I. OBJETIVOS

El presente Manual de Políticas tiene por objeto:

- Establecer un modelo de procesos que aborda los principales ciclos de gobierno, así como de control, relacionados con las Tecnologías y la Seguridad de la Información.

II. POLÍTICAS ESTABLECIDAS POR LA EMPRESA

N°	Descripción
RELATIVAS A GESTIONAR GOBIERNO TI	
1.	Es responsabilidad del Directorio y la Gerencia General definir la estructura organizativa de la unidad de tecnología informática y seguridad de la información, estableciendo sus roles, responsabilidades y la autoridad requerida para contribuir con el logro de la misión, las metas y objetivos de la organización.
2.	La evaluación del riesgo de la organización deberá estar alineada con la Política de Control Interno a modo de que el apetito y tolerancia al riesgo sean oportunamente identificados, evaluados y tratados apropiadamente.
3.	Las metas, métricas y acciones clave del desempeño de la unidad de tecnología, debe contar con la conformidad por parte de los interesados clave, para asegurar la transparencia en cuanto a la medición y elaboración de informes del área.
RELATIVAS A PLANIFICAR Y ORGANIZAR	
1.	El Marco de Gestión de TI, incluye el diseño e implementación del modelo organizacional, representado en el organigrama de la organización, que debe estar alineado con las necesidades de la Entidad, a fin de apoyar los objetivos de gobierno, alineados con las políticas corporativas.
2.	El plan estratégico de tecnología debe estar alineado a la misión, visión, valores, políticas y objetivos de la organización. Se podrán utilizar mecanismos de planeación estratégica para la comunicación y seguimiento de las actividades.
3.	La información que contienen los procesos debe ser integrada a las capacidades técnicas que deben ser estandarizadas en toda la empresa. Y deben ser incluidas en la arquitectura de tecnología.

4.	El presupuesto relacionado con las tecnologías de información, desde la priorización del gasto o de la inversión, debe establecerse mediante el uso de prácticas presupuestarias formales, hasta la registración y monitoreo de las mismas. El presupuesto debe estar aprobado por el Directorio.
5.	Los roles y responsabilidades del personal de la unidad de tecnología están descritas en sus respectivos manuales de funciones. Estos manuales deben ser comunicados al personal correspondiente y debe servir como base para la evaluación de desempeño de los mismos.
6.	Los niveles de servicios de TI deben estar alineados con las necesidades y expectativas de las distintas áreas de la organización, incluyendo la identificación, la especificación, el diseño, la publicación, el acuerdo y la supervisión de los niveles de servicio e indicadores de rendimiento
7.	Los servicios de tecnología de información que son prestados por los proveedores deben ser monitoreados, con la finalidad de satisfacer las necesidades del negocio, desde la selección del proveedor, la gestión de las relaciones, la gestión de los contratos, la revisión y supervisión del desempeño.
8.	El Sistema de Gestión de la Seguridad de la Información (SGSI), debe estar alineado con los procedimientos de control interno, identificando los riesgos relacionados con TI, con el objetivo de establecer acciones para resolver los riesgos dentro de los niveles de tolerancia establecidos por la organización.
RELATIVAS A ADQUIRIR E IMPLEMENTAR	
1.	Los proyectos, incluidos en el portafolio de proyectos, deben estar acordes con la estrategia de la organización. Los proyectos deben incluir actividades de análisis de viabilidad, planificación, ejecución, control de calidad, gestión de riegos para cerrarlos con una revisión post implementación.

2.	Para la adquisición o creación de soluciones (incluyendo aplicaciones, información/datos, infraestructura y servicios), requieren de un análisis de los requerimientos, para asegurar que estén en línea con las necesidades estratégicas de la organización. Se deben validar las opciones viables, incluyendo costos, análisis de riesgo, y aprobar los requerimientos, así como las soluciones propuestas. Debe contemplar el diseño, el desarrollo, la compra o contratación y asociación con proveedores o fabricantes, infraestructuras, así como los servicios de tecnología de la información.
3.	Las soluciones desarrolladas o adquiridas, para la implementación y hacerlas operativas, deben contar con la aceptación formal de los usuarios clave. Esta aceptación debe incluir la conformidad en cuanto a las pruebas, comunicación, capacitación, pase a producción y revisión de la post-implementación de la solución.
4.	Los cambios requeridos a las soluciones de TI (aplicaciones, servicios e infraestructura) deben contemplar las etapas de solicitud, el análisis de impacto, la priorización, la autorización, la ejecución, el cierre y el monitoreo o seguimiento y la documentación correspondiente.
5.	Se debe mantener un registro actualizado de los activos de tecnología, el cual permita individualizar, clasificar, valorizar claramente los mismos, y optimizar el valor de dichos activos. El registro debe contener datos del propietario del activo, costo, número identificación, ubicación, entre otros.
RELATIVAS A ENTREGAR SERVICIO Y DAR SOPORTE	
1.	Los procedimientos operativos para entregar los servicios de tecnología de información deben garantizar que las funciones de TI se ejecutan con normalidad, en forma ordenada y segura según lo planificado.
2.	Las solicitudes de los usuarios sobre incidentes o servicios deben ser registrados, así como la investigación, el diagnostico, el escalamiento y el cierre de las mismas. Los casos recurrentes deben ser analizados y clasificados, identificando las causas de origen para prevenir nuevos incidentes y establecer recomendaciones de mejora.
3.	Las estrategias de continuidad de tecnología establecidas deben permitir al negocio responder a situaciones de contingencia generadas por incidentes técnicos o desastres naturales que pueden afectar a los servicios e infraestructuras que soportan las operaciones de la organización.

4.	Los roles de seguridad, privilegios de acceso de la información y supervisión de la seguridad, así como la información procesada u operada, deben establecerse considerando los pilares de *Confidencialidad*, *Integridad* y *Disponibilidad* con el objetivo de mantener aceptable el nivel de riesgo de seguridad.
RELATIVAS A SUPERVISAR Y MONITOREAR	
1.	Para fortalecer y mejorar los niveles de confianza, así como de seguridad del entorno de tecnología, el Control Interno Informático requiere de una revisión anual mínimamente, incluyendo revisiones externas independientes que pueden ser llevadas a cabo por Auditores Certificados, reconocidos y habilitados por el regulador.
2.	Las políticas y procedimientos de Tecnología de Información (TI) así como de Seguridad de Información (SI), contemplan el cumplimiento de requisitos legales, regulatorios y contractuales.