CARACTERIZACIÓN DEL PROCESO
SISTEMAS DE INFORMACIÓN

OBJETIVO DEL PROCESO
Planificar, implementar, gestionar y mantener los sistemas de información para la transformación digital, evolución de las capacidades operativas, cumplimiento de los objetivos estratégicos y la toma de decisiones de la entidad en el marco de los estándares del Modelo de Seguridad y Privacidad de la Información (MSPI).
ALCANCE (LÍMITES)
Inicia con la definición de estrategias, políticas y lineamientos para la Gestión de los Sistemas de Información y finaliza con la implementación y mantenimiento de las soluciones tecnológicas alineadas al plan de transformación digital en articulación con el Modelo de Seguridad y Privacidad de la Información (MSPI).

LÍDER DE PROCESO	TIPO DE PROCESO
Gerente de Sistemas de Información	Estratégico

PROVEEDORES	ENTRADAS	DESARROLLO DEL PROCESO	SALIDAS	CLIENTES
• MINTIC • Agencia Nacional Digital • DNP • Direccionamiento Estratégico	• Lineamientos del MINTIC. • Plan Nacional de Desarrollo • Misión, Visión • Objetivos a corto, mediano y largo plazo. • Estrategias • Seguimiento al cumplimiento de los planes de tratamiento de riesgo operativo y de corrupción. • Seguimiento a planes sectoriales	**TRANSFORMACIÓN DIGITAL** • **P.** Establecer el plan estratégico para el cumplimiento de las guías, lineamientos, estándares y normas que aplica al Gobierno Digital. • **P.** Identificar nuevas oportunidades en tecnologías que mejoren los servicios a la ciudadanía. • **H.** Implementar el plan estratégico alineado a los objetivos estratégicos. • **P.H.** Establecer y ejecutar los proyectos de transformación digital. • **P.H.** Definir e implementar la arquitectura empresarial y sus dominios. • **P.H.** Establecer y ejecutar proyectos para decisiones basadas en datos – analítica de datos. • **P.H.** Definir e implementar la Interoperabilidad con entidades que apoyen el cumplimiento de la misionalidad mediante el protocolo establecido por el Estado. • **V.** Verificar el cumplimiento del plan estratégico, las guías, lineamientos, estándares y normas. • **A**. Gestionar las lecciones aprendidas.	• Cumplimiento de las guías, lineamientos, estándares y normas que aplica al Gobierno Digital. • Apropiación de la cultura de Gobierno Digital. • Proyectos ejecutados. • Planes de mejora.	• Todos los procesos de CISA • Organismos del Estado.
• Todos los procesos de CISA	• Solicitud o ajustes en la funcionalidad de los aplicativos.	**GESTIÓN DE SISTEMAS DE INFORMACIÓN** • **P**. Determinar y evaluar Software a implementar • **P.** Diseñar el plan de trabajo y la arquitectura del software **H**. Gestionar la Contratación de Software especializado a implementar o ejecutar el desarrollo del software. • **H.V.** Aprobar o rechazar cambios e Implementación de cambios aprobados. • **H**. Atender y gestionar las solicitudes recibidas.	• Software implementado de acuerdo con la solicitud realizada. • Capacitación del uso del aplicativo si aplica. • Mejoras, modificaciones y actualizaciones a los aplicativos institucionales. • Documentación asociada al desarrollo de software, si aplica.	• Todos los procesos de CISA

