Gobernación del Archipiélago
de San Andrés, Providencia y Santa Catalina

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

SECRETARIA DE LAS TICS

CONTENIDO

1. INTRODUCCIÓN

La Gobernación del Departamento Archipiélago de San Andrés, Providencia y Santa Catalina, en cumplimiento de los lineamientos establecidos por el **Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC)**, adopta el presente **Plan Estratégico de Seguridad y Privacidad de la Información (PESI)** como el instrumento rector para la protección de sus activos de información durante el periodo constitucional **2026**. Este documento se fundamenta en el **Modelo de Seguridad y Privacidad de la Información (MSPI)** Versión 4.0, el cual actúa como el habilitador transversal de la **Política de Gobierno Digital**.

En la actualidad, las entidades públicas se enfrentan a un entorno digital caracterizado por una exposición creciente a incidentes de seguridad digital, los cuales pueden comprometer la continuidad operativa y la prestación de servicios esenciales a la ciudadanía. Reconociendo esta realidad, la Gobernación formaliza su **Sistema de Gestión de Seguridad de la Información (SGSI)** y su estrategia de seguridad digital bajo un ciclo de mejora continua **PHVA** (Planear, Hacer, Verificar y Actuar), garantizando la gestión eficaz de los riesgos y la protección de la privacidad de los datos.

La visión estratégica de la entidad para este cuatrienio se centra en la transformación del territorio hacia un modelo de **"Territorio Inteligente y Seguro".** En este contexto, la seguridad de la información trasciende los controles perimetrales de la infraestructura interna donde la Gobernación ya posee una fortaleza técnica con un puntaje de **88.8** en la Política de Seguridad Digital del **FURAG** para evolucionar hacia una seguridad territorial integral.

Esta evolución implica el despliegue y aseguramiento de **infraestructura crítica** que incluye un **Data Center** modernizado de alta disponibilidad, una red de **Internet de las Cosas (IoT)** con 158 dispositivos (cámaras de reconocimiento facial, matriculas y sensores), sistemas de **aerovigilancia táctica** mediante drones y servicios de conectividad para 1.500 hogares vulnerables.

Mediante la ejecución técnica de este plan, la Gobernación busca consolidar la confianza en el entorno digital, garantizando la **confidencialidad, integridad y disponibilidad** de la información pública y privada, y asegurando que cada inversión en tecnologías de la información se traduzca en valor público y bienestar social para el Archipiélago.

2. DEFINICIONES

Para la correcta interpretación y ejecución del presente **PESI**, se establecen las siguientes definiciones técnicas basadas en los estándares internacionales (**ISO/IEC 27000**) y el marco normativo de **Gobierno Digital**:

2.1 Conceptos Fundamentales de Seguridad

- **Activo de Información:** Cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas, etc.) que tenga valor para la entidad.

- **Ciberseguridad:** Protección de activos de información mediante el tratamiento de las amenazas que ponen en riesgo la información procesada, almacenada y transportada por sistemas interconectados.

- **Confidencialidad:** Propiedad de la información que garantiza que esta no sea revelada ni esté disponible para individuos, procesos o entidades no autorizadas.

- **Disponibilidad:** Propiedad de la información de ser accesible y utilizable por solicitud de una persona, entidad o proceso autorizado cuando así lo requiera.

- **Integridad:** Propiedad que asegura la exactitud y completitud de la información y sus métodos de procesamiento desde su creación hasta su destrucción.

- **Riesgo:** Posibilidad de que una amenaza concreta explote una vulnerabilidad para causar una pérdida o daño en un activo de información. Se considera una combinación de la probabilidad de un evento y sus consecuencias.

- **Seguridad de la Información:** Preservación de la confidencialidad, integridad y disponibilidad de la información en cualquier medio (impreso o digital).

- **Seguridad Digital:** Preservación de los tres principios de seguridad aplicados específicamente a la información que se encuentra en medios digitales.

- **Vulnerabilidad:** Debilidad de un activo o control que puede ser explotada por una o más amenazas.

