza en el uso de los mecanismos tecnológicos para una mejor relación Estado – Ciudadano y la protección de los activos de información (PETI).

OBJETIVO

Definir un Plan Estratégico de Seguridad de la Información, en adelante PESI, liderada por la Dirección de Informática de la Gobernación de Antioquia, en adelante GOBANT, a partir de la vigencia 2020 hasta el año 2023, que responda a las necesidades de preservar la confidencialidad, la integridad y la disponibilidad sobre los activos de información.

Objetivos Específicos

1. Comunicar e implementar la Estrategia de Seguridad de la Información.
2. Incrementar el nivel de madurez en la gestión de la seguridad de la información.
3. Implementar y apropiar el Modelo de Privacidad y Seguridad de la Información MPSI, con el objetivo de proteger la información y los sistemas de información, de acceso, uso, divulgación, interrupción o destrucción no autorizada.
4. Hacer uso eficiente de los recursos de TI (Humano, Físico, Financiero, Tecnológico, etc.) para garantizar la continuidad en la prestación de los servicios.
5. Definir las responsabilidades relacionadas con el manejo de la seguridad.
6. Establecer una metodología de gestión de seguridad de la información clara y estructurada.
7. Reducir el riesgo de pérdida, robo o corrupción de información.
8. Garantizar que los usuarios tengan acceso a la información a través de medidas de seguridad que garanticen la confidencialidad, integridad y disponibilidad de esta.
9. Cumplir con la legislación vigente sobre información personal, propiedad intelectual y otras.
10. Optimizar la seguridad de la información con base en la gestión de procesos.

ALCANCE

El PESI tiene como finalidad el diagnóstico, análisis, definición y planeación del manejo de la seguridad de los procesos que se ejecutan en GOBANT y será actualizado anualmente; estos apoyarán el cumplimiento de los procesos y objetivos propuestos por las diferentes dependencias de la Entidad y está articulado de manera global en relación con la seguridad de la información. Teniendo en cuenta el análisis de contexto interno, externo y las partes interesadas, la GOBANT define el alcance de su Sistema de Gestión de Seguridad de la Información (SGSI) y del PESI, en términos de las características de la entidad, su ubicación, sus activos y su tecnología así:

Alcance: “La Gobernación de Antioquia (GOBANT) adopta, establece, implementa, opera, verifica y mejora el Sistema de Gestión de Seguridad de la Información (SGSI) para todos sus procesos: misionales, de apoyo y de direccionamiento”.

La GOBANT acorde con su naturaleza jurídica, misión y visión, encontró aplicables todos los requisitos de la NTC/ISO 27001:2013 y todos los controles del Anexo A, sin excepción alguna.

En la siguiente ilustración se muestran los procesos institucionales que hacen parte del alcance del SGSI:

Ilustración 1 – Mapa de procesos de la Gobernación de Antioquia

DEFINICIONES

Acción Correctiva: Acción para eliminar la causa de una no conformidad y prevenir su repetición. Va más allá de la simple corrección.

Acción preventiva: Medida de tipo proactivo orientada a prevenir potenciales no conformidades.

Aceptación del riesgo: Decisión informada de asumir un riesgo concreto.

Activo: En relación con seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas, etc.) que tengan valor para la organización.

Alcance: Ámbito de la organización que queda sometido al SGSI.

Amenaza: Causa potencial de un incidente no deseado, puede provocar daños a un sistema o a la organización.

Análisis de riesgos: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.

Autenticidad: Propiedad de que una entidad es lo que afirma ser.

CIA: Véase: CID. Acrónimo inglés de Confidentiality, Integrity y Availability, las dimensiones básicas de la seguridad de la información.

CID: (CIA). Acrónimo español de Confidencialidad, Integridad y Disponibilidad, las dimensiones básicas de la seguridad de la información.

COBIT: Control Objectives for Information and related Technology. Publicados y mantenidos por ISACA. Su misión es investigar, desarrollar, publicar y promover un conjunto de objetivos de control de tecnología de información rectores, actualizados, internacional y generalmente aceptados para ser empleados por gerentes de empresas y auditores.

Compromiso de la Dirección: (Management commitment). Alineamiento firme de la Dirección de la organización con el establecimiento, implementación, operación, monitorización, revisión, mantenimiento y mejora del SGSI. La versión de 2013 de ISO 27001 lo engloba bajo la cláusula de Liderazgo.

Confidencialidad: (Confidentiality). Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

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.

Control correctivo: (Corrective control). Control que corrige un riesgo, error, omisión o acto deliberado antes de que produzca pérdidas relevantes. Supone que la amenaza ya se ha materializado pero que se corrige.

Control detectivo: (Detective control). Control que detecta la aparición de un riesgo, error, omisión o acto deliberado. Supone que la amenaza ya se ha materializado, pero por sí mismo no la corrige.

Control disuasorio: (Deterrent control). Control que reduce la posibilidad de materialización de una amenaza, p.ej., por medio de avisos o de medidas que llevan al atacante a desistir de su intención.

Control preventivo: (Preventive control). Control que evita que se produzca un riesgo, error, omisión o acto deliberado. Impide que una amenaza llegue siquiera a materializarse.

Corrección: Acción para eliminar una No Conformidad detectada. Si lo que se elimina es la causa de la no conformidad, véase acción correctiva.

Cuadro de Mando Integral: (Balance Score Card - BSC), es un modelo de gestión que traduce la estrategia en objetivos relacionados entre sí, medidos a través de indicadores y ligados a unos planes de acción que permiten alinear el comportamiento de los miembros de la organización con la estrategia de la empresa.

Declaración de aplicabilidad: (Statement Of Applicability; SOA). Documento que enumera los controles aplicados por el 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.

Desastre: (Disaster). Cualquier evento accidental, natural o malintencionado que interrumpe las operaciones o servicios habituales de una organización durante el tiempo suficiente como para verse la misma afectada de manera significativa.

Directiva o directriz: (Guideline). Una descripción que clarifica qué debería ser hecho y cómo, con el propósito de alcanzar los objetivos establecidos en las políticas.

Disponibilidad: (Availability). Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

Estimación de riesgos: (Risk evaluation). Proceso de comparar los resultados del análisis de riesgos con los criterios de riesgo para determinar si el riesgo y/o su magnitud es aceptable o tolerable.

Evaluación de riesgos: (Risk assessment). Proceso global de identificación, análisis y estimación de riesgos.

Evidencia objetiva: (Objective evidence). Información, registro o declaración de hechos, cualitativa o cuantitativa, verificable y basada en observación, medida o test, sobre aspectos relacionados con la confidencialidad, integridad o disponibilidad de un proceso o servicio o con la existencia e implementación de un elemento del sistema de gestión de seguridad de la información.

Gestión de claves: (Key management). Controles referidos a la gestión de claves criptográficas.

Gestión de incidentes de seguridad de la información: (Information security incident management). Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información.

Gestión de riesgos: (Risk management). Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. Se compone de la evaluación y el tratamiento de riesgos.

Identificación de riesgos: (Risk identification). Proceso de encontrar, reconocer y describir riesgos.

Incidente de seguridad de la información: (Information security incident). Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Integridad: (Integrity). Propiedad de la información relativa a su exactitud y completitud.

Inventario de activos: (Assets inventory). Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) dentro del

alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.

ISO: Organización Internacional de Normalización, con sede en Ginebra (Suiza). Es una agrupación de entidades nacionales de normalización cuyo objetivo es establecer, promocionar y gestionar estándares (normas).

ISO 17799: Código de buenas prácticas en gestión de la seguridad de la información adoptado por ISO transcribiendo la primera parte de BS7799. Dio lugar a ISO 27002, por cambio de nomenclatura, el 1 de Julio de 2007. Ya no está en vigor.

ISO 19011: "Guidelines for auditing management systems". Norma con directrices para la auditoría de sistemas de gestión. Guía de utilidad para el desarrollo, ejecución y mejora del programa de auditoría interna de un SGSI.

ISO/IEC 27001: Norma que establece los requisitos para un sistema de gestión de la seguridad de la información (SGSI). Primera publicación en 2005; segunda edición en 2013. Es la norma en base a la cual se certifican los SGSI a nivel mundial.

ISO/IEC 27002: Código de buenas prácticas en gestión de la seguridad de la información. Primera publicación en 2005; segunda edición en 2013. No es certificable.

ITIL: IT Infrastructure Library. Un marco de gestión de los servicios de tecnologías de la información.

NIST: (National Institute of Standards and Technology**),** Agencia de la Administración de Tecnología del Departamento de Comercio de los Estados Unidos. La misión de este instituto es promover la innovación y la competencia industrial en Estados Unidos mediante avances en metrología, normas y tecnología de forma que mejoren la estabilidad económica y la calidad de vida.

No conformidad: (Nonconformity). Incumplimiento de un requisito.

No repudio: Según [CCN-STIC-405:2006]: El no repudio o irrenunciabilidad es un servicio de seguridad que permite probar la participación de las partes en una comunicación. Según [OSI ISO-7498-2]: Servicio de seguridad que previene que un emisor niegue haber remitido un mensaje (cuando realmente lo ha emitido) y que un receptor niegue su recepción (cuando realmente lo ha recibido).

Parte interesada: (Interested party / Stakeholder). Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

PDCA: Plan-Do-Check-Act. Modelo de proceso basado en un ciclo continuo de las actividades de planificar (establecer el SGSI), realizar (implementar y operar el SGSI), verificar (monitorizar y revisar el SGSI) y actuar (mantener y mejorar el SGSI). La actual versión de ISO 27001 ya no lo menciona directamente, pero sus cláusulas pueden verse como alineadas con él.

Plan de Continuidad del Negocio: (Bussines Continuity Plan). Plan orientado a permitir la continuación de las principales funciones del negocio en el caso de un evento imprevisto que las ponga en peligro.

Plan de tratamiento de riesgos: (Risk treatment plan). Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.

Política de escritorio despejado:(Clear desk policy). La política de la empresa que indica a los empleados que deben dejar su área de trabajo libre de cualquier tipo de informaciones susceptibles de mal uso en su ausencia.

Proceso: (Process). Conjunto de actividades interrelacionadas o interactuantes que transforman unas entradas en salidas.

Propietario del riesgo: (Risk owner). Persona o entidad con responsabilidad y autoridad para gestionar un riesgo.

Recursos de tratamiento de información: (Information processing facilities). Cualquier sistema, servicio o infraestructura de tratamiento de información o ubicaciones físicas utilizadas para su alojamiento.

Riesgo: (Risk). 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.

Riesgo residual: (Residual risk). El riesgo que permanece tras el tratamiento del riesgo.

Segregación de tareas: (Segregation Of Duties - SOD). Reparto de tareas sensibles entre distintos empleados para reducir el riesgo de un mal uso de los sistemas e informaciones deliberado o por negligencia.

Seguridad de la información: (Information Security). Preservación de la confidencialidad, integridad y disponibilidad de la información.

Selección de controles: (Control selection). Proceso de elección de los controles que aseguren la reducción de los riesgos a un nivel aceptable.

SGSI: (ISMS). Véase: Sistema de Gestión de la Seguridad de la Información.

Sistema de Gestión de la Seguridad de la Información: (Information Security Management System). 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 del riesgo y de mejora continua.

SoA: Acrónimo inglés de Statement of Applicability. Véase: Declaración de aplicabilidad.

Tratamiento de riesgos: (Risk Treatment). Proceso de modificar el riesgo, mediante la implementación de controles.

Trazabilidad: (Accountability). Según [CESID:1997]: 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.

Vulnerabilidad: (Vulnerability). Debilidad de un activo o control que puede ser explotada por una o más amenazas.

NORMAS APLICABLES

NORMAS APLICABLES
Constitución Política de Colombia 1991. Artículo 15. Reconoce como Derecho Fundamental el Habeas Data.
Artículo 20. Libertad de Información.
Código Penal Colombiano - Decreto 599 de 2000
Ley 906 de 2004, Código de Procedimiento Penal.
Ley 87 de 1993, por la cual se dictan Normas para el ejercicio de control interno en las entidades y organismos del Estado, y demás normas que la modifiquen.
Decreto 1599 de 2005, por el cual se adopta el Modelo Estándar de Control Interno MECI para el Estado Colombiano.
Ley 734 de 2002, del Congreso de la República de Colombia, Código Disciplinario Único.
Ley 23 de 1982 de Propiedad Intelectual - Derechos de Autor.
Ley 594 de 2000 - Ley General de Archivos.
Ley 80 de 1993, Ley 1150 de 2007 y decretos reglamentarios.
Ley 527 de 1999, por la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales y se establecen las entidades de certificación y se dictan otras disposiciones.
Directiva presidencial 02 del año 2000, Presidencia de la República de Colombia, Gobierno en línea.
Ley 1032 de 2006, por el cual se dictan disposiciones generales del Habeas Data y se regula el manejo de la información contenida en base de datos personales.
Ley 1266 de 2007, por la cual se dictan disposiciones generales del Habeas Data y se regula el manejo de la información contenida en base de datos personales.
Ley 1273 de 2009, "Delitos Informáticos" protección de la información y los datos.
Ley 1437 de 2011, "Código de procedimiento administrativo y de lo contencioso administrativo".
Ley 1581 de 2012, "Protección de Datos personales".
Decreto 2609 de 2012, por la cual se reglamenta la ley 594 de 200 y ley 1437 de 2011.
Decreto 1377 de 2013, por la cual se reglamenta la ley 1581 de 2012.
Ley 1712 de 2014, “De transparencia y del derecho de acceso a la información pública nacional”.
Ley 962 de 2005. “Simplificación y Racionalización de Trámite. Atributos de seguridad en la Información electrónica de entidades públicas;”
Ley 1150 de 2007. “Seguridad de la información electrónica en contratación en línea”
Ley 1341 de 2009. “Tecnologías de la Información y aplicación de seguridad”.
Decreto 2952 de 2010. “Por el cual se reglamentan los artículos 12 y 13 de la Ley 1266 de 2008”.
Decreto 886 de 2014. “Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012”.
Decreto 1083 de 2015. “Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012”. o CONPES 3701 de 2011 Lineamientos de Política para Ciberseguridad y Ciberdefensa.

CONPES 3975 de 2019 Política Nacional para la Transformación Digital e Inteligencia Artificial
CONPES 3995 de 2020 Política Nacional de Confianza y Seguridad Digital
MSPI - Modelo de Seguridad y Privacidad de la Información.

Tabla 2 - Normas y regulaciones aplicables

ESTRUCTURA ORGANIZACIONAL

Contexto de la Entidad

“La Gobernación de Antioquia, es una entidad del orden territorial, cabeza del Departamento de Antioquia, la sede central está ubicada en el Centro Administrativo Departamental, en el sector de La Alpujarra, Medellín, Calle 52B # 42-106, está compuesta por 13 Secretarías, 2 Departamentos Administrativos y 6 Gerencias así: Secretaría General, Secretaría de Gobierno, Secretaría de Hacienda, Secretaría de Gestión Humana y Desarrollo Organizacional, Secretaría de Infraestructura Física, Secretaría de Educación, Secretaría Seccional de Salud y Protección Social de Antioquia, Secretaría de Agricultura y Desarrollo Rural, Secretaría de Productividad y Competitividad, Secretaría de Minas, Secretaría de Participación Ciudadana y Desarrollo Social, Secretaría para las Mujeres de Antioquia, Secretaría del Medio Ambiente, Departamento Administrativo de Planeación, Departamento Administrativo del Sistema de Prevención, Atención y Recuperación de Desastres, Gerencias de Auditoría Interna, Gerencia Indígena, Gerencia de Afrodescendientes, Gerencia de Infancia Adolescencia y Juventud, Gerencia de Servicios Públicos y Gerencia de Seguridad Alimentaria y Nutricional de Antioquia. Adicionalmente, cuenta con las sedes externas de: Fábrica de Licores de Antioquia, Palacio de la Cultura, Cárcel de Yarumito, Hangar Dapard, Almacén Salud y la Casa Fiscal de Antioquia situada en Bogotá".

