



CORANTIOQUIA

ACTÚA

CON TRANSPARENCIA

**Formulación e Implementación del Modelo
Operativo de Tecnología acorde al Plan
Estratégico de Tecnología y Plan de
Seguridad Informática (MSPI)**

Implementación, evaluación y mejora continua del MSPI

Caracterización del documento y control de versiones

Caracterización del documento

Nombre del documento	Implementación, evaluación y mejora continua del MSPI		
Codificación		Versión	1.0
Fecha de última modificación	Diciembre 2019	Fecha de creación	Noviembre 2019
Aprobado por			

Control de versiones

Versión	Fecha	Autor	Descripción del Cambio
Inicial	Noviembre 2019	EY	Documento inicial de la implementación, evaluación y mejora continua del MSPI

Tabla de Contenido

	Introducción	4
	Antecedentes	5
	Roadmap del Modelo de Seguridad y Privacidad de la información	12
	Construcción del Modelo de Seguridad y Privacidad de la información	13
	Implementación del Modelo de Seguridad y Privacidad de la información	59
	Administración del Modelo de Seguridad y Privacidad de la información	111
	Bibliografía	119
	Apéndice 1: Glosario	124

Introducción

Con el propósito de contribuir a una estrategia a largo plazo que permita lograr la visión de la organización en un futuro y alineándose con el programa de transformación digital del Plan Nacional de Desarrollo, Corantioquia decidió realizar un estudio que permita mejorar, optimizar e implementar el modelo operativo de tecnología acorde al plan estratégico de las tecnologías y comunicaciones corporativas (PETICO) y el Plan Ambiental Regional 2020 – 2031 (PGAR).

Para lograr este objetivo, Corantioquia emprendió un proyecto en el segundo semestre del 2019 a través de la contratación de una Firma consultora externa que le apoyará en tan importante proyecto, siendo Ernst & Young (EY) el asesor estratégico seleccionado para liderar y acompañar a la Corporación en este ejercicio.

Este proyecto comprende dos alcances:

- (1) Construcción e implementación del modelo operativo de tecnología de Corantioquia alineado al PETICO
- (2) Desarrollo de las fases de implementación, evaluación y mejora continua del modelo de seguridad y privacidad de la información.

Este documento, es el resultado del alcance número 2, enmarcado dentro de las prácticas líderes y estándares internacionales que definen los requisitos para su establecimiento, implementación, mantenimiento y mejora continua, así como se encuentra alineado con la guía del Ministerio de Tecnologías de la Información y las Comunicaciones para la Seguridad de la Información en entidades públicas.



Antecedentes

Antecedentes

Ciberseguridad en Colombia

WannaCry, NotPetya, ExPetr, Stuxnet y Mirai son algunos de los ciberataques más famosos de la historia, generaron **millones de dólares de pérdidas** a empresas por todo el mundo gracias a su facilidad para expandirse rápidamente por internet. Estos también afectan las **empresas públicas y privadas de Colombia...**

WhatsApp, el más utilizado por los cibercriminales en Colombia

Según Kaspersky Lab, en el país se presentaron más de 100 millones de ataques de malware en 2019.

Colombia sufrió 42 billones de intentos de ciberataques en 3 meses

La cifra obedece al segundo trimestre del 2019 y demuestra los más altos niveles de la región.

ATAQUES A INFRAESTRUCTURAS CRÍTICAS

¿Puede un “hacker” dejar sin luz a Colombia?

Tecnología - 2 Nov 2018 - 10:00 PM
Por: Diego Ojeda / @diegoojeda95

Las infraestructuras críticas son las que proveen servicios indispensables para una sociedad, como la distribución de energía eléctrica. Camilo Gutiérrez, jefe de laboratorio de investigación de ESET, la empresa que detectó una red de ciberdelincuentes en Europa, destacó los avances del país en defensas informáticas.

TECNOLOGÍA

Colombia fue uno de los países con más ataques cibernéticos el año pasado

En 2019 se reportaron más de 28.000 casos de ciberataques en Colombia

Informe del C4 de la Policía, la CCIT y TIC1ac presenta el panorama en ciberseguridad del país.

El sector privado es el más perjudicado por ‘ransomware’

El ‘phishing’ es la técnica preferida por los criminales.

En Colombia hay 12 empresas afectadas por ciberataque mundial

De acuerdo con la firma Digiware, en Latinoamérica se han registrado 23 víctimas.

2 de cada 3 empresas fueron víctimas de un ciberataque en 2018

Informe “El rompecabezas imposible de la ciberseguridad” - Sophos

Contexto actual en materia de Seguridad de la información



Legislación regulatoria



MinTIC

Ministerio de Tecnologías
de la Información y las Comunicaciones

El Modelo de Seguridad y Privacidad de la Información – MSPI, conduce a la preservación de la **confidencialidad, integridad, disponibilidad** de la información, permitiendo garantizar la privacidad de los datos, mediante la aplicación de un proceso de gestión del riesgo, brindando confianza a las partes interesadas acerca de la adecuada gestión de riesgos.

A través del **decreto único reglamentario 1078 de 2015**, del sector de Tecnologías de Información y las Comunicaciones, se define el componente de seguridad y privacidad de la información, como parte integral de la estrategia de Gobierno Digital.

Marco Legal de Protección de la Información en Colombia

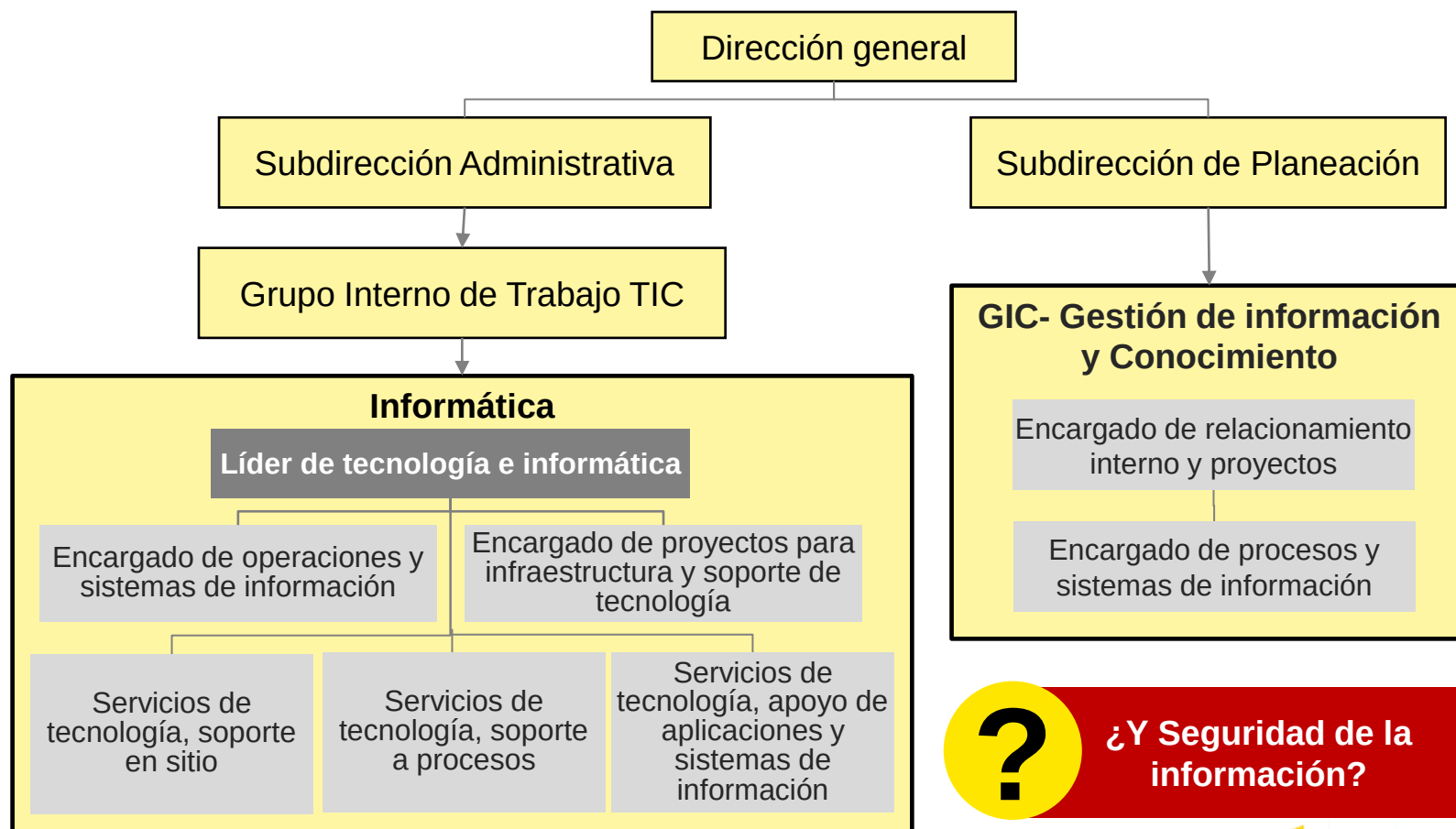


Situación actual de Seguridad de la información en Corantioquia

Estructura de TI

Mediante el **acuerdo 452 del Consejo Directivo de Corantioquia** se determinó la estructura organizacional de la Corporación y se fijaron las funciones de cada área.

El Gobierno de TI en Corantioquia está conformado por el **equipo de informática** y el **área de Gestión de la información y del conocimiento**.



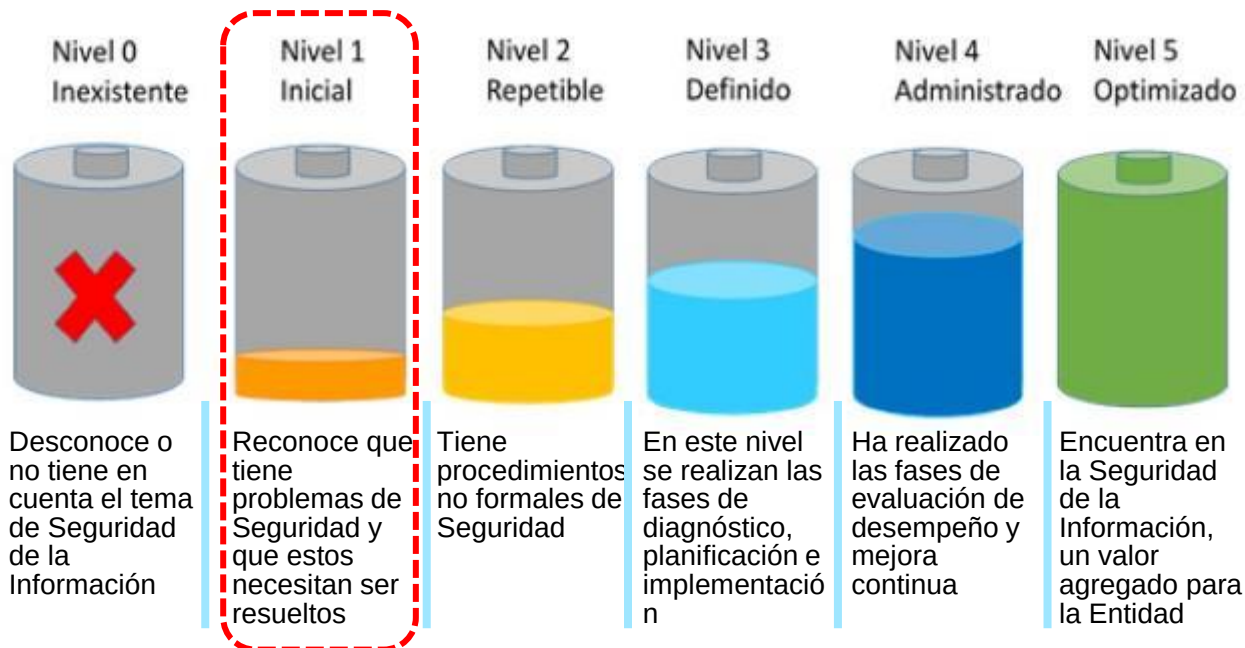
¿Y Seguridad de la información?

