PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Corpocaldas

CORPORACIÓN AUTÓNOMA REGIONAL DE CALDAS

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Versión 01

Manizales, enero de 2025

Corpocaldas
Corporación Autónoma Regional de Caldas

Calle 21 No. 23-22 Edificio Atlas Manizales PBX (606) 8931180 - Teléfono: (606) 884 14 09
Código Postal 170006 - Línea Verde: 01 8000 96 88 13
www.corpocaldas.gov.co - corpocaldas@corpocaldas.gov.co
@corpocaldas @corpocaldasoficial

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Proceso: Gestión Tecnológica
Subproceso: Gestión de TIC

Aprobadores

Aprobó	Reviso	Elaboro
Comité Institucional de Gestión y Desempeño Acta No. 01 de 2025	Subdirector Administrativo y Financiero Cesar Augusto Cano	Líder del subproceso Gestión de TIC Ruben Dario Jaramillo

CONTENIDO

1. INTRODUCCIÓN

La Corporación Autónoma Regional de Caldas establece el Plan de Seguridad y Privacidad de la Información con el fin de dar cumplimiento al Decreto 1008 de 2018 que establece los lineamientos generales de la Política de Gobierno Digital que deberán adoptar las entidades pertenecientes a la administración pública, encaminados hacia la transformación digital y el mejoramiento de las capacidades TIC, para el desarrollo del habilitador transversal "Seguridad de la Información" de la Política de Gobierno Digital; así mismo el Decreto 1499 de 2017 que determina el cumplimiento institucional de las Políticas de Gobierno y Seguridad Digital en relación con el habilitador "Seguridad de la Información" conforme a la Resolución 500 de 2021 de MinTIC y la resolución 3246 de 2019 y sus modificaciones, por el cual se constituye el comité institucional de gestión y desempeño de Corpocaldas, en donde se establece en una de sus funciones "*Asegurar la implementación y el desarrollo de las políticas de gestión y directrices en materia de seguridad digital y de la información*"

Este documento conduce a la preservación de la confidencialidad, integridad y disponibilidad de la información de la entidad, apoyada en un proceso de gestión del riesgo y 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. OBJETIVOS

Planear y ejecutar las acciones tendientes a fortalecer la seguridad y privacidad de la información en la Corporación Autónoma Regional de Caldas en el marco del Modelo de Seguridad y Privacidad de la Información – MSPI y la política de Gobierno Digital de MinTIC con el fin de asegurar la confidencialidad, integridad y disponibilidad de los activos de información de la entidad.

2.1. Objetivos específicos

1. Implementar la Política de Seguridad y Privacidad de la Información de la Corporación autónoma Regional de Caldas
2. Definir y establecer acciones y estrategias con el fin de dar cumplimiento a los requisitos legales y normativos en materia de seguridad y privacidad de la información, seguridad digital y protección de la información personal que le apliquen a la entidad, en el marco del Modelo de Seguridad y Privacidad de la Información – MSPI.
3. 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.

3. ALCANCE DEL DOCUMENTO

El presente documento aplica a todo el modelo de operación por procesos de la Corporación (procesos estratégicos, misionales, de apoyo y de evaluación) y partes interesadas que comparten, utilicen, recolecten, procesen, intercambien o consulten cualquier tipo de información, ya sea interna o externa.

Inicia con la definición del Plan de Seguridad y Privacidad de la Información, continua con la ejecución y finaliza con el seguimiento y evaluación de la gestión realizada.

4. DEFINICIONES

- **Acceso a la Información Pública**: Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4).
- **Activo**: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).
- **Activo de Información**: En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.
- **Archivo**: Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3)
- **Amenaza:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).
- **Auditoría**: Proceso sistemático, independiente y documentado para obtener evidencias de auditoria y obviamente para determinar el grado en el que se cumplen los criterios de auditoria. (ISO/IEC 27000).
- **Autorización:** Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3).
- **Bases de Datos Personales**: Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3).
- **Confidencialidad**: Se refiere a que la información solo puede ser conocida por individuos autorizados.
- **Control**: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.
- **Datos Abiertos**: Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a

disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6)