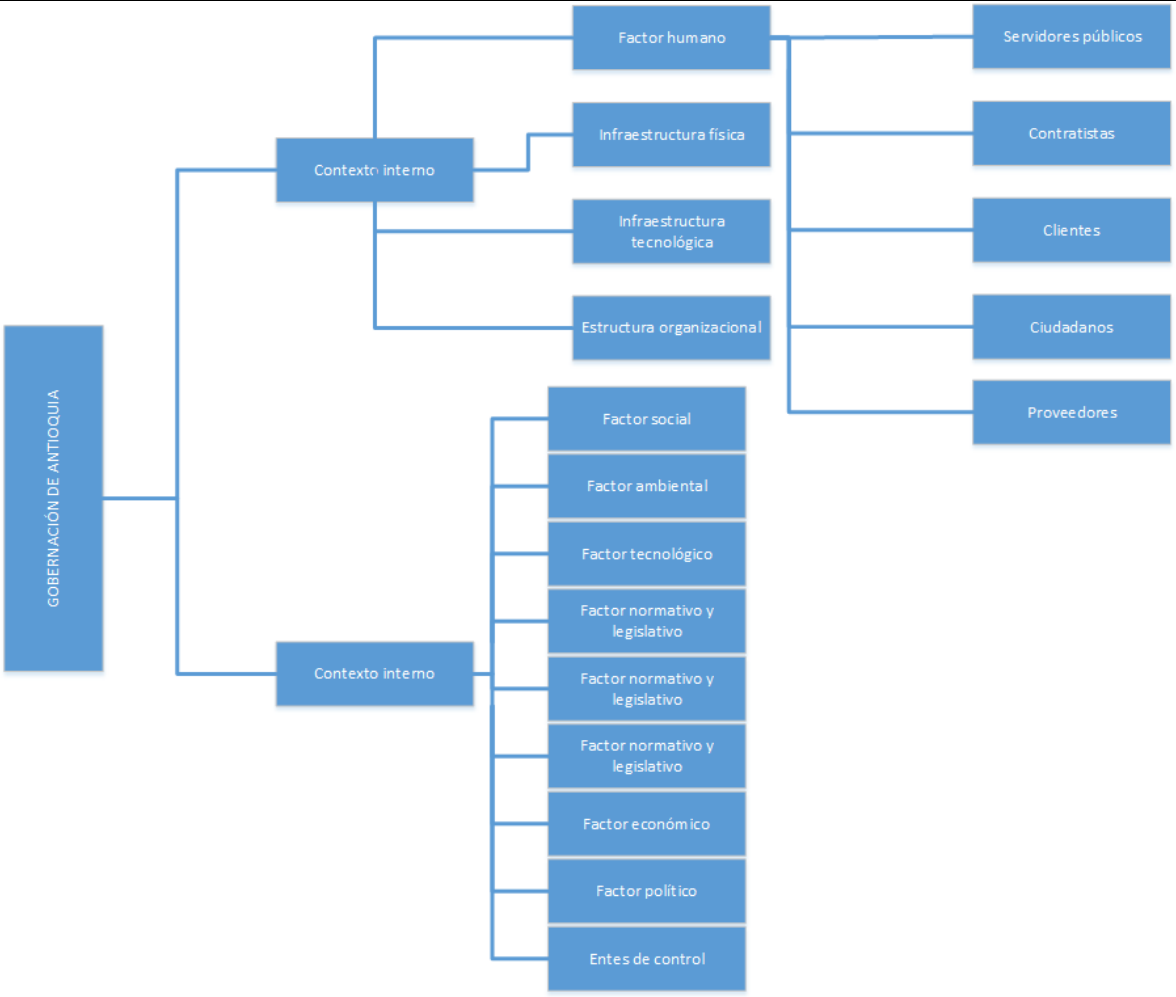

Ilustración 2 - Contexto organizacional Gobernación de Antioquia

Contexto Interno

Factor humano

Las personas también hacen parte de los activos de información más importantes dentro de una entidad. En la GOBANT se encuentran representados en servidores públicos, contratistas, proveedores, clientes y ciudadanos, que continuamente se encuentran en interacción con los procesos de la entidad, y, por ende, gestionan, procesan, almacenan, distribuyen, intercambian y/o consultan información que pueda ser pública, clasificada o reservada. En virtud de lo anterior, el factor humano representa un importante punto de referencia para el cumplimiento de los lineamientos y la política de seguridad de la información que ha establecido la entidad para minimizar el riesgo de que de alguna forma este factor representa para el SGSI; situación que está en un permanente refuerzo de concientización y sensibilización mediante comunicados, conferencias, y volantes en todo el edificio.

Contexto Externo

Análisis DOFA

DEBILIDADES (Internas): Factores negativos que se deben eliminar o reducir	OPORTUNIDADES (Externas): Aspectos positivos que se pueden aprovechar utilizando las fortalezas	FORTALEZAS (Interno): Factores positivos	AMENAZAS (Externas): Aspectos negativos que podrían obstaculizar el logro de los objetivos
No todas las personas relacionadas con el proceso GTI lo conocen ni lo aplican (social). VER NOTA DE MEJORA 1	Continua oferta (innovación) de tecnología en el mercado (tecnológico)	Aplicación rigurosa de la normatividad a nivel de TIC (legal)	Lentitud en el proceso de contratación. (Legal) Causa del riesgo de Interrupción de los servicios TIC por problemas asociados a la plataforma tecnológica
No existe una alta fluidez en la comunicación entre los equipos de trabajo y procedimientos del proceso GTI (social) VER NOTA DE MEJORA 1	Acuerdos marco por "Colombia compra eficiente" frente al tema de TI que facilitan y agilizan la contratación (económico)	Integración de las diferentes áreas de tecnología en el proceso (social)	Obsolescencia programada de TI por parte de los fabricantes.(Tecnológica) Causa del riesgo de Acceso ilegal e interrupción de los servicios TI
Falta de estrategias de uso y apropiación de las TI que impacten la organización.(tecnológica)	Buenas prácticas, normas, estándares y lineamientos que permiten adoptar mejores formas de hacer las cosas (social y legal)	Talento humano comprometido (social)	Compromisos políticos que desconocen los procesos de la organización.(político)
No se ha generalizado la aplicación del procedimiento de gestión de cambios. (tecnológico)	Modelo Integrado de Planeación y Gestión que da lineamientos, organiza e integra y le da importancia a las TIC (legal)	Centro de Servicios de Informática - CSI- fortalecido y en crecimiento (social y tecnológico)	Desarticulación entre los procesos del SIG
No se cuenta con un procedimiento de redes (tecnológico) VER NOTA DE MEJORA 2	Nuevos proyectos en la administración departamental que generan retos a las TI (tecnológico)	Comunicación oportuna a los usuarios de los eventos en TI y de alertas de seguridad (social y tecnológico)	Amenazas de seguridad de la información (delincuentes informáticos, fuga de información, software malicioso, ingeniería social) . (tecnológico) Riesgo de acceso ilegal

No se ha adoptado el procedimiento de gestión de problemas (tecnológico). VER NOTA DE MEJORA 3	Existencia de herramientas tecnológicas para identificar vulnerabilidades.(tecnológica)	Capacidad para trabajar bajo presión. (social)	No se cuenta con los suficientes recursos financieros, físicos y humanos idóneos para desarrollar los procedimientos del proceso (Económico) Causa de todos los riesgos del proceso
No se cuenta con una unidad o con personal de dedicación exclusiva o parcial para avanzar en temas de innovación en el sector público (analítica de datos, bigdata e inteligencia artificial) (tecnológico y económico)	Proyecto de Modernización Administrativa de la Gobernación de Antioquia que puede potenciar el proceso PATIC dentro de la organización (política y legal)	Mantenimiento y actualización continua de las herramientas de seguridad de la información (tecnológico)	Desastres de tipo natural o tecnológico que interrumpen la continuidad en TI. (ambiental y tecnológico). Causa de rIesgo de interrupción de los servicios de TI
Debilidad en la capacitación sobre temáticas técnicas dirigida a los servidores que apoyan el proceso GTI. (social). VER NOTA DE MEJORA 4	La pandemia del COVID 19 que le ha dado relevancia al proceso PATIC y ha obligado a los servidores a apropiarse de las herramientas de tecnología (tecnológica, social y ambiental)	Oferta del servicio de almacenamiento de información en la nube lo que evita el uso del papel contribuyendo a la sostenibilidad ambiental (ambiental)	No existe una adecuada gestión del conocimiento en la organización. (Social)
No acatamiento de la política de seguridad de la información por préstamos de contraseñas de acceso a sistemas de información o por incorrecta administración de cuentas especiales (tecnológico y social). Causa de los riesgos de acceso ilegal y de manipulación de información.	Asesoría técnica por parte del MINTIC en los temas de gobierno digital (tecnológica)	Exigencia en la contratación de equipos TI e impresoras de bajo consumo de energía, favoreciendo el cumplimiento del criterio de sostenibilidad ambiental. (ambiental)	Covid-19 que está obligando a modificar la estrategia de la entidad y a generar nuevas formas de relacionamiento a nivel nacional y territorial. Ha generado además un incremento en los precios de los equipos de tecnología, una disminución de stock

			de hardware y nuevas dinámicas de trabajo. (social y económica).
No tener dispuestos totalmente en línea los servicios y trámites susceptibles de ello, lo cual puede generar insatisfacción de los usuarios (tecnológico, social, político, económico)	Medidas ambientales (cultura de cero papel, ´por ejemplo) que hacen que los procesos migren cada vez mas hacia lo digital (ambiental y tecnológica)		La selección de personal por fuera de los concursos que no considera las competencias necesarias para el cargo. (político)
Vulnerabilidad de los componentes tecnológicos frente a la dinámica de los atacantes. Causa del riesgo de acceso ilegal	Ingreso de servidores a la Gobernación por la CNSC, con mayor aceptación y manejo de las tecnologías de información y comunicación. (social)		No hay una adecuada gestión de la información en la organización (sistemas de información que no cuentan con interoperabilidad). (tecnológico y social)
Obsolescencia tecnológica. Causa del riesgo de acceso ilegal y deL riesgo de Interrupción de los servicios TIC			No se tiene definido, documentado ni introyectado el concepto de arquitectura empresarial lo que dificulta la arquitectura de TI. (Político, tecnológico)
			Los procesos y procedimientos del SIG no están suficientemente detallados (metodología y herramienta) para establecer los flujos

			de información. (Social y tecnológico)
			No hay relación efectiva cargo–perfil. El quehacer de los servidores no está relacionado con lo establecido en el manual de funciones.(Político)
			No se tiene plan de continuidad del negocio en la entidad. (Tecnológico). VER NOTA DE MEJORA 5
			Expedición de numerosas y continuas normas en el marco del COVID 19 cuya implementación no se alcanza a cubrir con la rapidez que se espera (legal, técnológica y económica)
			Se derogan o se declaran inconstitucionales normas (Covid 19) que apenas se están implementando lo que genera reprocesos e ineficiencia en el uso de los recursos (legal, técnológica y económica)

			Fallas en el servicio de internet privado de los servidores públicos que están en la modalidad de trabajo en casa, que podrían afectar la conectividad con la Gobernación en tiempos de COVID 19. Tecnológico
			Fallas en los servicios de TIC que contrata la Gobernación (tecnológica) Causa del riegos de Interrupción de los servicios TIC por problemas asociados a la plataforma tecnológica.
			Avales para el uso de TIC con condiciones que no se cumplen una vez se aprueban. Tecnológico y social
			Colaboradores con permisos de administrador en los equipos de la Entidad. Causa del riesgo de acceso ilegal y del riesgo de Manipulación de la información
			Desconocimiento, apatía y falta de empoderamiento y conciencia respecto a la seguridad de la información por parte de los servidores públicos, contratistas y/o practicantes de la Entidad.(social, tecnológica). Causa

			de riego de Acceso Ilegal
			Renovación no oportuna de los contratos de mantenimiento y soporte de TIC. Control del Riesgo de Interrupción de los servicios TIC
			Ataques informáticos a la infraestructura y sistemas de información de TIC.

Tabla 3 - Matriz DOFA

Partes interesadas

La Gobernación de Antioquia reconoce como sus grupos de interés a:

Parte interesada	Descripción
Usuarios directos	Funcionarios, contratistas, practicantes de la Gobernación de Antioquia.
Usuarios indirectos	Ciudadanos, Hospital La María, Hospital General, PAS, CRUE, Fábrica de Licores de Antioquia, Palacio de la Cultura, Pensiones Antioquia.
Entidades públicas	Gobierno, Fiscalía, Procuraduría, Contraloría, etc.
Terceros relacionados	Ciudadanía en general, líderes de opinión, medios y opinión pública.
Entidades externas	Proveedores (outsourcing).

Tabla 4 - Partes interesadas

MARCO CONCEPTUAL DEL PESI

Para la Gobernación de Antioquia son muy importantes los resultados obtenidos por el PESI con el fin de apoyar la implementación del SGSI. El PESI se apoya en el Plan Estratégico de Tecnologías de la Información PETI y el Proceso de Administración de las TIC - PATIC, el cual se fundamenta en la metodología de BSC o Cuadro de Mando Integral, debido a su gran utilidad en el direccionamiento de las entidades.

De acuerdo con la expedición del Decreto 2573 de 2014 contenida en el Decreto Único Reglamentario 1078 de 2015 del sector de Tecnologías de la Información y las Comunicaciones y actualizado según el decreto No 1008 del 14 de junio del 2018, Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones, La Gobernación de Antioquia en asesoría de la Dirección de informática, trabajan en la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI), el cual se encuentra alineado con el Marco de Referencia de Arquitectura TI, el Modelo Integrado de Planeación y Gestión (MIPG) y La Guía para la Administración del Riesgo y el Diseño Controles en entidades Públicas, este modelo pertenece al habilitador transversal de Seguridad y Privacidad, de la Política de Gobierno Digital.[1]

El modelo se va a basar en el ciclo PHVA, el cual recomienda la norma NTCISO/IEC 27001:2013 y la GTC-ISO/IEC 27002:2015.

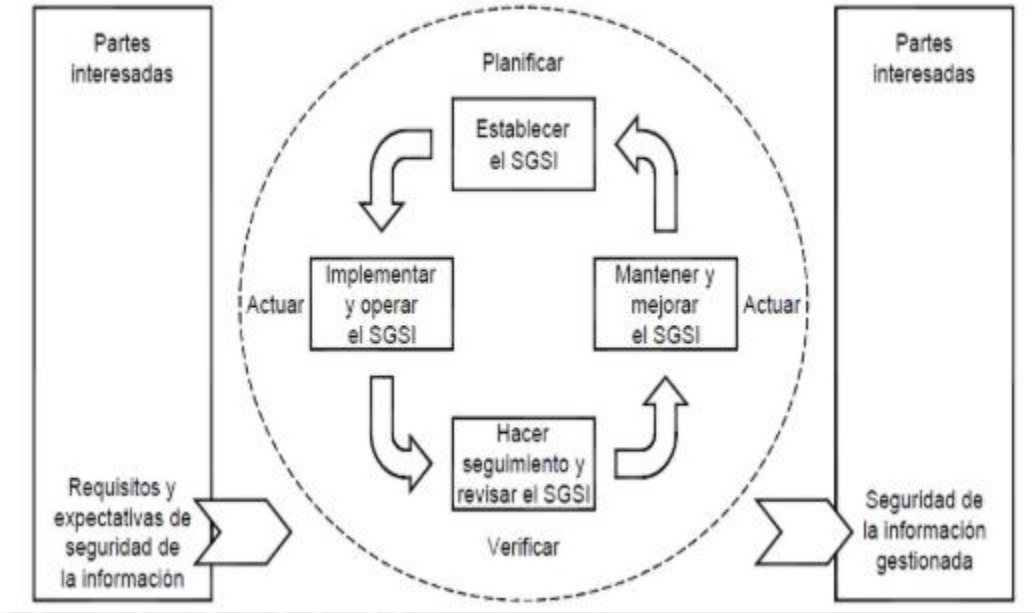

Ilustración 3 - Modelo PHVA del SGSI Fuente: https://ticcolombia.webnode.com.co/news/iso-9001/

[1] https://www.mintic.gov.co/gestion-ti/Seguridad-TI/Modelo-de-Seguridad/

Metodología utilizada

La metodología utilizada para el desarrollo del PESI se muestra y se explica a continuación