2.2 Conceptos de Infraestructura y Operación (Smart Island)

- **Aerovigilancia:** Uso de sistemas aéreos no tripulados (drones) equipados con sensores para el monitoreo y control de áreas geográficas, apoyando labores de seguridad y gestión de riesgos.
- **Alta Disponibilidad:** Característica de un sistema que asegura la continuidad operacional absoluta, minimizando tiempos de inactividad mediante redundancia de componentes.
- **Cluster:** Conjunto de servidores conectados que trabajan como una sola unidad para mejorar el rendimiento y la disponibilidad de servicios críticos.
- **Failover (Conmutación por error):** Modo de respaldo donde las funciones de un sistema principal son asumidas por componentes secundarios ante una indisponibilidad del primero.
- **IoT (Internet of Things):** Interconexión digital de objetos cotidianos (cámaras, sensores, altavoces) con internet, permitiendo el intercambio de datos para monitoreo y toma de decisiones.
- **Territorio Inteligente:** Territorio que utiliza las TIC para mejorar la calidad de vida, la eficiencia de los servicios urbanos y la competitividad mediante la gestión inteligente de datos.
- **Trazabilidad:** Cualidad que permite asociar de modo inequívoco todas las acciones realizadas sobre la información o un sistema a un individuo o entidad específica.

2.3 Conceptos Legales y de Privacidad

- **Datos Personales:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.
- **Información Pública Clasificada:** Información en poder de un sujeto obligado que pertenece al ámbito privado o semiprivado de una persona, cuyo acceso puede ser negado por ley.
- **Información Pública Reservada:** Información exceptuada de acceso a la ciudadanía para evitar daños a intereses públicos legítimos, según los requisitos legales.
- **Tratamiento de Datos Personales:** Cualquier operación realizada sobre datos personales, tales como recolección, almacenamiento, uso o supresión.

3. OBJETIVO

Establecer la hoja de ruta estratégica y técnica para la implementación, operación y mejora continua del **Sistema de Gestión de Seguridad de la Información (SGSI)** de la Gobernación del Archipiélago de San Andrés, Providencia y Santa Catalina, con el fin de proteger los activos de información institucionales y ciudadanos contra amenazas internas y externas, garantizando la resiliencia operativa y el cumplimiento legal en la transición hacia un modelo de Territorio Inteligente.

3.1 OBJETIVOS ESPECÍFICOS

Para dar cumplimiento al objetivo general, se definen los siguientes objetivos técnicos y estratégicos:

- **Institucionalizar la Gobernanza de Seguridad:** Fortalecer la estructura organizacional del SGSI, asegurando que las decisiones de seguridad digital estén alineadas con el **Comité Institucional de Gestión y Desempeño** y cuenten con el respaldo presupuestal necesario para la protección de la infraestructura crítica.
- **Gestionar el Riesgo Digital con Enfoque Territorial:** Implementar una metodología de gestión de riesgos (basada en ISO 31000 y Magerit) que permita identificar y mitigar las vulnerabilidades asociadas a los nuevos activos de Tecnoligas de la información y las comunicaciones, incluyendo la red de 158 dispositivos IoT, sistemas de videovigilancia y drones de aerovigilancia.
- **Asegurar la Disponibilidad y Continuidad del Negocio:** Desplegar una arquitectura de **Alta Disponibilidad** en el Data Center institucional, garantizando un tiempo de actividad superior al 99.9% para los servicios críticos y los 38 trámites digitalizados, incluso ante desastres naturales o incidentes cibernéticos.
- **Garantizar la Privacidad y Protección de Datos Personales:** Aplicar los controles técnicos y administrativos requeridos por la **Ley 1581 de 2012**, especialmente en el tratamiento de datos biométricos captados por la infraestructura de Smart City y la información recolectada en los 3 Hubs de Innovación.
- **Fomentar la Cultura de Seguridad Digital:** Desarrollar un programa de sensibilización y formación técnica que alcance al 100% de los funcionarios y

contratistas, y que promueva el uso seguro de las TIC entre los **9.000 ciudadanos** impactados por los proyectos de conectividad y transformación digital.

- **Cumplir con los Estándares de Gobierno Digital:** Elevar y mantener el desempeño de la entidad en el índice de **FURAG** (Política de Seguridad Digital), cerrando las brechas actuales en los componentes de innovación y servicios ciudadanos digitales mediante controles de seguridad por diseño y por defecto.