- **Datos Personales**: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).
- **Disponibilidad**: Se refiere a la seguridad que la información puede ser recuperada en el momento que se necesite, esto es, evitar su pérdida o bloqueo, bien sea por ataque doloso, mala operación accidental o situaciones fortuitas o de fuerza mayor.
- **Gestión de incidentes de seguridad de la información**: Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).
- **Integridad**: Se refiere a la garantía de que una información no ha sido alterada, borrada, reordenada, copiada, etc., bien durante el proceso de transmisión o en su propio equipo de origen.
- **Privacidad**: En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL la correlativa obligación de proteger dicha información en observancia del marco legal vigente.
- **Riesgo**: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).
- **Seguridad de la información**: Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).
- **Sistema de Gestión de Seguridad de la Información SGSI**: Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000)
- **Titulares de la información**: Personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3)
- **Tratamiento de Datos Personales**: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley 1581 de 2012, art 3).

- **Vulnerabilidad**: Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).
- **Partes interesadas**: Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

5. MARCO NORMATIVO

Tipo de norma	Numero	Año	Descripción
CONSTITUCIÓN POLÍTICA DE COLOMBIA.	ARTÍCULO 74		Todas las personas tienen derecho a acceder a los documentos públicos salvo los casos que establezca la ley. El secreto profesional es inviolable.
LEY	527	1999	Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.
LEY	1266	2008	Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.
LEY	1581	2012	Por la cual se dictan disposiciones generales para la protección de datos personales.
Decreto Reglamentario	1377	2013	Por el cual se reglamenta parcialmente la Ley 1581 de 2012"
LEY	1273	2009	Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
LEY	1712	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
DECRETO	2609	2012	Por medio de la cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras

Tipo de norma	Numero	Año	Descripción
			disposiciones en materia de Gestión Documental para todas las Entidades del Estado
DECRETO	2573	2014	Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones.
DECRETO	103	2015	Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
RESOLUCIÓN	500	2021	Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital.
RESOLUCIÓN	1519	2020	Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos
DECRETO	767	2022	Establece los lineamientos generales de la Política de Gobierno Digital. El objetivo de esta política es mejorar la calidad de vida de los colombianos y aumentar la competitividad del país
DECRETO	338	2022	Se establecen los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital NTC ISO/IEC 27001 DE 2022 Esta norma internacional especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información dentro del contexto de la organización.
ICONTEC NTC/ISO 27001 y NTC/ISO 27002			Las recomendaciones y buenas prácticas

6. CONTEXTO INSTITUCIONAL

6.1. Forma jurídica

Mediante acuerdo número 015 de 1991, aprobado mediante decreto ordinario por la Junta Directiva de la Corporación Autónoma Regional de Desarrollo de Caldas (Corpocaldas), establece la adopción de los Estatutos de la Corporación, definiéndose como un ente público con personalidad jurídica propia, autonomía administrativa y patrimonio independiente. Esta vinculada al Departamento Nacional de Planeación y se rige por las disposiciones de la Ley 22 de 1991, así como por los Decretos 1050 y 3130 de 1968.

