Plan de Seguridad y Privacidad de la Información

Corpocaldas

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
2024

CORPORACIÓN AUTÓNOMA REGIONAL DE CALDAS – CORPOCALDAS

Subdirección Administrativa y Financiera
Proceso Gestión tecnológica

Manizales, enero de 2024

PLAN INSTITUCIONAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
VIGENCIA 2024

Proceso Gestión Tecnológica
Subproceso Gestión de TIC

Autores:
Ruben Dario Jaramillo Parra, Líder del Subproceso de Gestión TIC
Luisa Fernanda Callejas Orrego, Oficial de seguridad de la información (Contratista)

Aprobado por:
Comité Institucional de Gestión y Desempeño
Fecha de aprobación: 26 de enero de 2024
Acta de Aprobación No. 1 de 2024
Fecha de publicación: enero 31 de 2024

Tabla de contenido

1. INTRODUCCIÓN

La defensa y protección de los activos de información es una tarea esencial para asegurar la continuidad y el desarrollo de los objetivos institucionales, así como para mantener el cumplimiento normativo y regulatorio aplicable a la entidad, además traslada confianza a las partes interesadas, cuanto mayor es el valor de la información, mayores son los riesgos asociados a su pérdida, deterioro, manipulación indebida o malintencionada.

Es por esta razón, cabe resaltar que a través del Decreto Presidencial 612 de 2018, Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado", en su artículo 1, adiciona al Capítulo 3 del Título 22 de la Parte 2 del Libro 2 del Decreto Presidencial 1083 de 2015, Único Reglamentario del Sector de Función Pública, agregando al anterior Decreto el artículo 2.2.22.3.14, por medio del cual se integran los planes institucionales y estratégicos al Plan de Acción, considerando en su numeral 12 como obligación la elaboración anual del "Plan de Seguridad y Privacidad de la Información" para la entidad.

Dado lo anterior, el presente documento conduce a la preservación de la confidencialidad, integridad y disponibilidad de la información, apoyada en un proceso de gestión del riesgo, brindando confianza a las partes interesadas acerca de la adecuada gestión de riesgos; igualmente se basa en las recomendaciones técnicas establecidas en el Manual de la política de Gobierno Digital expedido por el Ministerio de Tecnologías de información y de las Comunicaciones (MinTIC), detalladas en el compendio denominado Modelo de Seguridad y Privacidad de la Información.

La seguridad de la información es una responsabilidad compartida de todos los niveles de la organización, que requiere del apoyo de todos ellos, facilitando la construcción de un estado más transparente, colaborativo y participativo, en la interacción con el ciudadano, empresas privadas y demás entidades del estado, tal como es el propósito de Gobierno digital.