4. ALCANCE

El alcance del presente **PESI** define los límites y la aplicabilidad del **Sistema de Gestión de Seguridad de la Información (SGSI)** de la Gobernación del Archipiélago. Este marco asegura que los controles de seguridad y privacidad se apliquen de manera integral a todos los activos que soportan la operación institucional y la estrategia de **Territorio Inteligente**.

4.1 Alcance sobre Procesos Institucionales

El SGSI es transversal y aplica al 100% de los procesos definidos en el Mapa de Procesos institucional:

- **Procesos Estratégicos:** Direccionamiento Estratégico, Gestión de Comunicaciones y Planeación Territorial.
- **Procesos Misionales:** Gestión de Salud, Educación, Turismo, Agricultura y Pesca, y de manera crítica, la **Gestión de Seguridad y Convivencia Ciudadana** (que opera los sistemas de vigilancia).
- **Procesos de Apoyo:** Gestión de TIC, Gestión Jurídica, Gestión Financiera, Gestión de Talento Humano y Gestión Documental.
- **Procesos de Evaluación:** Control Interno y Control Disciplinario.

4.2 Alcance sobre Activos de Información

La protección se extiende a las siguientes categorías de activos críticos identificados en el inventario institucional:

- **Información y Datos:** Bases de datos de ciudadanos (bases de salud), registros financieros (SIIF o equivalente territorial), expedientes administrativos y toda la información clasificada y reservada de la Gobernación.
- **Software y Aplicaciones:** Sede Electrónica, sistema de gestión documental, ERP financiero, y las nuevas plataformas de analítica de video y el **Sistema de Información Territorial (SIT)**.
- **Infraestructura Tecnológica (Hardware):** Servidores en clúster del Data Center principal, sistemas de almacenamiento (SAN), equipos de networking (Switches, Firewalls, WAF).
- **Infraestructura Crítica IoT y Territorio:** Los **158 nodos sensores** que incluyen 63 cámaras PTZ, 35 cámaras LPR (reconocimiento de placas), 60 altavoces IP, y las unidades de **aerovigilancia (drones)** con sus estaciones de control.
- **Recurso Humano:** Todos los servidores públicos, contratistas y terceros que tengan acceso a los activos de información o traten datos personales a nombre de la entidad.

4.3 Alcance sobre Partes Interesadas

El PESI regula las interacciones de seguridad con:

- **Ciudadanos y Usuarios:** Residentes del Archipiélago, turistas y beneficiarios de los proyectos de conectividad social (1.500 hogares).
- **Entidades de Gobierno y Control:** MinTIC, Agencia Nacional del Espectro (ANE), Ministerio de Defensa (para operación del SIES), Procuraduría y Contraloría.
- **Proveedores y Terceros:** Operadores de servicios de conectividad, empresas de mantenimiento de hardware, desarrolladores de software y proveedores de servicios en la nube.

4.4 Alcance Geográfico y Lógico

- **Alcance Geográfico:**
    - Sedes administrativas de la Gobernación en San Andrés (Coral Palace) y Providencia.
    - Los **3 Hubs de Innovación** (Laboratorios de CTeI).

- Los puntos físicos de las 63 Zonas Wifi públicas y los nodos de videovigilancia distribuidos en el territorio insular.

- **Alcance Lógico:**
  - **Red Administrativa:** Tráfico de datos interno de las secretarías y dependencias.
  - **Red de Seguridad Ciudadana (SIES):** Segmento de red dedicado exclusivamente a la transmisión de video y datos de seguridad pública.
  - **Servicios Ciudadanos:** La capa lógica de la Sede Electrónica y los canales digitales de atención.
  - **Acceso Remoto:** Conexiones mediante VPN para teletrabajo y soporte de proveedores autorizados.

5. DOCUMENTOS DE REFERENCIA

El presente Plan Estratégico se fundamenta en un marco normativo y técnico sólido que garantiza la legalidad y la calidad de los controles implementados. Esta estructura jerárquica asegura que las acciones de seguridad digital estén alineadas con los mandatos nacionales y las necesidades específicas del Archipiélago.

