TECNOLOGÍA DE LA INFORMACIÓN

Gobernanza esencial de TI v1.0

DOCUMENTO PÚBLICO

ÍNDICE

Control documental

Esta sección define los controles para este documento; Te permite llevar un control de los controles a lo largo del tiempo y asegurarte de que son oficialmente oficiales.

1. APROBACIÓN

VERSIÓN	ACCIÓN	TÍTULO	Nombre	FIRMA
V1.0	Preparado y aprobado por:	Director de Información CIO	HAIDAR Ibrahim	

Versión

VERSIÓN DEL DOCUMENTO	FECHA	DESCRIPCIÓN	MODIFICADO POR
V1.0	Mayo de 2026	Documento inicial	ARIAS Diego Fernando

Contacto

Título	CONTACTO	Firma	Correo electrónico
Director de Información (CIO)	HAIDAR Ibrahim		ihaidar@puerto-antioquia.com
Responsable de Operaciones de TI	ARIAS Diego Fernando	Diego arias	darias@puerto-antiqouia.com
Gestor de Aplicaciones TI	SEQUERA Juan Pablo		Jsequera@puerto-antioquia.com

Distribución

Público	Se puede compartir una copia públicamente

2. INTRODUCCIÓN

Este documento debe proporcionar un marco público que se origina a partir del documento interno (CONFIDENCIAL) de Gobernanza Esencial de TI. Ilustra las directrices para gestionar los activos tecnológicos de PBCU a un nivel general, para evitar exponer el marco, ya que este documento está destinado a publicarse externamente.

Aunque este documento refleja una visión general de la gobernanza interna de CONFIDENTIAL, sigue resumiendo el acuerdo entre empresa y tecnología sobre las prácticas para, ejecutar y mantener activos de TI a lo largo de su ciclo de vida.

3. OBJETIVOS

Alinear negocio y TI para que los servicios apoyen los objetivos empresariales; formula la gobernanza de TI (digital y documental) e implementa un ISMS eficaz; proteger activos de información (confidencialidad, integridad y disponibilidad — CIA); identificar, evaluar y mitigar los riesgos de TI y ciberseguridad de forma continua; garantizar el cumplimiento legal, regulatorio y contractual; control de acceso bajo RBAC; Promover la concienciación, la cultura de notificación de incidentes y la mejora continua mediante auditorías.

4. ÁMBITO DE TRABAJO (LÍMITES)

Siete grandes áreas conforman la gobernanza esencial de TI de PBCU:

Dispositivos	Instalación, entrega, recuperación, sustitución y soporte BYOD de todo el equipo tecnológico.
Acceso	Control físico y digital: redes, aplicaciones, MFA, RBAC, SSO, BYOD, periféricos y acceso web.
Correo	Creación, acceso, buzones compartidos, reenvío y terminación/retención de cuentas institucionales.
Ciberseguridad	Formación anual, campañas de phishing, SOC 24/7, ejercicios de mesa y gestión de incidentes.
Datos	Clasificación (4 niveles), copias de seguridad, restauración, protección y confidencialidad.
Riesgo	Categorización, mitigación, evaluación semestral y registro de riesgos.
Incidente	Registro 24/7 en tres niveles (S1, S2, S3) y activación de SLA con proveedores.
Continuidad del negocio	Alta disponibilidad, redundancia, soporte y sustitución de dispositivos críticos.
Cumplimiento	Auditorías rutinarias, escalada disciplinaria y responsabilidad de cada líder.

5. GESTIÓN DE DISPOSITIVOS INFORMÁTICOS

Configuración: TI preconfigura todos los dispositivos antes de la entrega — unión al dominio, endurecimiento, ajustes básicos (idioma, región, zona horaria, nombre), solo software autorizado, antivirus, cortafuegos, MFA, último sistema operativo parcheado y borrado/bloqueo en caso de robo o pérdida. Los procesos de incorporación, transferencia y salida están integrados.

Reemplazo de dispositivos:

Hasta que falla	Se reemplaza en caso de fallo. Se aplica la regla del porcentaje de repuestos o garantía del proveedor.
Condicional	Cuando el rendimiento dificulta las tareas diarias o el dispositivo está obsoleto. Evaluado por IT.
Excepcional	Requiere la aprobación del CEO. Necesidades empresariales específicas no planificadas.