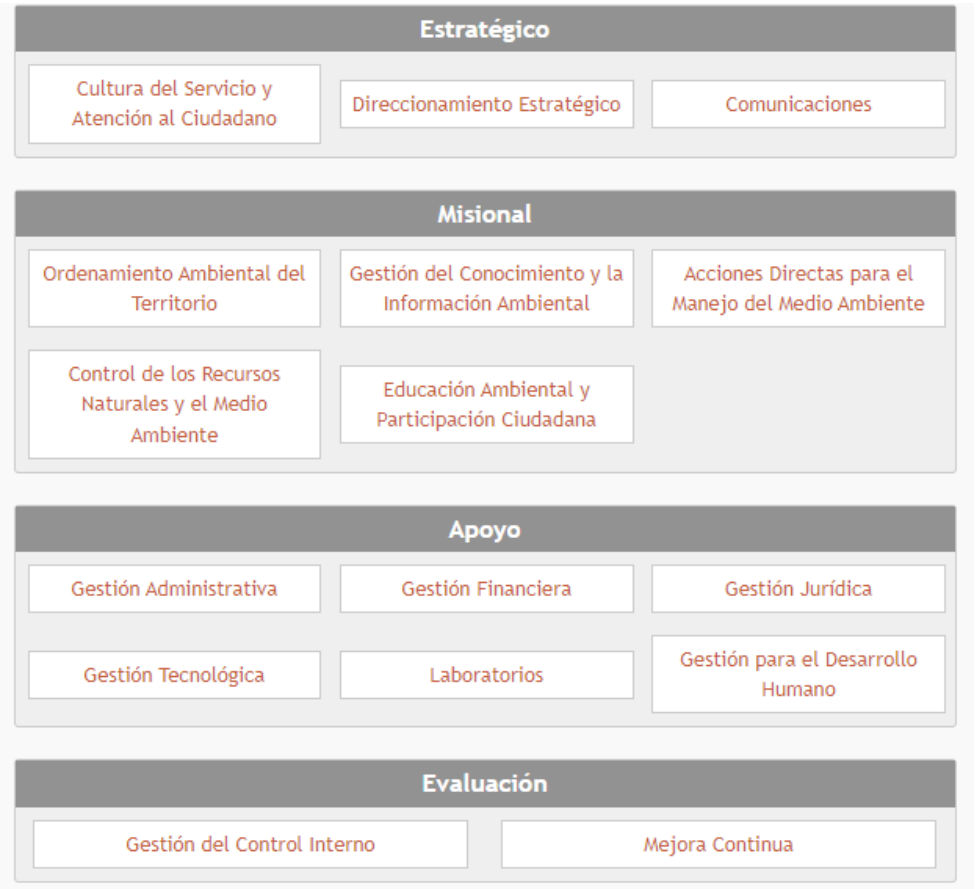
2. CONTEXTO ESTRATÉGICO DE LA ENTIDAD

Misión: Contribuimos al desarrollo sostenible del territorio, a través de la conservación y uso racional de los recursos naturales y el medio ambiente en el departamento de Caldas, mediante la aplicación de las normas y políticas ambientales, la modernización institucional y el fortalecimiento de la cultura del servicio hacia nuestros grupos de interés, con un talento humano comprometido y calificado.

Visión: Al 2031 Corpocaldas será el principal promotor del desarrollo sostenible del territorio para el bienestar de las generaciones presentes y futuras.

Mapa de operación por procesos:
Dentro del Sistema de Gestión Integrado, Corpocaldas cuenta con el mapa de procesos el cual se compone de cuatro tipos de procesos: ESTRATÉGICOS, MISIONALES, APOYO Y DE EVALUACIÓN. (Ver Mapa de Operación de Procesos).

Imagen 1. Mapa de operación por procesos



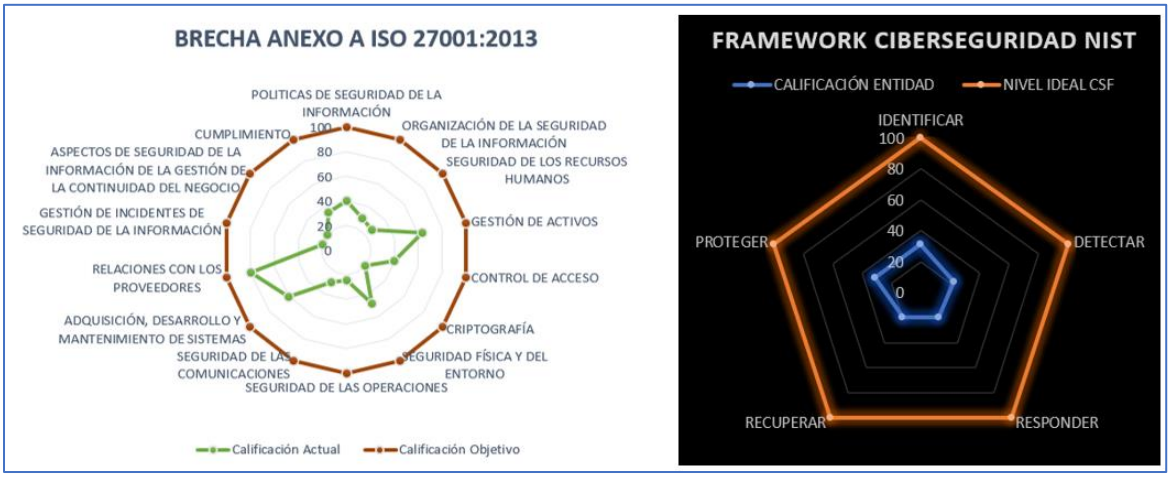
Fuente: Tomado del Sistema de gestión Integral de Corpocaldas - SGI

3. ANÁLISIS DE LA SITUACIÓN ACTUAL

La Corporación Autónoma Regional de Caldas, al 31 de diciembre de 2023 se encuentra en proceso de implementación del Modelo de Seguridad y Privacidad de la Información reflejando un porcentaje de implementación del 55%, alineado los objetivos estratégicos y misionales de la entidad, lo que indica que se ha incrementado el nivel de madurez con respecto a la del año 2022, además se incrementa el porcentaje de cumplimiento en la Corporación frente a la normatividad que aplica y con base en las mejores prácticas que ofrecen las normas internacionales tales como ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 31000 y NIST.

