Plan Estratégico de Seguridad de la Información

PESI

2020 2023

El Plan Estratégico de Seguridad de la Información "PESI" determina los objetivos a cumplir para salvaguardar la información de la entidad en sus pilares de confidencialidad, integridad y disponibilidad.

Manizales, enero de 2022

Calle 21 No. 23 – 22 Edificio Atlas Manizales
Teléfono: (6) 884 14 09 – Fax: 884 19 52
Código Postal 170006 - Línea Verde: 01 8000 96 88 13
www.corpocaldas.gov.co - corpocaldas@corpocaldas.gov.co
NIT: 890803005-2

Versión	Fecha versión	Observaciones
1	31 de enero de 2022	

CONTENIDO

1. INTRODUCCIÓN 4
   1.1 Definiciones 5
   1.2 Normas y modelos aplicables 6
2. OBJETIVO 7
   2.1 Objetivos Específicos 7
3. ALCANCE 8
4. METODOLOGÍA DE IMPLEMENTACIÓN 8
5. PROGRAMA DE SEGURIDAD DE LA INFORMACIÓN DE CORPOCALDAS 2020-2023 12

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.

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, como se propone desde Gobierno en Línea.

1.1 Definiciones

- **Activo de información:** En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).

- **Análisis de riesgos:** Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000:2013).

- **Confidencialidad:** Propiedad que determina que la información no esté disponible ni sea revelada a individuos entidades o procesos no autorizados. [NTC5411- 1:2006].

- **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. ISO 27000.

- **Evaluación de riesgos:** Proceso global de identificación, análisis y estimación de riesgos [Fuente: ISO Guide 73:2009].

- **Disponibilidad:** Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada. [NTC 5411-1:2006].

- **Dato personal:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. LEY 1581.

- **Gestión del riesgo:** Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. Se compone de la evaluación y tratamiento de riesgos. ISO 27000.

- **Integridad:** Propiedad de salvaguardar la exactitud y estado completo de los activos de información. [NTC 5411-1:2006].

- **Política:** Conjunto de orientaciones o directrices que rigen la actuación de una persona o entidad en un asunto o campo determinado.

- **Política de Seguridad de la Información:** Conjunto de Directrices que permiten resguardar los activos de información.

- **Procedimiento:** Define los pasos para realizar una actividad específica. Evita quese aplique el criterio personal.

- **Riesgo:** Un efecto es una desviación de lo esperado: positivo o negativo Seguridadde la Información. El riesgo de seguridad de la información está asociado con el potencial de que las amenazas exploten las vulnerabilidades de un activo de información o grupo de activos de información y, por lo tanto, causen daños a unaorganización.

- **Tratamiento:** Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. LEY 1581.

1.2 Normas y modelos aplicables

- Serie NTC/ISO 27000:2013
- NTC/ISO 31000:2013
- NTC/ISO 22301
- Modelo de Seguridad y Privacidad de la Información MinTIC v.3.0.2
- Guías Seguridad de la Información MinTIC
- Guía para la administración del riesgo y diseño de controles en entidades públicas.2018.

2. OBJETIVO

El objetivo de este documento es definir la estrategia de Seguridad y Privacidad de la Información para Corpocaldas, en cumplimiento del Modelo de Seguridad y Privacidad de la información (MSPI) y alineado con el Modelo Integrado de Planeación y Gestión (MIPG), en las políticas de Gobierno Digital y Seguridad Digital, que responda a las necesidades de preservar la confidencialidad, la integridad y la disponibilidad sobre los activos de información.

2.1 Objetivos Específicos

- Identificar los activos de información de los procesos estratégicos de la Entidad.
- Identificar y analizar los riesgos de los activos de información y establecer un plan de tratamiento de los riesgos que generan mayor impacto para la Entidad.
- Sensibilizar a los funcionarios y contratistas de la Entidad acerca del Modelo de Seguridad y Privacidad de la Información, fortaleciendo el nivel de conciencia de los mismos, en cuanto a la necesidad de salvaguardar los activos de información críticos de la Entidad.
- Implementar las políticas y controles de seguridad de la información y privacidad de la información alineado con el MSPI.
- Implementar el modelo de gestión de incidentes de seguridad y Ciberseguridad de la Entidad.
- Monitorear el cumplimiento de los requisitos de seguridad de la información.

- Implementar acciones correctivas y de mejora para el Modelo de Seguridad y Privacidad de la Información.

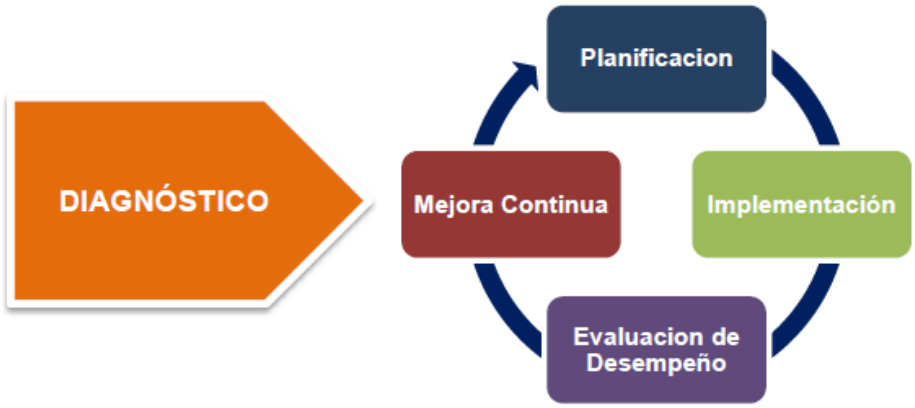
3. ALCANCE

El Plan Estratégico de Seguridad de la Información, tiene como finalidad establecer, implementar, mantener y mejorar, la Seguridad y Privacidad de la Información en la Corporación Autónoma Regional de Caldas, para todos sus procesos identificando sus activos críticos, implementando controles y gestionando los riesgos de seguridad.