---

6. GESTIÓN DE ACCESOS

Acceso físico: restringido al personal de Infraestructura de TI autorizado por el CIO; las visitas externas requieren la aprobación previa del CIO, deben ser registradas y acompañadas.
Acceso digital y red: Redes terminales solo para dispositivos y usuarios registrados; Wi-Fi aislado para invitados, acceso temporal por solicitud formal; Solo terceros mediante pasarela segura (monitorizada y registrada) con MFA; BYOD limitado a internet, aislado de las redes PBCU; Periféricos USB restringidos.
Autenticación: MFA, SSO y biometría obligatoria en sistemas críticos – si es técnicamente factible; contraseñas complejas con expiración periódica; el acceso a aplicaciones se gestiona bajo RBAC.

7. GESTIÓN DE CORREOS ELECTRÓNICOS

Creación y normas de uso: solo para personal legalmente vinculado, formato de la primera letra de nombre + apellido (por ejemplo: darias@puerto-antioquia.com); cuentas genéricas o no activas prohibidas; el reenvío automático a terceros prohibido salvo que sea aprobado por el CIO; los buzones compartidos siguen una estructura predefinida; las cuentas de servicio son limitadas al mínimo y aprobadas solo por el CIO; el acceso está restringido geográficamente (principalmente Colombia) y por tipo de dispositivo. La terminación y retención de correos electrónicos siguen un proceso estricto y confidencial.

8. GESTIÓN DE LA CIBERSEGURIDAD

formación anual obligatoria en ciberseguridad para todos los usuarios con acceso a sistemas digitales; Publicaciones mensuales de sensibilización; TI ejecuta campañas rutinarias (phishing, ingeniería social, uso inseguro) y analiza las lecciones aprendidas. monitorización 24/7 de redes, sistemas y dispositivos con una matriz de escalado global; El marco NIST en 5 fases: Preparar, Detectar, Analizar, Remediar y Post-Incidente se considera como línea base.

9. GESTIÓN DE DATOS

Clasificación de datos:

Nivel 4	**Público**	Compartible públicamente. No hay daño en caso de revelación.
Nivel 3	**Interno**	Solo para uso interno. No hay impacto grave en caso de divulgación.
Nivel 2	**Confidencial**	Acceso restringido. La divulgación causa graves interrupciones a corto plazo.
Nivel 1	**Crítico / Top Confidencial**	Acceso muy restringido. La divulgación causa una grave interrupción con un impacto a largo plazo.

Copia de seguridad y protección: almacenada en medios seguros y cifrados; la restauración sigue un estricto proceso de validación para garantizar la integridad de los datos; se consideran múltiples medios, ubicaciones geográficas y tecnologías según la criticidad; NDA obligatorio para usuarios internos y externos; intercambiar con los proveedores solo a través de canales seguros bajo principios de necesidad y control.

10. GESTIÓN DE RIESGOS

Práctica continua. Los sistemas se categorizan según criterios de riesgo, objetivos de disponibilidad/confidencialidad, amenazas, mitigaciones y plausibilidad/impacto. Evaluación global dos veces al año con registro de riesgos.

---

11. GESTIÓN DE INCIDENTES

Las solicitudes deben registrarse (24/7) en tres niveles:

S1	**Línea del Frente 24/7**	Resolver problemas básicos para individuos. Tareas recurrentes.
S2	**Especialista de área**	Activado por T1. Conocimiento profundo de sistemas específicos. Investiga la causa raíz.
S3	**Alta Dirección de TI**	Problemas graves con un impacto directo en el negocio. Activa los SLA con los proveedores.

12. GOBERNANZA DE LA CONTINUIDAD DEL NEGOCIO

Alta disponibilidad evitando puntos únicos de fallo en componentes críticos (siempre que sea técnicamente factible o asequible). Clasificación de las solicitudes según los niveles de nivel. Sustitución y soporte de dispositivos.

13. CUMPLIMIENTO Y AUTORIDAD

Las auditorías rutinarias garantizan la eficiencia. El incumplimiento conlleva acciones internas por cada canal de escalada. Cada líder de equipo se asegura de que sus subordinados cumplan con este marco.