Situación actual de Seguridad de la información en Corantioquia

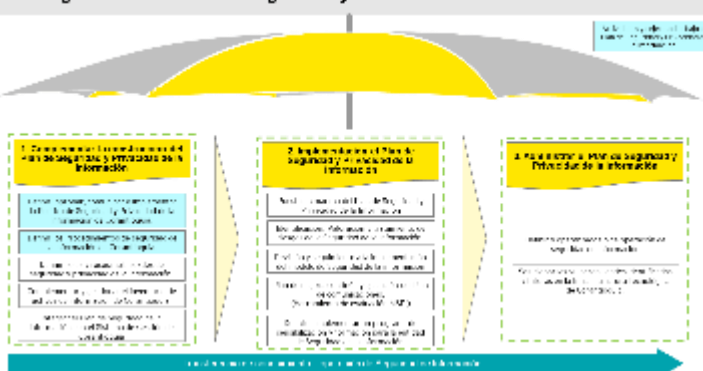
Que se ha realizado

En 2017, EY apoyo a Corantioquia en la **Formulación del Programa de Seguridad de la Información**. En el proyecto se identificaron múltiples vulnerabilidades y se planteó unas acciones requeridas por parte de Corantioquia para cerrar las brechas de seguridad de la información.

Nivel de Madurez de Corantioquia



Pasos siguientes del Plan de Seguridad y Privacidad de la Información...



Roadmap del MSPi

Definir los Procedimientos de seguridad de la información de Corantioquia.

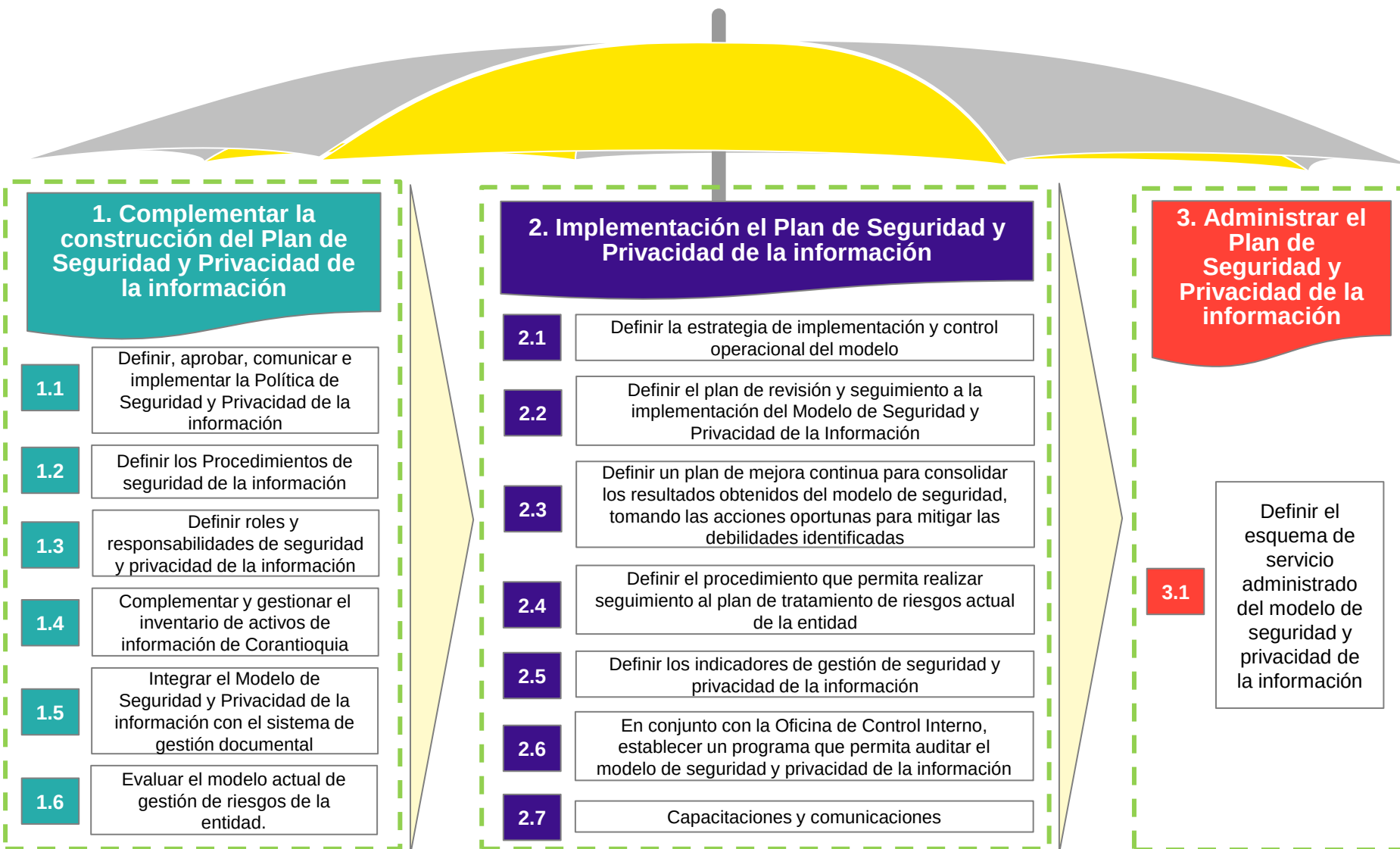
Definir, aprobar, comunicar e implementar la Política de Seguridad y Privacidad de la información de Corantioquia.

Cobertura de funciones en seguridad de la información

Basados en estándares líderes de la industria como ISO 27001, se analizó las funciones de Seguridad de la Información en Corantioquia en todos los dominios que se presentan en el Marco EY CPM (Cyber Program Management). Se evidencia que existen dominios de Seguridad de la Información que no se encuentran cubiertos con la estructura y función actual de tecnología en Corantioquia.



Roadmap del Modelo de Seguridad y Privacidad de la Información (MSPI)



A photograph of a person walking across a narrow suspension bridge made of wooden planks, surrounded by a dense green forest. The bridge is suspended by ropes and has a net-like side railing. The person is seen from behind, walking away from the camera towards the far end of the bridge where another person is visible. The forest is lush with various shades of green foliage.

1

Construcción del Modelo de Seguridad y Privacidad de la Información (MSPI)



1.1-1.2

**Políticas y procedimientos de
seguridad de la información**

Políticas y procedimientos de seguridad de la información

En el año 2018 y 2019, se ha iniciado a formular y adoptar en Corantioquia la Política General de Seguridad de la Información en la Corporación Autónoma Regional del Centro de Antioquia –CORANTIOQUIA-. a continuación se mencionan la propuesta de los artículos del acto administrativo que adopta dicha política en construcción:

Artículo 1º. Objeto: Adoptar en la Corporación Autónoma Regional del Centro de Antioquia CORANTIOQUIA, la Política General de Seguridad y Privacidad de la Información, en cumplimiento del numeral 5.2 de la Norma ISO/IEC 27001:2013 como norma fundamental para el desarrollo de proyectos de tecnología con una gestión eficiente y optimización de los recursos, servicios TIC, y los sistemas de información.

Artículo 2º. Ámbito de aplicación: La política aplica a los servidores públicos, contratistas, proveedores y/o terceros usuarios de la información impresa, digital, y la soportada sobre las Tecnologías de la Información y las Comunicaciones de la Corporación Autónoma Regional del Centro de Antioquia CORANTIOQUIA.

Artículo 3º. Implementación: Todas las dependencias de la Corporación Autónoma Regional del Centro de Antioquia CORANTIOQUIA deberán implementar la política adoptada a través del presente acto administrativo, conforme a sus responsabilidades y competencias.

Artículo 4º. Vigencia: La presente Resolución rige a partir de la fecha de su expedición y deja sin efecto cualquiera otra contraria a estas disposiciones.



Políticas y procedimientos de seguridad de la información

Los capítulos que contiene los lineamiento de la Política General de Seguridad y Privacidad de la Información.

Procedimientos:

- 1. Capacitación y sensibilización del personal
- 2. Ingreso y desvinculación del personal
- 3. Identificación y clasificación de activos
- 4. Ingreso seguro a los sistemas de información, gestión de usuarios y contraseñas
- 5. Controles criptográficos
- 6. Gestión de llaves criptográficas
- 7. Control de acceso físico
- 8. Retiro de activos
- 9. Protección de activos
- 10. Mantenimiento de equipos
- 11. Gestión de cambios
- 12. Gestión de capacidad
- 13. Separación de ambientes
- 14. Protección contra códigos maliciosos
- 15. Aseguramiento de servicios en la red
- 16. Transferencia de información
- 17. Tratamiento de la seguridad en los acuerdos con los proveedores
- 18. Adquisición, desarrollo y mantenimiento de software
- 19. Control software
- 20. Gestión de incidentes de seguridad de la información
- 21. Gestión de la continuidad de negocio



1.3

Roles y responsabilidades

Roles y responsabilidades

Importancia de su definición en el MSPI

Cuando la entidad toma la decisión de implementar un Modelo de Seguridad de la Información como un sistema vivo, el primer paso es la **definición de una estructura organizacional con funciones y responsabilidades** para la ejecución de las actividades que esto conlleve, puesto que la designación del personal a estas tareas es necesaria a tal punto que, si no se entregan las responsabilidades para ciertos perfiles, no se obtendrá la eficacia y efectividad que se requiere.

En el momento de asumir un rol, un individuo tiene la responsabilidad de alcanzar ciertos objetivos trazados conforme a unas determinadas funciones y capacidades descritas para ello. Es así como el establecer los roles y la asignación de un responsable para **cada acción** definida dentro de la planeación de seguridad de la información en cada entidad **es un aspecto clave para el correcto funcionamiento** del Modelo de Seguridad de la Información (MSPI).

La definición de **Roles y Responsabilidades** también permite hacer una segregación de funciones que permite detectar errores involuntarios o intencionales.

Roles y responsabilidades

Equipo responsable de Seguridad de la información



Se ha sugerido, que a través de una resolución (a través de un acto administrativo) la Corporación, crea o modifica el **Equipo Responsable de Seguridad de la Información de la Entidad:**

- Líder de seguridad de la información
- Comité de seguridad de la información (CSI)
- Participantes del CSI

Para convenir de manera *Estratégica, Táctica, Operativa y de Participación*, lo concerniente a Seguridad de la Información.

En la propuesta de dicho acto administrativo, se definen los roles y las responsabilidades de seguridad de la información en su estructura organizativa. Siendo su función principal el permitir tomar las decisiones más acertadas, precisando la gestión a seguir, para la realización y el cumplimiento de los objetivos de la Corporación.

Adicional, en el primer comité de seguridad de la información, el equipo de la corporación, ha definido que se unificará dicho comité y las responsabilidades de protección de datos personales.

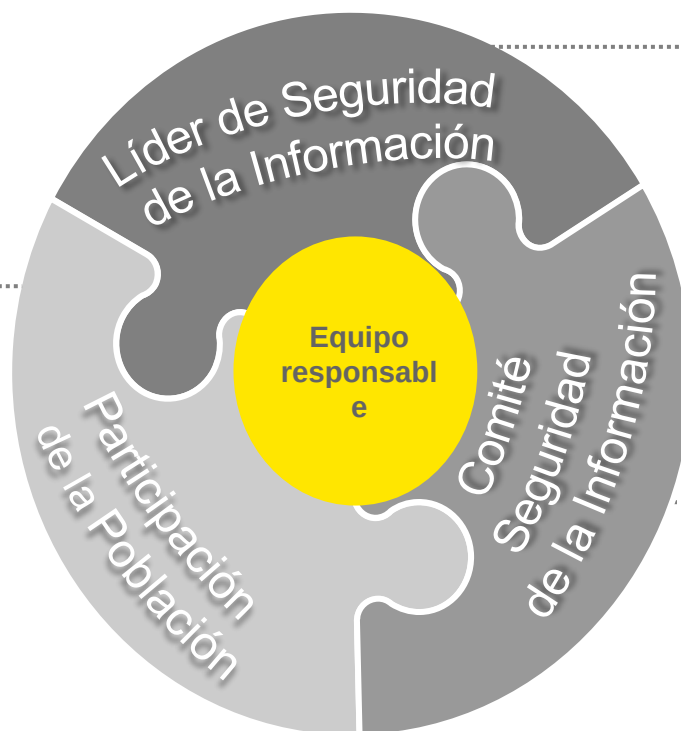
Roles y responsabilidades

Equipo responsable de Seguridad de la información (cont.)

Con el fin de poder realizar la labor de la manera más eficiente, se define el conjunto de integrantes para el equipo del comité de seguridad de la información de la Corporación, denominados de la siguiente forma:



- Funcionarios
- Contratistas
- Proveedores
- Usuarios
- Ciudadanos



Vela porque las directrices estratégicas de seguridad de la información se cumplan en la Entidad

Respaldar y apoyar las iniciativas de seguridad, avalando y definiendo las directrices estratégicas de seguridad de la información.