PROVEEDORES	ENTRADAS	DESARROLLO DEL PROCESO	SALIDAS	CLIENTES
		• **H.V.A**. Llevar a cabo las pruebas y poner en producción. Velar por la integridad, continuidad, disponibilidad y seguridad de la información implementando y ejecutando políticas que permitan la correcta operabilidad de la compañía.		
• Todos los procesos de CISA	• Solicitud de Modificación o Adición de Información en Bases de Datos. • Incidentes o fallas en los aplicativos institucionales y de terceros. • Solicitud de Informes Especiales.	**SOPORTE DE SOTWARE ESPECIALIZADO** • **H.** Recibir radicado de fallas en aplicativos institucionales o de terceros. • **P**. Planear y asignar el recurso. • **H**. Ejecutar la planeación para dar solución al problema. • **V. A**. Verificar y validar el resultado del soporte realizado.	• Modificación a información de las bases de datos de acuerdo con las solicitudes realizadas por cada uno de los procesos. • Informes de acuerdo con las solicitudes realizadas por cada uno de los procesos. Soluciones a los soportes reportados por cada uno de los procesos a satisfacción	• Todos los procesos de CISA
• Procesos Solicitante	• Solicitud de proyectos de Software Especializado.	**GESTIÓN DE NUEVOS PROYECTOS Y/O REQUERIMIENTOS** • **P.** Priorizar y Planear ejecución del proyecto de Tecnología. • **P.** Establecer responsabilidades en la implementación del proyecto. • **H.** Ejecutar proyecto conforme a lo planificado • **V.** Realizar comités de seguimiento de proyectos • **P.H.** Evaluar, gestionar e implementar cambios • **V.** Revisar, verificar y validar los entregables del proyecto. • **P.V. A**. Gestionar los riesgos del proyecto. • **A**. Gestionar las lecciones aprendidas de los proyectos.	• Planes de gestión del Proyecto. • Acta de inicio del proyecto. • Artefactos del proyecto. • Acta de entrega /aceptación del proyecto de tecnología. • Documentos de seguimiento de cronogramas.	• Proceso Solicitante
• Junta directiva y presidencia. • Comité institucional de Gestión y Desempeño. • Organismos del estado.	• Plan estratégico de CISA. • Plan estratégico sectorial. • Políticas y lineamientos de CISA. • Políticas y lineamientos sectoriales. • Modelo integrado de planeación y gestión.	**PLANEACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN:** • **P:** Definir la estrategia de seguridad de la información de la entidad con su alcance, objetivos, metas e indicadores. • **P:** Definir los planes, programas y proyectos para la implementación de la estrategia de seguridad de la información. • **H:** Comunicar el plan estratégico de seguridad de la	• Plan estratégico de seguridad de la información. • Reportes de seguimiento e implementación de ACPM.	• Presidente de CISA. • Todos los procesos de CISA. • Organismos del estado.

PROVEEDORES	ENTRADAS	DESARROLLO DEL PROCESO	SALIDAS	CLIENTES
		información a todos los interesados. • **H:** Implementar los planes, programas y proyectos requeridos por la estrategia de seguridad de la información. • **V.A:** Medir y hacer seguimiento a los indicadores para verificar la consecución de los objetivos de la seguridad de la información de la entidad. • **V.A.** Identificar e Implementar acciones correctivas o de mejora para la implementación eficaz del plan estratégico de seguridad de la información.		
• Todos los procesos de CISA. • Organismos del estado	• Inventario de activos • Tablas de retención documental. • Caracterización de procesos. • Modelos de gestión, de riesgos y de seguridad de la información del estado colombiano	**GESTIÓN DE ACTIVOS DE INFORMACIÓN:** • **P:** Definir políticas y procedimientos para la identificación, valoración y clasificación de activos de información y protección de datos personales de la entidad. • **H:** Identificar, valorar y clasificar los activos de información de los procesos de la entidad y asegurar su tratamiento adecuado. • **H:** Identificar las bases de datos que contengan datos personales de la entidad y asegurar su tratamiento adecuado. • **H:** Reportar el estado de la gestión de activos de información y del cumplimiento de la protección de datos personales a las partes interesadas. • **V:** Asegurar que los activos de información permanecen inventariados, valorados y actualizados. • **V:** Realizar el seguimiento al cumplimiento de las políticas y metodologías de gestión de activos de información. • **V.A:** Identificar e Implementar acciones correctivas o de mejora para la gestión eficaz de los activos de información.	• Inventario de activos de información valorados y clasificados. • Inventario de base de datos que contienen datos personales. • Políticas y procedimientos para la gestión de activos de información. • Reportes de seguimiento e implementación de ACPM	• Todos los procesos de CISA. • Organismos del estado. • Auditoría Interna