A continuación, se muestran los resultados de la aplicación de la herramienta sugerida por MinTIC para realizar el autodiagnóstico de Seguridad y privacidad de la información, como análisis en la fase inicial del MSPI, para medir el nivel de madurez en materia de seguridad de la información y de Ciberseguridad.

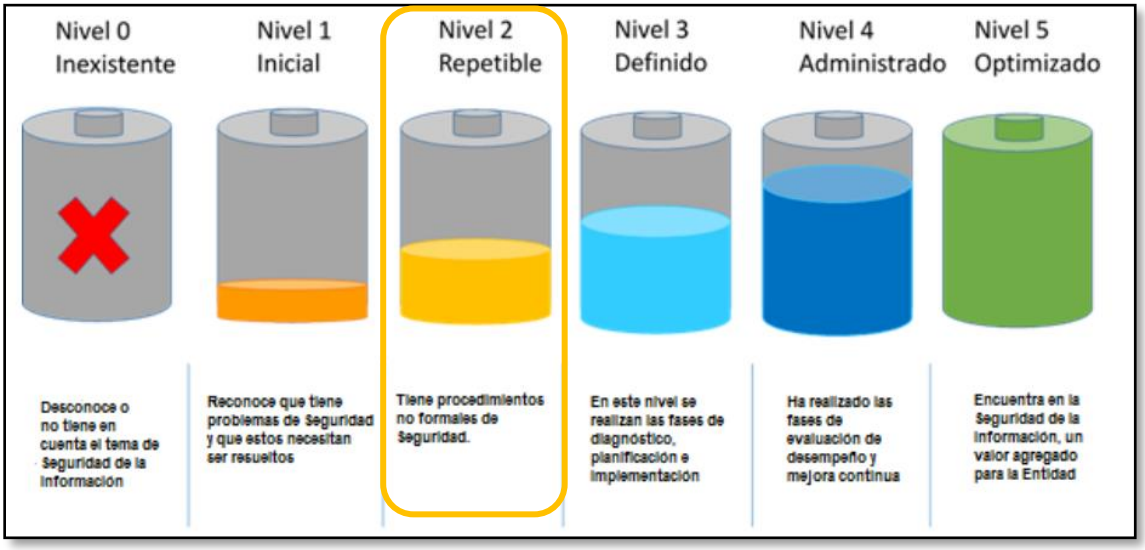
Imagen 2. Nivel de madurez de seguridad de la información y Ciberseguridad 2023



Fuente: Resultado de herramienta de medición de madurez de MSPI

De acuerdo con este resultado de nivel de madurez, se puede analizar que la entidad, en este último año, ha avanzado a nivel 2 ya que se ha realizado todo el diagnostico, logrando la documentación de procesos y procedimientos los cuales se encuentran en fase de revisión y aprobación por parte de los directivos.

Imagen 3. Nivel de madurez 2023



Fuente: Tomado de modelo de seguridad y privacidad de la información. En: https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf y adaptado por Corpocaldas.

De acuerdo con el diagnóstico realizado, se construye en conjunto una matriz FODA que nos permite dimensionar las cuestiones internas y externas de la Corporación, de acuerdo con la dimensión actual

Tabla 1. Matriz FODA. Cuestiones internas.

FACTORES	FORTALEZAS	DEBILIDADES
ECONÓMICO	• Inversión en innovación de tecnología.	
SOCIO CULTURAL	• Personal con facilidades y conocimientos tecnológicos.	• Falencia en la administración y gestión de contraseñas. • Posibles incidentes de seguridad por computadores desatendidos. • Reforzar cultura y capacitación en temas de seguridad de la información. • Empleados desmotivados o inconformes.

FACTORES	FORTALEZAS	DEBILIDADES
TECNOLÓGICO	• Cuentan con licenciamiento de software. • Se realizan inversiones en tecnología (infraestructura). • Se realizan actualizaciones en componentes de infraestructura. • Se tiene control a los accesos de red. • Se cuenta con página web interactiva. • Se cuenta con soporte a servicios dentro de la corporación. • Se realiza mantenimiento a los equipos de cómputo.	• Falta de implementación de nuevas herramientas DLP. • Falta de protección en correos electrónicos y firewall de aplicaciones web. • No se cuenta con software y hardware protegido con firewalls, programas antimalware y antivirus para comunicación a medios como WhatsApp, correos, entre otros. • Acceso no controlado a los sistemas de información. • Errores de aplicaciones. • No se cuenta con un DRP: plan de recuperación de desastres.
FISICO		• Falencias en la seguridad de las oficinas. • Falta de control en los accesos físicos
ECOLÓGICO		• Falta de políticas de “cero papel”. • No hay control en las áreas de impresión
LEGAL	• Se cuenta con apoyo de alta gerencia para mejora continua en seguridad de la información. • Aumento del nivel de madurez en cuando a la seguridad de la información.	• Falta integrar al comité institucional de gestión y desempeño temas Seguridad de la Información. • Incumplimiento de relaciones contractuales. • Fuga o revelación de información.