Roles y responsabilidades

Definición en Corantioquia

Actualmente, no existe un esquema organizativo de seguridad de la información en Corantioquia', por lo cual hemos propuesto el modelo descrito a continuación. La gestión de la Seguridad de la información no recae exclusivamente sobre el área de tecnología de una organización, por el contrario es responsabilidad de **toda la Entidad**.



Roles en

Gestión de procesos tecnológicos y de la información (GPTI)

- ▶ Líder de seguridad de la información
- ▶ Servicios e Infraestructura tecnológica
- ▶ Sistemas de información

Rol del

Comité de seguridad de la información (CSI)

- ▶ Se encontrará conformado por cada uno de los responsables de los Roles definidos para la organización y para TI. El comité será responsable de la implementación de la Estrategia de Gobierno Digital respecto a Seguridad de la información

Roles en la

Organización

- ▶ Control interno
- ▶ Planeación
- ▶ Sistema de Gestión Integral (SGI)
- ▶ Jurídica
- ▶ Talento Humano
- ▶ Comunicaciones

Roles y responsabilidades

Gobierno de TI

Líder de Seguridad de la Información

- ▶ Aplicar conocimientos, habilidades, herramientas, y técnicas a las actividades propias del proyecto, de manera que cumpla o exceda las necesidades y expectativas de los interesados en el mismo
- ▶ Identificar la brecha entre el Modelo de seguridad y privacidad de la información y la situación de la entidad.
- ▶ Generar el cronograma de la implementación del Modelo de Seguridad y privacidad de la información.
- ▶ Planear, implementar y hacer seguimiento a las tareas, fechas, costos y plan de trabajo de los objetivos específicos del cronograma definido.
- ▶ Gestionar el equipo de proyecto de la entidad, definiendo roles, responsabilidades, entregables y tiempos.
- ▶ Coordinar las actividades diarias del equipo y proporcionar apoyo administrativo
- ▶ Encarrilar el proyecto hacia el cumplimiento de la implementación del Modelo de Seguridad y privacidad de la Información para la entidad.
- ▶ Realizar un seguimiento permanente a la ejecución de los planes de trabajo, monitoreando los riesgos del proyecto para darle solución oportuna y escalar al Comité de seguridad en caso de ser necesario.
- ▶ Monitorear el estado del proyecto en términos de calidad de los productos, tiempo y los costos.
- ▶ Trabajar de manera integrada con el grupo o áreas asignadas.
- ▶ Asegurar la calidad de los entregables y del proyecto en su totalidad.
- ▶ Velar por el mantenimiento de la documentación del proyecto, su custodia y protección.
- ▶ Contribuir al enriquecimiento del esquema de gestión del conocimiento sobre el proyecto en cuanto a la documentación de las lecciones aprendidas.
- ▶ Liderar la programación de reuniones de seguimiento y velar por la actualización de los indicadores de gestión del proyecto.

Roles y responsabilidades

Gobierno de TI

Para el rol de **Líder de Seguridad de la Información** se identifican adicionalmente unas responsabilidades específicas enfocadas en **6 Dominios entregados en el Marco de arquitectura Empresarial**, propuesto por el Ministerio de Tecnologías por medio de la estrategia Gobierno Digital:

DOMINIO	RESPONSABILIDAD
SERVICIOS TECNOLÓGICOS	Liderar la gestión de riesgos de seguridad sobre la gestión de TI y de información de la institución.
	Gestionar el desarrollo e implementación de políticas, normas, directrices y procedimientos de seguridad de gestión de TI e información.
	Definir mecanismos de control y seguimiento que permitan medir el nivel de cumplimiento de implantación de las medidas de seguridad.
	Supervisar la respuesta a incidentes, así como la investigación de violaciones de la seguridad, ayudando con las cuestiones disciplinarias y legales necesarias.
	Trabajar con la alta dirección y los dueños de los procesos misionales dentro de la entidad en el desarrollo de los planes de recuperación de desastres y los planes de continuidad del negocio.
	Realizar y/o supervisar pruebas de vulnerabilidad sobre los diferentes servicios tecnológicos para detectar vulnerabilidades y oportunidades de mejora a nivel de seguridad de la información."
ESTRATEGIA TI	Definir la estrategia informática que permita lograr los objetivos y minimizar de los riesgos de la institución. Es el encargado de guiar la prestación del servicio y la adquisición de bienes y servicios relacionados y requeridos para garantizar la seguridad de la información.



Roles y responsabilidades

Gobierno de TI

DOMINIO	RESPONSABILIDAD
GOBIERNO TI	Seguir y controlar la estrategia de TI, que permita el logro de los objetivos y la minimización de los riesgos del componente de TI. Encargado monitorear y gestionar la prestación del servicio y la adquisición de bienes y/o servicios relacionados y requeridos para garantizar la seguridad de información.
SISTEMAS DE INFORMACIÓN	Establecer los requerimientos mínimos de seguridad que deberán cumplir los sistemas de información a desarrollar, actualizar o adquirir dentro de la entidad.
	Apoyar la implementación segura de los sistemas de información, de acuerdo con el modelo de seguridad y privacidad de la información del estado colombiano.
	Desarrollar pruebas periódicas de vulnerabilidad sobre los diferentes sistemas de información para detectar vulnerabilidades y oportunidades de mejora a nivel de seguridad de la información.
	Liderar el proceso de gestión de incidentes de seguridad así como la posterior investigación de dichos eventos para determinar causas, posibles responsables y recomendaciones de mejora para los sistemas afectados.
	Trabajar con la alta dirección y los dueños de los procesos misionales dentro de la entidad en el desarrollo de los planes de recuperación de desastres y los planes de continuidad del negocio.
DE INFORMACIÓN	Supervisar que se garantice la confidencialidad, integridad y disponibilidad de la información a través de los distintos componentes de información implementados.
	Verificar el cumplimiento de las obligaciones legales y regulatorias del estado relacionadas con la seguridad de la información.

Roles y responsabilidades

Gobierno de TI

DOMINIO	RESPONSABILIDAD
USO Y APROPIACIÓN	Desarrollar el plan de formación y sensibilización de la entidad incorporando el componente de seguridad de la información en diferentes niveles.
	Supervisar los resultados del plan de formación y sensibilización establecido para la entidad, con el fin de identificar oportunidades de mejora.
	Participar en la elaboración de los planes de gestión de cambio, garantizando la inclusión del componente de seguridad de la información en la implementación de los proyectos de TI.



Roles y responsabilidades

Gobierno de TI

Servicios e Infraestructura tecnológica

- ▶ Proporcionar concepto y liderar el aseguramiento, a nivel de seguridad de la información, para la implementación de los componentes pertenecientes a los servicios e infraestructura tecnológica: sistemas operativos, redes, infraestructura de comunicaciones, servidores y bases de datos, gestionando la capacidad y disponibilidad requerida.
- ▶ Planear, coordinar y administrar procesos que afiancen los servicios de seguridad de la información. Siendo multiplicador de la cultura de la seguridad informática.
- ▶ Velar por el cumplimiento de seguridad y respaldo de la información proponiendo y desarrollando técnicas de ejecución, monitoreo y respaldo para clientes internos.
- ▶ Garantizar el correcto funcionamiento en disponibilidad, operatividad, confiabilidad e integridad de los sistemas de información, servicios y aplicaciones que se encuentran bajo su jurisdicción y, que respondan a las necesidades del cliente interno a nivel de hardware y/o software.

Sistemas de información

- ▶ Definir y aprobar el modelo, tipo y forma con que se debe ejecutar los mantenimientos a los equipos de cómputos y equipos de telecomunicaciones que hace parte de la infraestructura tecnológica de la entidad.
- ▶ Aplicar conocimientos metodológicos para el desarrollo, ejecución e implementación que se requiera para los servicios e infraestructura tecnológica de la Corporación, salvaguardando el flujo operacional en la misma.

Roles y responsabilidades

Gobierno de TI

Servicios e Infraestructura tecnológica

- ▶ Diseño, evaluación, implementación, coordinación y desarrollo de planes estratégicos, de seguridad, de gestión de riesgo y de gestión de proveedores de Tecnologías de la Información.
- ▶ Liderar, proveer concepto y velar porque los flujos de los procesos se encuentren acordes a los lineamientos de seguridad de la entidad, mediante el control y seguimiento en todos los niveles: misionales, estratégicos y de apoyo.
- ▶ Investigar, analizar, planear e implementar soluciones en situaciones donde se presente casos de riesgo y/o vulnerabilidades a los sistemas de información de la entidad.
- ▶ Establecer planes que impliquen técnicas y herramientas forenses digitales en la recuperación de datos en los sistemas de información, o cuando se requiera de evidencia digital (identificación de fraude u otro).

Sistemas de información

- ▶ Guiar en la gestión de herramientas informáticas y analíticas de datos de la entidad.
- ▶ Asegurar un alto nivel de seguridad en los sistemas de información, plataformas y recursos tecnológicos. Preservando la seguridad de la información y las comunicaciones, identificando y tomando medidas.
- ▶ Proveer el concepto si se debe realizar alguna modificación a los estándares definidos en el SGSI de la Corporación.
- ▶ Apoyar la implementación, monitoreo y funcionamiento del MSPI de la entidad.
- ▶ Brindar asesoría y capacitación al personal de TIC y al personal en general, para fortalecer sus conocimientos y competencias requeridas en el SGSI.
- ▶ Valorar, supervisar y reportar resultados del SGSI a alta dirección.

Roles y responsabilidades

Comité de Seguridad de la Información (CSI)

¿Qué es el
Comité de
Seguridad de la
Información?

El Comité de Seguridad de la Información (CSI) puede entenderse como un cuerpo integrado por representantes de todas las áreas sustantivas de la organización, destinado a garantizar el apoyo manifiesto de las autoridades a las iniciativas de seguridad para lograr un trabajo eficaz y seguro.

¿Cuál es su
importancia?

El Comité deberá asegurar que exista una dirección y apoyo gerencial para soportar la administración y desarrollo de iniciativas sobre seguridad de la información, así como de la formulación y mantenimiento de una política de seguridad de la información a través de toda la Corporación.

¿Quiénes lo
conformarían?

- ▶ Líder de Seguridad de la Información
- ▶ Representante del área de Tecnología
- ▶ Representante del área de Control interno
- ▶ Representante del área de Planeación
- ▶ Representante del área de Sistema Gestión Integral (SGI)
- ▶ Representante del área Jurídica
- ▶ Representante del área de Talento humano
- ▶ Representante del área de Comunicaciones

Roles y responsabilidades

Comité de Seguridad de la Información (CSI)

Responsabilidades del Comité de Seguridad de la Información (CSI)

- ▶ Coordinar la implementación del Modelo de Seguridad y privacidad de la Información al interior de la entidad.
- ▶ Direccionar el programa integral de gestión de datos personales (PIGDP)
- ▶ Revisar los diagnósticos del estado de la seguridad de la información
- ▶ Acompañar e impulsar el desarrollo de proyectos de seguridad.
- ▶ Coordinar y dirigir acciones específicas que ayuden a proveer un ambiente seguro y establecer los recursos de información que sean consistentes con las metas y objetivos.
- ▶ Recomendar roles y responsabilidades específicos que se relacionen con la seguridad de la información.
- ▶ Aprobar el uso de metodologías y procesos específicos para la seguridad de la información.
- ▶ Participar en la formulación y evaluación de planes de acción para mitigar y/o eliminar riesgos.
- ▶ Realizar revisiones periódicas del SGSI (por lo menos una vez al año) y según los resultados de esta revisión definir las acciones pertinentes.
- ▶ Promover la difusión y sensibilización de la seguridad de la información dentro de la entidad.
- ▶ Poner en conocimiento de la entidad, los documentos generados al interior del comité de seguridad de la información que impacten de manera transversal a la misma.
- ▶ Las demás funciones inherentes a la naturaleza del Comité.

Roles y responsabilidades

Organización

Control interno

Con el propósito que haya fiabilidad, transparencia y cumplimiento normativo de la información, Control Interno en materia de Seguridad de la Información aportará en:

Planeación

- ▶ Realizar revisión y control a las acciones que constituya seguridad de la información, dando cumplimiento con las políticas y normas.
- ▶ Aportar en la definición y construcción de un ambiente de control, en el ámbito de seguridad de la información, donde las normas, los procesos y las estructuras se lleven acabo.
- ▶ Nutrir los componentes de la información y la comunicación al interior de la entidad, de manera que ésta se dé de manera continua, fluida, compartida y que se pueda adquirir la información necesaria.
- ▶ Ejecutar auditoría interna: planes, desarrollo y subsanación de hallazgos y brechas en la seguridad de la información.
- ▶ Determinando si los componentes del Sistema de Gestión de Seguridad de la Información SGSI están presentes y funcionan correctamente, haciendo seguimiento y acompañamiento a diversas actividades de la entidad.