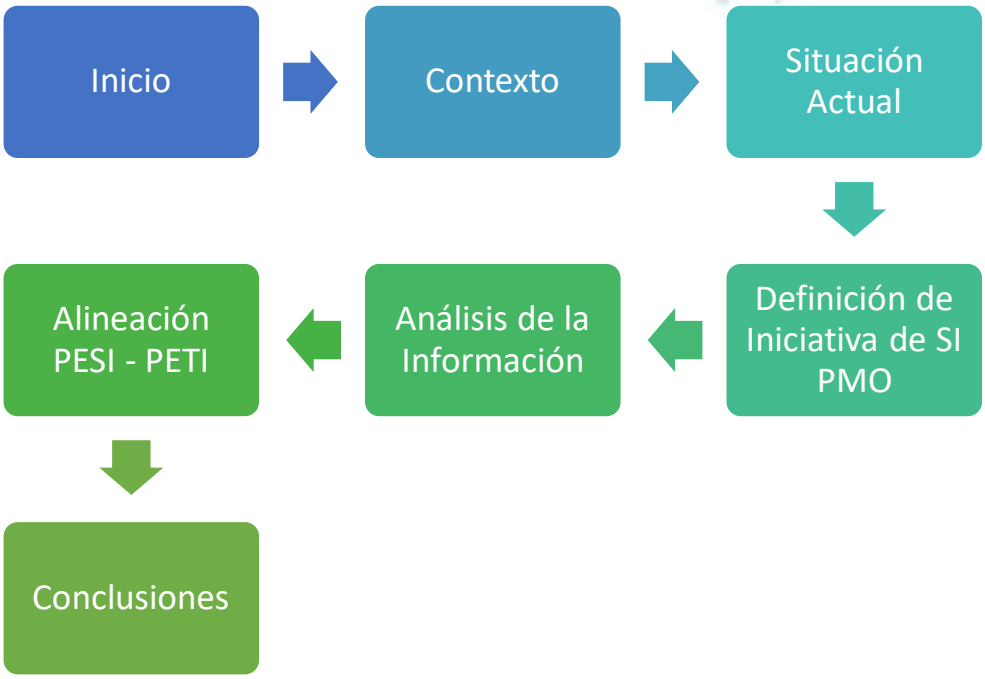

Ilustración 4 - Flujograma de desarrollo del PESI

Contexto

La fase inicial del desarrollo del PESI busca alinear las características principales de la Gobernación de Antioquia con el fin de que los objetivos de este Plan estén alineados con los objetivos estratégicos de la entidad. Entre los aspectos que se deben considerar para este entendimiento están:

- Misión
- Visión
- Estructura organizacional
- Procesos
- Cultura y procesos
- Legislación aplicable

Según la misión de la Gobernación de Antioquia, articulados con la Constitución Política de 1991, uno de los objetivos fundamentales es servir a la comunidad, adicionalmente la Visión se enfoca en convertir a Antioquia en una región “próspera, productiva, competitiva, pujante y ambientalmente sostenible, a partir de la ejecución de proyectos visionarios y de la lucha frontal contra la desigualdad social, la inequidad, el desempleo, el analfabetismo, el pesimismo, el atraso, la miseria y el hambre”, apalancados en los modelos de Gobierno Digital y Ciudadanos digitales propuestos por el Ministerio de Tecnologías de la Información, las Tecnologías de Información y Comunicaciones son “Promover el uso y aprovechamiento de las tecnologías de la información y las comunicaciones para consolidar

un Estado y ciudadanos competitivos, proactivos, e innovadores, que generen valor público en un entorno de confianza digital"[2].

En este sentido, los procesos que proporciona la Gobernación de Antioquia a la ciudadanía están apalancados en una estrategia de mejoramiento, y aumento de eficacia desde la perspectiva de la explotación y apoyo de las TIC como eje fundamental mediante el cual se apoya la política de gobierno digital, razón por la cual, la protección de la información contenida en los sistemas de TIC se hace vital, orientados en la confidencialidad, integridad y disponibilidad de la misma, como atributos vitales, por lo que la Gobernación de Antioquia, en reconocimiento a la importancia que esta adquiere dentro del cumplimiento de la política de gobierno digital planeada por el gobierno nacional.

La seguridad y privacidad de la información, como componente transversal a la Estrategia de Gobierno en línea, permite alinearse al componente de TIC para la Gestión al aportar en el uso estratégico de las tecnologías de la información con la formulación e implementación del modelo de seguridad enfocado a preservar la confidencialidad, integridad y disponibilidad de la información, lo que contribuye al cumplimiento de la misión y los objetivos estratégicos de la entidad.

La Seguridad y Privacidad de la Información se alinea al componente de TIC para Servicios apoyando el tratamiento de la información utilizada en los trámites y servicios que ofrece la Entidad, observando en todo momento las normas sobre protección de datos personales, así como otros derechos garantizados por la Ley que exceptúa el acceso público a determinada información.

Situación Actual

En Julio de 2011, se emite el CONPES 3701, mediante el cual se establecen los lineamientos de política para ciberseguridad y ciberdefensa. El objetivo central de esta política es la de fortalecer las capacidades del Estado para enfrentar las amenazas que atentan contra su seguridad y defensa en el ámbito cibernético (ciberseguridad y ciberdefensa), creando el ambiente y las condiciones necesarias para brindar protección en el ciberespacio. Este documento identifica tres ejes problemáticos: Las iniciativas y operaciones en ciberseguridad y ciberdefensa no están adecuadamente coordinadas, existe una debilidad en la regulación y legislación de la protección de la información y los datos, y finalmente, se detecta una debilidad en la oferta y cobertura de capacitación especializada en ciberseguridad y ciberdefensa. El enfoque fundamental de este lineamiento de políticas de ciberseguridad y ciberdefensa busca implementar las instancias apropiadas para prevenir, coordinar, atender, controlar, generar recomendaciones y regular los incidentes o emergencias cibernéticas para afrontar las amenazas y los riesgos que atentan contra la ciberseguridad y la ciberdefensa; brindar capacitación especializada en seguridad de la información y ampliar las líneas de investigación en ciberseguridad y ciberdefensa y fortalecer la legislación en materia de ciberseguridad y ciberdefensa, la cooperación internacional y adelantar la adhesión de Colombia a los diferentes instrumentos internacionales en esta temática.

[2] https://www.dnp.gov.co/Paginas/Gobierno-presenta-al-Congreso-Pacto-por-Colombia-pacto-por-la-equidad.aspx

Posteriormente, en abril de 2016, El Departamento Nacional de Planeación DNP emite el CONPES 3854, en el cual se establece la Política de Seguridad Digital. Dicha política tiene como objetivos la defensa del país desde la ciberseguridad, y la lucha contra el crimen cibernético. Dicha Política se define bajo cuatro principios fundamentales y cinco dimensiones estratégicas, las cuales rigen el desarrollo de esta política. El objetivo general del Documento CONPES 3701 fue fortalecer las capacidades del Estado para enfrentar las amenazas que atentan contra la defensa y seguridad nacional en el ámbito cibernético (ciberseguridad y ciberdefensa), creando un ambiente y unas condiciones para brindar protección en el ciberespacio. Para cumplir este objetivo general, se formularon tres objetivos específicos: (i) implementar instancias apropiadas para prevenir, coordinar, atender, controlar, generar recomendaciones y regular los incidentes o emergencias cibernéticas para afrontar las amenazas y los riesgos que atentan contra la ciberseguridad y ciberdefensa nacional; (ii) brindar capacitación especializada en seguridad de la información y ampliar las líneas de investigación en ciberdefensa y ciberseguridad; y (iii) fortalecer la legislación en materia de ciberseguridad y ciberdefensa, la cooperación internacional y adelantar la adhesión de Colombia a los diferentes instrumentos internacionales en esta temática.

Adicionalmente, en cumplimiento del decreto 1499 del 11 de septiembre de 2017, que formaliza el Modelo Integrado de Planeación y Gestión –MIPG, el cual busca alinear varios procesos de la gestión administrativa y volverla más eficiente, por ello toda la Administración Territorial con un enfoque más integral relaciona 7 dimensiones (Talento Humano , Direccionamiento Estratégico y Planeación, Gestión con valores para Resultados, Evaluación de Resultados, Información y Comunicación, Gestión del Conocimiento y la Innovación y Control Interno) las cuales convergen en materia de TIC en la dimensión 3 ”Valores para Resultados”.

La Política de Gobierno Digital actúa como una política transversal que se relaciona con las demás políticas del Modelo Integrado de Planeación y Gestión, facilitando su implementación y potenciando los beneficios tanto para las entidades del Estado, como para ciudadanos, usuarios y grupos de interés. A partir de ello, políticas como Talento Humano, Planeación Institucional, Gestión Presupuestal, Transparencia y Acceso a la Información Pública, Fortalecimiento Organizacional y Simplificación de Procesos, Servicio al Ciudadano, Participación ciudadana, Racionalización de Trámites, Gestión Documental, Seguridad Digital, Gestión del conocimiento y la innovación, entre otras, son apalancadas a través de Gobierno digital. Dicha política tiene como habilitadores transversales la Seguridad de la Información, la Arquitectura y Servicios Ciudadanos Digitales, los cuales permiten el logro de los propósitos definidos por esta política.

Busca que las entidades públicas implementen los lineamientos de seguridad de la información en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y en general, en todos los activos de información con el fin de preservar la confidencialidad, integridad y disponibilidad y privacidad de los datos.

Este habilitador se soporta en el Modelo de Seguridad y Privacidad de la Información – MSPI, dicho modelo tiene como objetivo el ser un lineamiento de buenas prácticas en materia de seguridad y privacidad de la información. El MSPI contempla un ciclo de operación que consta de cinco (5) fases, las cuales permiten que las entidades puedan

gestionar adecuadamente la seguridad y la privacidad de sus activos de información. También contempla seis (6) niveles de madurez, los cuales corresponden a la implementación de la operación del modelo.

Estructura Organizacional

El Comité de Seguridad de la Información de constituye de manera oficial mediante la Resolución 108373 del 30 de octubre de 2013. Mediante esta resolución, se establece que este Comité deberá asegurar que exista una dirección y apoyo gerencial para soportar la administración y desarrollo de iniciativas sobre seguridad de la Entidad, promoviendo la seguridad a través compromisos y recursos adecuados.

Organigrama Operativo

La siguiente gráfica representa la estructura organizacional del área de Seguridad de la Información.

Ilustración 5 - Organigrama del área de seguridad de la información

Áreas de Enfoque:

La división del área comprende tres enfoques:

- Estratégico: está orientado al análisis, evaluación y tratamiento de los riesgos de seguridad de la información, la alineación del MSPI de la Gobernación, así como el manejo de las herramientas técnicas que permiten darle seguimiento a las operaciones de seguridad de la información.
- Táctico: está orientado a la atención de requerimientos de los entes de control, así como la capacitación y sensibilización de los funcionarios de la Gobernación.
- Operativo: Gestiona lo concerniente a las herramientas técnicas de punto final, como el antivirus, las herramientas de detección de intrusiones, herramientas de

auditoría para Directorio Activo y File Server, monitoreo e Identificación de vulnerabilidades, identificación de malware avanzado y monitoreo de navegación de funcionarios de la gobernación.

El funcionamiento de estos enfoques se soporta sobre la Mesa de Servicios Tecnológicos, y finalmente los funcionarios, contratistas y practicantes, así como usuarios de los servicios de la Gobernación de Antioquia, quienes son el primer punto de defensa de la seguridad de la información.

Herramientas de Seguridad Informática

La siguiente es la lista de herramientas técnicas que se tiene al interior del área de Seguridad de la Información:

Kaspersky Endpoint Security for Business

La herramienta Kaspersky Endpoint Security for Business actualmente cubre 3300 licencias dentro de la Gobernación de Antioquia, cumpliendo una función de protección al tráfico web, correo electrónico, proporciona seguridad adaptativa contra las últimas ciber amenazas, elimina vulnerabilidades para bloquear los puntos de entrada de ataques y reduce la exposición a ataques, gracias al fortalecimiento de los endpoints corporativos. Esta herramienta ha sido actualizada en el año 2021 por lo cual permite adicionar algunos elementos de seguridad que refuerzan los esfuerzos que se brinda desde el equipo de Seguridad de la Información.

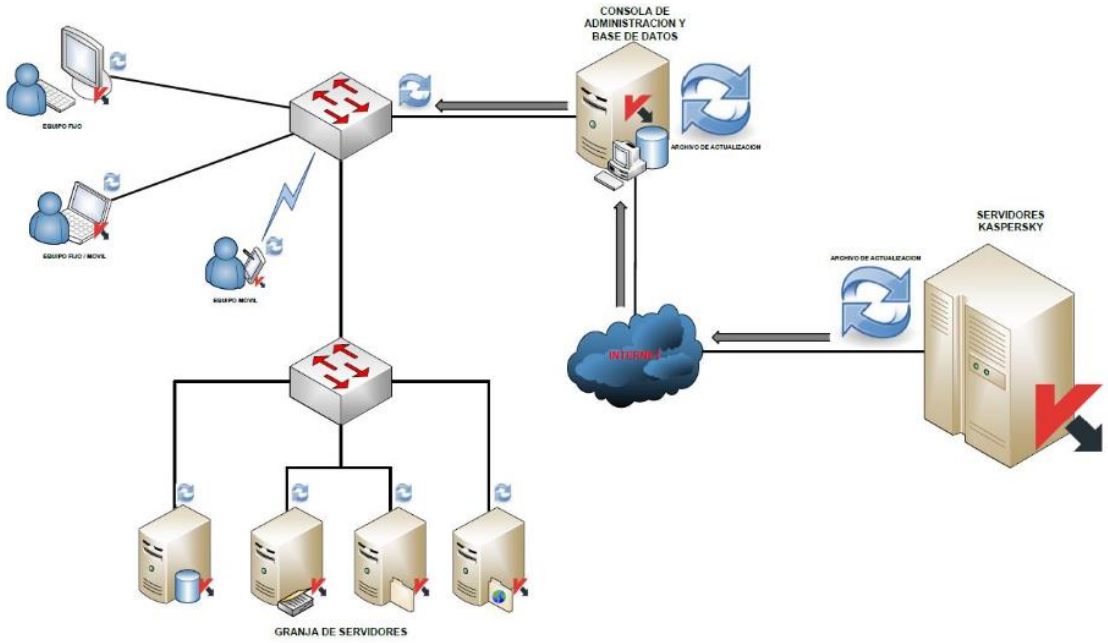

Ilustración 6 - Topología Kaspersky

ManageEngine ADAudit Plus Professional Edition

ADAudit Plus es un software de auditoría de cambios de Active Directory que otorga visibilidad completa sobre todos los cambios realizados. Permite generar informes y alertas que garantizan la trazabilidad y ayudan a implantar un sistema de control alineado con las mejores prácticas de TI, permitiendo responder las cuatro preguntas vitales de la auditoría

de Active Directory: ¿"quién" hizo? ¿"qué" acción?, ¿"cuándo"? y ¿desde "dónde"? Actualmente ManageEngine ADAudit facilita el monitoreo continuo de los usuarios de la Gobernación asegurando la disponibilidad, integridad y confidencialidad de la información en cada una de las áreas por medio de alertas y generación de reportes que se analizan para validar tendencias y patrones en conductas sospechosas de los funcionarios.

ManageEngine DataSecurity Plus Professional File Server Auditing Edition

DataSecurity Plus es una valiosa herramienta utilizada generalmente para asegurar la integridad del sistema de archivos, la prevención de pérdida de datos y ayuda a cumplir con las normas reguladoras en algunos sectores de la industria. Esta herramienta genera alertas por correo electrónico definidas el Equipo de Seguridad de la Información mientras realiza respuestas automáticas predefinidas cuando hay potenciales amenazas de seguridad, como un ransomware; Así mismo monitorea de manera selectiva archivos, carpetas, o incluso usuarios para detallar de manera efectiva cualquier cambio no autorizado.