Fuente: Elaboración propia

Tabla 2. Matriz FODA. Cuestiones internas.

FACTORES	OPORTUNIDADES	AMENAZAS
POLÍTICO		• Convocatorias a huelgas.
SOCIAL	• Se cuenta con seguridad en comunicaciones. •	• Concurrencia de personal externo.
TECNOLÓGICO	• Se cuenta con seguridad en comunicaciones. • Se controlan los errores de mantenimiento. • Se tiene soporte en los servicios con los proveedores. • Se cuenta con servicios y seguridad en nube.	• Riesgo de pérdida y suplantación de información por parte de ataques informáticos u otros. • Sesiones activas después del horario laboral. • No se tienen directrices establecidas para el Teletrabajo. • Sobre dependencia en un dispositivo o sistema. • Descarga de internet sin control, bloqueo de páginas maliciosas, uso de ancho de banda priorizado. • No se cuenta con control contra Código malicioso. • No se tienen controles contra la Ingeniería social. • Aumento de ataques de ciberseguridad a empresas del estado.
FISICO		• Factores externos de alto riesgo (incendios, terremotos, inundaciones, entre otros) (Se tiene un riesgo medio de acuerdo con estudio de la propiedad horizontal).
LEGAL	• Se tiene cumplimiento legal.	• Desconocimiento de políticas de proveedores.

Fuente: Elaboración propia

Hasta la fecha, se han desarrollado las Políticas generales de seguridad y privacidad de la información que enmarcan las mejores prácticas a llevar cabo bajo los controles normativos de la ISO27001 con un área de aplicación a todos los procesos y subprocesos de la Corporación y de acuerdo con las responsabilidades que se tienen frente a los activos de información; estas Políticas generales se encuentran en proceso de revisión y aprobación por parte del comité directivo, las cuales se espera que dentro del primer trimestre del presente año, ya se cuente con estas políticas aprobadas para dar inicio a la socialización con los directivos y con los funcionarios y de esta manera iniciar el seguimiento a la implementación de dichas políticas que nos llevara a la mejora de los controles.

Se cuenta con el registro de activos de seguridad de la información se encuentran en proceso de revisión y aprobación por la nueva dirección. Las políticas de tratamiento de datos personales están aprobadas y se realiza socialización de estas a través de los canales de difusión oficiales de la Corporación Correo electrónico, redes sociales y grupos internos de WhatsApp.

Durante el 2023, se realizo el levantamiento de los riesgos de seguridad de la información para cada uno de los procesos y subprocesos de las Corporación en mesas de trabajo con los líderes, en donde se identificaron de manera individual cada uno de los riesgos asociados a sus funciones y actividades propias de cada subdirección, a su vez se determinaron los controles mínimos que se pueden establecer para iniciar con la mitigación del riesgo. La Matriz de riesgos de seguridad de la información se encuentra en proceso de aprobación por parte del comité Institucional de gestión y despeño.

En la siguiente tabla se identifican los procesos y subprocesos de la Corporación:

Tabla 3. Identificación de procesos y subprocesos

Nombre del Proceso	Nombre del Subproceso
Cultura del Servicio y Atención al Ciudadano	Cultura del Servicio y Atención al Ciudadano
Direccionamiento Estratégico	Estrategias corporativas
	Gestión del ciclo de proyectos

Nombre del Proceso	Nombre del Subproceso
Comunicaciones	Comunicaciones
Ordenamiento Ambiental del Territorio	Planificación para la declaratoria y el manejo de las áreas de interés ambiental
	Direccionamiento Ambiental para el Ordenamiento Territorial
	Ordenación de Cuencas
Gestión del Conocimiento y la Información Ambiental	Gestión de la Información Ambiental
	Monitoreo Ambiental
Acciones Directas para el Manejo del Medio Ambiente	Manejo Sostenible de la Biodiversidad y el Medio Ambiente
	Atención y Manejo de la Flora y Fauna Recuperada
	Obras de Infraestructura Ambiental
	Promoción en Producción y Consumo Sostenible
Control de los Recursos Naturales y el Medio Ambiente	Evaluación de solicitudes de Licencias Ambientales, Permisos, Concesiones y Autorizaciones
	Seguimiento y Control al Uso y Aprovechamiento de los Recursos Naturales y el Medio Ambiente
Educación Ambiental y Participación Ciudadana (Gobernanza ambiental)	Educación Ambiental
	Participación Ciudadana
Gestión Administrativa	Bienes y Suministros
	Gestión Documental
Gestión Financiera	Análisis Económico y Financiero
	Contabilidad
	Cobro Coactivo
	Facturación
	Presupuesto
	Tesorería