5.1 Marco Legal y Normativo Nacional

La Gobernación da cumplimiento a las leyes y decretos que rigen la seguridad de la información y la protección de datos en el Estado colombiano:

- **Ley 1581 de 2012:** Ley General de Protección de Datos Personales, la cual dicta las disposiciones para el tratamiento de datos de ciudadanos, incluyendo datos biométricos captados por sistemas de vigilancia.
- **Ley 1273 de 2009:** Ley de Delitos Informáticos, que define los tipos penales relacionados con el acceso abusivo a sistemas, interceptación de datos y daño informático.

- **Ley 1712 de 2014:** Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional.
- **Decreto 1078 de 2015:** Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, que establece los lineamientos de la Política de Gobierno Digital.
- **Decreto 620 de 2020:** Establece los lineamientos generales en el uso y operación de los servicios ciudadanos digitales.
- **Resolución 500 de 2021 (MinTIC):** Por la cual se establecen los lineamientos y estándares para el uso de la seguridad y privacidad de la información.

5.2 Marco Técnico y Estándares

Para la implementación técnica de los controles, la entidad adopta los siguientes marcos de referencia internacionales:

- **ISO/IEC 27001:2022:** Estándar internacional para los Sistemas de Gestión de Seguridad de la Información (SGSI).
- **ISO/IEC 27002:2022:** Guía de buenas prácticas para los controles de seguridad de la información.
- **Modelo de Seguridad y Privacidad de la Información (MSPI) V 4.0 de MinTIC:** Adaptación nacional de la ISO 27001 para el sector público colombiano.
- **NIST Cybersecurity Framework (CSF):** Marco de referencia para mejorar la ciberseguridad de infraestructuras críticas, aplicado especialmente a la red IoT y Smart Island.
- **Metodología MAGERIT v3:** Metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica (España), recomendada por MinTIC.
- **ISO 31000:2018:** Directrices para la gestión de riesgos corporativos.

5.3 Marco Institucional

Documentos internos que dan contexto y operatividad al sistema dentro de la entidad:

- **Plan de Desarrollo Departamental "El Archipiélago Avanza":** Mandato estratégico que prioriza la transformación digital y la seguridad ciudadana.
- **Plan Estratégico de Tecnologías de la Información (PETI) 2024-2027:** Documento que integra la visión de Smart Island y los proyectos de inversión tecnológica.
- **Política General de Seguridad de la Información V1 (2026):** Documento de alto nivel que establece las directrices de seguridad de la Gobernación.
- **Manual de Políticas de Seguridad de la Información V1 (2026):** Guía detallada de controles operativos y administrativos para funcionarios y terceros.
- **Plan de Continuidad del Negocio (BCP) y Recuperación ante Desastres (DRP):** (En proceso de actualización para el contexto de Smart Island).

6. ESTADO ACTUAL DE LA ENTIDAD RESPECTO AL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

El diagnóstico de la situación actual de la Gobernación del Archipiélago revela una gestión de TI con una madurez asimétrica: una sólida fortaleza en la protección de activos internos contrastada con brechas críticas en la entrega de servicios digitales innovadores. Este análisis es fundamental para orientar los controles del MSPI hacia la nueva realidad del territorio.

6.1. Análisis de Resultados FURAG (Habilitador de Seguridad)

De acuerdo con el reporte oficial del Formulario Único de Reporte de Avances de la Gestión (FURAG) 2024, el estado de la seguridad digital se resume en los siguientes indicadores:

- **Política de Seguridad Digital:** La entidad presenta un puntaje sobresaliente de **88.8**, lo que indica un nivel de madurez "Gestionado" o "Consolidado". Esto demuestra que la Gobernación posee controles efectivos para la ciberseguridad y la protección de su infraestructura interna actual.

- **Componente de Seguridad y Privacidad (dentro de POL07):** Este subcomponente alcanzó los **84.6 puntos**, ratificando la robustez de los mecanismos de protección de la información institucional.
- **Contraste con Gobierno Digital:** Mientras la seguridad es una fortaleza, el Índice de Gobierno Digital general es de **55.7**, afectado por puntajes de **0.0** en Innovación Pública Digital y Servicios Ciudadanos Digitales.