Sistema de Gestión Integral (SGI)

Jurídica

Talento Humano

Comunicaciones

- ▶ Control de software operacional y consideraciones sobre auditorías de sistemas de información.

Roles y responsabilidades

Organización

Control interno

Para lograr eficiencia y efectividad de las operaciones en la entidad y la seguridad de la información, desde planeación se velará por:

► Gestión y administración del PIGDP (Programa Integral de Gestión de Datos Personales)

Planeación

► Valoración y tratamiento de los riesgos de la información.

Sistema de Gestión Integral (SGI)

► Identificación y evaluación de vulnerabilidades que se presenten, o se puedan presentar, en seguridad de la información para la entidad.

► Seguridad de la información en las relaciones con los proveedores.

Jurídica

► Gestión de la prestación de servicios de funcionarios, contratistas y proveedores.

Talento Humano

► Aspectos de seguridad de la información y gestión de su continuidad: planificación, implementación, verificación, revisión, evaluación, redundancias y disponibilidad en todo el procesamiento de información.

Comunicaciones

► Consideraciones seguridad de la información para: teletrabajo, manejo de medios, derechos de propiedad intelectual, controles de acceso, seguridad de operaciones, procedimientos operacionales y responsabilidades, copias de respaldo, seguridad de las comunicaciones, gestión de la seguridad de las redes, transferencia de información, adquisición, desarrollo y mantenimientos de sistemas y, gestión de incidentes de seguridad de la información.

Roles y responsabilidades

Organización

Control interno

El SGI se permitirá la definición e implementación de lineamientos que aporten a la seguridad de la información, con el fin de alcanzar los objetivos, de acuerdo a estándares adoptados:

Planeación

- ▶ Procedimientos de control documental del MSPI, que incluya políticas y organización de la seguridad de la información.
- ▶ Tratamiento de temas de seguridad y privacidad de la información en los comités del modelo integrado de gestión, o en los comités directivos interdisciplinarios de la entidad.
- ▶ En base en el inventario de activos de información clasificado, se establece la caracterización de cada uno de los sistemas de información.
- ▶ La entidad conoce su papel dentro del estado Colombiano, identifica y comunica a las partes interesadas la infraestructura crítica.
- ▶ Las prioridades relacionadas con la misión, objetivos y actividades de la Entidad son establecidas y comunicadas.
- ▶ Toma de conciencia, educación y formación en la seguridad de la información que implique al SGSI como transversal a cualquier tema.
- ▶ Indicadores de gestión del MSPI para seguridad de la información.

Sistema de Gestión Integral (SGI)

Jurídica

Talento Humano

Comunicaciones

Roles y responsabilidades

Organización

Control interno

Toda gestión en relación a la seguridad de la información y que haga parte del SGSI, debe protegerse y, asegurar el acogimiento a lo reglamentario, conforme a las normatividad vigente para entidades públicas:

Planeación

- ▶ Adopción y cumplimiento de políticas del Gobierno Nacional en seguridad de la información para entidades públicas.
- ▶ Procedimientos operacionales y de gestión en el marco de correspondencia legal de la corporación frente a las entidades control y, en cumplimiento al objeto de su razón de ser.
- ▶ Cumplimiento de requisitos legales y contractuales con los funcionarios, contratistas, proveedores, practicantes, usuarios, comunidad o cualquier otra persona sea natural o jurídica que establezca una relación con la entidad.
- ▶ Protección legal de los activos de información de la Corporación.

Sistema de Gestión Integral (SGI)

Jurídica

Talento Humano

Comunicaciones

Roles y responsabilidades

Organización

Control interno

Planeación

Sistema de Gestión Integral (SGI)

Jurídica

Talento Humano

Comunicaciones

El personal de la Corporación, indistinto de su situación contractual, la dependencia a la cual este asignado y la ejecución de sus funciones, debe tener asociado un perfil de uso, determinado por el CSI, en relación a los recursos de información, incluyendo el hardware y software que le sea asociado. El aporte del área de Talento Humano en el CSI será:

- ▶ Mantener el directorio completo y actualizado de tales perfiles.
- ▶ Selección e investigación de antecedentes del personal.
- ▶ Términos y condiciones del empleo.
- ▶ Seguridad de los recursos humanos.
- ▶ La protección de cualquier activo de información producido, usado o mantenido por el personal que se retira o cambia de rol, recae sobre la Coordinación o Subdirección del contrato. Talento humano vigilará el proceso de cambio en la protección del activo, el cual hará parte integral del procedimiento de terminación contractual o cambio de rol.

Roles y responsabilidades

Organización

Control interno

Planeación

Sistema de Gestión Integral (SGI)

Jurídica

Talento Humano

Comunicaciones

El área de comunicaciones será responsable de establecer lineamientos para la construcción y mantenimiento del plan de capacitación, sensibilización y comunicación de la seguridad de la información, para así asegurar que este, cubra en su totalidad los funcionarios de la Corporación.

Asegurando que cada uno cumpla con sus roles y responsabilidades de seguridad y privacidad de la información dentro de Corantioquia, se busca:

- ▶ Definir los temas para la capacitación en seguridad de la información, de acuerdo con el público objetivo.
- ▶ Establecer la metodología que les permita evidencias cuales son las necesidades de capacitación para la entidad.
- ▶ Construir materiales para sensibilización y entrenamiento.
- ▶ Evaluar, medir y cuantificar, si el programa implementado genera impacto en el desarrollo de las actividades de la Corporación.

Roles y responsabilidades

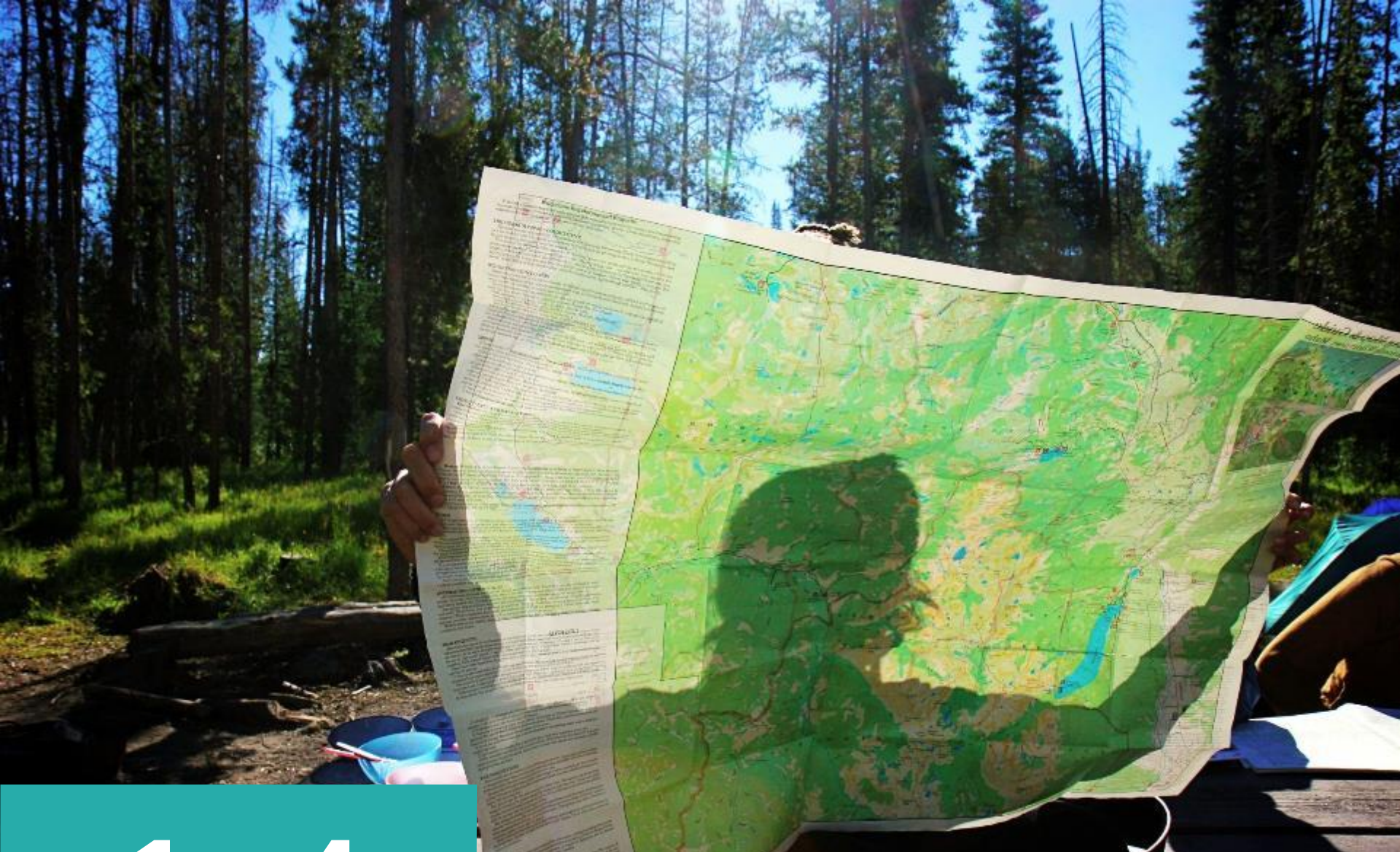
Todos los funcionarios

¿Cuál es su importancia?

Todos los funcionarios, proveedores y ciudadanos deben ser responsables del manejo adecuado de la información dentro y fuera de la Entidad, de su comunicación y divulgación, deben conocer la política general y las políticas específicas de la seguridad de la información y estar en la obligación de cumplirlas.

¿Qué responsabilidades tienen?

- ▶ Conocer, cumplir y velar por el cumplimiento de la política de seguridad de la información.
- ▶ Velar por la protección de la información que manejan en el desempeño de sus responsabilidades.
- ▶ Reportar cualquier incumplimiento de la política de seguridad de la información o cualquier evento o situación relacionada incidentes de seguridad de la información de la empresa o sus clientes.
- ▶ Comunicar periódicamente al propietario del activo para reportes de los resultados de la aplicación de los controles.
- ▶ Hacer cumplir las políticas de uso aceptable de activos.



1.4

Inventario de Activos de Información

Inventario de activos de información

¿Qué es un activo de información?

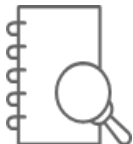


Activo de información

“Es el elemento de información que la entidad recibe o produce en el ejercicio de sus funciones. Incluye la información que se encuentre presente en forma impresa, escrita, en papel, transmitida por cualquier medio electrónico o almacenado en equipos de cómputo, incluyendo software, hardware, recurso humano, datos contenidos en registros, archivos, bases de datos, videos e imágenes.”

Inventario de activos de información

¿Qué tipos de activos de información existen?



Información

Toda información física o digital, en cualquier formato, que se genera, recoge, gestiona, transmite y destruye en la entidad. Ejemplos: Bases de datos de cualquier índole, contratos, manuales de usuario, procedimientos, informes de auditoría, código desarrollo, documentos y carpetas de documentos relativos a las investigaciones, procedimientos, guías, protocolos, archivos de audio, entre otros.



Software

Aplicaciones o programas Informáticos que se utilizan para la gestión de la información y servicios. Ejemplo: Aplicaciones del negocio, sistemas operativos, herramientas de desarrollo, motor de bases de datos, controladores de dispositivos, herramientas ofimáticas, antivirus, software de diseño y programación, compiladores, entre otros.



Hardware

Son elementos y equipos electrónicos que almacenan y soportan el procesamiento de la información digital. Ejemplo: Servidores, equipos de cómputo de escritorio, equipos de cómputo portátiles, dispositivos móviles, memorias, discos duros, entre otros.

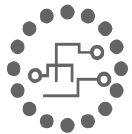


Infraestructura física

Hace referencia a las locaciones físicas o instalaciones dentro de las cuales se procesa la información que soporta el funcionamiento de la entidad. Ejemplo: edificios, centros de datos, centros de cableado etc.

Inventario de activos de información

¿Qué tipos de activos de información existen? (cont.)



Redes

Comprende todos los medios y equipos de telecomunicaciones de interconexión de elementos electrónicos y computadores físicamente separados, interconectando física y remotamente los equipos de cómputo y/o sistemas de información. Ejemplo: Switches, Hubs, Firewall; también Servicios de computación y comunicaciones como: Internet, páginas de consulta, directorios compartidos, etc.