Nombre del Proceso	Nombre del Subproceso
Gestión Jurídica	Gestión Jurídica
Gestión Tecnológica	Gestión de la Infraestructura Tecnológica
Laboratorios	Laboratorio de Aguas
	Laboratorio de Suelos
Gestión para el Desarrollo Humano	Control Disciplinario Interno
	Gestión para el Desarrollo Humano
	Nómina
	Seguridad y Salud en el Trabajo
Gestión del Control Interno	Evaluación Independiente
Mejora Continua	Gestión Integral Institucional

Fuente: Creación propia

En cuanto a la sensibilización y concientización en temas sobre seguridad de la información, seguridad digital y ciberseguridad, se realizaron diferentes estrategias que permitieron llegar a los funcionarios de la entidad, con información clara y precisa sobre los temas en relación por medio de tips de seguridad, videos y charlas informativas.

Contexto interno:

- Factor humano: Compuesto por funcionarios, contratistas y proveedores
- Infraestructura física: Cuenta con sede principal en la calle 21 en el sector centro de la ciudad de Manizales, en el edificio Atlas en los pisos, 12 (Infraestructura ambiental), 13 (Planificación ambiental del territorio), 14 (Administrativa y financiera), 15 (Biodiversidad y Ecosistemas), 16 (Evaluación y seguimiento ambiental), 20 (Secretaría General) y 22 (dirección general). En la sede de la Carrera 24 como punto de atención al usuario se tienen los servicios de Recepción de correspondencia, Ventanilla ambiental y se integra en la misma sede las áreas de Comunicaciones y gestión documental. Laboratorio ambiental ubicado en la

Carrera 19 No 33-17 (Sector fundadores). Y 21 sedes de atención al usuario ubicadas en diferentes Municipios de Caldas.

- Infraestructura tecnológica: Se cuenta con un Data center ubicado en la sede principal en donde se cuenta con servidores, almacenamiento y seguridad perimetral.
- Gestión por procesos: La corporación dentro de su esquema contiene los procesos Estratégicos, Misionales, de apoyo y de Evaluación.

Contexto Externo:

- Factor social: Como propósito superior se construye al desarrollo sostenible del territorio, está la razón por la cual se tiene el interés de proteger la información que se obtienen de las actividades.
- Factor tecnológico: Corpocaldas como entidad pública del Orden Nacional debe realizar la implementación de la política de Gobierno Digital liderada por MinTIC que es la política de Gobierno Nacional que propende por la transformación digital pública hacia un estado abierto para fortalecer la relación con el ciudadano en la prestación del servicio por medio del uso y aprovechamiento de las TIC. Esta política hace parte del modelo integrado de Planeación y Gestión MIPG.
- Factor normativo y legislativo: Corpocaldas como entidad pública, dispone de un marco normativo y regulatorio en materia de seguridad y privacidad de la información, de acuerdo con recomendaciones dadas por normas internacionales y la normativa legal vigente para nuestro país. Las normas, leyes, decretos, resoluciones y demás, se encuentran en el Numeral de Marco Jurídico del presente documento, las cuales son tenidas en cuenta para la implementación del sistema de gestión de seguridad y privacidad de la información.
- Factor económico: Para Corpocaldas, el aspecto más importante, es la asignación de presupuesto que proviene de la sobretasa del pago del impuesto predial de los habitantes de Caldas para la inversión en aspectos misionales y de funcionamiento.
- Entes de control: Corpocaldas y sus activos de información, se encuentran expuestos a revisiones y seguimientos por parte de los entes de control:
  - Contraloría General de la Nación
  - Procuraduría General de la Nación
  - Contaduría General de la Nación
  - Ministerio de Medio Ambiente
  - Secretaría de transparencia