6.2. Direccionamiento Estratégico

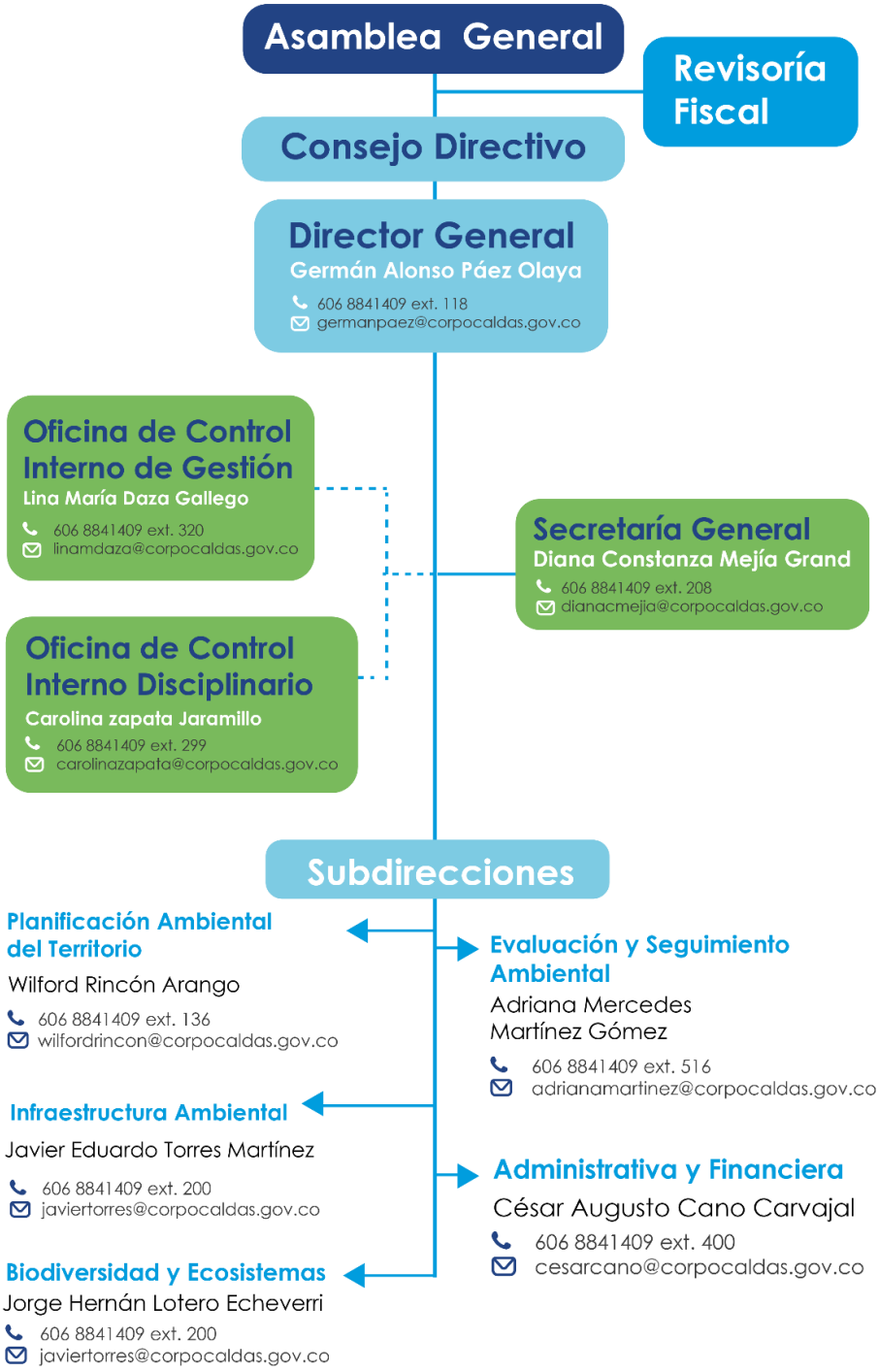
Propósito Superior: Al 2031 Corpocaldas será el principal promotor del desarrollo sostenible del territorio para el bienestar de las generaciones presentes y futuras.

Mega Meta: 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.

6.3. Organigrama

La estructura organizacional de Corpocaldas está definida mediante el Acuerdo del Consejo Directivo No. 22 de noviembre 30 de 2021. Esté muestra una estructura organizativa que permite una gestión eficiente y transparente, promoviendo un ambiente de trabajo organizado y alineado con los objetivos estratégicos de la entidad.

Ilustración 1. Organigrama de Corpocaldas.



Fuente: https://corpocaldas.gov.co/Corpocaldas/Contenido/?pag_Id=56

7. ANÁLISIS DE LA SITUACIÓN ACTUAL

En CORPOCALDAS se han llevado a cabo una identificación y evaluación exhaustiva de los factores internos y externos que son cruciales para la alineación con nuestra visión estratégica y para garantizar la obtención de los resultados proyectados en materia de seguridad de la información. Se ha utilizado un enfoque combinado de análisis PESTEL y DOFA como herramientas de planificación estratégica. Este enfoque dual permite definir con precisión el contexto operativo de la corporación, así como analizar los factores políticos, económicos, sociales, tecnológicos, ambientales y legales externos, junto con las fortalezas, oportunidades, debilidades y amenazas internas. El resultado de estos análisis se refleja en la Matriz de Contexto, proporcionando una visión integral de los elementos que impactan en nuestra corporación.