Servicios tercerizados

Corresponde a toda aquella información, software, hardware, infraestructura física, redes y personas que no pertenecen a la nómina de la entidad, y que sus actividades dentro de la corporación representa una relevancia significativa de la gestión de información dentro de los parámetros de Seguridad y Privacidad de la información.



Personas

Personas que por su conocimiento, experiencia e importancia son consideradas activos de información. En esencia quienes manejan información o elementos sensibles, datos personales, personas que administran elementos o información que no está documentada con procesos, procedimientos, guías, instructivos u otros. Ejemplo: Contralor (a) general, Administrador de bases de datos, etc.

Inventario de activos de información

Beneficios

Costos

- Confirmar las prioridades de disponibilidad, confidencialidad e integridad de la información de las dependencias.
- Identificar de forma ágil los incidentes relacionados con la gestión de activos de información, reduciendo tiempos de respuesta.

Riesgo y regulaciones

- Demostrar la existencia de un inventario de activos de información que incorpora elementos de clasificación de activos de información en función de su confidencialidad.
- Establecer instancias claras de supervisión y el seguimiento sobre la ejecución de las políticas y estándares de relacionados con la gestión de activos de información.
- Habilitar el desarrollo seguro de las operaciones de la organización.

Eficiencia

- Reducir los re-procesos de negocio al usar una terminología común en la gestión de activos de información.
- Identificar claramente a los responsables de cada uno de los activos de información.
- Alinear los conceptos del Gobierno de datos con la gestión de activos de información, con el fin de realizar un análisis detallado de impactos y dependencias entre dominios de información y activos de información.
- Facilitar la gestión de incidentes sobre activos de información, mediante la definición de procedimientos estándar.

Inventario de activos de información

Resultados

Entendiendo la importancia y la regulación aplicable a Corantioquia, se realizó un proceso de levantamiento del inventario de activos de información, proceso que incluyó talleres y espacios personalizados para la solución de inquietudes y validaciones requeridas sobre los activos de información. Para lograr el objetivo, se trabajó en conjunto con todas las dependencias de la Corporación:

No.	Dependencia
1	Dirección General
2	Oficina Asesora de Comunicaciones
3	Oficina de Control Interno
4	Subdirección de Planeación
5	Subdirección Financiera
6	Secretaría General
7	Oficina de Gestión Jurídico Ambiental
8	Subdirección de Gestión Ambiental
9	Subdirección de Ecosistemas
10	Subdirección de Cultura Ambiental
11	Subdirección Administrativa
12	Subdirección de Regionalización
13	Oficina Territorial Aburrá Norte en Medellín y Sede Local en Bello
14	Oficina Territorial Aburrá Sur en Medellín y Sede Local en Caldas
15	Oficina Territorial Cartama en Jericó
16	Oficina Territorial Citará en Andes
17	Oficina Territorial Hevéxicos en Santa Fe de Antioquia
18	Oficina Territorial Panzenú en Cauca y Sede Local en el Bagre
19	Oficina Territorial Tahamíes en Santa Rosa de Osos y Sede Local en San Andrés de Cuerquia
20	Oficina Territorial Zenufaná en Vegachí y Sede Local en Puerto Berrío

Con corte al 29 de noviembre de 2019, no se recibieron los activos de información de la Subdirección de Cultura Ambiental y el Grupo Interno de Trabajo TIC de la subdirección Administrativa

Inventario de activos de información

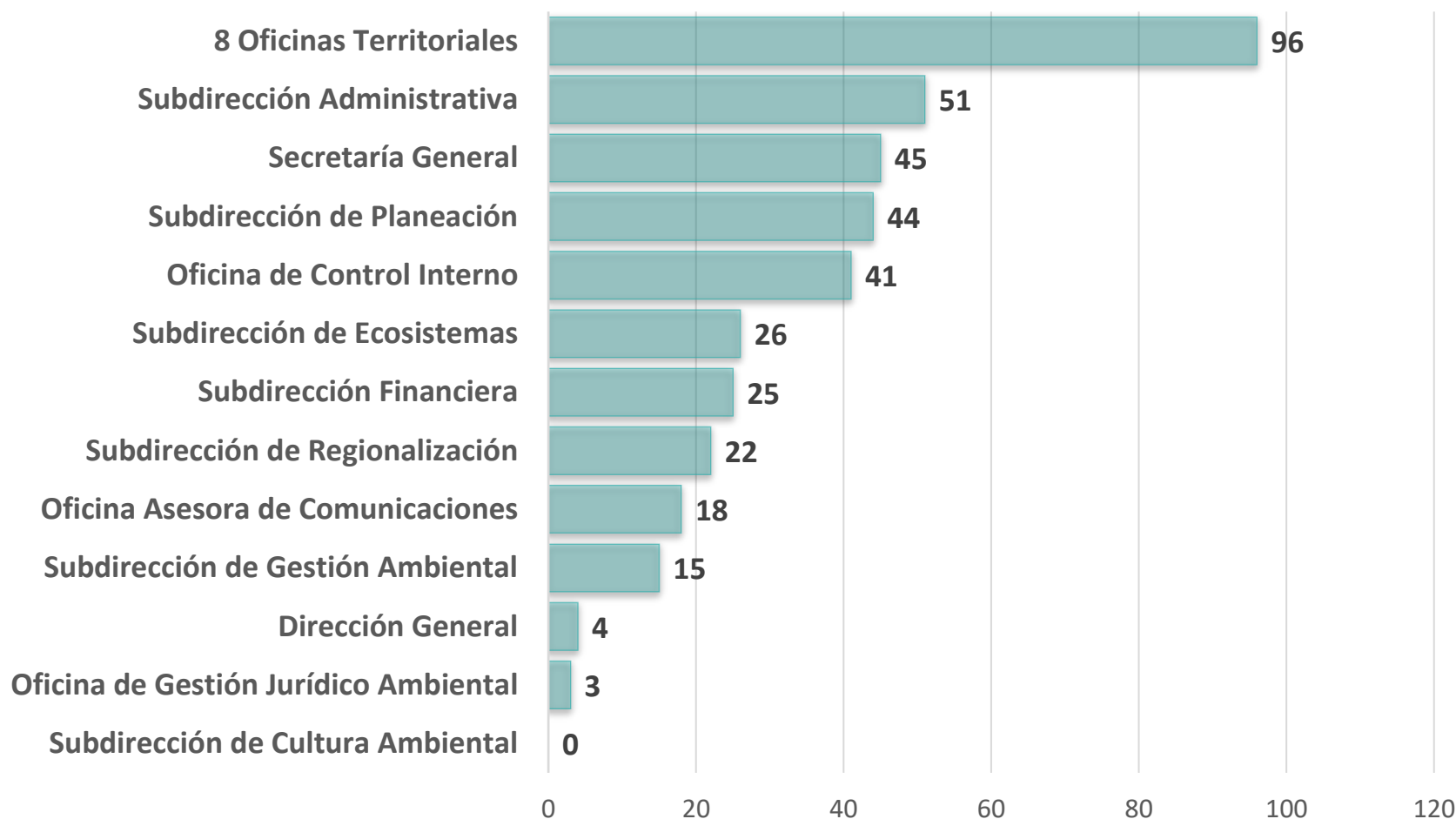
Resultados

20

Dependencias identificaron
activos de información

390

Activos de información identificados
para CORANTIOQUIA (corte al 29 Nov
2019)



Inventario de activos de información

Resultados

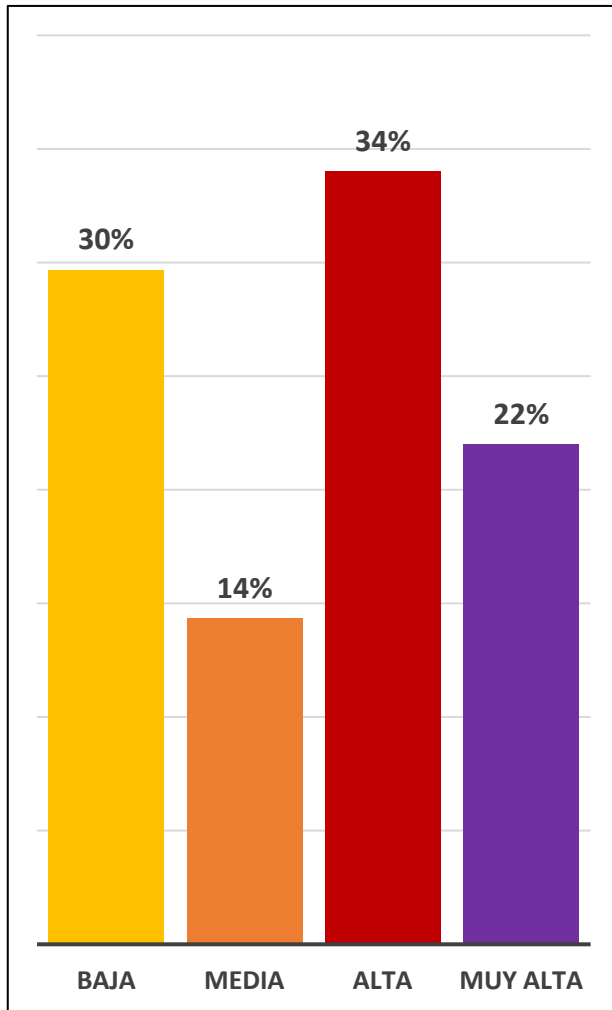


Gráfico. Clasificación en Disponibilidad de los Activos de Información CORANTIOQUIA

Disponibilidad de la información

Es la propiedad que posee la información para ser accesible y utilizable por solicitud de un individuo, entidad o proceso debidamente autorizado.

En CORANTIOQUIA la disponibilidad de la información se realiza con respecto a la disposición de la información para quienes deben acceder a ella (personas, procesos, aplicaciones u otros autorizados), comparado con el efecto que se genera para la entidad cuando el activo de información no puede estar disponible al momento de requerirse.

Valoración cualitativa	Descripción
Baja	Información cuya imposibilidad de acceso no afecta en forma significativa la operación de la entidad y puede no estar disponible más de una semana.
Media	Información cuya imposibilidad de acceso por un periodo de entre 3 y 7 días puede ocasionar pérdidas o sanciones la entidad.
Alta	Información cuya imposibilidad de acceso por un periodo entre 1 y 3 días ocasiona pérdidas significativas o sanciones a la entidad.
Muy Alta	Información cuya imposibilidad de acceso por menos de 1 día ocasiona pérdidas muy significativas o sanciones a la entidad.

Tabla. Valoración de seguridad de la Información para la DISPONIBILIDAD del Activo de Información

Inventario de activos de información

Resultados

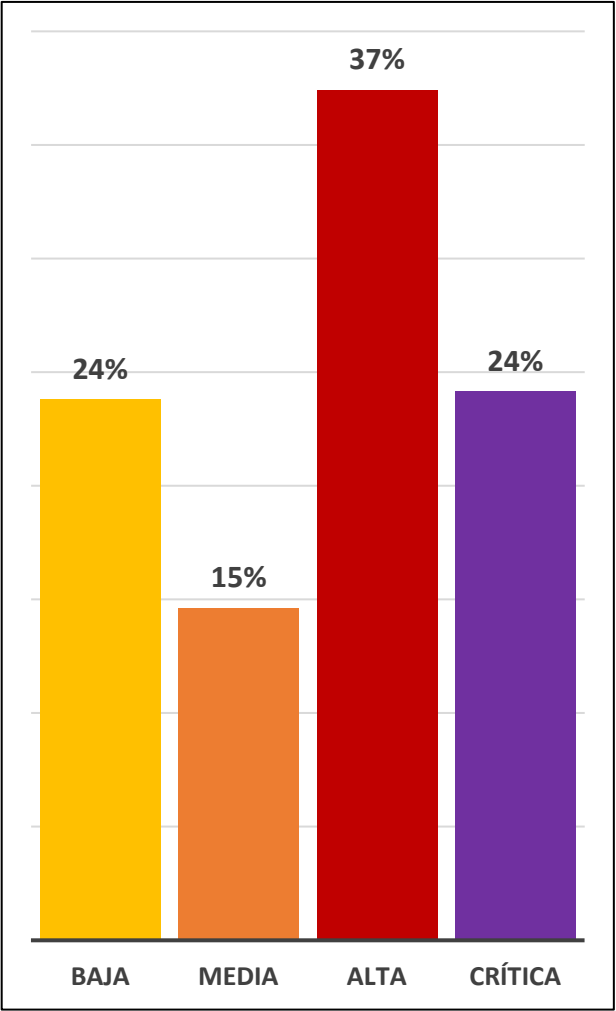


Gráfico. Clasificación en Integridad de los Activos de Información CORANTIOQUIA

Integridad de la información

Es la propiedad de salvaguardar la exactitud y completitud de los activos de información. En CORANTIOQUIA la integridad de la información se realiza con respecto al efecto de la modificación no autorizada de los datos del activo de información, el impacto que tendría la modificación no autorizada en los procesos donde se encuentra involucrado y a su vez que consecuencias tendría para la entidad.