4. MARCO NORMATIVO

Tabla 4. Marco normativo

NORMA	DESCRIPCIÓN
Ley 1581 de 2012	Por la cual se dictan disposiciones generales para la protección de datos personales.
Ley 1712 de 2014	Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
CONPES 3995	Política Nacional de Confianza y Seguridad digital
CONPES 3854	Política Nacional de Seguridad Digital
Serie NTC/ISO 27000:2013	Estándar internacional que establece los requisitos para un sistema de gestión de seguridad de la información (SGSI) publicada en el año 2013
Serie NTC/ISO 27000:2022	Estándar internacional que establece los requisitos para un sistema de gestión de seguridad de la información (SGSI) publicada en el año 2022
NTC/ISO 22301	Sistemas de Gestión de Continuidad de Negocio
NTC/ISO 31000:2013	Gestión del Riesgo. Principios y directrices
Modelo de Seguridad y Privacidad de la Información MinTIC	Se encuentra alineado con el Marco de Referencia de Arquitectura TI y soporta transversalmente los otros componentes de la Política de Gobierno Digital, TIC para el Estado y TIC para la Sociedad. TIC, que son habilitados por tres elementos transversales: Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales
Guía para la administración del riesgo y diseño de controles en entidades públicas Versión 6 (2022)	Riesgos de Gestión, Corrupción y Seguridad Digital Función Pública

5. OBJETIVO GENERAL

Definir las actividades a llevar a cabo para mantener y dar continuidad de acuerdo con las fases contempladas en el Modelo de Seguridad y Privacidad de la Información – MSPI, de la política de Gobierno Digital del MinTIC, alineadas con la NTC/IEC ISO 27001, gestión de riesgos y los criterios de Continuidad de la operación, cumpliendo con los principios de confidencialidad, integridad y disponibilidad del activo de información, dando cumplimiento a la normatividad vigente de Gobierno Digital y bajo el enfoque de mejoramiento continuo..

5.1 Objetivos específicos

- Implementar acciones correctivas y de mejora para el Modelo de Seguridad y Privacidad de la Información.
- Hacer seguimiento a los controles y actualizar los riesgos de los activos de información con cada uno de los procesos y subprocesos
- Implementar el modelo de gestión de incidentes y eventos de seguridad digital y ciberseguridad de la Corporación.
- Sensibilizar a los funcionarios y contratistas de la Entidad acerca de las mejores prácticas en cuanto seguridad de la información, seguridad digital y ciberseguridad para fortalecer el nivel de conciencia de estos.

6. ALCANCE DEL DOCUMENTO

La ejecución del plan de seguridad y privacidad de la información para la Corporación se ejecutará de cara al cumplimiento del marco normativo de la función pública y acorde con las necesidades de la Corporación en búsqueda del cumplimiento de los objetivos institucionales de manera anual.

El plan de seguridad y privacidad de la información de CORPOCALDAS, se fundamenta en los lineamientos establecidos por el MinTIC y la serie ISO 27000:2013, plasmados en su modelo de seguridad y privacidad de la información - MSPI y el marco de ciberseguridad del Instituto Nacional de Estándares y Tecnología – NIST, pero desde la Corporación se tiene en cuenta la actualización de la ISO/IEC 27000:2022 para realizar la homologación hacia la nueva vigencia de esta norma.

Con la implementación del Modelo de Seguridad y Privacidad de la información – MSPI, se tiene ya establecido un marco de referencia para la operación de las mejores prácticas a nivel de la Corporación, el ciclo de operación del Modelo de seguridad y Privacidad de la Información está conformado por cinco fases que son Diagnóstico, Planificación, Implementación, Evaluación de desempeño y Mejora continua; cumpliendo con el ciclo PHVA de tal manera que las actividades implementadas, deban ser revisadas y ajustadas de acuerdo con las necesidades de seguridad de la información, seguridad digital y ciberseguridad de la Corporación.

Acorde con el avance que se ha tenido en materia de seguridad y privacidad de la información al interior de la Corporación y teniendo en cuenta que ya se cuenta Con el registro de los activos de información y con la Matriz de riesgos de Seguridad de la información (aun en aprobación), se dispone de estos, como insumo para iniciar las actualizaciones y ajustes tanto a procesos y actividades como a la documentación ya implementada por los procesos y subprocesos. De esta manera ya se tienen las bases para iniciar con el Análisis de Impacto del Negocio – BIA, mejorar la política de protección de datos personales, plan de recuperación de desastres del área de TI (DRP) y plan de continuidad del negocio de Corpocaldas (BCP).

En materia de datos personales y teniendo en cuenta la normatividad colombiana para el tratamiento de datos personales, se deben adoptar medidas que se ajusten a las necesidades de la Corporación y de acuerdo con su particularidad desde la misional con el fin de poner en marcha las mejores prácticas en estas obligaciones y dar cumplimiento a la normativa. Para establecer los lineamientos que garanticen la protección de los datos personales dentro de los criterios de recolección, almacenamiento, uso, circulación y retención de los datos personales en las bases de otros de los sistemas de información y datos recolectados de manera física, así mismo con los externos que para el cumplimiento de vínculos contractuales con la Corporación, deben tener como insumo datos propios o de terceros. Dado esto se deben realizar actividades en torno a la gestión del riesgo de los datos personales, establecer medidas de seguridad e informar a los interesados, finalmente realizar el ajuste a la política actual.