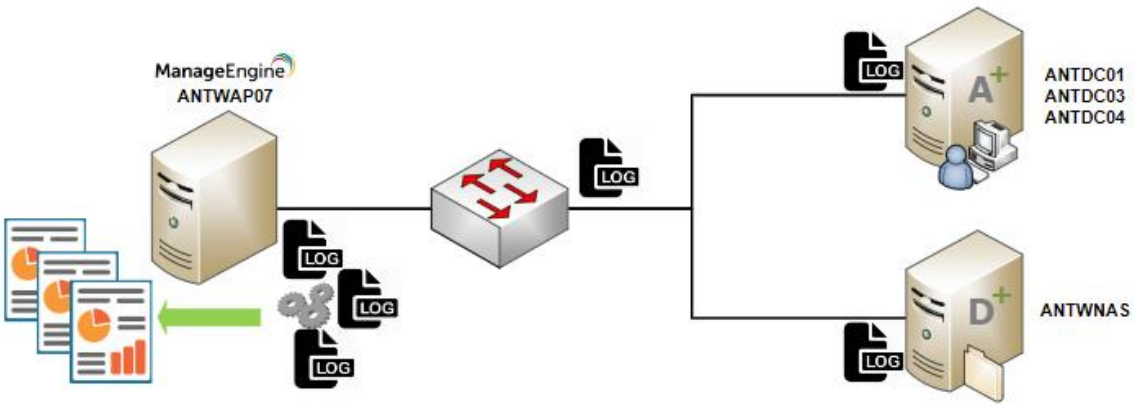

Ilustración 7 - Topología de Red ManageEngine

Deep Security

La herramienta Deep Security actualmente protege 46 elementos de la infraestructura de la Gobernación. Su función es la de proporcionar las aplicaciones y datos de la entidad contenidos en estos servidores de brechas e interrupciones de negocio sin tener que acudir al parcheo de los equipos, la siguiente gráfica representa la arquitectura de la solución:

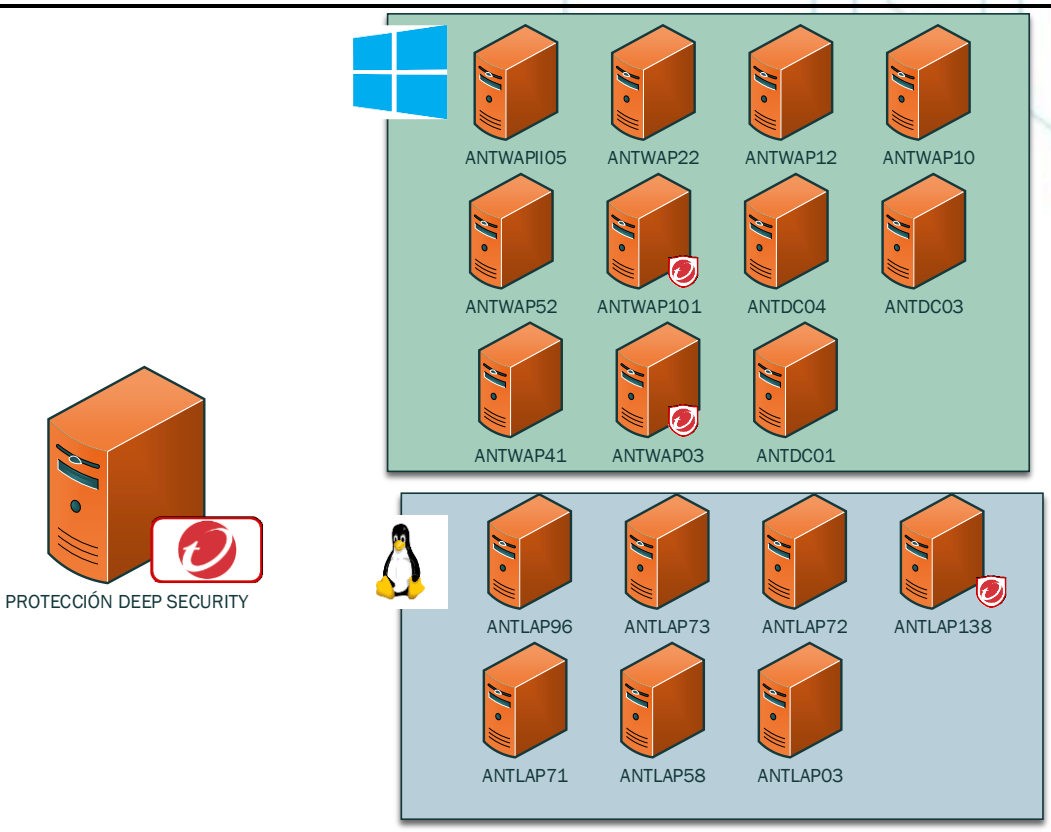

Ilustración 8 - Topología Deep Security

WAF Imperva Incapsula

Imperva Incapsula es una solución WAF (Web Application Firewall), la cual analiza e inspecciona paquetes y solicitudes que llegan a aplicaciones Web y las detiene en caso de que se requiera, la siguiente es la lista de sitios protegidos por el Incapsula:

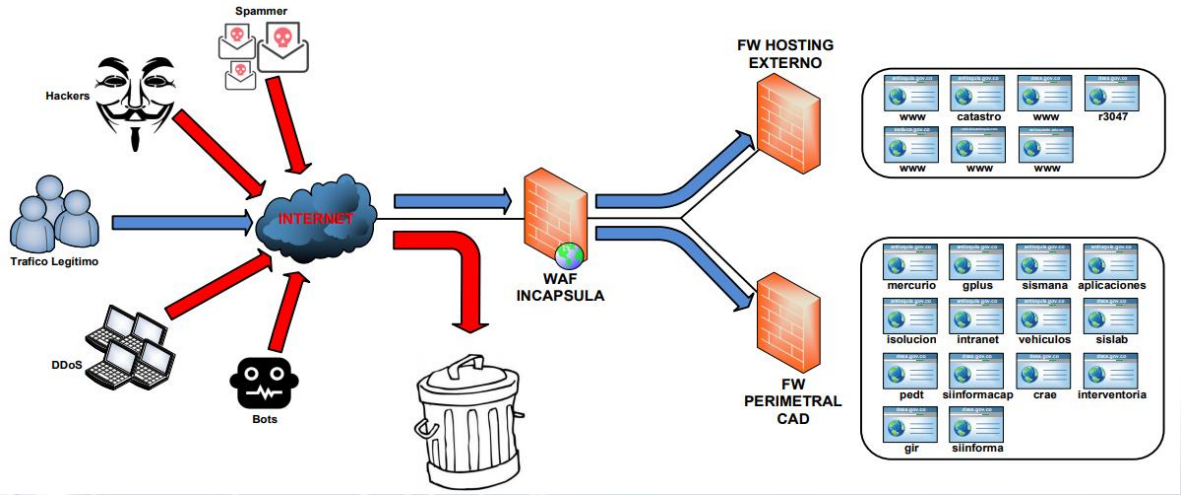

Ilustración 9 - Diagrama de Operatividad

Tenable.io Vulnerability Management TIOVM

Es una herramienta gestionada en la nube y con tecnología Nessus, que proporciona la cobertura de vulnerabilidades más completa de la industria, con la capacidad para predecir qué problemas de seguridad deben corregirse primero. Es una solución completa de gestión de vulnerabilidades, de extremo a extremo.

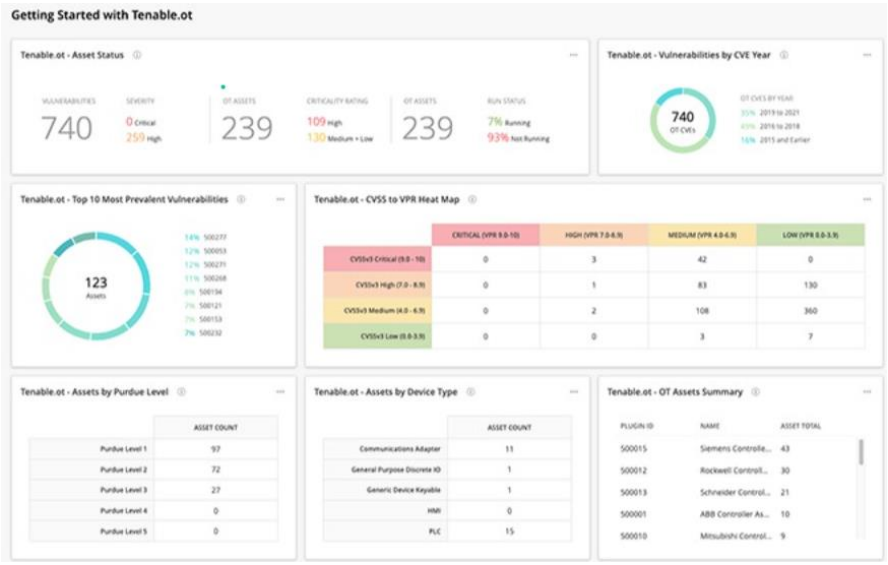

Ilustración 10 – Cuadro de Mando Tenable.io

DiskGenius - Recuperación de datos

Esta herramienta es un administrador de particiones con todas las funciones, que está diseñado para optimizar el uso del disco para los usuarios de Windows.

Características:

- Recuperación de datos y particiones.
- Administre el disco duro (Particiones):
  - Partición de cambio de tamaño / división.
  - Partición con un solo clic en un disco duro.
  - Partición de borrado completo.
  - Partición de creación / formato (Admite NTFS, exFAT, FAT32, FAT16, FAT12, EXT2, EXT3 y EXT4 sistemas de archivos.)
  - Crear disco de arranque WinPE.
- Partición de conversión:
  - Convertir disco MBR / GPT.
  - Convertir dinámico / básico Disco.
  - Convertir unidad principal / lógica.
  - Convertir formato de disco virtual como VMware ".VMDK", Virtual PC ".VHD" y Virtual Box ".VDI".

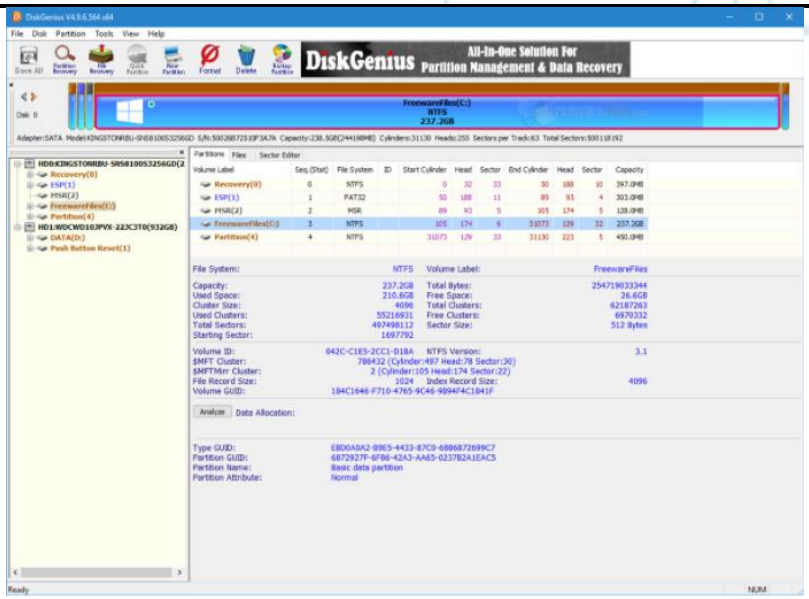

Ilustración 11 - DiskGenius - Recuperación de datos

Palo Alto Networks

Este dispositivo ofrece funcionalidades como: Bloqueo de conexiones no autorizadas en la red (firewall), visibilidad y control de aplicaciones (AVC), IPS de última generación (NGIPS), protección frente a malware avanzado y filtrado de navegación a Internet. Es un dispositivo reconocido a nivel mundial para la protección de redes informáticas, según los informes de organizaciones expertas en la valoración de tecnologías de la información (Gartner, Nss Labs).

La seguridad perimetral se define como el conjunto de aquellos elementos y sistemas que permiten proteger unos perímetros en instalaciones sensibles de ser atacadas por intrusos que se encuentran en una red de datos. Elementos como cortafuegos, brindan mediante políticas de acceso que tipo de tráfico se permite o se deniega en la red corporativa. Sistemas de detección y prevención de intrusos (IPS) permite identificar posibles ataques, registros de eventos y el bloqueo de estos.

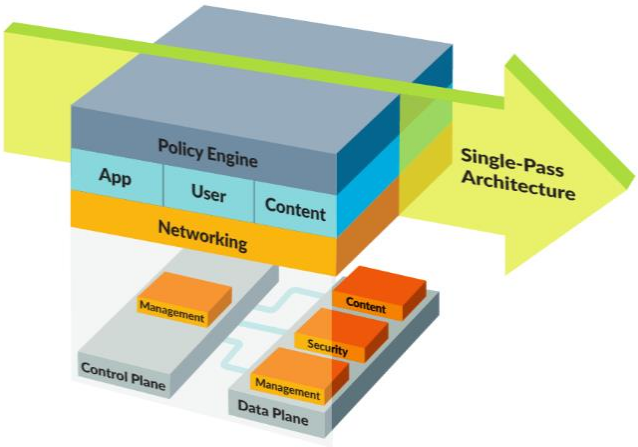

Ilustración 12 - Palo Alto Networks

Proyectos activos al 2021

A Diciembre de 2021, el presupuesto de las herramientas es el siguiente:

Tabla 5 – Proyectos activos 2021

ITEM	CANTIDAD	DESCRIPCIÓN
1	Kaspersky Endpoint Security for Business	3504 Licencias
2	Licencia Tenable.sc (SecurityCenter)	1
3	Herramienta en File server auditing & data Discovery (Renovación)	1
4	Herramienta en Active Directory ADAudit Plus (Renovación)	1
6	Deep security Antimalware + XDR Pro	241
7	WAF Imperva Incapsula 20 Mbps	1
8	WAF Imperva Incapsula 21 Sitios Management TIOVM	1
9	Tenable IOPaquete 5 Servidores	1
10	Adquisición Herramienta Firewall	1

	de Nueva Generación (Palo Alto Networks)	

PLANEACIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Cobertura del PESI

Teniendo en cuenta el análisis del contexto externo, interno y las partes interesadas, la Gobernación de Antioquia define su Sistema de Gestión de Seguridad de la Información (SGSI), desde el cual se articula el Plan Estratégico de Seguridad de la Información (PESI), en términos de las características de la Entidad, su ubicación, sus activos, procesos, personal y tecnología involucrada.

La Gobernación de Antioquia, acorde con su naturaleza jurídica, misión y visión, encuentra aplicables todos los requisitos de la Norma ISO/IEC 27001:2013, y los controles del Anexo A incluidos en la Norma ISO/IEC 27002:2013.

Declaración de Aplicabilidad

En la Declaración de Aplicabilidad; Statement of Applicability (SoA) por sus siglas en inglés, el SGSI se acopla al Modelo de Seguridad y Privacidad de la Información MSPI, con el objetivo de delimitar los controles que propone y deben ser tenidos en cuenta con relación a los controles mandatorios de la norma ISO/IEC 27001:2013. El objetivo de la declaración de aplicabilidad es poder establecer las iniciativas y los proyectos que se definirán para establecer el SGSI acorde a los objetivos estratégicos de la Gobernación de Antioquia. Estos se encuentran definidos dentro de la columna de Declaración de Aplicabilidad de las dos tablas.

SoA Procesos Administrativos

ITEM	DESCRIPCIÓN	OBJETIVO DE CONTROL	SoA	Mandatorio
POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	Orientación de la dirección para gestión de la seguridad de la información		Si	Si
ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	Marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización Garantizar la seguridad del teletrabajo y el uso de los dispositivos móviles		Si	No

ITEM	DESCRIPCIÓN	OBJETIVO DE CONTROL	SoA	Mandatorio
Antes de asumir el empleo	Asegurar que el personal y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que son considerados.		Si	No
Durante la ejecución del empleo	Asegurar que los funcionarios y contratistas tomen consciencia de sus responsabilidades sobre la seguridad de la información y las cumplan.		Si	SI
Terminación y cambio de empleo	Proteger los intereses de la Entidad como parte del proceso de cambio o terminación de empleo.		Si	No
Responsabilidad de los activos	Identificar los activos organizacionales y definir las responsabilidades de protección apropiadas.		Si	SI
Devolución de activos	Todos los empleados y usuarios de partes externas deben devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.	Se tiene definido un procedimiento para que funcionarios y contratistas devuelvan los activos que son propiedad de la entidad (equipos, software, aplicaciones, etc.) que se encuentran a su cargo al terminar sus funciones o el vínculo laboral.	Si	No

ITEM	DESCRIPCIÓN	OBJETIVO DE CONTROL	SoA	Mandatorio
Clasificación de la información	La información se debería clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.	Se tiene clasificada la información en términos de su valor, requisitos legales, sensibilidad y criticidad a la entidad.	Si	No
Manejo de medios	Evitar la divulgación, la modificación, el retiro o la destrucción no autorizados de la información almacenada en los medios.		Si	No
Transferencia de medios físicos		Los medios que contienen información son protegidos del acceso no autorizado cuando están en tránsito.	Si	No
Verificación, revisión y evaluación de la continuidad de la seguridad de la información.		Se realizan pruebas periódicas de los planes de continuidad de negocio y recuperación de desastres para validar que estos son válidos durante situaciones adversas.	Si	Si
Disponibilidad de instalaciones de procesamiento de información		Se tienen implementadas suficientes redundancias en las instalaciones para cumplir el requisito de disponibilidad de la información.	Si	Si

ITEM	DESCRIPCIÓN	OBJETIVO DE CONTROL	SoA	Mandatorio
Cumplimiento de requisitos legales y contractuales	Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información y de cualquier requisito de seguridad.		Si	No
Identificación de la legislación aplicable y de los requisitos contractuales.		Se tienen identificados todos los requisitos legales, estatutarios, contractuales y regulatorios y se tienen procedimientos para documentarlos y mantenerlos actualizados en cada sistema.	Si	Si
Derechos de propiedad intelectual.		Se tienen implementados procedimientos para garantizar los requisitos legales, regulatorios y contractuales relacionados con el uso de la propiedad intelectual y el uso de productos de software.	Si	No
Revisiones de seguridad de la información			Si	No
Seguridad de la información en las relaciones	Asegurar la protección de los activos de la entidad que sean accesibles	Se tienen establecidos los requerimientos de protección de	Si	Si