6.2. Brechas Técnicas y Normativas (MSPI vs. Realidad)

A pesar de los altos puntajes en seguridad, el diagnóstico identifica vacíos técnicos que representan un riesgo para los nuevos proyectos de inversión:

- **Obsolescencia Tecnológica:** El parque computacional presenta una obsolescencia marcada, con equipos que superan los **5 años de antigüedad**, lo que dificulta la implementación de agentes de seguridad modernos y actualizaciones de parches críticos.
- **Capacidad de Procesamiento:** La infraestructura actual del Data Center es limitada para soportar las nuevas cargas de trabajo que exigen los proyectos del Sistema General de Regalías (SGR), específicamente para el almacenamiento masivo y análisis de video.
- **Seguridad de Infraestructura Crítica Territorial:** Los controles actuales están diseñados para un entorno de "oficina". Existe una brecha en la definición de protocolos de seguridad para la red de **Internet de las Cosas (IoT)**, que incluye 158 dispositivos distribuidos en el territorio (cámaras LPR, reconocimiento facial y drones).
- **Continuidad y Resiliencia:** Se identifica la falta de un Plan de Continuidad del Negocio (BCP) y Recuperación ante Desastres (DRP) formalizado y probado, lo cual es crítico dada la alta exposición del archipiélago a riesgos climáticos como huracanes.

6.3. Conclusión del Diagnóstico

La Gobernación se define actualmente como una entidad **"segura pero ineficiente"** en su relación con el ciudadano. El desafío del presente PESI no es corregir fallos estructurales en la ciberseguridad existente, sino **evolucionar el SGSI de un enfoque perimetral interno a uno de seguridad territorial inteligente**.

Se debe aprovechar la madurez de 88.8 puntos para habilitar de forma confiable los servicios digitales y la infraestructura crítica de **Smart Island**, garantizando que la innovación no comprometa la privacidad ni la integridad de los datos de los habitantes del Archipiélago.

7. ESTRATEGIA DE SEGURIDAD DIGITAL: FORTALECIMIENTO DEL MODELO MSPI

La estrategia de la Gobernación del Archipiélago para el periodo 2026 se centra en la **consolidación y evolución del Modelo de Seguridad y Privacidad de la Información (MSPI)**. El objetivo primordial es transformar los controles aislados en un ecosistema de gestión robusto, capaz de proteger la infraestructura de **Smart Island** y elevar el desempeño institucional en el marco del ciclo de mejora continua **PHVA**.

Esta estrategia no se limita a la adquisición de tecnología; busca el fortalecimiento institucional a través de la estandarización de procesos, la gestión proactiva de riesgos territoriales y la garantía de la privacidad por diseño en cada servicio ciudadano.

7.1. DESCRIPCIÓN DE LAS ESTRATEGIAS ESPECÍFICAS (EJES DE FORTALECIMIENTO)

A continuación, se describen los ejes diseñados para fortalecer la postura defensiva de la entidad, alineando la operación técnica con los dominios de la norma **NTC-ISO/IEC 27001** y las guías de **MinTIC**:

ESTRATEGIA / EJE	**ENFOQUE DE FORTALECIMIENTO DEL MODELO**
1. Gobernanza y Liderazgo del SGSI	Fortalecer la toma de decisiones estratégicas mediante la integración del **CISO** en el Comité Institucional de Gestión y Desempeño. El objetivo es asegurar que la seguridad digital sea un requisito transversal en la planeación de la entidad, garantizando recursos y el cumplimiento del marco normativo (Políticas v.2026).