Ahora bien, dentro del proceso de identificación de riesgos con falencias que apuntan a los controles 6.1 selección, 6.2 términos y condiciones del empleo, 6.4 Proceso Disciplinario y 6.5, Responsabilidades después del empleo, de la ISO2007:2022 y para efectos contractuales de la Corporación, se debe hacer mención a diferentes subdirecciones y subprocesos que ejecutan esta labor, pero que se encuentran alienadas a los procesos desde el procesos de subcontratación en la Secretaria general (Contratistas y Terceros) o desde Talento Humano en la Subdirección Administrativa y Financiera (Funcionarios de planta, provisionalidad, libre nombramiento y remoción), con el fin de mejorar los aspectos en cuanto a seguridad de la información, en este plan se denomina una actividad para realizar controles de contratación antes durante y después de contrato y/o cambio de empleo.

Para continuar con la inmersión y conciencia en temas de seguridad de la información, seguridad digital y ciberseguridad, se contempla actividades que se ejecutan constantemente para que los funcionarios adquieran conocimientos y habilidades que conlleven a la protección de los activos de la información y de esta manera prevenir y responder de manera adecuada ante un incidente de seguridad. Todas esas actividades se encuentran descritas dentro del documento denominado: *Plan de concientización, educación y formación en seguridad y privacidad de la información.*

Además, dentro del plan de capacitación de Corpocaldas se plantean dos capacitaciones presenciales de seguridad informática para los funcionarios, por parte de un ente capacitador externo.

Ámbito de aplicación:

El ámbito de aplicación del presente plan tiene presencia a toda la Corporación logrando un marco integral de Seguridad de la Información que cubre procesos críticos para la organización y de acuerdo con su estructura, la cual se encuentra socializada a través de la *Tabla No 1. Identificación de procesos y subprocesos***.**

Partes interesadas:

Las partes interesadas internas incluyen:

- Dirección: Constituida por el Director General y el Consejo Directivo.
- Procesos misionales: Comprenden Subdirecciones de Planeación Ambiental del Territorio, Evaluación y Seguimiento Ambiental, Diversidad y Ecosistemas, e Infraestructura Ambiental
- Procesos estratégicos: Enfocados en la cultura de servicio y la atención al ciudadano, junto con el direccionamiento estratégico y comunicaciones.
- Proceso de Apoyo: Incluyen la Gestión Administrativa, de Bienes y Suministros, Documental, Financiera, Contabilidad, Recaudo Coactivo, Facturación y Cartera, Presupuesto y Tesorería, Gestión Judicial, y la Secretaría General. Además, se abarcan la Gestión Tecnológica, OTIC, Desarrollo Humano, Control Interno Disciplinario, Nómina, y Salud y Seguridad en el Trabajo, así como los Laboratorios de Aguas y de Suelos.
- Evaluación: Encargada de la Gestión de Control Interno y Mejora Continua.

Las partes interesadas externas comprenden:

- Entes Regulatorios: Incluyen la Contraloría, Procuraduría, Contaduría General de la Nación, Ministerio de Medio Ambiente, Archivo General de la Nación y Función Pública.
- Alcaldías: Alcaldías Municipales y la Gobernación de Caldas.

- Revisoría Fiscal: Entidad externa responsable de supervisar la gestión financiera, contable y administrativa, en conformidad con la Ley 87 de 1993, la cual estipula la obligatoriedad de la revisoría fiscal en entidades públicas del orden nacional.
- Usuarios: Definidos como ciudadanos del Departamento de Caldas que requieren servicios ambientales y PQRS.
- Proveedores: Entidades que suministran bienes y servicios a la corporación

7. MODELO DE PLANEACIÓN Y CRONOGRAMA DE EJECUCIÓN

Se presenta cronograma actividades a ejecutar, algunas actividades registradas dentro del plan de comunicación y sensibilización no tiene asignación de fecha de ejecución, ya se encuentran supeditadas a las planeaciones institucionales dentro del marco de capacitaciones, inducciones y reinducciones para los funcionarios de la Corporación.