CARACTERIZACIÓN DEL PROCESO
SISTEMAS DE INFORMACIÓN

PROVEEDORES	ENTRADAS	DESARROLLO DEL PROCESO	SALIDAS	CLIENTES
• Todos los procesos de CISA. • Organismos del estado. • Ciudadanos. • Auditoría Interna. • Proveedores	• Eventos de seguridad de la información, seguridad informática o tecnología. • Informes de auditoría interna y externa. • Resultados de análisis de vulnerabilidades. • Resultados de pruebas de ingeniería social. • PQR's de la ciudadanía.	**GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN:** • **P:** Definir políticas y procedimientos para la gestión de incidentes de seguridad de la información. • **H:** Identificar, valorar, dar tratamiento y documentar los incidentes de seguridad de la información. • **H:** Liderar y coordinar las actividades de gestión de los incidentes con los diferentes procesos y partes externas involucradas. • **H:** Generar reportes de la gestión de incidentes a las partes interesadas. • **V:** Hacer seguimiento a los incidentes de seguridad de la información para determinar su adecuada contención, erradicación y recuperación. • **V.A**: Identificar lecciones aprendidas e Implementar acciones correctivas o de mejora para la gestión eficaz de los incidentes de seguridad de la información.	• Incidentes de seguridad de la información clasificados, valorados, tratados y documentados. • Informes ejecutivos y técnicos de la gestión de incidentes a las partes interesadas. • Reportes de seguimiento e implementación de ACPM.	• Presidente de CISA. • Organismos del estado. • Entes de control. • Auditoría Interna.
• Todos los procesos de CISA. • Proveedores	• Inventario de activos de información valorados y clasificados. • Matriz de riesgos de seguridad de la información. • Informes de auditoría de seguridad de la información. • Incidentes de seguridad de la información clasificados, valorados, tratados y documentados. • Reportes de seguimiento e implementación de ACPM.	**SEGUIMIENTO Y MEDICIÓN DEL DESEMPEÑO DE LA SEGURIDAD DE LA INFORMACIÓN:** • **P:** Definir los mecanismos y procedimientos a través de los cuales se le hace medición y seguimiento a la gestión de la seguridad de la información. • **H:** Recopilar resultados del desempeño de la gestión de la seguridad de la información. • **H:** Realizar la revisión por la dirección. • **V:** Verificar el cumplimiento de la estrategia de seguridad de la información. • **V.A:** Realizar seguimiento al cierre de hallazgos de revisiones y auditorías internas y externas de seguridad de la información. • **V:** Verificar el cumplimiento de las metas • **V.A.** Controlar y realizar seguimiento a la implementación y cierre de acciones correctivas o de mejora relacionadas con la seguridad de la información.	• Informe de revisión de la seguridad de la información por la dirección de CISA. • Informe de seguimiento y cierre de ACPM. • Informe de medición de avance de la implementación de la estrategia de seguridad de la información	• Presidente de CISA. • Organismos del estado.

CARACTERIZACIÓN DEL PROCESO
SISTEMAS DE INFORMACIÓN

PROVEEDORES	ENTRADAS	DESARROLLO DEL PROCESO	SALIDAS	CLIENTES

INDICADORES DE GESTIÓN		RIESGOS DEL PROCESO	RECURSOS TECNOLÓGICOS
Eficacia	• Acciones para Tratamiento de Riesgos • Cumplimiento Portafolio de Proyectos de Transformación Digital • Gestión de Vulnerabilidades Técnicas • Porcentaje de solicitudes de soporte pendientes por atender (Backlog).	El detalle de los riesgos del proceso se debe consultar en el aplicativo ASE – Aplicativo de seguimiento la estrategia.	• Sistema IMC • Portal WEB / Comercialización - Desarrollo • SIGA - Desarrollo • Sistema SGI - Desarrollo • ZIRUMA / RPA - Desarrollo • ORFEO - Desarrollo • Ambientes de Desarrollo AQUILES (Software DevopServer para versión del código fuente) • Ambientes de QA TARTARO Windows - Desarrollo • Ambiente de Preproducción HERA Windows • Ambientes de Desarrollo TST Linux • Ambientes de QA - Preproducción QA Linux • Códigos fuentes de Desarrollos (Conbra, Concisa, Temis, Olympus, Sigep, Gescam y portal web) • Plataforma Microsoft Defender (sensibilización, reportes de operación de cuentas y licencias). • ZEUS - desarrollo • ISOlución • ASE - Aplicativo para el seguimiento a la Estrategia
Eficiencia	• Gestión de la Cultura en Seguridad de la información • Porcentaje de Incidentes de Seguridad de la Información		
Nota: Para verificar el detalle del indicador, hoja de vida y los resultados de las mediciones, debe consultarse el aplicativo ISOlución, módulo "Medición".			

DOCUMENTACIÓN APLICABLE	
DOCUMENTOS PROPIOS DEL PROCESO	**DOCUMENTOS TRANSVERSALES**
• CN127: Políticas y Procedimiento para la Gestión de Proyectos de Tecnología • CN128: Políticas y Procedimientos de Seguridad de la Información • MC037: Política de Tratamiento de Datos Personales	• CN023: Programa de Gestión Documental • CN107: Política de administración del riesgo en Central de Inversiones S.A. • MN011: Código de Buen Gobierno • MN013: Manual del SIG • MN018: Sistema de Gestión de Seguridad y Salud en el Trabajo (SGSST) • MN022: Manual del Sistema de Gestión de Continuidad del Negocio • MN023: Código de Integridad • MN024: Manual para la Gestión de Conflictos de Interés • MN026: Manual de Contratación • MN032: Manual de autocontrol, prevención y gestión de riesgo integral contra el lavado de activos, financiación del terrorismo financiación de la proliferación de armas de destrucción masiva. • MN033: Programa de Cumplimiento en materia de libre competencia económica –

DOCUMENTACIÓN APLICABLE	
DOCUMENTOS PROPIOS DEL PROCESO	**DOCUMENTOS TRANSVERSALES**
	PLCE • MC001: Reglamento Interno de Trabajo de Central de Inversiones S.A. • MC046: Política para la Prevención y Lucha Contra la Corrupción • MC048: Política de Derechos Humanos • Docs. de Interés Gral. 006: Normograma por Procesos