ITEM	DESCRIPCIÓN	OBJETIVO DE CONTROL	SoA	Mandatorio
con los proveedores	para los proveedores	la información relacionados al acceso de los proveedores a la misma y están acordados y documentados con el proveedor.		
Gestión de la prestación de servicios de proveedores	Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores	Se tienen identificados y establecidos todos los requerimientos de seguridad de la información con cada proveedor que puede acceder, almacenar, comunicar, o proporcionar componentes de infraestructura de TI para la información de la entidad.	Si	Si

Tabla 6 - Declaración de Aplicabilidad Controles Administrativos

SoA Procesos Técnicos

ITEM	DESCRIPCIÓN	MSPI	OBJETIVOS DE CONTROL	SoA	Mandatorio
CONTROL DE ACCESO		Componente planificación y modelo de madurez nivel gestionado		Si	Si
Política de control de acceso	Se debe establecer, documentar y revisar una política de control de acceso		Se tiene una política de control de acceso y se hace una revisión de la misma	Si	Si

ITEM	DESCRIPCIÓN	MSPI	OBJETIVOS DE CONTROL	SoA	Mandatorio
	con base en los requisitos del negocio y de seguridad de la información.		basados en los requisitos de la entidad y de la seguridad de la información. Se tienen en cuenta los controles de acceso lógicos y físicos dentro de la política.		
GESTIÓN DE ACCESO DE USUARIOS	Se debe asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.	Modelo de madurez gestionado cuantitativamente		Si	No
RESPONSABILIDADES DE LOS USUARIOS	Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación.	Modelo de madurez definido		Si	No
CONTROL DE ACCESO A SISTEMAS Y APLICACIONES	Se debe evitar el acceso no autorizado a sistemas y aplicaciones.	Modelo de madurez gestionado cuantitativamente		Si	No
SEGURIDAD DE LAS				Si	Si

ITEM	DESCRIPCIÓN	MSPI	OBJETIVOS DE CONTROL	SoA	Mandatorio
OPERACIONES					
PROCEDIMIENTOS OPERACIONALES Y RESPONSABILIDADES	Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.	Modelo de madurez definido		Si	Si
Procedimientos de operación documentados	Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesiten.		Se cuenta con procedimientos operativos documentados, y están disponibles cuando se requiera.	Si	Si
PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS	Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.			Si	No
COPIAS DE RESPALDO	Proteger contra la pérdida de datos.	Modelo de madurez gestionado		Si	No

ITEM	DESCRIPCIÓN	MSPI	OBJETIVOS DE CONTROL	SoA	Mandatorio
REGISTRO Y SEGUIMIENTO	Registrar eventos y generar evidencia.	Modelo de madurez gestionado cuantitativamente		Si	No
CONTROL DE SOFTWARE OPERACIONAL	Asegurar la integridad de los sistemas operacionales.	Modelo de madurez definido		Si	No
CONSIDERACIONES SOBRE AUDITORÍAS DE SISTEMAS DE INFORMACIÓN	Minimizar el impacto de las actividades de auditoría sobre los sistemas operacionales.	Modelo de madurez gestionado cuantitativamente		Si	No
SEGURIDAD DE LAS COMUNICACIONES				Si	No
GESTIÓN DE LA SEGURIDAD DE LAS REDES	Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.	Modelo de madurez definido		Si	No
TRANSFERENCIA DE INFORMACIÓN	Mantener la seguridad de la información transferida dentro de una organización y con cualquier	Modelo de madurez definido		Si	No

ITEM	DESCRIPCIÓN	MSPI	OBJETIVOS DE CONTROL	SoA	Mandatorio
	entidad externa.				
ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS				Si	No
SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y DE SOPORTE	Asegurar de que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.	Modelo de madurez definido		Si	No
Principios de construcción de sistemas seguros	Se deben establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.		Se tienen establecidos, documentados, mantenidos y aplicados los principios de ingeniería para sistemas seguros a cualquier esfuerzo de implementación de sistemas de información.	Si	Si

ITEM	DESCRIPCIÓN	MSPI	OBJETIVOS DE CONTROL	SoA	Mandatorio
DATOS DE PRUEBA	Asegurar la protección de los datos usados para pruebas.	Modelo de madurez definido		Si	No
GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN				Si	No
GESTIÓN DE INCIDENTES Y MEJORAS EN LA SEGURIDAD DE LA INFORMACIÓN	Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.			Si	Si
Respuesta a incidentes de seguridad de la información	Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.	Modelo de madurez gestionado cuantitativamente	Se tiene un mecanismo de respuesta a incidentes de seguridad de la información acorde con los procedimientos documentados.	Si	Si

Tabla 7 - Declaración de Aplicabilidad Controles Técnicos

Para el desarrollo del PESI, se evaluará la adición dentro de la declaración de aplicabilidad (SoA) los siguientes controles correspondientes Seguridad física de la Norma ISO/IEC 27002:2013, en virtud de que la Gobernación se está alineando con los proyectos y directrices del MINTIC por medio del MSPI, que año tras año tiene un crecimiento en proyectos, personal e infraestructura lo que conlleva estar atentos al cambio y ver la necesidad de que estos controles de la norma sean incluidos y que su monitoreo se integre a las funciones del Área de Seguridad de la Información:

11.1	**ÁREAS SEGURAS**	**Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización.**
11.1.1.	Perímetro de seguridad física	Se debe definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información sensible o crítica, e instalaciones de manejo de información.
11.1.2.	Controles físicos de entrada	Las áreas seguras se deben proteger mediante controles de entrada apropiados para asegurar que solamente se permite el acceso a personal autorizado.
11.1.3.	Seguridad de oficinas, recintos e instalaciones	Se debe diseñar y aplicar seguridad física a oficinas, recintos e instalaciones.
11.1.4.	Protección contra amenazas externas y ambientales	Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.
11.1.5.	Trabajo en áreas seguras	Se debe diseñar y aplicar procedimientos para trabajo en áreas seguras.

11.1.6.	Áreas de despacho y carga	Se debe controlar los puntos de acceso tales como áreas de despacho y de carga, y otros puntos en donde pueden entrar personas no autorizadas, y si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.

Tabla 8 - Controles por incluir al alcance del SGSI

Los controles pertenecientes al numeral A11.2 Seguridad en los equipos:

EQUIPOS	A.11.2
Ubicación y protección de los equipos	A.11.2.1
Servicios de suministro	A.11.2.2
Seguridad del cableado	A.11.2.3
Mantenimiento de equipos	A.11.2.4
Retiro de activos	A.11.2.5
Seguridad de equipos y activos fuera de las instalaciones	A.11.2.6
Disposición segura o reutilización de equipos	A.11.2.7
Equipos de usuario desatendidos	A.11.2.8
Política de escritorio y pantalla limpios	A.11.2.9

Tabla 9 - Controles Seguridad en los equipos - ISO27001

Fases del proceso

Fase de diagnóstico

En esta fase se identifica el estado actual de la entidad con respecto a los requerimientos del MSPI. Tiene las siguientes metas:

Metas	Resultados	Instrumentación MSPI	Alineación MRAE
Determinar el estado actual de la gestión de la seguridad y privacidad de la información al interior de la entidad.	Diligenciamiento de la herramienta MSPI	Herramienta de diagnóstico	LI.ES.01 LI.ES.02 LI.GO.01 LI.GO.04 LI.GO.05 LI.GO.07 LI.ST.14
Identificar el nivel de madurez de la seguridad y privacidad de la información de la entidad.	Diligenciamiento de la herramienta e identificación del nivel de madurez de la entidad.	Herramienta de diagnóstico	

Metas	Resultados	Instrumentación MSPI	Alineación MRAE
Identificar vulnerabilidades técnicas y administrativas que sirvan como insumo para la fase de planificación.	Diagnóstico con los hallazgos encontrados en las pruebas de vulnerabilidades.	Herramienta de diagnóstico	

Tabla 10 - Fase de Diagnóstico MSPI

En virtud de estos lineamientos, la Dirección de Informática gestiona y tiene establecida una política y sus lineamientos, cuyo fin es gobernar y controlar las Tecnologías de la Información y Comunicación, así como para la seguridad y privacidad de la información.

Fase de Planificación

Metas	Resultados	Instrumentos MSPI	MRAE
Política de seguridad de la información	Documento con la política de seguridad de la información, debidamente aprobado por la Alta Dirección y socializada al interior de la Entidad.	Guia No 2 – Política general MSPI	LI.ES.02 LI.ES.06 LI.ES.07 LI.ES.08 LI.ES.09 LI.ES.10 LI.GO.01 LI.GO.04 LI.GO.07 LI.GO.08
Procedimientos de seguridad e la información	Procedimientos, debidamente documentados, socializados y aprobados por el comité que integre los sistemas de gestión institucional.	Guía No 3 – Procedimientos de seguridad y privacidad de la información	LI.GO.09 LI.GO.10 LI.INF.01 LI.INF.02 LI.INF.09 LI.INF.10 LI.INF.11 LI.INF.14
Roles y responsabilidades de la seguridad y privacidad de la información	Acto administrativo a través del cual se crea o se modifica las funciones del comité de gestión institucional (o el que haga sus veces), en donde se incluyan los temas de seguridad de la información en la entidad, revisado y aprobado por la alta	Guía No 3 – Roles y responsabilidades de seguridad y privacidad de la información	LI.SIS.22 LI.SIS.23 LI.SIS.01 LI.ST.05 LI.ST.06 LI.ST.09 LI.ST.10 LI.ST.12 LI.ST.13 LI.ST.14 LI.UA.01 LI.UA.02 LI.UA.03

Metas	Resultados	Instrumentos MSPI	MRAE
	dirección, deberá designarse quién será el encargado de seguridad de la información dentro de la entidad.		LI.UA.04 LI.UA.05 LI.UA.06
Inventario de activos	Documento con la metodología para la identificación, clasificación y valoración de activos de información, validado por el comité de seguridad de la información o quien haga sus veces y revisado y aprobado por la alta dirección. Matriz con la identificación, valoración y clasificación de activos de información. Documento con la caracterización de activos de información, que contengan datos personales. Inventario de activos de IPv6.	Guía No 5 – Gestión de Activos Guía No 20 – Transición de IPv4 a IPv6	
Integración del MSPI con el Sistema de Gestión Documental	Integración del MSPI, con el sistema de gestión documental de la entidad	Guía No 6 – Gestión documental	
Identificación, valoración y tratamiento del riesgo	Documento con la metodología de gestión de riesgos. Documento con el análisis y evaluación de riesgos. Documento con el plan de	Guía No 7 – Gestión de Riesgos Guía No 8 – Controles de seguridad	

Metas	Resultados	Instrumentos MSPI	MRAE
	tratamientos del riesgo. Documento con la declaración de aplicabilidad. Documentos revisados y aprobados por la Alta Dirección.		
Plan de comunicaciones	Documento con el plan de comunicación, sensibilización y capacitación para la entidad	Guía No 14 – Plan de comunicación, sensibilización y capacitación	
Plan de diagnóstico de IPv4 a IPv6	Documento con el Plan de diagnóstico para la transición de IPv4 a IPv6.	Guía No 20 – Transición de IPv4 a IPv6	

Tabla 11 - Fase Planificación MSPI

Fase de Implementación

En esta fase se ejecuta la implementación de la planificación realizada en la fase anterior.

Metas	Resultados	Instrumentos	
		MSPI	MRAE
Planificación y control operacional	Documento con la estrategia de planificación y control operacional, revisado y aprobado por la alta dirección.	Documento con el plan de tratamiento de riesgos. Documento con la declaración de aplicabilidad.	LI.ES.09 LI.ES.10 LI.GO.04 LI.GO.09 LI.GO.10 LI.GO.14 LI.GO.15 LI.INF.09
Implementación de plan de tratamiento de riesgos	Informe de ejecución del plan de tratamiento de riesgos aprobado por el dueño de cada proceso.	Documento con la declaración de aplicabilidad. Documento con el plan de tratamiento de riesgos.	LI.INF.10 LI.INF.11 LI.INF.14 LI.INF.15 LI.SIS.22 LI.SIS.23 LI.ST.05 LI.ST.06
Indicadores de gestión	Documento con la descripción de los indicadores de gestión de seguridad y privacidad de la información.	Guía no. 9 Indicadores de gestión de SI	LI.ST.09 LI.ST.10 LI.ST.12 LI.ST.13 LI.UA.01

Metas	Resultados	Instrumentos	
		MSPI	MRAE
Plan de transición de IPv4 a IPv6	Documento con las estrategias del plan de implementación de IPv6 en la entidad, aprobado por la Dirección de Informática.	Documento con el Plan de diagnóstico para la transición de IPv4 a IPv6. Guía No 20 - Transición de IPv4 a IPv6 para Colombia. Guía No 19 – Aseguramiento del Protocolo IPv6.	

Tabla 12 - Fase de Implementación MSPI

Fase de evaluación de desempeño

El seguimiento y monitoreo del MSPI se hace con base en los resultados que arrojan los indicadores de la seguridad de la información propuestos para verificar la efectividad, la eficiencia y la eficacia de las acciones implementadas.

Metas	Resultados	Instrumentos	
		MSPI	MRAE
Plan de revisión y seguimiento a la implementación del MSPI	Documento con el plan de seguimiento y revisión del MSPI revisado y aprobado por la alta dirección.	Guía No 16 – Evaluación del desempeño.	LI.ES.12 LI.ES.13 LI.GO.03 LI.GO.11 LI.GO.12
Plan de ejecución de auditorías	Documento con el plan de ejecución de auditorías y revisiones independientes del MSPI, revisado y aprobado por la alta dirección.	Guía No 15 – Guía de Auditoría.	LI.INF.09 LI.INF.11 LI.INF.13 LI.INF.14 LI.INF.15 LI.SIS.23 LI.ST.05 LI.ST.06 LI.ST.08 LI.ST.15 LI.UA.07 LI.UA.08

Tabla 13 - Fase Evaluación MSPI

Cronograma

% Completado

La siguiente es la lista de etapas y el porcentaje de avance:

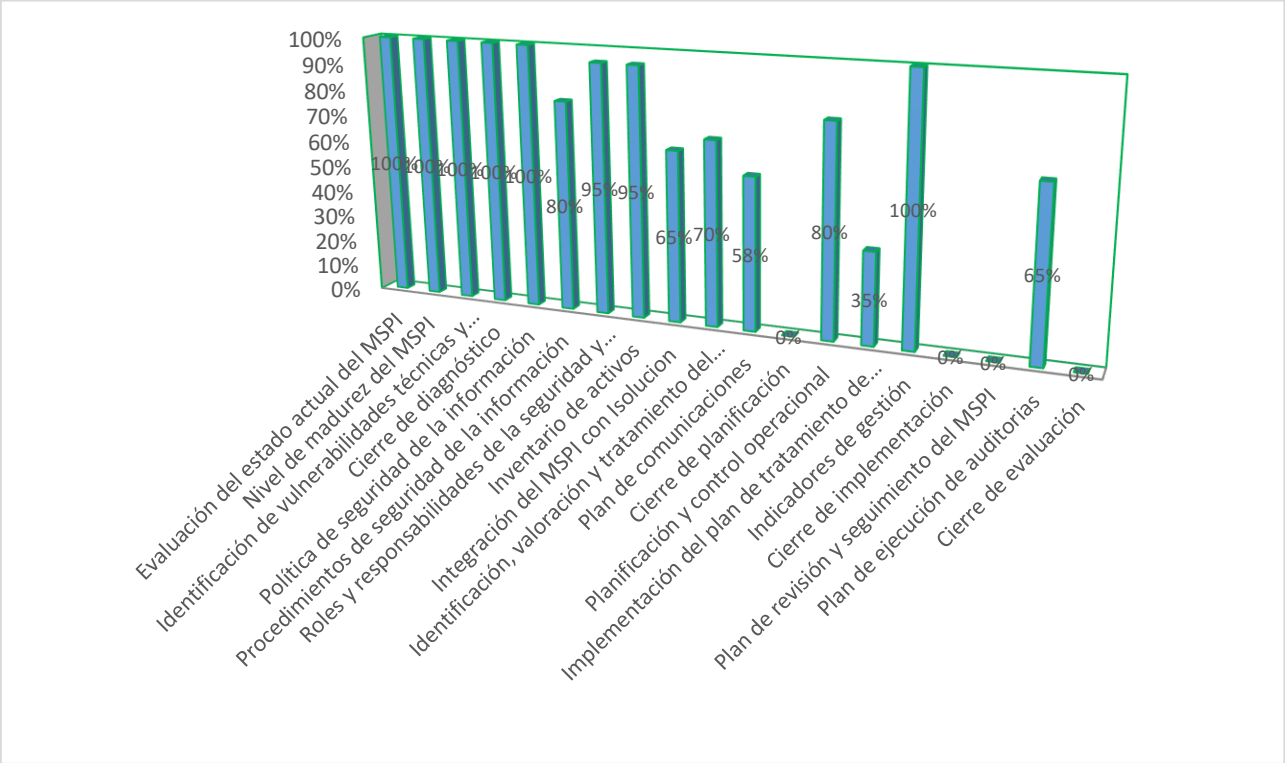

Ilustración 13 - Ejecución de etapas

Porcentaje total de avance

% COMPLETADO
77%

Actividades pendientes

Nombre	Fin
Cierre de planificación	lun 25/01/21
Cierre de implementación	lun 10/08/21
Cierre de evaluación	mar 23/02/21