Valoración cualitativa	Descripción
Baja	Información cuya modificación no autorizada, pérdida de exactitud y completitud puede repararse. Se afecta solo una parte del proceso y no hay pérdida económica.
Media	Información cuya modificación no autorizada, pérdida de exactitud y completitud podría repararse parcialmente, puede conllevar a un impacto negativo de índole legal, se afectan varios procesos generando retrasos en las actividades y los daños implican pérdidas económicas moderadas.
Alta	Información cuya modificación no autorizada, causa pérdida de exactitud y/o completitud, podría no repararse completamente, se afectan varios procesos misionales generando un impacto negativo de índole legal y/o pérdidas económicas y se retrasan las funciones de la entidad.
Crítica	Información cuya modificación no autorizada, causa pérdida de exactitud y completitud la información, podría no repararse completamente, afecta a toda la organización generando un impacto negativo de índole legal y económico, retrasa las funciones, y los daños son casi irreparables.

Tabla. Valoración de seguridad de la Información para la INTEGRIDAD del Activo de Información

Inventario de activos de información

Resultados

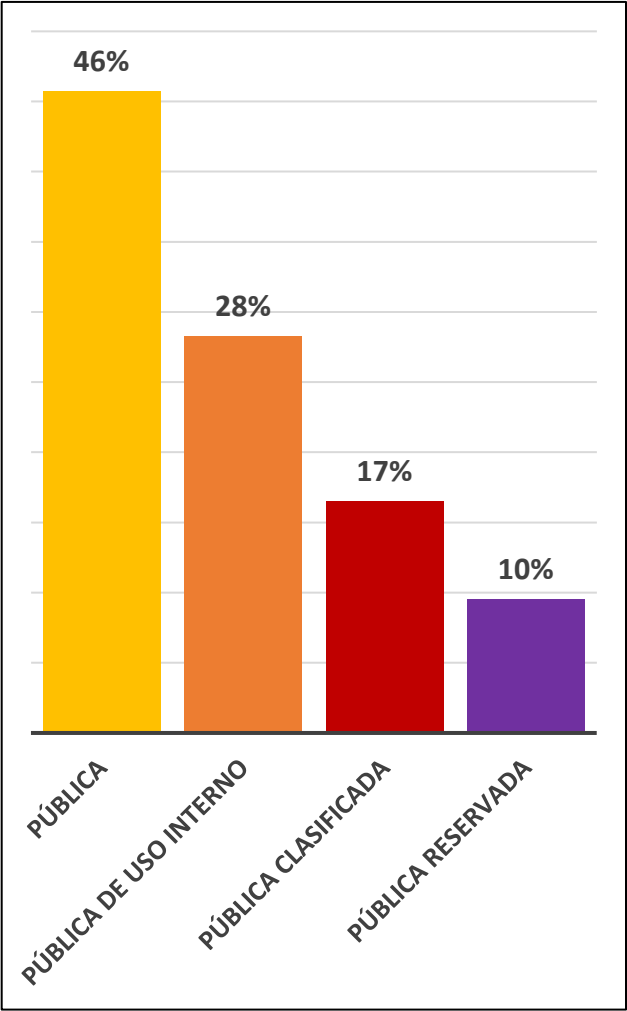


Gráfico. Clasificación en Confidencialidad de los Activos de Información CORANTIOQUIA

Confidencialidad de la información

Es la propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

En CORANTIOQUIA la confidencialidad de la información se realiza con respecto al acceso autorizado teniendo en cuenta el marco legal y regulatorio aplicable y el impacto que tendría el incumplimiento de esta condición.

Valoración cualitativa	Descripción
Pública	Es toda información que ha sido declarada de acceso público, de acuerdo con las normas existentes por la persona o grupo de personas de la Entidad responsables del activo de información y que por lo tanto no tienen requerimientos de seguridad frente a la Confidencialidad.
Pública de uso interno	Es toda información que puede ser conocida y utilizada por todos los funcionarios de la entidad, puede ser divulgada a algunas entidades externas debidamente autorizadas por el propietario, puede encontrarse en proceso de construcción y no requiere su divulgación a terceros, pero es necesaria para las actividades internas de la Entidad, y cuya divulgación y uso no autorizados podría ocasionar riesgos o pérdidas leves para la entidad.
Pública clasificada	Como lo prescribe la Ley 1712 de 2014, información pública clasificada es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al propio, particular y privado o semiprivado de una persona.
Pública reservada	En los términos de la Ley 1712 de 2014, la información pública reservada es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la ley 1712 de 2014.

Tabla. Valoración de seguridad de la Información para la CONFIDENCIALIDAD del Activo de Información

Inventario de activos de información

Resultados

Criticidad del Activo de Información

Este es un indicador proporcional al riesgo, medido conforme a la importancia del mismo para la dependencia/entidad. Ayuda a construir primacías en los procesos, sistemas, equipos y cualquier otro componente del cual haga parte el Activo de Información. Permite brindar concepto para direccionar recursos y elementos de áreas, con un valor preponderante y fundamental que permita la toma de decisiones acertadas, efectivas y, que garanticen la disponibilidad, confidencialidad e integridad del activo, como también la administración y gestión de los riesgos asociados al mismo.

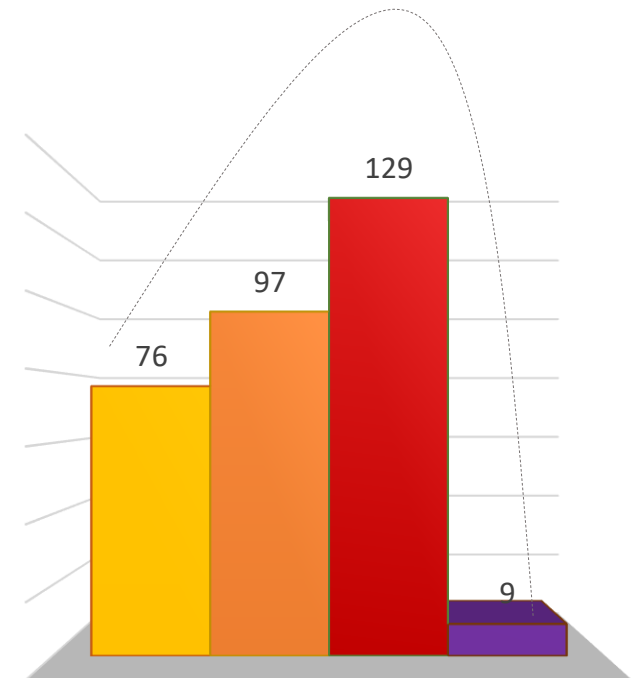
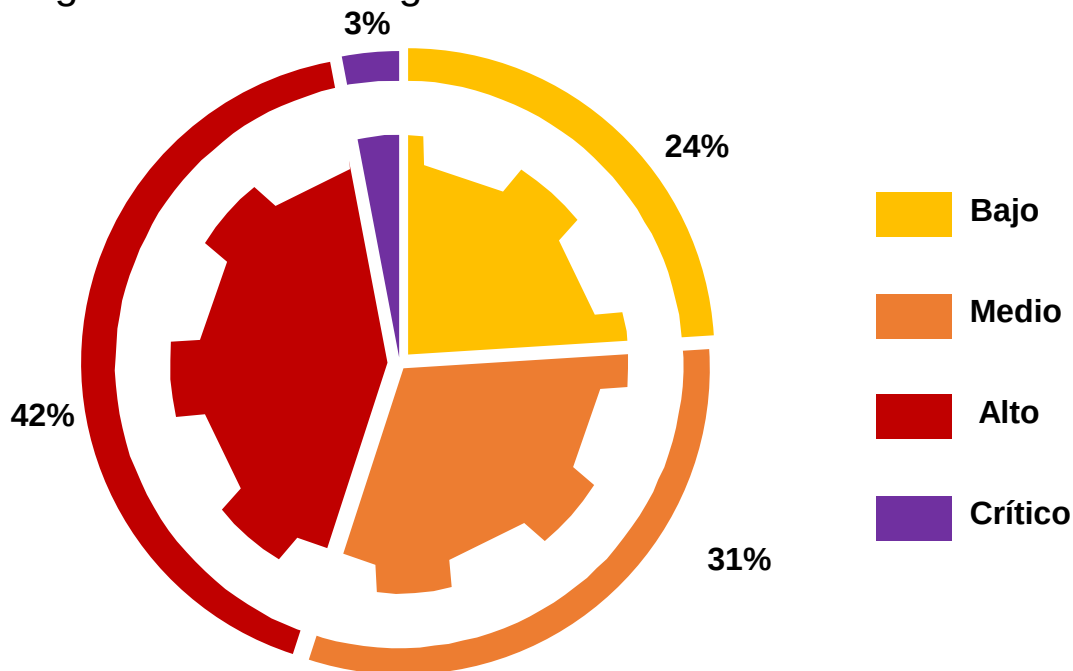


Tabla. Relación de Activos de Información valorados según su Criticidad para la Corporación.

Inventario de activos de información

Resultados

Cantidad de Activos reportados y valorados por dependencias

 Crítico
  Alto
  Medio
  Bajo

DEPENDENCIA	ACTIVO
Subdirección Financiera	1
Subdirección de Gestión Ambiental	2
Subdirección Administrativa	6
TOTAL	9

DEPENDENCIA	ACTIVO
Oficina Asesora de Comunicaciones	1
Todas las dependencias	1
Subdirección de Gestión Ambiental	3
Oficinas Territoriales	4
Subdirección de Ecosistemas	4
Subdirección de Regionalización	7
Secretaría General	14
Subdirección Financiera	14
Subdirección de Planeación	15
Oficina de Control Interno	24
Subdirección Administrativa	42
TOTAL	129

DEPENDENCIA	ACTIVO
Subdirección de Regionalización	1
Todas las dependencias	1
Oficina Asesora de Comunicaciones	3
Subdirección Administrativa	3
Procesos Disciplinarios	4
Subdirección de Ecosistemas	5
Oficinas Territoriales	6
Subdirección de Gestión Ambiental	6
Subdirección Financiera	7
Oficina de Control Interno	15
Secretaría General	22
Subdirección de Planeación	24
TOTAL	97

DEPENDENCIA	ACTIVO
Subdirección de Planeación	2
Subdirección de Regionalización	2
Subdirección Financiera	3
Subdirección de Gestión Ambiental	4
Secretaría General	9
Oficina Asesora de Comunicaciones	14
Subdirección de Ecosistemas	16
Oficinas Territoriales	26
TOTAL	76

Inventario de activos de información

Próximos pasos

Con base en los resultados anteriores, la Corporación contará con los insumos necesarios para conocer en detalle cuales son los activos de información más críticos, esto, con el fin de ser una herramienta clave para los demás componentes del Modelo de Seguridad y Privacidad de la Información.

La gestión del inventario de activos de información debe ser un trabajo en constante actualización, responsabilidad definida de acuerdo a los Roles y responsabilidades definidos en el MSPI. La periodicidad de la actualización debe ser definida por la Corporación de acuerdo a la dinámica que se evidencie que se presente respecto a los Activos de Información. Esta actualización corresponderá a las mismas etapas utilizadas en el levantamiento inicial: Definición, revisión, actualización y publicación.





1.5

**Integración del MSPI con el
Sistema de gestión documental**

Integración del MSPI con el Sistema de gestión documental

Definiciones y conceptos

¿Qué son las Tablas de Retención Documental (TRD)?

De acuerdo con el MinTIC, “constituyen un instrumento archivístico que permite la clasificación documental de la entidad acorde a su estructura orgánico - funcional, e indica los criterios de retención y disposición final resultante de la valoración documental por cada una de las agrupaciones documentales.”

¿Cómo se integra el MSPI y el Sistema de gestión documental?

La integración del MSPI a través de su componente de Inventario de Activos de Información permite integrar con el Sistema de gestión documental a través de las Tablas de Retención Documental, ya que de acuerdo a la **Ley 1712 de 2014**, en el **artículo 13** describe que: “(...) Todo sujeto obligado deberá asegurarse de que sus **Registros de Activos de Información** cumplan con los estándares establecidos por el Ministerio Público y con aquellos dictados por el Archivo General de la Nación, en relación a la constitución de las **Tablas de Retención Documental (TRD)** y los inventarios documentales.”