A continuación, se describen los resultados obtenidos:

Cuestiones Externas:

FACTORES	OPORTUNIDADES	AMENAZAS
POLÍTICO		• A1: Convocatorias a huelgas.
SOCIAL		• A2: Concurrencia de personal externo.
TECNOLÓGICO	• O1: Se cuenta con seguridad en comunicaciones. • O2: Se controlan los errores de mantenimiento. • O3: Se tiene soporte en los servicios con los proveedores. • O4: Se cuenta con servicios y seguridad en nube.	• A3: Riesgo de pérdida y suplantación de información por parte de ataques informáticos u otros. • A4: Sesiones activas después del horario laboral. • A5: No se tienen directrices establecidas para el Teletrabajo. • A6: Sobre dependencia en un dispositivo o sistema. • A7: Descarga de internet sin control, bloqueo de páginas maliciosas, uso de ancho de banda priorizado. • A8: No se cuenta con control contra Código malicioso.

FACTORES	OPORTUNIDADES	AMENAZAS
		• A:9 No se tienen controles contra la Ingeniería social. • A:10 Aumento de ataques de ciberseguridad a empresas del estado.
ECOLOGICO		• A11: Factores externos de alto riesgo (incendios, terremotos, inundaciones, entre otros) (Se tiene un riesgo medio de acuerdo con estudio de la propiedad horizontal). • A12: Acceso físico no autorizado.
LEGAL	• O5: Se tiene cumplimiento legal.	• A13: Desconocimiento de políticas de proveedores.

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.
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.	• 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.

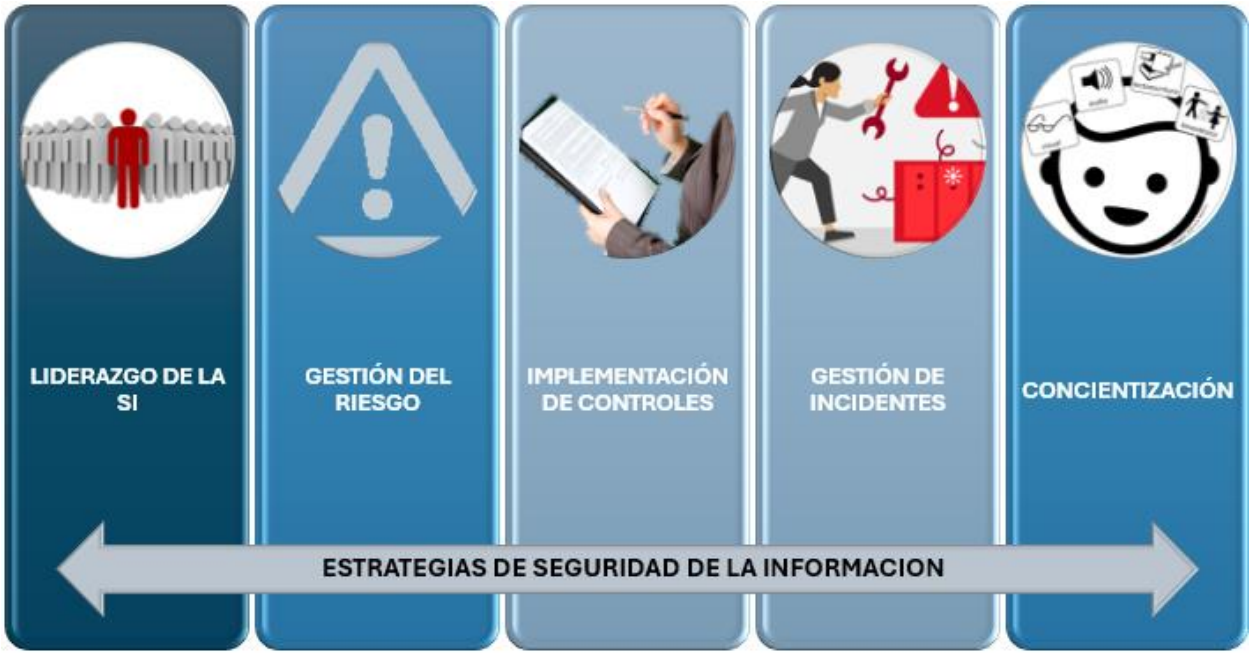
FACTORES	FORTALEZAS	DEBILIDADES
	• Se cuenta con página web interactiva. • Se cuenta con soporte a servicios dentro de la corporación. • Se realiza mantenimiento a los equipos de cómputo.	• Acceso no controlado a los sistemas de información. • Errores de aplicaciones. • No se cuenta con un DRP: plan de recuperación de desastres.
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.