Nivel de Cumplimiento

A diciembre de 2021 se ejecuta la última revisión del MSPI, adicionalmente se define una Declaración de Aplicabilidad, en la que se establece el alcance de los controles propuestos por el MSPI, en la cual se excluye la gestión de la seguridad física, ya que ésta según el organigrama de la Gobernación de Antioquia, no hace parte del área de Seguridad de la Información. El resultado a la fecha de la evaluación es el siguiente:

Autodiagnóstico Año 2021

	CONTROLES	SITUACIÓN INICIAL	% DE IMPLEMENTACIÓN	% META 2019	%META 2020	%META 2021	%META 2022
ADMINISTRATIVOS	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	40	95	70	95	95	95
	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	45	83	75	90	95	95
	SEGURIDAD DE LOS RECURSOS HUMANOS	36	67	65	85	95	95
	GESTIÓN DE ACTIVOS	59	90	75	95	95	95
	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	6,5	75	75	90	95	95
	CUMPLIMIENTO	51,5	79	75	85	95	95
	RELACIONES CON LOS PROVEEDORES	50	60	70	85	95	95
TÉCNICOS	CONTROL DE ACCESO	47	64	75	90	95	95
	SEGURIDAD DE LAS OPERACIONES	39	68	70	85	95	95
	SEGURIDAD DE LAS COMUNICACIONES	50	75	75	90	95	95
	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	59	70	75	90	95	95
	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	54	97	95	95	95	95
	VALORACIÓN DE IMPLEMENTACIÓN	**45**	**76**	**75**	**90**	**95**	**95**

Tabla 14 - Autodiagnóstico Año 2021

Autodiagnóstico a Diciembre de 2021

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	93	100	OPTIMIZADO
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	81	100	OPTIMIZADO
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	78	100	GESTIONADO
A.8	GESTIÓN DE ACTIVOS	80	100	GESTIONADO
A.9	CONTROL DE ACCESO	78	100	GESTIONADO
A.10	CRIPTOGRAFÍA	77	100	GESTIONADO
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	85	100	OPTIMIZADO
A.12	SEGURIDAD DE LAS OPERACIONES	76	100	GESTIONADO
A.13	SEGURIDAD DE LAS COMUNICACIONES	30	100	#¡REF!
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	22	100	REPETIBLE
A.15	RELACIONES CON LOS PROVEEDORES	94	100	OPTIMIZADO
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	92	100	OPTIMIZADO
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	90	100	OPTIMIZADO
A.18	CUMPLIMIENTO	90	100	OPTIMIZADO
PROMEDIO EVALUACIÓN DE CONTROLES		**76**	**100**	GESTIONADO

Tabla 15 - Autodiagnóstico a diciembre de 2021

EVALUACIÓN DE EFECTIVIDAD DE CONTROLES - ISO 27001:2013 ANEXO A – diciembre 2021

Ilustración 14 - Evaluación De Efectividad De Controles - ISO 27001:2013

Avance de PHVA (Planear – Hacer – Verificar y Actuar) a Diciembre de 2021

Año	AVANCE PHVA		
	COMPONENTE	% de Avance Actual Entidad	% Avance Esperado
2021	Planificación	36%	40%
2021	Implementación	18%	20%
2021	Evaluación de desempeño	19%	20%
2021	Mejora continua	18%	20%
TOTAL		**90%**	**100%**

Tabla 16- Avance de PHVA

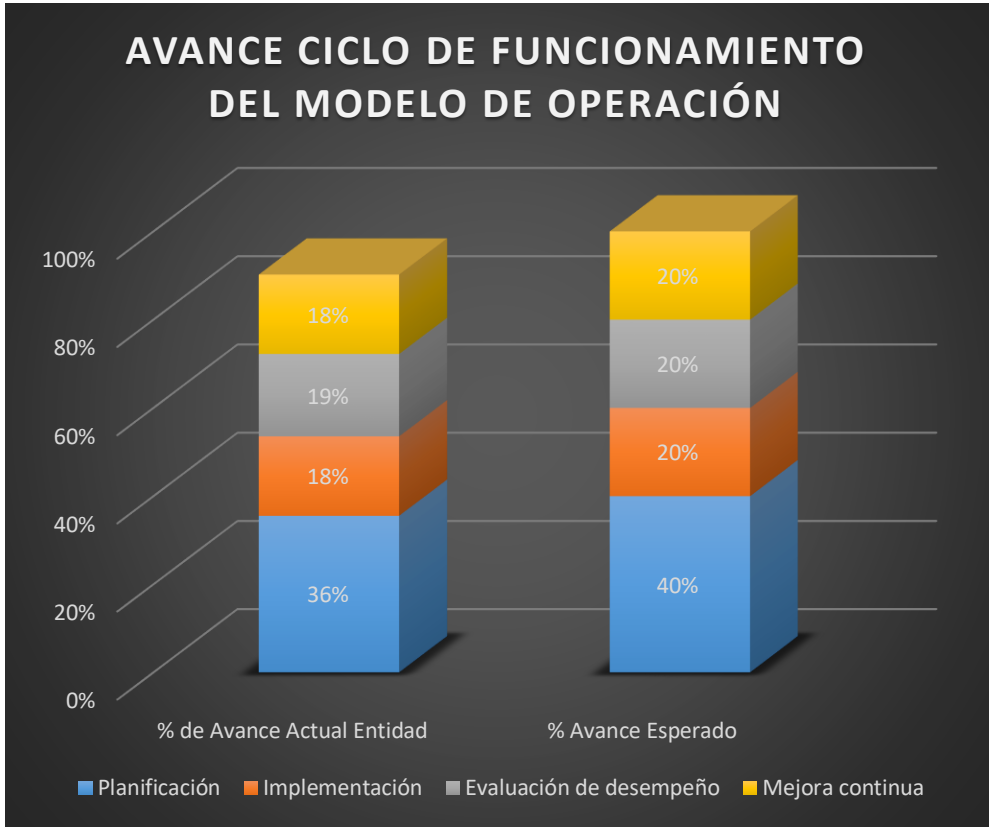

Ilustración 15 - Avance Ciclo De Funcionamiento Del Modelo de Operación

MODELO FRAMEWORK CIBERSEGURIDAD NIST 2020

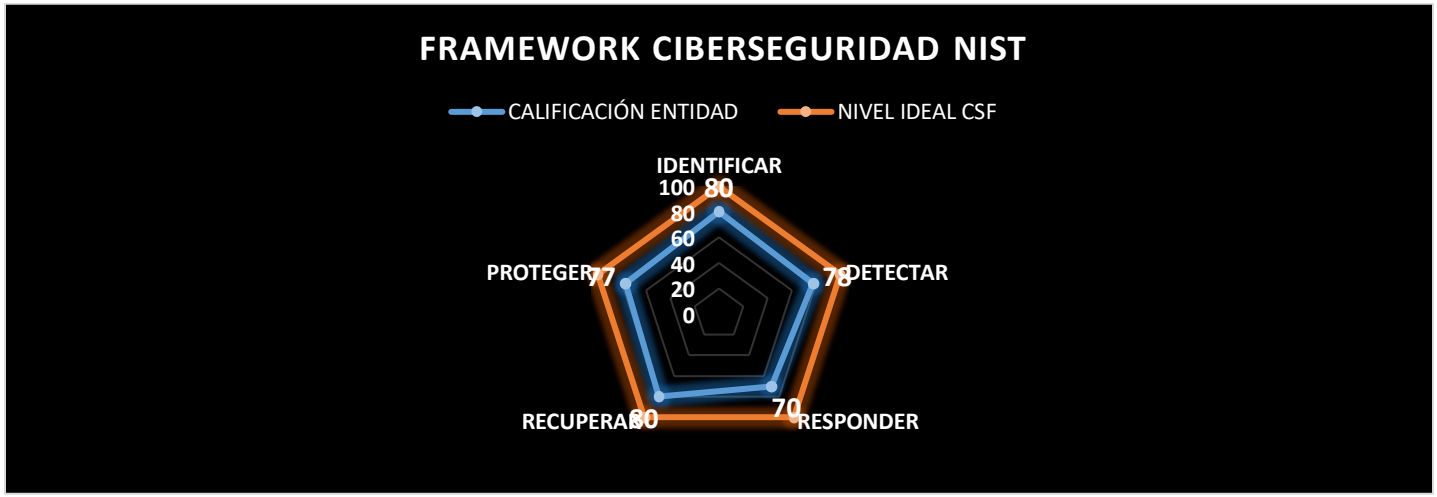

Ilustración 16- Modelo Framework Ciberseguridad NIST

MODELO FRAMEWORK CIBERSEGURIDAD NIST		
Etiquetas de fila	CALIFICACIÓN ENTIDAD	NIVEL IDEAL CSF
IDENTIFICAR	80	100
DETECTAR	78	100
RESPONDER	70	100
RECUPERAR	80	100
PROTEGER	77	100

Tabla 17 - Modelo Framework Ciberseguridad NIST

Mapa de Ruta MSPI de la Gobernación de Antioquia a diciembre 2021

A diciembre de 2021, esto es lo que se tiene en la implementación, con un porcentaje de 76% completado, con el objetivo de alcanzar el 75% promedio en 2020.

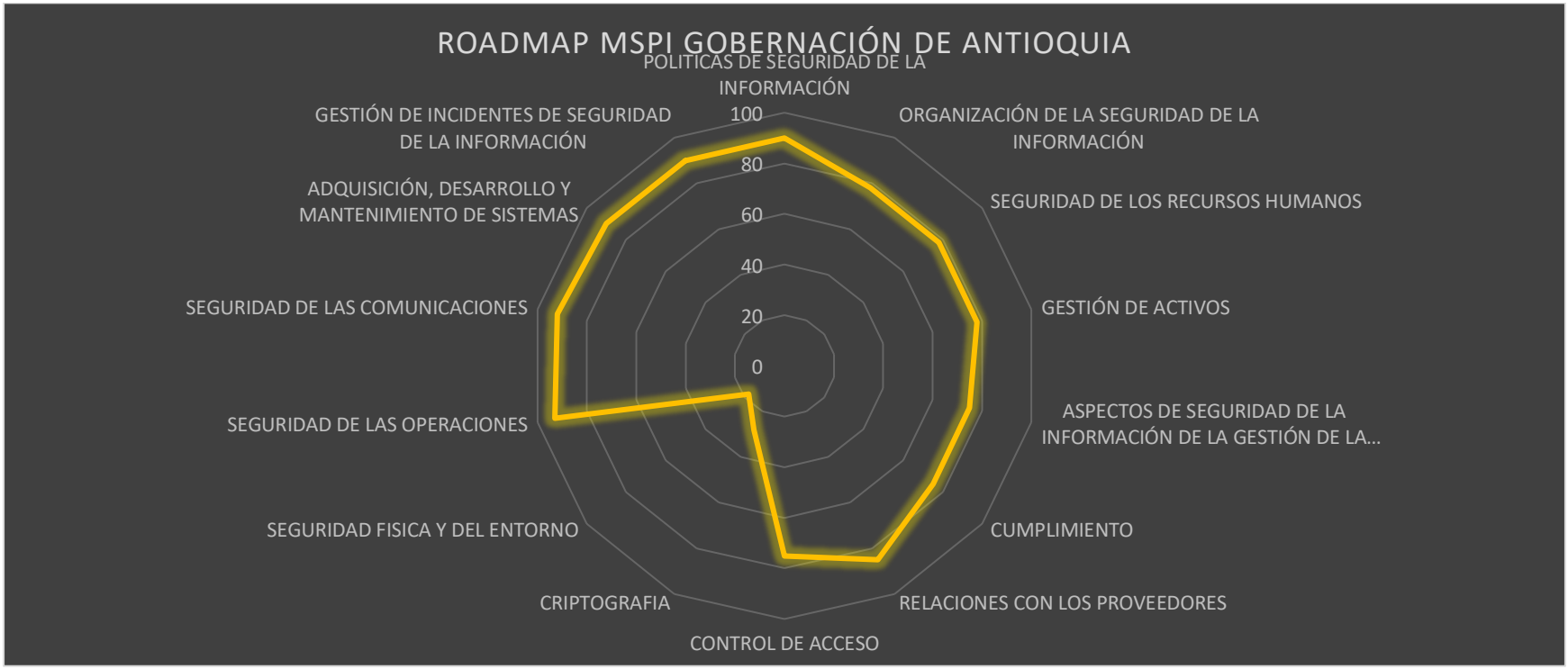

Tabla 18 -Mapa de Ruta MSPI diciembre 2021

Variación de la Implementación

Durante el período de septiembre a diciembre de 2021, la siguiente ha sido la variación en los dominios del MSPI:

Tabla 19 - Variación MSPI 2021

Macro Indicadores de Seguridad de la Información

Se establecen los macro indicadores en tres grandes grupos en los cuales se resume la operación de cada uno de los frentes que involucra la seguridad de la información.

Seguridad Organizacional, la cual comprende la política de seguridad de la información, la organización de la seguridad, los activos de información involucrados con la seguridad, la relación con los proveedores, la gestión de incidentes de seguridad de la información y la gestión de la seguridad de la información de la continuidad de negocio.

Seguridad Lógica, la que comprende los controles de acceso, la criptografía, la seguridad de las operaciones y la adquisición, desarrollo y mantenimiento de los sistemas de información.

Y la seguridad legal, que involucra el cumplimiento.

