PROYECTA
EMPRESA PARA EL DESARROLLO TERRITORIAL

GOBIERNO DEL QUINDÍO

PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (PESPI)

EMPRESA PARA EL DESARROLLO TERRITORIAL

PROYECTA

2026

1. Introducción y Alcance

En la era de la transformación digital, la **Empresa para el Desarrollo Territorial - PROYECTA** reconoce que la información es uno de sus activos más críticos para el cumplimiento de su misión en la ejecución de proyectos de infraestructura y vivienda. El presente **Plan Estratégico de Seguridad y Privacidad de la Información (PESPI)** para la vigencia 2026, se constituye como la hoja de ruta para garantizar la protección de este activo frente a un entorno de amenazas cibernéticas cada vez más sofisticadas.

Este plan no es solo un documento de cumplimiento normativo, sino una herramienta de gestión de riesgos que busca:

- **Asegurar la confianza ciudadana:** Garantizando que los datos personales tratados por la entidad estén protegidos bajo los más altos estándares de la Ley 1581 de 2012.
- **Garantizar la continuidad del negocio:** Estableciendo controles para que los servicios digitales, como el portal institucional y los sistemas financieros (Publifinanzas), operen sin interrupciones.
- **Fomentar la resiliencia:** Preparando a la entidad para detectar, responder y recuperarse de incidentes de seguridad de manera oportuna.

El PESPI 2026 se integra transversalmente con el **Modelo Integrado de Planeación y Gestión (MIPG)** y se fundamenta en la **Resolución 2239 de 2024 del MinTIC**, adoptando un enfoque basado en riesgos para la toma de decisiones tecnológicas.

Este plan define las directrices para proteger los activos de información de PROYECTA contra amenazas internas y externas.

ALCANCE

El alcance del PESPI de **PROYECTA** para el periodo 2026 es integral y cubre todas las dimensiones de la operación institucional:

Alcance Organizacional

Aplica a todos los procesos de la entidad, incluyendo la Dirección Administrativa y Financiera, las áreas operativas de proyectos y la oficina de control interno. Es de obligatorio cumplimiento para:

- Funcionarios públicos de planta.
- Contratistas y prestadores de servicios.
- Pasantes y terceros que tengan acceso a los activos de información de la empresa.

Alcance Tecnológico

El plan cubre la protección y gobernanza sobre los siguientes recursos físicos y lógicos identificados en el inventario institucional:

- **Infraestructura de Red:** Gestión segura de los Routers Mikrotik, switches corporativos Capa 2 y 4, y los 65 Access Points que conforman la red interna y las zonas Wi-Fi.
- **Dispositivos Finales:** Las 16 estaciones de trabajo principales y equipos portátiles utilizados para la gestión de proyectos.
- **Protocolos de Comunicación:** Aseguramiento de la continuidad de la operación en **Dual Stack (IPv4/IPv6)**, garantizando que el direccionamiento IP no genere brechas de seguridad.
- **Sistemas y Datos:** Protección de la información contenida en el portal proyecta.gov.co, bases de datos de contratistas, y el software misional y financiero.

2. Marco Normativo Actualizado

Se basa en el cumplimiento de:

- **Ley 1581 de 2012:** Protección de Datos Personales.
- **Decreto 1078 de 2015:** Lineamientos de TI y Seguridad Digital.
- **Resolución 2239 de 2024 (MinTIC):** Nuevos estándares de seguridad digital.
- **Conpes 3995 de 2020:** Política nacional de confianza y seguridad digital.

3. Objetivos Estratégicos de Seguridad

1. **Garantizar la Tríada de la Información:** Asegurar la Confidencialidad, Integridad y Disponibilidad de los datos de proyectos de infraestructura.
2. **Cultura de Seguridad:** Capacitar al 100% del personal en prevención de ingeniería social y manejo de datos.
3. **Resiliencia Operativa:** Establecer mecanismos de respuesta ante incidentes (Ciberseguridad).

4. Diagnóstico de los Componentes del Plan (Basado en MSPI)

A. Gestión de Activos y Riesgos

- **Inventario:** Clasificar la información de los aplicativos, los existentes son

Publifinanzas
Página web
Ventanilla Única Virtual

- **Análisis de Riesgos:** Identificar amenazas sobre la infraestructura **IPv6** y los dispositivos de red para aplicar *Hardening* (endurecimiento de seguridad).

B. Control de Acceso y Gestión de Identidad

- Implementación de políticas de contraseñas seguras y doble factor de autenticación (MFA) donde sea técnicamente posible.
- Gestión de perfiles de usuario según el rol dentro de la entidad.

C. Seguridad Física y Perimetral

- **Red Segura:** Aprovechar la actualización de los **Switches Capa 2 y 4** para crear segmentación de redes (VLANs) que aíslen el tráfico administrativo del tráfico público (Zonas Wi-Fi).

- **Protección Endpoint:** Mantener la vigencia y **actualización** de las licencias de **Kaspersky** en todos los terminales.

D. Privacidad de la Información (Ley 1581)

- Actualización del Registro en el sistema de datos abiertos(en proceso con registro pero sin documentos aprobados)

- Inclusión de cláusulas de confidencialidad en todos los contratos de prestación de servicios.

- Implementación del aviso de privacidad y políticas de tratamiento de datos en el portal proyecta.gov.co.

5. Hoja de Ruta de Proyectos 2026

Proyecto	Acción Específica	Meta 2026
Backup y Recuperación	Configurar esquemas de respaldo local y en nube para información crítica.	100% de datos críticos con respaldo mensual. Con almacenamiento en Nube o Storage
Seguridad en IPv6	Configurar filtros y listas de control de acceso (ACL) específicos para el nuevo protocolo.	Protocolo IPv6 operando de forma segura.
Monitoreo de Eventos	Uso del servicio **NTP** para sincronizar logs y detectar intentos de intrusión.	Logs centralizados y sincronizados.
Cero Papel Seguro	Digitalización de archivos bajo estándares de integridad (firmas digitales).	Reducción de riesgos de pérdida física de documentos.

6. Responsables

- **Gestión Administrativa y Gerencia:** Liderar la asignación de recursos.
- **Gestión Administrativa y área de sistemas:** Ejecución técnica y monitoreo de riesgos.
- **Control Interno:** Verificación y cumplimiento de políticas.

LINA MARCELA ROLDAN PRIETO
GERENTE GENERAL
ENERO 29 DE 2026