ESTRATEGIA / EJE	ENFOQUE DE FORTALECIMIENTO DEL MODELO
2. Gestión Dinámica de Riesgos Digitales	Evolucionar de una matriz de riesgos estática a un proceso de gestión de riesgos en tiempo real. Se fortalecerá la capacidad de identificar y valorar amenazas específicas de **infraestructura crítica IoT**, drones y servicios en la nube, definiendo planes de tratamiento proporcionales al impacto territorial.
3. Operación y Blindaje de Infraestructura	Institucionalizar la práctica de "Hardening" o endurecimiento de sistemas. Se implementarán controles técnicos de nivel avanzado (Alta Disponibilidad, WAF, IPS) para blindar los activos que soportan los **38 trámites digitales** y el Sistema de Información Territorial, asegurando la integridad de los datos ciudadanos.
4. Resiliencia, Monitoreo y Mejora Continua	Consolidar la capacidad de detección y respuesta ante incidentes mediante la formalización de un ciclo de vida de respuesta organizado. Se fortalecerá el modelo a través de **Hacking Ético** periódico y auditorías internas que permitan retroalimentar el sistema y garantizar la mejora continua.
5. Cultura de Seguridad y Privacidad	Fortalecer el factor humano como la línea de defensa principal. El modelo se fortalecerá mediante un Plan de Apropiación diferenciado para funcionarios y ciudadanos, asegurando que la privacidad de datos (Ley 1581) sea un valor intrínseco en la cultura organizacional del Archipiélago.

7.2. PORTAFOLIO DE ACTIVIDADES PARA EL FORTALECIMIENTO DEL MSPI

Para materializar el fortalecimiento del modelo, se definen las siguientes actividades clave, las cuales responden directamente a las brechas identificadas en el diagnóstico FURAG y a los requisitos de excelencia técnica:

EJE DE MODELO	PROYECTO / ACTIVIDAD DE FORTALECIMIENTO	PRODUCTOS O ENTREGABLES ESPERADOS
Gobernanza	**F1. Institucionalización del Rol y Normativa**	1. Estructura de Roles y Responsabilidades formalizada. 2. Política General y Manual de Políticas socializados al 100% de la entidad. 3. Tablero de control de indicadores de cumplimiento MSPI.
Riesgos	**F2. Ciclo de Gestión de Riesgos loT y CTeI**	1. Inventario de Activos de Información territoriales valorado. 2. Matriz de Riesgos actualizada con escenarios de ciberamenazas y desastres naturales. 3. Plan de Tratamiento de Riesgos ejecutado y monitoreado.
Operación	**F3. Despliegue de Controles Técnicos de Alta Disponibilidad**	1. Infraestructura de clúster y failover configurada y probada. 2. Configuración de seguridad (Hardening) en servidores y dispositivos loT. 3. Implementación de certificados SSL y protección perimetral activa.
Resiliencia	**F4. Sistema de Respuesta y Mejora**	1. Procedimiento de Gestión de Incidentes de Seguridad Digital operando.

EJE DE MODELO	PROYECTO / ACTIVIDAD DE FORTALECIMIENTO	PRODUCTOS O ENTREGABLES ESPERADOS
		2. Informe de hallazgos de Ethical Hacking y plan de remediación. 3. Plan de Continuidad del Negocio (BCP/DRP) actualizado y probado.
Cultura	**F5. Programa de Apropiación "Confianza Digital"**	1. Plan de capacitación ejecutado (funcionarios y Ciudadanía). 2. Políticas de tratamiento de datos biométricos aplicadas en Smart Island. 3. Reporte de reducción de incidentes por error humano (Ingeniería Social).

7.3. CRONOGRAMA DE ACTIVIDADES / PROYECTOS

El Responsable de Seguridad de la Información (CISO), con base en los ejes de fortalecimiento definidos, establece el siguiente cronograma de ejecución. Este plan asegura que la seguridad sea un habilitador de la transformación digital, protegiendo los activos críticos desde la fase de diagnóstico hasta la mejora continua.

Vigencia: 2026

PERIODO	EJE / FASE	ACTIVIDAD / PROYECTO	RESPONSABLE	FECHA LÍMITE / DURACIÓN
TRIMESTRE 1 (Ene - Mar)	**Diagnóstico**	**1. Autodiagnóstico MSPI Territorial:** Valoración del estado de seguridad post-implementación de nodos IoT, utilizando el instrumento oficial de MinTIC.	Líder TIC / CISO	20/02/2026
	Diagnóstico	**2. Análisis de Vulnerabilidades (Red IoT/SIES):** Escaneos técnicos a la red de videovigilancia, drones y Sede Electrónica para identificar brechas de seguridad.	Especialista Seguridad	20/02/2026
	Planeación	**3. Actualización Normativa (Políticas 2026):** Socialización y ajuste final de la Política General y Manuales para alinearlos con la realidad de Smart Island.	Líder TIC / CISO	20/03/2026