A diciembre de 2021, este es el estado de los macro indicadores:

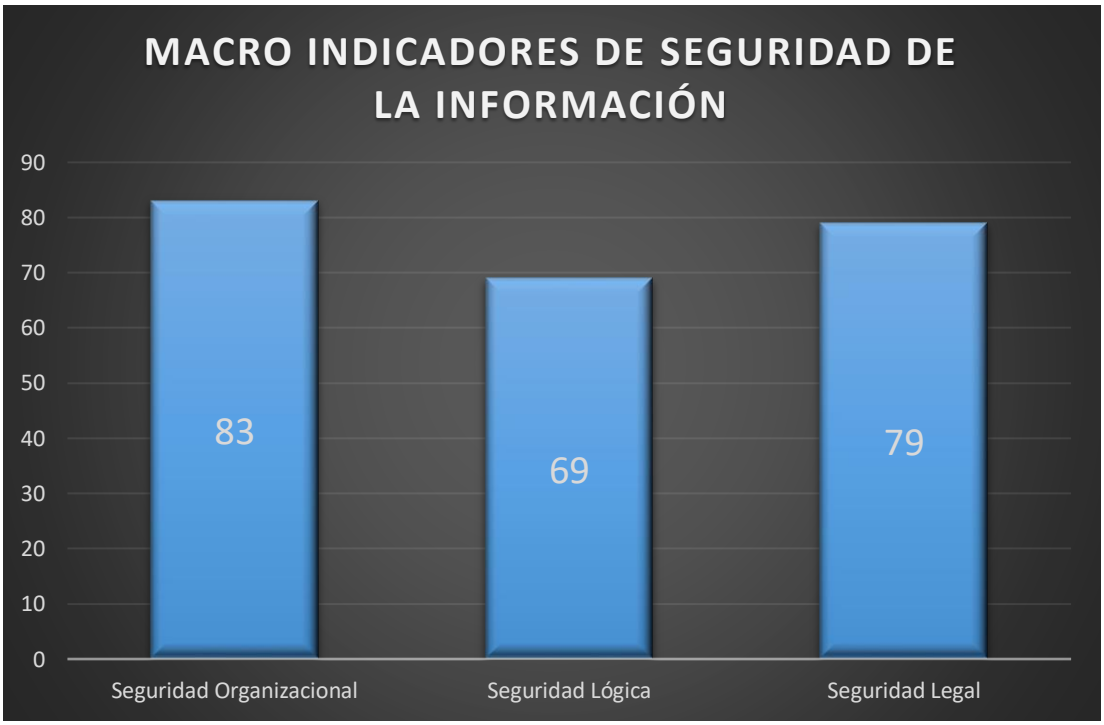

Ilustración 17 - Macroindicadores MSPI

Indicador de Gestión de Seguridad de la Información

A partir del segundo semestre de 2020, se definió que el indicador de gestión de seguridad de la información se basaría en el MSPI, haciendo un promedio ponderado de los controles administrativos y los controles técnicos, así:

$$IGSI = \frac{(Promedio\ de\ controles\ administrativos) + (Promedio\ de\ controles\ técnicos)}{2}$$

A diciembre de 2022, el indicador de gestión se presenta con referencia al objetivo planteado a finales de 2020:

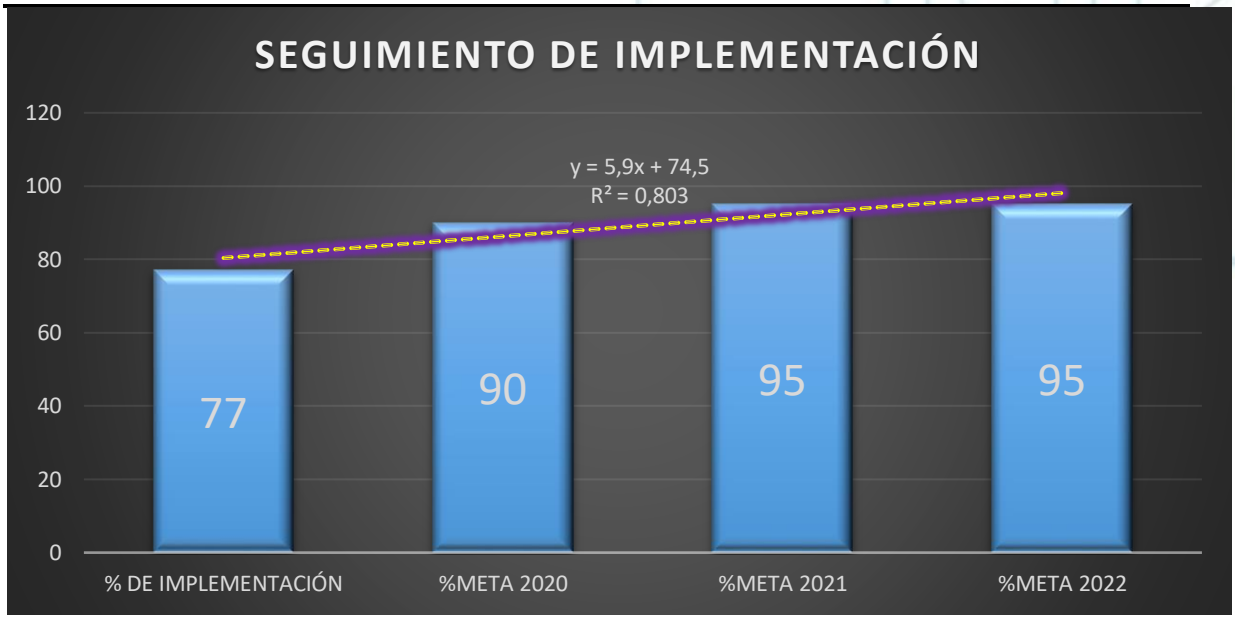

Ilustración 18 - Resumen de Controles de Gestión de Seguridad

Esto indica que el modelo está bien ajustado (R^2= 0,803) y adicionalmente se requiere un esfuerzo del 6% para alcanzar el objetivo planteado para finales de 2020.

En términos de cumplimiento de objetivos, la meta trazada para finales de 2020 era un 75% del indicador de gestión interna de seguridad de la información, para diciembre de 2021 tenemos un 76% de cumplimiento, un punto porcentual por encima de la meta trazada. La siguiente gráfica muestra el resumen de los controles de seguridad de la información:

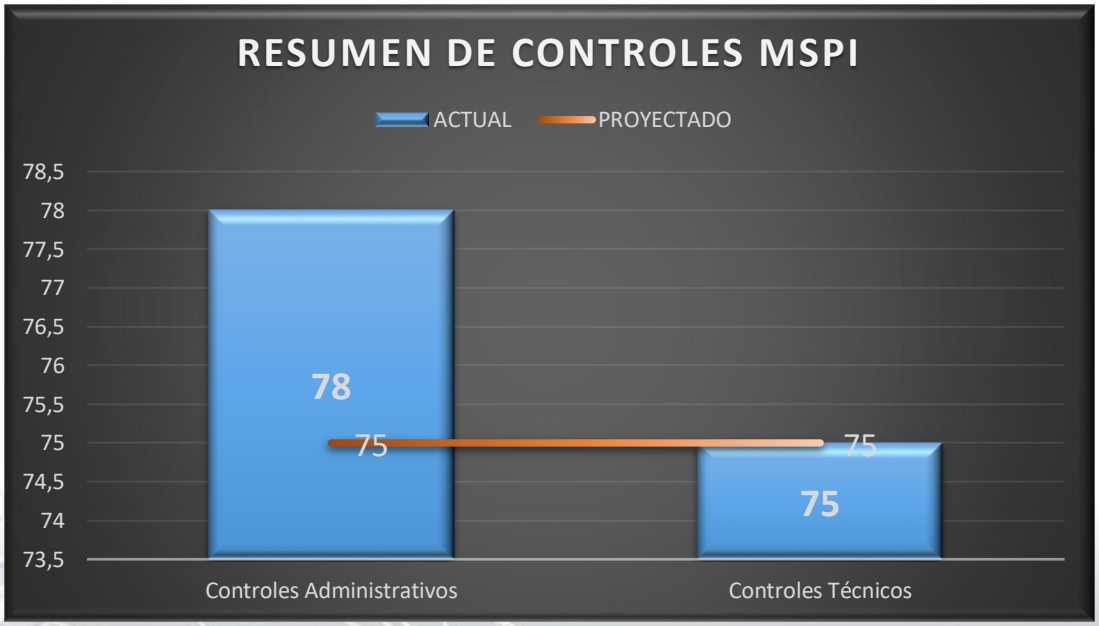

Ilustración 19 - Resumen de controles SGSI

Indicadores de Gestión Interna

Se definieron cuatro tipos de indicadores para medir la gestión interna.

Gestión de Vulnerabilidades

El indicador de gestión de vulnerabilidades apunta a revisar el nivel de cobertura que se tiene respecto a las vulnerabilidades que se encuentra en los servidores que deben ser analizados mensualmente por temas de actualizaciones, parcheo y vulnerabilidades técnicas en general. Se cuenta con dos indicadores de gestión de vulnerabilidades:

Campo	Datos	
ID del indicador	Porcentaje de vulnerabilidades de alto impacto mitigadas.	
Objetivo	La organización debe tratar a tiempo las vulnerabilidades conocidas.	
Indicador	Porcentaje de vulnerabilidades de alto impacto mitigadas dentro del plazo definido por la organización desde su descubrimiento.	
Datos Primarios	- Número de vulnerabilidades identificadas dentro del plazo especificado por la organización. (No olvidar que el número de vulnerabilidades de alto impacto identificadas dentro del plazo especificado por la organización debe ser calculado a partir de los datos primarios.) - Número de vulnerabilidades de alto impacto mitigadas dentro del plazo.	
Fórmula	(Número total de vulnerabilidades de alto impacto mitigadas a tiempo/Número total de vulnerabilidades de alto impacto identificadas) × 100.	
Frecuencia	Mensual	
Tipo	Eficacia/eficiencia.	
Unidades de Medida	Porcentual	
METAS		
Mínima **0 – 60%**	**Satisfactoria** **61% - 90%**	**Sobresaliente** **91% - 100%**
Observaciones	Para el levantamiento de la información que permita obtener datos para la medición el responsable debe idear planes, laboratorios o actividades periódicas que permitan medir lo capacitado o divulgado.	

Campo	Datos
ID del indicador	Tiempo medio para mitigar vulnerabilidades.
Objetivo	Indicar el rendimiento de la organización en la resolución de las vulnerabilidades detectadas. Cuanto menos tiempo requiera, mayor será la probabilidad de que la organización pueda reducir con eficacia el riesgo de explotación de vulnerabilidades.
Indicador	Tiempo medio para mitigar vulnerabilidades cuantifica el tiempo medio para mitigar las vulnerabilidades identificadas en una organización
Datos Primarios	• Fecha de detección de las vulnerabilidades.

	• Fecha de mitigación de las vulnerabilidades. • Número total de vulnerabilidades detectadas. • Número total de vulnerabilidades mitigadas notificadas.	
Fórmula	Suma (Día_vulnerabilidad_resuelta – Día de detección)/Número (vulnerabilidades_resueltas).	
Frecuencia	Mensual	
Tipo	Gestión (Eficacia/eficiencia).	
Unidades de Medida	Porcentual	
METAS		
Mínima **0 – 60%**	**Satisfactoria** **61% - 90%**	**Sobresaliente** **91% - 100%**
Observaciones	Para el levantamiento de la información que permita obtener datos para la medición el responsable debe idear planes, laboratorios o actividades periódicas que permitan medir lo capacitado o divulgado.	

Gestión de Sensibilización

La gestión de sensibilización busca medir la cobertura de la sensibilización en seguridad de la información a lo largo de toda la Gobernación de Antioquia, busca que cada año se mida un promedio mensual que determine que la cobertura en sensibilización y concientización de los funcionarios y contratistas sea igual o superior a un promedio del 85% anual. Se define de la siguiente manera:

Campo	Datos	
ID del indicador	Programa de sensibilización de la organización.	
Objetivo	Establecer la efectividad de un plan de capacitación y sensibilización previamente definido como medio para el control de incidentes de seguridad.	
Indicador	Porcentaje de empleados que participan en el programa de sensibilización.	
Datos Primarios	• Número de empleados que participan en programas de sensibilización. • Número de empleados.	
Fórmula	(Número de empleados que participan en programas de sensibilización/Número total de empleados) × 100.	
Frecuencia	Trimestral	
Tipo	Gestión (Eficacia/eficiencia y aplicación)	
Unidades de Medida	Porcentual	
METAS		
Mínima **0 – 60%**	**Satisfactoria** **61% - 90%**	**Sobresaliente** **91% - 100%**
Observaciones	Para el levantamiento de la información que permita obtener datos para la medición el responsable debe idear planes, laboratorios o	

	actividades periódicas que permitan medir lo capacitado o divulgado.

Se busca que este ámbito de la seguridad de la información tenga un medidor adicional, el cual incluye el tema de la evaluación de la sensibilización y concientización en seguridad mediante alguna herramienta de gestión de conocimiento que nos permita evaluar los conocimientos adquiridos.

Gestión Operativa

La gestión operativa busca medir el grado de aprendizaje en incidentes de seguridad de la información, busca medir cada que ocurra un incidente, que tengamos documentado los eventos que rodearon el mismo, las actividades que se ejecutaron para resolverlo y las oportunidades de mejora, está definido de la siguiente manera:

Campo	Datos	
ID del indicador	Respuesta a incidentes.	
Objetivo	La organización debe notificar los incidentes a tiempo para cada categoría de incidentes.	
Indicador	Porcentaje de incidentes notificados dentro del plazo estipulado para la categoría del caso.	
Datos Primarios	• Número de incidentes notificados dentro del plazo estipulado por la organización. • Número total de incidentes notificados.	
Fórmula	(Número de incidentes notificados a tiempo/Número total de incidentes notificados) × 100, para cada categoría.	
Frecuencia	Mensual	
Tipo	Gestión (Eficacia/eficiencia y aplicación)	
Unidades de Medida	Porcentual	
METAS		
Mínima **0 – 60%**	**Satisfactoria** **61% - 90%**	**Sobresaliente** **91% - 100%**
Observaciones	Para el levantamiento de la información que permita obtener datos para la medición el responsable debe idear planes, laboratorios o actividades periódicas que permitan medir lo capacitado o divulgado.	

Gestión de Antivirus/Antispyware

Este indicador busca medir la cobertura que tenemos en materia de firmas digitales en los equipos de usuario final, así como la tendencia de ataques a causa de virus o software malicioso, se define de la siguiente manera:

Campo	Datos
ID del indicador	Cobertura del programa de detección y tratamiento de malware.

Objetivo	Dispositivos de usuario final con programas antivirus para mitigar el malware, incluidos los virus que residen en esos dispositivos.	
Indicador	Porcentaje de dispositivos de punto extremo con programas de detección y tratamiento de malware.	
Datos Primarios	Número total de dispositivos de punto extremo con programas antivirus. Número de dispositivos de punto extremo.	
Fórmula	(Número total de dispositivos de punto extremo con programas de detección y tratamiento de malware/número total de dispositivos de punto extremo) × 100.	
Frecuencia	Mensual	
Tipo	Gestión (Eficacia/eficiencia y aplicación)	
Unidades de Medida	Porcentual	
METAS		
Mínima **0 – 60%**	**Satisfactoria** **61% - 90%**	**Sobresaliente** **91% - 100%**
Observaciones	Para el levantamiento de la información que permita obtener datos para la medición el responsable debe idear planes, laboratorios o actividades periódicas que permitan medir lo capacitado o divulgado.	

Distribución de programa de parches de seguridad

Este indicador mide la gestión de parches, identificando la correcta y oportuna instalación de parches en los equipos corporativos frente a las necesidades de seguridad en la Entidad.

Campo	Datos
ID del indicador	Programa de parches de seguridad.
Objetivo	Que los dispositivos de punto extremo instalen un programa de parches de seguridad para mitigar las vulnerabilidades.
Indicador	Porcentaje de dispositivos de punto extremo que tienen instalado el sistema de gestión de parches.
Datos Primarios	• Número total de dispositivos de punto extremo que disponen de un programa de parches de seguridad. • Número de dispositivos de punto extremo.
Fórmula	(Número total de dispositivos de punto extremo que utilizan un programa de parches de seguridad/Número total de dispositivos de punto extremo) × 100.
Frecuencia	Mensual
Tipo	Gestión (Eficacia/eficiencia y aplicación)
Unidades de Medida	Porcentual
METAS	

Mínima **0 – 60%**	**Satisfactoria** **61% - 90%**	**Sobresaliente** **91% - 100%**
Observaciones	Para el levantamiento de la información que permita obtener datos para la medición el responsable debe idear planes, laboratorios o actividades periódicas que permitan medir lo capacitado o divulgado.	

Control de acceso a distancia con función de seguridad para la prevención de intrusiones o la detección de intrusiones

Campo	Datos	
ID del indicador	Puntos de acceso a distancia protegidos.	
Objetivo	La organización debería instalar una función de seguridad para detectar o prevenir las intrusiones a fin de proteger los activos internos de la organización.	
Indicador	Porcentaje de puntos de acceso a distancia protegidos	
Datos Primarios	• Número de puntos de acceso a distancia que aplican la función de seguridad para la detección o prevención de intrusiones. • Número de puntos de acceso a distancia.	
Fórmula	(Número de puntos de acceso a distancia que aplican la función de seguridad para la detección y prevención de intrusiones/Número total de puntos de acceso a distancia) × 100.	
Frecuencia	Mensual	
Tipo	Gestión (Eficacia/eficiencia y aplicación)	
Unidades de Medida	Porcentual	
METAS		
Mínima **0 – 60%**	**Satisfactoria** **61% - 90%**	**Sobresaliente** **91% - 100%**
Observaciones	Para el levantamiento de la información que permita obtener datos para la medición el responsable debe idear planes, laboratorios o actividades periódicas que permitan medir lo capacitado o divulgado.	

Spam recibido

Campo	Datos
ID del indicador	Promedio Spam recibido
Objetivo	La organización debería utilizar filtros para bloquear los mensajes spam para que no los reciban los empleados.
Indicador	Porcentaje de empleados que reciben un número de mensajes spam mayor que el definido por la organización en un determinado intervalo de tiempo.

Datos Primarios	• Número de empleados que reciben un número de mensajes spam mayor que el definido por la organización en un determinado intervalo de tiempo. • Número de empleados.	
Fórmula	(Número de empleados que recibe un determinado número de mensajes spam/Número total de empleados) × 100.	
Frecuencia	Mensual	
Tipo	Gestión (Eficacia/eficiencia y aplicación)	
Unidades de Medida	Porcentual	
METAS		
Mínima **0 – 60%**	**Satisfactoria** **61% - 90%**	**Sobresaliente** **91% - 100%**
Observaciones	Para el levantamiento de la información que permita obtener datos para la medición el responsable debe idear planes, laboratorios o actividades periódicas que permitan medir lo capacitado o divulgado.	