Integración del MSPI con el Sistema de gestión documental

Metodología

Basados en lo anterior, se construyó un documento que permita realizar la trazabilidad entre el **Inventario de activos de información** y las **Tablas de retención documental** de una manera clara y sencilla, tomando como identificadores el código de la Serie/Subserie y el número consecutivo, respectivamente.

Integración del MSPI con el Sistema de Gestión Documental							
Tabla de retención documental						Inventario de activos de información	
Unidad Administrativa	Oficina Productora	Codigo			Serie/Subserie	Número consecutivo	Identificador mnemotécnico
		D	S	SB			
DIRECCIÓN GENERAL	Dirección General	040	14		DERECHOS DE PETICIÓN	25	TRD-040-14

Información perteneciente a las Tablas de Retención Documental de Corantioquia (F-GIC-28, versión 4)

Información perteneciente al Inventario Consolidado de Activos de Información de la Corporación

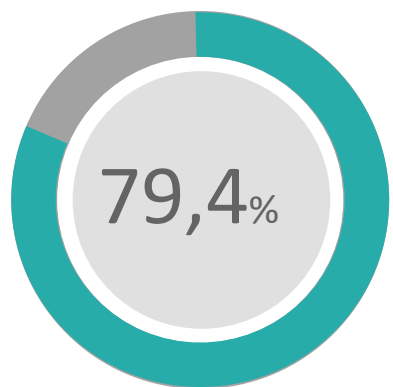
* El documento completo se presenta en el **Anexo 4**

Integración del MSPI con el Sistema de gestión documental

Resultados

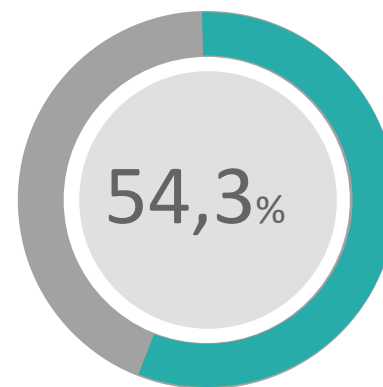
Si bien el resultado ideal de la integración del MSPI con el Sistema de gestión integral sería la trazabilidad del 100% de las Tablas de Retención Documental (TRD) en el Inventario de activos de información, la realidad actual de la entidad genera que esta totalidad no sea alcanzable, pues las TRD se encuentran desactualizadas y la entidad en el momento se encuentra trabajando en una nueva versión (versión 5).

En el momento en que estas nuevas TRD sean publicadas, se ve la necesidad de que la Corporación realice la actualización del Inventario de activos de información y la integración que se realiza entre estos dos elementos.



201 de las **253**

Series/Subseries se encuentran integrados con el Inventario de Activos de Información



De **370** activos de información,

201 pertenecen a Series/Subseries de las TRD



1.6

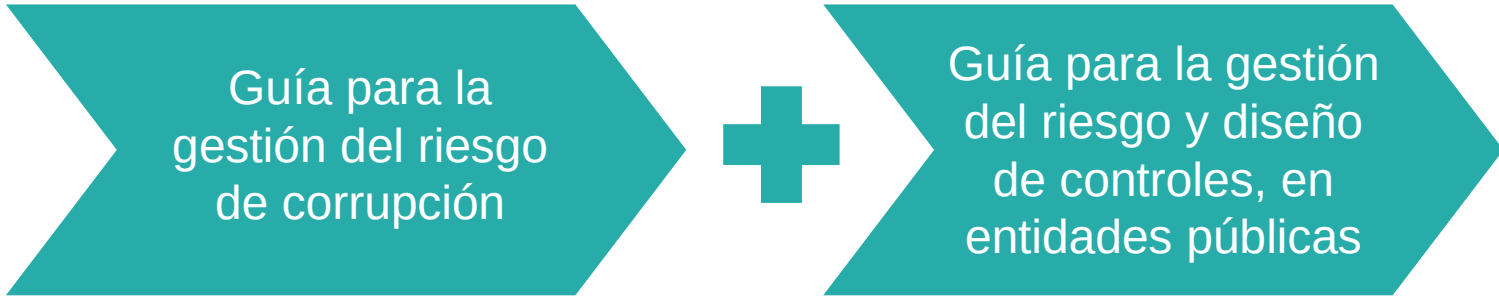
Evaluación al modelo de gestión de riesgos

Evaluación al modelo de gestión de riesgos

El Procedimiento de identificación, valoración del riesgo y controles definido en Corantioquia define desde la clasificación del riesgo identificado, la valoración de los riesgos y los controles, hasta monitoreo y revisión de la eficacia de los controles propuestos.

Dicha metodología se basa en los parámetros establecidos en las Guías: Gestión de riesgo corrupción y Gestión del riesgo y diseño de controles, en entidades públicas.

Procedimiento actual de identificación, valoración del riesgo y controles en Corantioquia (2019)



Guía para la
gestión del riesgo
de corrupción



Guía para la gestión
del riesgo y diseño
de controles, en
entidades públicas

Evaluación al modelo de gestión de riesgos

El Procedimiento de identificación, valoración del riesgo y controles define 18 tareas que buscan detallar metodológicamente los pasos a seguir para lograr una identificación correcta y unificada de los riesgos de la Corporación

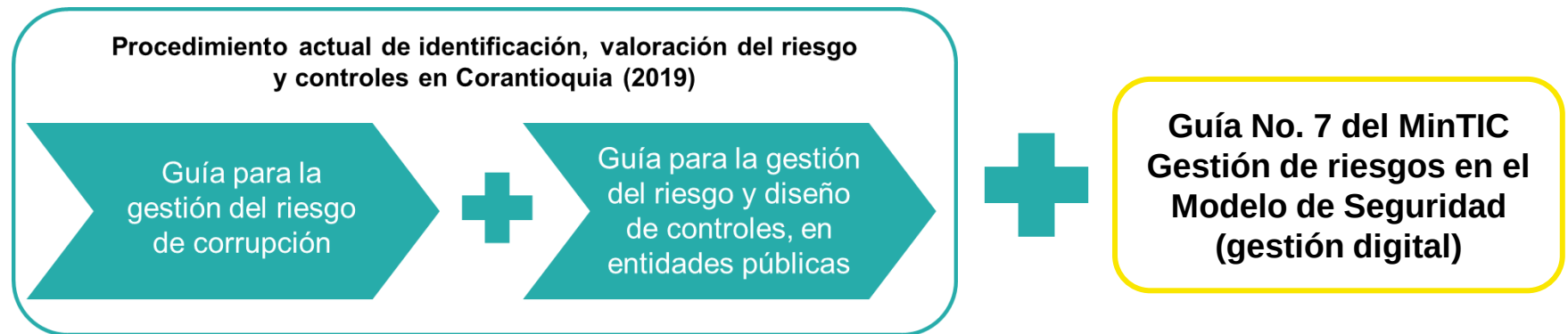
1. Identificar los riesgos generados de las actividades Corporativas
2. Clasificar el tipo de riesgo identificado, (De corrupción, De Gestión, De seguridad de la información o Transversal)
3. Seleccionar los procesos corporativos en los cuales se puede presentar el riesgo identificado
4. Asignar un nombre al riesgo identificado y describir brevemente en que consiste el riesgo identificado
5. Definir el medio, circunstancia, situación o agente generador del riesgo
6. Identificar cuáles con las consecuencias o efectos ocasionados por la ocurrencia de un riesgo que afecta el cumplimiento de los objetivos
7. Analizar el riesgo bajo las variables establecidas por la Corporación (Probabilidad e Impacto)
8. Describir el control que aplique según el riesgo identificado
9. Seleccionar uno o varios tipos de control a aplicar, en coherencia al control descrito
10. Analizar y evaluar los controles, bajo los criterios definidos, para identificar la valoración de los controles

Evaluación al modelo de gestión de riesgos

11. Valorar el riesgo residual una vez definidos los tratamientos y controles a aplicar
12. Definir los responsables de ejecutar los controles propuestos
13. Establecer el indicador y la unidad de medida, mediante el cual se hará seguimiento a los riesgos y controles definidos
14. Realizar monitoreo y revisión a la Matriz de Riesgos de Corrupción y Gestión en cuanto a las causas, los riesgos y controles incorporados de manera periódica
15. Consolidar en la MT-SG-05 Matriz de Riesgos de Corrupción y Gestión, con el informe de Seguimiento y evaluación a los Riesgos FT-MAS-04. Realizar modificaciones cuando se requieran actualizaciones, se identifiquen nuevos riesgos, controles o según sugerencias del informe Seguimiento y Evaluación a los Riesgos FT-MAS-04
16. Realizar modificaciones cuando se requieran actualizaciones, se identifiquen nuevos riesgos, controles o según sugerencias del informe Seguimiento y Evaluación a los Riesgos FT-MAS-04.
17. Actualizar la MT-SG-05 Matriz de Riesgos de Corrupción y Gestión
18. Socializar la Matriz de Riesgos de Corrupción y Gestión y todas las actualizaciones que se deriven de esta a las partes interesadas

Evaluación al modelo de gestión de riesgos

En la Guía No. 7 del MinTIC se define la gestión de riesgos dentro del modelo de seguridad, identificando la gestión de riesgos como un tema decisivo que se utiliza en la toma de decisiones dentro del Modelo de Seguridad y Privacidad de la Información (MSPI). Teniendo en cuenta el contexto organizacional y el procedimiento para la gestión de riesgos de Corantioquia, el cual se detalló anteriormente, se buscó la integración con el MSPI, de manera que se aproveche el trabajo adelantado en la identificación de Riesgos para ser complementados por los Riesgos de Seguridad.



De esta manera, se recomienda integrar al sistema de riesgos actual de la entidad los riesgos de seguridad de la información por medio de la metodología recomendada por el MinTIC que integra Riesgos con el MSPI.

Durante la ejecución del primer Comité de Seguridad de la Información se realizó un ejercicio de definición de riesgos de seguridad de la información y se puede encontrar su detalle en la sección 2.4 del presente documento.

A person in a red shirt stands on the edge of a dark, rocky cliff, looking out over a vast, hazy mountain range under a clear sky. The mountains are layered, creating a sense of depth and scale.

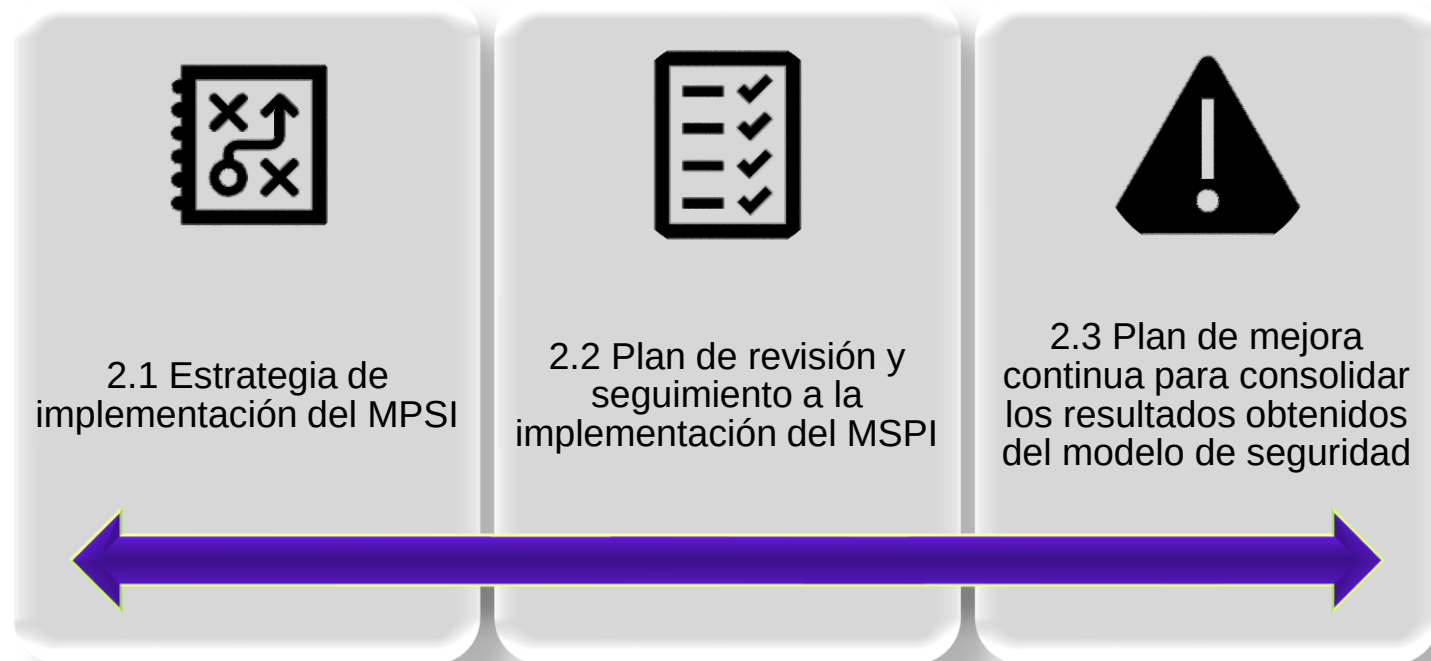
2

Implementación del Modelo de Seguridad y Privacidad de la Información (MSPI)

Implementación del Modelo de Seguridad y Privacidad de la Información (MSPI)

La implementación del MSPI centra sus esfuerzos en la preservación, la confidencialidad, integridad y disponibilidad tanto de la información como de los sistemas que la procesan, siendo un competente estratégico y esencial de las TIC que aporta al logro de los objetivos, misión y visión organizacional en Corantioquia.