4. METODOLOGÍA DE IMPLEMENTACIÓN

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.

Se toma como base el ciclo de operación del modelo de seguridad y privacidad de la información el cual consta de cinco (5) fases, de esta forma funcionará el plan de seguridad y privacidad de la información en la entidad.



Planeación

En este componente, se define el alcance, objetivos, procesos y procedimientos, pertinentes a la gestión del riesgo y mejora de seguridad de la información, en procura de los resultados que permitan dar cumplimiento con las metas propuestas del MSPI.

- ✓ Responsables de implementar el MSPI – Equipo del proyecto
- ✓ Objetivos y alcance del MSPI
- ✓ Políticas de seguridad y privacidad de la información
- ✓ Procedimiento de control documental del MSPI
- ✓ Roles y responsabilidades para la seguridad de la información
- ✓ Inventario de los activos de información
- ✓ Evaluación de riesgos y plan para su tratamiento

- ✓ Plan para la toma de conciencia, educación y formación en seguridad de la información
- ✓ Plan y estrategia de transición IPv4 a IPv6

- **Implementación**:

Este componente permitirá la implementación del componente de planificación del MSPI, teniendo en cuenta los aspectos más relevantes en los procesos de implementación del MSPI.

- ✓ Estrategia de planificación y control operacional con la aprobación de la Alta Dirección
- ✓ Implementar controles aprobados
- ✓ Planes de tratamientos de riesgos
- ✓ Indicadores de gestión del MSPI.

- **Evaluación de desempeño**:

Este componente permitirá evaluar el desempeño y la eficacia del MSPI, a través de instrumentos que permita determinar la efectividad de la implantación del MSPI.

- ✓ Evaluación del desempeño de los controles
- ✓ Planes de concientización
- ✓ Planes de tratamiento de riesgos con el objetivo de verificar la efectividad y eficacia de los mismos
- ✓ De forma conjunta se realizan auditorías internas del MSPI con los

responsables de Control Interno.

- **Mejora continua:**

Este componente permitirá consolidar los resultados obtenidos del componente de evaluación de desempeño, para diseñar el plan de mejoramiento continuo de seguridad y privacidad de la información, que permita realizar el plan de implementación de las acciones correctivas identificadas para el MSPI.

- ✓ Plan de seguimiento, evaluación y análisis para el MSPI.
- ✓ Comunicación de resultados y plan de mejoramiento
- ✓ Revisión y aprobación por la alta dirección

5. PROGRAMA DE SEGURIDAD DE LA INFORMACIÓN DE CORPOCALDAS 2020-2023

Fase	Actividad	Fecha Inicio	Fecha Fin	Responsable	Entregable
Planeación	Establecimiento del MSPI en Comité de Gestión y Desempeño Definir equipo de seguridad de la información	15/02/2022	15/04/2022	Subdirección de Planificación Ambiental Subproceso de Infraestructura Tecnológica	Resolución o Acta interna por la cual se adopta el MSPI
	Revisión de requisitos legales del MSPI	15/02/2022	15/04/2022	Equipo MSPI	Requisitos legales de seguridad y privacidad
	Definición y aprobación de alcance y la política de seguridad y privacidad de la información de la Entidad	15/03/2022	15/05/2022	Equipo MSPI Comité de Gestión y Desempeño	Resolución interna con aprobación de Política SPI Comunicados internos y externos de la Política
	Definición de procedimiento de control documental del MSPI, roles y responsabilidades para la SI	15/03/2022	15/08/2022	Equipo MSPI	Procedimiento de control documental Roles y responsabilidades para la SI
	Elaboración de inventario de activos de información y datos personales bajo el alcance del MSPI	1/04/2022	30/08/2022	Líderes de proceso con acompañamiento del Equipo MSPI	Matrices con inventario y clasificación de activos de información Reporte de datos personales Publicación de activos de información
	Adopción y adaptación de metodología de evaluación de riesgos	1/05/2022	1/08/2022	Equipo MSPI	Metodología de Evaluación de riesgos con matriz de riesgos Formularios de evaluación de riesgos en Almera
	Identificación y valoración de riesgos de seguridad y privacidad de la información	1/06/2022	1/08/2022	Equipo MSPI	Matriz de evaluación de riesgos Publicación de resultados de evaluación de riesgos Comunicación interna de resultados de evaluación de riesgos

Fase	Actividad	Fecha Inicio	Fecha Fin	Responsable	Entregable
	Definición de planes de tratamiento de riesgos (PTR) de información y privacidad	1/08/2022	15/10/2022	Equipo MSPI	Plan de tratamiento de riesgos de seguridad y privacidad de la información Resolución interna con aprobación de PTR y aceptación de riesgos residuales Comunicación interna de PTR
	Definición e inicio de ejecución de plan de concientización, educación y formación en seguridad y privacidad de la información	1/10/2022	15/12/2022	Equipo MSPI Comunicaciones Talento Humano	Plan de concientización Comunicaciones internas Informe de ejecución Informe de resultados de plan de concientización
	Plan y estrategia de transición IPv4 a IPv6	15/02/2022	31/012/2022	Subproceso de Infraestructura Tecnológica	Estrategia de transición