PERIODO	EJE / FASE	ACTIVIDAD / PROYECTO	RESPONSABLE	FECHA LÍMITE / DURACIÓN
TRIMESTRE 2 (Abr - Jun)	**Planeación**	**4. Gestión de Activos Críticos:** Actualización del inventario, incluyendo dispositivos IoT y activos de información de los 38 trámites digitales.	Líder TIC / CISO	20/04/2026
	Planeación	**5. Gestión de Riesgos de Resiliencia:** Actualización de la matriz de riesgos ante ciberamenazas y fenómenos climáticos (Plan de Tratamiento).	Líder TIC / CISO	20/05/2026
	Cultura	**6. Plan "Archipiélago Seguro":** Diseño y aprobación del plan de capacitación en seguridad digital (en español y creole) para funcionarios y ciudadanía.	CISO / Comunicaciones	20/05/2026
	Controles	**7. Diagnóstico e Ingeniería IPv6:** Elaboración del plan técnico para la	Líder TIC	20/06/2026

PERIODO	EJE / FASE	ACTIVIDAD / PROYECTO	RESPONSABLE	FECHA LÍMITE / DURACIÓN
		transición de la infraestructura institucional hacia el protocolo IPv6.		
TRIMESTRE 3 (Jul - Sep)	**Implementación**	**8. Despliegue de Controles de Blindaje:** Ejecución del plan de tratamiento (Cifrado de nodos IoT, Hardening de servidores y WAF).	CISO	20/07/2026
	Controles	**9. Ejecución de Transición IPv6:** Implementación técnica del protocolo IPv6 en los servicios digitales y red administrativa.	Líder TIC	20/08/2026
	Medición	**10. Indicadores de Eficacia (KPI/KRI):** Primera medición del desempeño del SGSI frente a los objetivos estratégicos y nivel de madurez FURAG.	CISO / Planeación	20/08/2026

PERIODO	EJE / FASE	ACTIVIDAD / PROYECTO	RESPONSABLE	FECHA LÍMITE / DURACIÓN
	Evaluación	**11. Auditoría Interna MSPI:** Ejecución del plan de revisión anual de cumplimiento de controles para preparar el reporte FURAG.	Control Interno	20/09/2026
TRIMESTRE 4 (Oct - Dic)	**Mejora**	**12. Plan de Mejora Continua:** Diseño de acciones correctivas basadas en hallazgos de auditoría y resultados de pruebas de Ethical Hacking.	Líder TIC / CISO	20/11/2026
	Cierre	**13. Revisión por la Alta Dirección:** Presentación de resultados al Gobernador y Comité de Gestión para el cierre de la vigencia.	Gobernador / CISO	Diciembre 2026

8. APROBACIÓN

El presente Plan Estratégico de Seguridad y Privacidad de la Información (PESI) 2026, en su versión actualizada para la vigencia 2026, ha sido estructurado bajo los lineamientos del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) y los estándares internacionales ISO/IEC 27001:2022 e ISO 27035.

La Alta Dirección de la Gobernación del Archipiélago de San Andrés, Providencia y Santa Catalina, a través del Comité Institucional de Gestión y Desempeño, manifiesta su compromiso formal con la implementación de los controles aquí descritos, garantizando la asignación de los recursos financieros, técnicos y humanos necesarios para proteger la infraestructura crítica del territorio y asegurar la confianza digital de la ciudadanía.

REGISTRO DE APROBACIÓN		
ELABORÓ	**REVISÓ**	**APROBÓ**
Nombre: Contratista	**Nombre:** Comité de Gestión y Desempeño	**Nombre:** (Gobernador)
Cargo: Contratista - Oficial de Seguridad Digital	**Cargo:** presidente del Comité	**Cargo:** Gobernador
Fecha: 19-01-2026	**Fecha:** 19-01-2026	**Fecha:** 19-01-2026

CONTROL DE CAMBIOS

VERSIÓN	FECHA VIGENCIA	NATURALEZA DEL CAMBIO
01	19-01-2026	Construcción del PESI alineado a la Resolución 02277 de 2025, ISO 27001 de 2022 y resultados FURAG.