Matrices de Riesgo

El procedimiento de gestión de riesgos se ciñe al documento PR-M1-P5-013 definido en el sistema de iSolucion. En la cual se establece el riesgo como la probabilidad de un evento a futuro que depende de la probabilidad de que se materialice una vulnerabilidad y el impacto de la materialización de esta.

Actividades críticas de 2021

- Evaluación del FURAG sobre Seguridad Digital
- Actualización de la evaluación del MSPI (Modelo de Seguridad y Privacidad de la Información)
- Participar en los retos de Máxima Velocidad con respecto a Seguridad de la Información.
- Sensibilización en seguridad de la información a 1450 servidores públicos, contratistas y practicantes.
- Celebrar el día Internacional de Seguridad de la Información por medio de Facebook Live el día 30/nov/2021.
- Actualizar el Manual y Política de Lineamientos de Seguridad de la Información. (Isolucion)
- Actualizar el Plan de Tratamiento de Riesgos de Seguridad de la Información en Isolucion.
- Diagnóstico de brechas de Seguridad a los ambientes Web y La Infraestructura Tecnológica.
- Indicadores de la Operación en Seguridad de la Información en Power BI.
- Actualizar los Criterios de Seguridad para el Desarrollo de Software Seguro. (OWASP Top 10 - Actualizado).
- Indicador del Proceso GTI de Gestión de la Seguridad de la Información

Reportes de la Operación periódicos y actualización de componentes tecnológicos.

Actividades críticas de 2022

- Formalizar el procedimiento de transferencia de información.
- Adquirir soluciones de integración de acceso, gestión automatizada de usuarios y cifrado de contraseñas.
- Oficializar e implementar un procedimiento de desarrollo de software seguro para aplicaciones de la Gobernación de Antioquia, así como controles para el desarrollo implementado por terceros.
- Formalizar y documentar el proceso de gestión de cambios, protección de la información de registro, adquisición de una solución tipo SIEM.
- Ejecutar como mínimo una prueba de escritorio en 2022 en continuidad de negocio, y dejarla documentada como evidencia.
- Puesta en marcha de nuevos indicadores internos de seguridad de la información.
- Charlas de Seguridad de la Información para los funcionarios, contratistas y practicantes.
- Continuar ejecutando actividades de sensibilización y concursos en seguridad de la información.
- Adquirir un Firewall de nueva generación en alta disponibilidad para la Gobernación de Antioquia.

INFORME DE RESULTADOS

Alineación PESI y PETI

La alineación del PESI y el PETI busca sincronizar los objetivos estratégicos de TI incluidos en el PETI, el cual establece los lineamientos para el mejoramiento del nivel de madurez institucional en la implementación de soluciones tecnológicas que generen valor y promuevan el cumplimiento de sostenibilidad tecnológica. Así mismo el PESI define los objetivos que permiten garantizar la confidencialidad, integridad y disponibilidad de los activos de información. Para ello se establecen los objetivos de TI que están directamente relacionados con el plan estratégico de seguridad de la información. En negrilla se resaltan los objetivos relacionados directamente con seguridad de la información.

# Objetivo PETI	Descripción
1	Alinear la estrategia de TI con la estrategia de Gobierno Digital.
2	Maximizar el aporte de las TIC en los procesos internos de la Gobernación de Antioquia para la transformación de la misma.
3	Ejercer el Gobierno de las TIC de la Gobernación de Antioquia.
4	Posicionarse como un aliado estratégico de todos los procesos internos de la Gobernación de Antioquia.
5	Mejorar la satisfacción de las partes involucradas en el uso de los sistemas de información, así como el ciudadano, de la Gobernación de Antioquia.

# Objetivo PETI	Descripción
6	Proveer información oportuna y de calidad para la toma de decisiones de los procesos internos de la Gobernación de Antioquia.
7	Entregar oportunamente sistemas de información de calidad, funcionales, eficientes y confiables que fortalezcan los procesos internos de la Gobernación de Antioquia.
8	Fortalecer la gestión de las TIC y de la seguridad de la información en los procesos internos de la Gobernación de Antioquia.
9	Fortalecer las competencias y desarrollo profesional del equipo de TI de la Gobernación de Antioquia.
10	Desarrollar la capacidad de innovación y prospectiva tecnológica.

Tabla 20- Alineación PESI y PETI

Análisis y Priorización de las Iniciativas de Seguridad de la Información

Priorización del Portafolio de Proyectos

Una vez identificadas las iniciativas y los proyectos con base en el resultado de diagnóstico de la situación actual del instrumento del MSPI del MinTIC, se hace necesario priorizar los proyectos, para lo cual se tuvo en cuenta la estrategia de seguridad de la información (Modelo de Seguridad y Privacidad de la Información, Gestión de Riesgos de Seguridad de la Información, Desarrollo y Gestión del Programa de Seguridad de la Información). Para ello se construyeron las siguientes categorías de prioridad que permiten evaluar y determinar una secuencia sistemática para el desarrollo del PESI.

PRIORIDAD	
PRIORIDAD	**DESCRIPCIÓN**
0	Elaboración del Plan Estratégico de Seguridad de la Información PESI.
1	Modelo de Seguridad y Privacidad de la Información, el cual incluye las iniciativas que soportan el desarrollo del modelo de la seguridad de la información.
2	Gestión de riesgos operacionales, los cuales hace referencia a los proyectos y actividades que mitigan los riesgos de la seguridad de la información catalogados como relevantes, garantizando la salvaguarda de la información en lo relacionado a la confidencialidad, integridad y disponibilidad.
3	Desarrollo y gestión del programa de seguridad de la información; hace referencia a aquellos proyectos que permiten la operación y el mantenimiento del SGSI.
4	Desempeño: Soportan aquellos proyectos que permiten la evaluación del desempeño y mejora continua del SGSI.

Tabla 21 - Priorización del Portafolio de Proyectos

A continuación, se presentan por prioridad los proyectos que se deben desarrollar a partir de la vigencia 2019 y hasta la vigencia 2022.

PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN

Con base en el Nivel de Cumplimiento reportado, se definen las iniciativas de seguridad de la información, las cuales deben estar alineadas con el PESI de la Gobernación de Antioquia, y a los resultados de la calificación actual del instrumento de diagnóstico del

MSPI. Por otro lado, es importante que las iniciativas estén enmarcadas dentro de los controles sugeridos para garantizar una adecuada arquitectura de seguridad de la información y un esquema de defensa en profundidad basado en las soluciones y tendencias de seguridad de la información y tecnología de punta. Estas iniciativas fueron definidas de acuerdo con el nivel de madurez de cada dominio, teniendo como referencia una calificación igual o inferior al sesenta por ciento (76%) de efectividad:

Indicador	Actividades	Estrategia de seguridad de la información			
		Gobierno	**Riesgos**	**Desarrollo y gestión**	**Incidentes**
I-01	Planificación y control operacional. Elaboración del plan estratégico de seguridad de la información 2020-2023	**X**			
I-02	Definir e integrar la seguridad de la información al ciclo de vida de los proyectos			**X**	
I-03	Diseño y documentación del plan anual de sensibilización en seguridad de la información para funcionarios, terceros y proveedores		**X**		
I-04	Actualizar los activos de información y realizar su valoración según la criticidad para la entidad, igualmente identificar los riesgos de seguridad de la información asociados		**X**		
I-05	Identificar los riesgos de seguridad de la información para cada uno de los procesos		**X**		
I-06	Gestionar el tratamiento de los riesgos de seguridad de la información para cada uno de los riesgos identificados en cada uno de los procesos		**X**		
I-07	Implementación de soluciones de seguridad perimetral con firewall de nueva generación			**X**	

I-08	Definición de procedimiento formal para el tratamiento de la información de producción en ambientes de desarrollo y pruebas, para proteger la confidencialidad de la información			**X**	
I-09	Definición y establecimiento de políticas de acceso de usuarios privilegiados que administren plataformas TIC (servidores, elementos de red, bbdd), así como de funciones de la entidad.			**X**	
I-010	Monitorear el cumplimiento del ciclo de vida de gestión de usuarios (creación, modificación, activación, desactivación, eliminación, etc.) verificando que se cumple para todos los procesos.			**X**	
I-011	Definición e implementación de una política de controles criptográficos para la protección de la información			**X**	
I-012	Actualización de política de seguridad de la información	**X**			
I-013	Separación de tareas y deberes para segmentar las responsabilidades y evitar conflictos de interés		**X**		
I-014	Establecer el procedimiento disciplinario coordinado con control interno.	**X**			
I-015	Actualización y prueba de los planes de DRP		**X**		

	para los procesos misionales.				
I-016	Creación del área de auditoría interna del MSPI	**X**			
I-017	Ejecución de revisiones de cumplimiento técnico.			**X**	
I-018	Establecer las políticas de control de acceso con base en la clasificación de la información.		**X**		
I-019	Restricción de acceso privilegiado a los sistemas de información.			**X**	
I-020	Definición de procedimiento para controlar la información secreta de autenticación.			**X**	
I-021	Procedimiento para la revisión de privilegios de acceso.		**X**		
I-022	Seguimiento a manejo de información secreta.			**X**	
I-023	Acceso a sistemas y aplicaciones controlado por un procedimiento de acceso seguro.			**X**	
I-024	Implementar un sistema centralizado de gestión de contraseñas.			**X**	
I-025	Oficializar el procedimiento de gestión de cambios.			**X**	
I-026	Ejecución de pruebas de copias de respaldo.			**X**	
I-027	Implementación de solución SIEM centralizada.			**X**	
I-028	Diseño de acuerdos de transferencia de información.		**X**		
I-029	Definición de política para el desarrollo seguro de software			**X**	
I-030	Procedimiento de criterios de aceptación de pruebas para nuevos sistemas de información.			**X**	

I-031	Implementación de solución de DLP para usuarios críticos.		**X**		
I-032	Lograr certificación ISO/NTC 27001 para el proceso de Gestión Ciudadana	**X**			

Tabla 22 - Tabla de iniciativas

EJECUCIÓN DE ACTIVIDADES POR PRIORIZACIÓN

Indicador	Actividades	Q 2021				Q 2022			
		1	2	3	4	1	2	3	4
I-01	Planificación y control operacional. Elaboración del plan estratégico de seguridad de la información 2020-2023								
I-02	Definir e integrar la seguridad de la información al ciclo de vida de los proyectos	**X**				**X**			
I-03	Diseño y documentación del plan anual de sensibilización en seguridad de la información para funcionarios, terceros y proveedores	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**
I-04	Actualizar los activos de información y realizar su valoración según la criticidad para la entidad, igualmente identificar los riesgos de	**X**				**X**			

Indicador	Actividades	Q 2021				Q 2022			
		1	2	3	4	1	2	3	4
	seguridad de la información asociados								
I-05	Identificar los riesgos de seguridad de la información para cada uno de los procesos				X				
I-06	Gestionar el tratamiento de los riesgos de seguridad de la información para cada uno de los riesgos identificados en cada uno de los procesos					X			
I-07	Implementación de soluciones de seguridad perimetral con firewall de nueva generación				X				
I-08	Definición de procedimiento formal para el tratamiento de la información de producción en ambientes de desarrollo y pruebas, para proteger la confidencialidad de la información						X		
I-09	Definición y establecimiento de políticas de acceso de usuarios privilegiados que					X			

Indicador	Actividades	Q 2021				Q 2022			
		1	2	3	4	1	2	3	4
	administren plataformas TIC (servidores, elementos de red, bbdd), así como de funciones de la entidad.								
I-010	Monitorear el cumplimiento del ciclo de vida de gestión de usuarios (creación, modificación, activación, desactivación, eliminación, etc.) verificando que se cumple para todos los procesos.							**X**	
I-011	Definición e implementación de una política de controles criptográficos para la protección de la información				**X**				
I-012	Actualización de política de seguridad de la información		**X**				**X**		
I-013	Separación de tareas y deberes para segmentar las responsabilidades y evitar conflictos de interés		**X**						
I-014	Establecer el procedimiento disciplinario			**X**					

Indicador	Actividades	Q 2021				Q 2022			
		1	2	3	4	1	2	3	4
	coordinado con control interno.								
I-015	Actualización y prueba de los planes de DRP para los procesos misionales.							X	
I-016	Creación del área de auditoría interna del MSPI			X					
I-017	Ejecución de revisiones de cumplimiento técnico.				X		X		X
I-018	Establecer las políticas de control de acceso con base en la clasificación de la información.				X				
I-019	Restricción de acceso privilegiado a los sistemas de información.					X			
I-020	Definición de procedimiento para controlar la información secreta de autenticación.						X		
I-021	Procedimiento para la revisión de privilegios de acceso.						X		
I-022	Seguimiento a manejo de información secreta.					X			
I-023	Acceso a sistemas y aplicaciones controlado por un							X	

Indicador	Actividades	Q 2021				Q 2022			
		1	2	3	4	1	2	3	4
	procedimiento de acceso seguro.								
I-024	Implementar un sistema centralizado de gestión de contraseñas.								**X**
I-025	Oficializar el procedimiento de gestión de cambios.			**X**					
I-026	Ejecución de pruebas de copias de respaldo.				**X**				
I-027	Implementación de solución SIEM centralizada.							**X**	
I-028	Diseño de acuerdos de transferencia de información.			**X**					
I-029	Definición de política para el desarrollo seguro de software			**X**					
I-030	Procedimiento de criterios de aceptación de pruebas para nuevos sistemas de información.				**X**				
I-031	Implementación de solución de DLP para usuarios críticos.		**X**	**X**					
I-032	Lograr certificación ISO/NTC 27001 para el proceso de Atención Ciudadana								**Q3 2022**
I-033	Implementar solución de				**X**				

Indicador	Actividades	Q 2021				Q 2022			
		1	2	3	4	1	2	3	4
	certificados digitales para acceso a redes inalámbricas								
I-034	Definir la conveniencia de tener un centro de cómputo alterno para operación mínima.						X		

Tabla 23 - Priorización de Iniciativas

ANEXO I - CONTACTO CON LAS AUTORIDADES.

La Gobernación de Antioquia mantiene contacto continuo con diversas autoridades en Seguridad de la Información para estar informado, realizar consultas, comunicar actividades y denunciar anomalías que atenten contra la integridad, confidencialidad y disponibilidad de la información.

Toda denuncia de actos ilegales conlleva una lectura, análisis y evaluación previa por parte del equipo de seguridad de la información de la Gobernación de Antioquia, previo a la comunicación oficial vía correo electrónico a las autoridades que se mencionan a continuación:

- Portal del CSIRT: https://cc-csirt.policia.gov.co/
- Portal del COLCERT: http://www.colcert.gov.co/
- Centro Cibernético Policial: https://caivirtual.policia.gov.co/
- UT Transformación Digital: https://uttransformaciondigital.com/
- Seguridad Digital de la presidencia: http://es.presidencia.gov.co
  seguridaddigital@presidencia.gov.co

ANEXO II - CONTACTO CON GRUPOS DE INTERÉS ESPECIALES

El equipo de seguridad de la información de la Gobernación de Antioquia a fin de mantenerse actualizado y a la vanguardia de temas relevantes en el área de seguridad establece contacto con diversos grupos de interés que le permiten estar informado de las novedades, nuevas tendencias, herramientas, técnicas, guías y metodologías que permitan dar garantía de la Integridad, confidencialidad y disponibilidad de la información.

El equipo de trabajo tiene contacto en redes sociales (Twitter, Facebook, Instagram, WhatsApp, correo electrónico) con diferentes grupos y compañías que brindan asesoramiento continuo en los temas más relevantes del campo de la Seguridad como lo son la gestión de riesgos, los ciberataques, nuevos vectores de amenazas, las nuevas vulnerabilidades, riesgos materializados, protección de la infraestructura tecnológica; algunos de estos grupos son:

- NIST: National Institute of Standards and Technology
- CSIRT - Equipo de Respuesta a Incidentes de Seguridad Informática de la Policía Nacional
- ISACA - Asociación de Control y Auditoria de Sistemas de Información.
- OWASP - Open Web Application Security Project
- Ciberseguridad LATAM: Canal de Noticias de CiberSeguridad
- Grupo de CIO MINTIC Colombia
- Grupos de Interés en Seguridad Colombia vía WhatsApp

Índice de Tablas

Índice de Ilustraciones