8. ESTRATEGIAS DE SEGURIDAD DE LA INFORMACIÓN

La Corporación establecer una Estrategia de Seguridad Digital en la que se integran los principios, políticas, procedimientos, guías, manuales, formatos y lineamientos para la gestión de la seguridad de la información, teniendo como premisa que dicha estrategia está enmarcada em el Modelo de Seguridad y Privacidad de la Información -MSPI de MINTIC, así como de la guía de gestión de riesgos de seguridad de la información y del procedimiento de gestión de incidentes que debe establecerse (Ver Resolución 500 de 2021).

SE definen 5 estrategias que permitirán establecer en su conjunto una estrategia general de seguridad digital:

Ilustración 2. Estrategias de Seguridad de la información de Corpocaldas.



Fuente: Elaboración propia. Corpocaldas. Enero 2025.

ESTRATEGIA	DESCRIPCIÓN
LIDERAZGO DE LA SI	Establecer los roles y responsabilidades en seguridad de la información, vinculando a la alta dirección y a los líderes de las diferentes procesos y subprocesos de la Entidad, con el fin de asegurar la implementación y desarrollo de las políticas y directrices en materia de seguridad digital.
GESTIÓN DEL RIESGO	Gestionar los riesgos de seguridad de la información a través de la planificación y valoración, buscando prevenir o reducir los efectos indeseados.
IMPLEMENTACIÓN DE CONTROLES	Implementar y gestionar los controles de seguridad para el tratamiento de los riesgos, planificando e implementando las acciones necesarias para lograr los objetivos de seguridad y privacidad de la información y mantener la confianza en la ejecución de los procesos de la Entidad.
GESTIÓN DE INCIDENTES	Garantizar una administración de incidentes de seguridad de la información con base a un enfoque de integración, análisis, comunicación de los eventos e incidentes y las debilidades de seguridad en pro de conocerlos y resolverlos para minimizar el impacto negativo de estos en la Entidad
CONCIENTIZACIÓN	Fortalecer la construcción de la cultura organizacional con base en la seguridad de la información para que convierta en un hábito, promoviendo las políticas, procedimientos, normas, buenas prácticas y demás lineamientos, la transferencia de conocimiento, la asignación y divulgación de responsabilidades de todo el personal de la entidad en seguridad y privacidad de la información

9. CRONOGRAMA

Todos los planes o estrategias (sin excepción) deben contener un cronograma de ejecución en tablas de Excel y contener como mínimo los siguientes elementos. La última fila llevara un control de ejecución de cada acción.

ESTRATEGIA	ACTIVIDAD	META	FECHA	RESPONSABLE	RECURSOS
LIDERAZGO DE LA SI	Formular, aprobar y gestionar los planes estratégicos PETI, PESI.	1 plan formulado y aprobado	Enero a diciembre	Líder del subproceso gestión de TI	Recursos humanos propios
	Revisar y aprobar la política de seguridad de la información.	1 política aprobada	Segundo semestre del 2025	Comité Institucional de gestión y desempeñó	Recursos humanos propios
	Elaborar e implementar un Plan para la implementación de las políticas de seguridad de la información	1 plan de implementación	Segundo semestre del 2025	Profesional en seguridad de la Información y lideres d procesos y subprocesos	Contratista
	Elaborar e implementar un Plan para la gestión y monitoreo de riesgos de seguridad	1 plan de implementación	Enero a diciembre	Profesional en seguridad de la Información	Contratista
	Fortalecer y/o mantener la seguridad de la información, con los controles de seguridad perimetral y local (firewall y	Informe	Enero a diciembre	Profesional en seguridad de la Información y profesional de infraestructura	Contratista

ESTRATEGIA	ACTIVIDAD	META	FECHA	RESPONSABLE	RECURSOS
IMPLEMENTACIÓN DE CONTROLES	sistema de seguridad antivirus)				
	Adquisición de Firewall	Firewall adquirido	Mayo - agosto	Líder del subproceso gestión de TI, profesional en seguridad y profesional de infraestructura	Recurso incluido en el PETI
	Renovación de software base: Antivirus Endpoint, Microsoft 365, Meraki, Windows (Server y Desktop), Office, Oracle, entre otros.	Renovación realizada	Enero a diciembre	Profesionales oficina TIC	Recurso incluido en el PETI
GESTIÓN DE INCIDENTES	Gestionar los incidentes de seguridad de la información reportados	Gestiones realizadas	Enero a diciembre	Profesional en seguridad de la Información	Contratista
CONCIENTIZACIÓN	Elaborar y ejecutar el Plan de Cultura y Sensibilización de Seguridad de la Información.	1 plan ejecutado	Segundo semestre del 2025	Profesional en seguridad de la información	Contratista

10. RECURSOS

La fuente de financiación que soporta la ejecución del Plan en la vigencia 2025 hace parte del presupuesto funcionamiento de la Entidad de la vigencia 2024-2027.