Tabla 5. Cronograma de actividades

Actividad	Producto	Fecha inicio	Fecha fin	Responsable
Actualizar la matriz de activos de información de la seguridad de la información según la necesidad.	Documento de metodología de gestión de levantamiento de activos de información Matriz de activos de información actualizada 2024	01/03/2024	27/11/2024	Oficial de seguridad de la información Líder de gestión documental
Revisar y aprobar la Política de seguridad y privacidad de la información 2024	Política de Seguridad y privacidad de la Información de Corpocaldas 2024 aprobada	1/03/2024	22/03/2024	Oficial de seguridad de la información
Socializar roles y responsabilidades de seguridad y privacidad de la información para aprobación de responsabilidades.	Documento de roles y responsabilidades de seguridad y privacidad de la	1/03/2024	23/03/2024	Oficial de seguridad de la información Comité de gestión y desempeño

Actividad	Producto	Fecha inicio	Fecha fin	Responsable
	información socializado			
Socializar la Política de seguridad y privacidad de la información 2024	1 capacitación realizada para funcionarios y contratistas.	2/05/2024	30/06/2024	Oficial de seguridad de la información
Elaborar el procedimiento de gestión de incidentes	Procedimiento de gestión de incidentes elaborado Formato de registro de incidentes	01/03/2024	21/03/2024	Oficial de seguridad de la información Gestión de la infraestructura tecnológica Acompañamiento del Equipo MSPI
Elaborar el flujo de datos general de la Corporación para el Catálogo de Componentes de la Corporación en un nivel 1	Catálogo de Componentes de Información Nivel 1	05/03/2024	03/04/2024	Oficial de seguridad de la información
Socializar el despeño del MSPI a la oficina TIC y directivos	Informe socializado	01/04/2024	30/04/2024	Oficial de seguridad de la información Líder de TIC Equipo MSPI
Identificar acciones de mejora al MSPI y elaborar plan de mejoramiento del MSPI en Corpocaldas	Plan de mejoramiento	15/04/2024	29/04/204	Oficial de seguridad de la información Líder de TIC

Actividad	Producto	Fecha inicio	Fecha fin	Responsable
				Equipo MSPI
Realizar informe de nivel de madurez de seguridad de la información de la Corporación	Informe de nivel de madurez de seguridad de la información	15/04/2024	26/04/2024	Oficial de seguridad de la información Equipo MSPI
Revisar y ajustar el Plan de Recuperación de desastres DRP de TI y el plan de continuidad de negocios de Corpocaldas	Documento de Plan de Recuperación de desastres DRP de TI Documento de plan de continuidad de negocios de Corpocaldas.	29/04/2024	28/06/2024	Oficial de seguridad de la información Líder de infraestructura (DRP) Lideres de procesos transversales (BCP)
Revisar y actualizar la política de tratamiento de datos personales con alcance a todos los procesos de la corporación	Política de tratamiento de datos personales para vigencia 2025 actualizada.	2/07/2024	18/10/2024	Lideres de procesos involucrados (RRHH, SST, Servicio al ciudadano, Contratación, subdirectores)
Implementar controles de contratación antes durante y después de contrato y/o cambio de empleo.	Controles implementados	1/08/2024	6/12/2024	Oficial de seguridad de la información Lideres de procesos y subdirectores
Revisar las Políticas de seguridad y privacidad de la información y actualizar si es el caso	Política de seguridad y privacidad de la información revisadas	11/10/2024	13/12/2024	Oficial de seguridad de la información Equipo MSPI
Elaborar y ejecutar el plan de capacitación,	Documento de Plan de	13/02/2024	30/12/2024	Oficial de seguridad de la información

Actividad	Producto	Fecha inicio	Fecha fin	Responsable
sensibilización y comunicación de seguridad de la información.	capacitación, sensibilización y comunicación de seguridad de la información elaborado y ejecutado.			Gestión humana
Elaborar y presentar informe de avance de implementación del plan institucional de seguridad y privacidad de la información.	Presentación de informe de avance de ejecución del plan 2024	02/12/2024	30/12/2024	Oficial de seguridad de la información

8. SEGUIMIENTO Y CONTROL

El comité de gestión y desempeño realizara seguimiento al cumplimiento del plan a través de la aplicación del siguiente indicador:

Nombre del Indicador:	Madurez del MSPI
Tipo de indicador:	Indicador de desempeño
Medición:	Instrumento de evaluación de MSPI
Meta de indicador:	Nivel 3 de madurez de SGSI
Frecuencia:	Anual

Control de cambios

VERSION	FECHA APROBACION	RESPONSABLE	DESCRIPCION DEL CAMBIO
V1	31/01/2024	Rubén Darío Jaramillo Parra	Creación del documento