11. PLAN DE COMUNICACIONES

Sensibilización: La comunicación es uno de los procesos más relevantes y complejos que lleva a cabo el ser humano. Por ello, es importante tomar conciencia y asumir el control de lo que se comunica para ser eficientes y obtener el máximo de las personas y las situaciones. De acuerdo con la norma técnica ISO/IEC 27002:2022, entre los temas más sensibles a socializar se seleccionaron los siguientes:

a) La política general de Seguridad de la Información.
b) Las responsabilidades en Seguridad de la Información y los medios por los cuales se cumplen dichas responsabilidades.
c) Las políticas, riesgos y controles y procedimientos de Seguridad de la Información.
d) La necesidad de conocer y cumplir con las reglas y obligaciones de seguridad de la información aplicable, tal como se definen en las políticas, normas, leyes, reglamentos, contratos y acuerdos.
e) La rendición personal de cuentas por las acciones y omisiones propias, y las responsabilidades generales relacionadas con la seguridad y la protección de la información que pertenece a la Entidad y a las partes externas.

Modalidad: Se seleccionaron las siguientes modalidades más acorde con el tipo de información a comunicar:

a) Infografía: es una representación gráfica que pretende explicar o resumir una información, combinando iconos como imágenes, gráficos, entre otros, con descripciones, narraciones, interpretaciones y datos. Son interpretaciones visuales de los propios textos y resultan más atractivas para el lector.
b) c. Videos: Consiste en diseñar presentaciones y videos explicativos muy cortos de máximo de cinco minutos de duración.
c) Papel tapiz: Conocido además como wallpaper, fondo de escritorio o fondo de pantalla, se trata de la fotografía o la ilustración que el administrador de una computadora (ordenador), escoge como fondo de la pantalla.

Medios: se seleccionaron los siguientes medios o canales por los cuales se realizará el envío o publicación de las piezas gráficas, entre los canales existentes en la Entidad se encuentran:

a) Correo: Se trata del correo institucional establecido por la Entidad para todos los comunicados oficiales.
b) Portal web: Se trata de la página web oficial: https://www.corpocaldas.gov.co de la Entidad.
c) Pantallas: Se trata de pantallas DE LOS COMPUTADORES D ELOS FUCNIONARIOS de la Entidad.

12. SEGUIMIENTO Y MEDICION DEL PLAN

Seguimiento al cumplimiento de lo establecido en el Plan por parte del líder del subproceso Gestión de TIC a través de las siguientes estrategias:

- Seguimiento y control al cronograma de ejecución, identificando las actividades que se deben desarrollar durante el año, los responsables, fecha prevista de cumplimiento, avance mensual, medición de los indicadores y desviaciones que se puedan presentar.

Seguimiento al estado de implementación del plan por parte del subdirector Administrativo y Financiero en el marco de las reuniones de grupo primario.

Elaboración y envió del informe semestral del plan al área de Planeación institucional con el cronograma de actividades programadas y el comportamiento de los indicadores.

Seguimiento al estado de implementación del plan de manera semestral en sesión del Comité Institucional de Gestión y Desempeño a fin de tomar decisiones tempranas por parte de la alta dirección.

Los indicadores que permitirán la medición del cumplimiento del Plan Institucional de Seguridad y Privacidad de la Información en cada anualidad son los siguientes:

$$\frac{\text{N° de Actividades Ejecutadas}}{\text{N° de Actividades Programada}} \text{ X } 100$$

CONTROL DE CAMBIOS

Versión	Fecha	Descripción	Actualizado Por
01	Enero 27 de 2025	Versión inicial del Plan de Seguridad y Privacidad de la Información	Comité Institucional de Gestión y Desempeño