La implementación cuenta con una serie de pasos para lograr el cumplimiento de sus objetivos:





2.1

Estrategia de implementación y control operacional del modelo

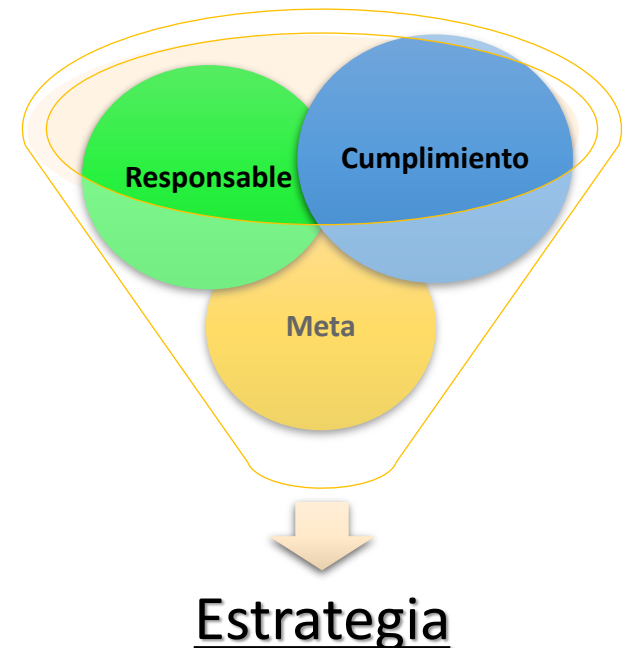
Estrategia de Implementación del MSPI

CORANTIOQUIA establecerá, implementará, controlará y mantendrá el flujo de los procesos requeridos y necesarios para su funcionamiento, con los condicionamientos propios del Modelo de Seguridad y Privacidad de la Información y, del Sistema de Gestión de Seguridad de la Informa.

A fin de estar preparado ante situaciones adversas, atender consecuencias de cambio no estimados, tomar medidas de mitigación de riesgos y dar atención oportuna, eficiente, efectiva y eficaz en seguridad y privacidad de la información.

La organización debe asegurar cada proceso y actividad que desarrolle, esto incluye los procesos internos y externos. Para lo cual la estrategia a ejecutar será una metodología mediante la cual se efectuará la implementación y control operacional del modelo, así:

- Meta
- Responsable
- Implementación



Estrategia de Implementación del MSPI

META	RESPONSABLE	FECHA CUMPLIMIENTO	ESTADO
Políticas de Seguridad y Privacidad de la Información	Líder SI Jurídica	Diciembre 2019	Finalizado
Procedimientos de Seguridad de la Información	SGI Líder SI	Noviembre 2019	Finalizado
Roles y Responsabilidades de Seguridad y Privacidad de la Información	Comité de Seguridad de la Información (CSI)	Noviembre 2019	Finalizado
Inventario Consolidado de Activos de Información	Toda la Corporación	Diciembre 2019	Finalizado
Integración del MSPI con el Sistema de Gestión Documental	Líder SI CAD	Noviembre 2019	Finalizado
Evaluación del Modelo de Gestión de Riesgos	Control Interno Líder SI	Noviembre 2019	Finalizado
Estrategia de Implementación y Control Operacional del Modelo	Toda la Corporación	Diciembre 2019	Finalizado

*SI: Seguridad de la Información

Estrategia de Implementación del MSPI

META	RESPONSABLE	FECHA CUMPLIMIENTO	ESTADO
Procedimiento para seguimiento del Plan de tratamiento de Riesgos	Líder SI SGI	Noviembre 2019	Pendiente
Indicadores d Gestión de Seguridad y Privacidad de la Información	SGI Líder SI	Noviembre 2019	Pendiente
Plan de Revisión y Seguimiento a la Implementación del MSPI	Comité de Seguridad de la Información (CSI)	Noviembre 2019	Pendiente
Programa para auditar el MSPI	Control Interno	Noviembre 2019	Pendiente
Plan de mejoramiento continuo	Comité de Seguridad de la Información (CSI)	Noviembre 2019	Pendiente
Comunicaciones y Capacitaciones	Oficina de Comunicaciones Talento Humano	Noviembre 2019	Pendiente
Esquema de Servicio Administrado del MSPI	SGI	Noviembre 2019	Pendiente

*SI: Seguridad de la Información

Agenda de Implementación del MSPi

Agenda de implementación del MSPi	Responsable	Encargado	Fecha DD/MM/AAAA
Activación del Comité de Seguridad de la información	✓ Comité de Seguridad de la información	✓ Comité de Seguridad de la información	27/11/2019
Definir, aprobar, comunicar e implementar la Política de Seguridad y Privacidad de la información, los procedimientos de la corporación y el comité de Seguridad de la Información	✓ Dirección General	✓ Equipo de TI ✓ Jurídico (Legal) ✓ Control Interno	
Definir roles y responsabilidades de Seguridad y Privacidad de la información	✓ Talento Humano	✓ Comité de Seguridad de la Información ✓ Equipo de TI	
Complementar, gestionar el inventario de Activos de Información de Corantioquia e, Integrar el Modelo de Seguridad y Privacidad de la información con el Sistema de Gestión Documental	✓ TI	✓ Equipo de TI ✓ Gestión Documental	
Operar el modelo actual de gestión de riesgos en materia de Seguridad de la Información	✓ SGI	✓ Comité de Seguridad de la Información	
Establecer un programa que permita auditar el modelo de seguridad y privacidad de la información	✓ Auditoría Interna	✓ Comité de Seguridad de la Información	
Comunicaciones	✓ Comunicaciones		
Capacitaciones	✓ Talento Humano		
Definir el esquema de servicio administrado del modelo de seguridad y privacidad de la información	✓ TI		
Segundo Comité de Seguridad de la Información	✓ Comité de Seguridad de la información	✓ Comité de Seguridad de la información	13/12/2019



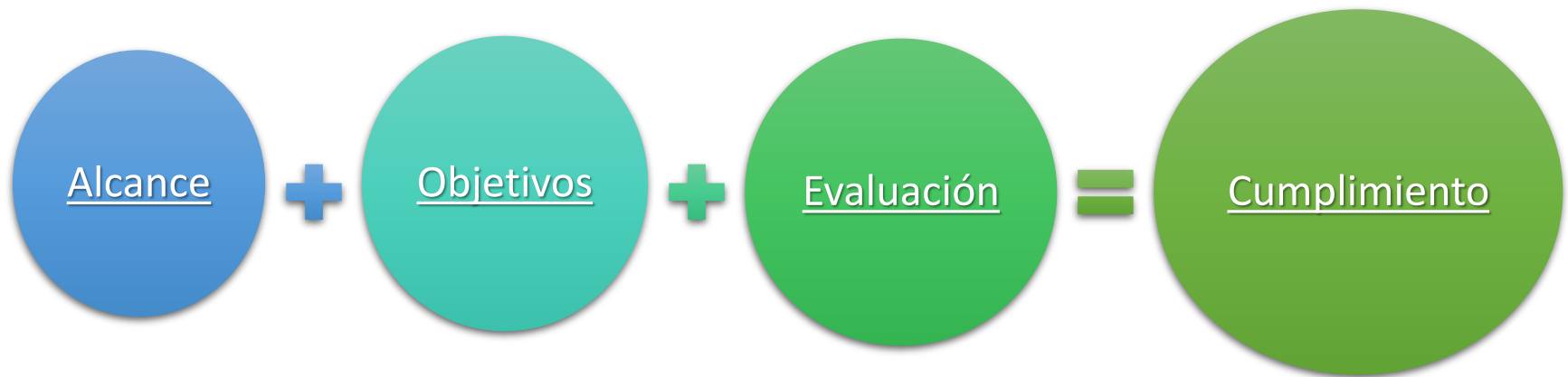
2.2

Plan de revisión y seguimiento a la implementación del MSPI

Plan de revisión y seguimiento a la implementación del MSPI

Permite a Corantioquia estimar el verdadero alcance y la efectividad que ha tenido la fase de construcción del MSPI mediante el cumplimiento de cada objetivo.

Adicionalmente se considera el estado actual de los procesos desarrollados y controles adoptados del MSPI y, la valoración de los componentes claves para la ejecución, seguimiento, evaluación, análisis y administración del MSPI.



Plan de revisión y seguimiento a la implementación del MSPI

Como **metodología para el desarrollo del plan**, en el siguiente listado cada alcance será enunciado y descrito, permitiendo la evaluación para lograr el cumplimiento deseado. Se debe estimar su desempeño en un periodo trimestral que vislumbre los resultados propuestos.

ALCANCE	OBJETIVO	CUMPLIMIENTO			
		Q1	Q2	Q3	Q4
Políticas	Marco por el cual se crea, implementa, gestiona, inspecciona, mantiene y mejora la seguridad y privacidad de la información y, de los sistemas que la procesa.				
Procedimientos	Estable los mecanismos para concebir, gestionar, evaluar y tomar acciones en materia del SGSI.				
Roles y Responsabilidades	Define el equipo responsable de la seguridad y privacidad de la información para la entidad, como parte del MSPI.				
Activos de Información	Consolida un inventario con todos los activos de información de la Corporación con el fin de dar cumplimiento a la normatividad para entidades públicas y, determinar con cuales activos cuenta, su uso actual y responsabilidades frente al mismo.				
MSPI y Gestión Documental	Da cumplimiento a lo dispuesto por el Archivo General de la Nación en relación a alinear, con el sistema de Gestión Documental, la documentación de la entidad vinculada con seguridad y privacidad de la información.				
Gestión de Riesgos	Implementa una metodología que permita identificar, evaluar, dar tratamiento y seguimiento a los riesgos de seguridad de la información que puedan afectar los activos de información y los sistemas que los procesa.				
Implementación y Control del MSPI	Lleva a cabo la implementación de la planificación y provee los controles necesarios para su verificación y cumplimiento.				

Plan de revisión y seguimiento a la implementación del MSPI

ALCANCE	OBJETIVO	CUMPLIMIENTO			
		Q1	Q2	Q3	Q4
Plan de tratamiento de Riesgos	Implementa un plan de tratamiento de riesgos de la seguridad de la información, detallando el control aplicable según sea el caso.				
Indicadores de Gestión	Adopción de indicadores que permiten cuantificar y cualificar la eficiencia, efectividad y eficacia de las acciones y gestiones implementada en seguridad de la información.				
Plan de Revisión y Seguimiento	Ejecución del plan que contiene los alcances y objetivos propuestos del MSPI evaluados periódicamente. Donde se evidencia los resultados esperados y, permite analizar causas e impactos de su cumplimiento o no cumplimiento.				
Auditoría al MSPI	Realización del plan de auditorías para el MSPI, con: periodicidad, métodos, responsabilidades, requisitos de planificación y elaboración de informes.				
Mejoramiento continuo	Aplicación de métodos de recolección y evaluación de desempeño, que desligue particularidades de mejoramiento de seguridad y privacidad de la información, por medio de acciones apropiadas que ajuste controles y procedimientos del MSPI.				
Plan de comunicaciones	Genera competencias y hábitos, a modo de cultura organizacional, mediante la comunicación, sensibilización y capacitación estratégica para la seguridad de la información.				
Plan de capacitaciones	Provee capacitación efectiva y oportuna a funcionario, contratistas, proveedores, practicantes, visitantes, usuarios, entre otros, en relación a seguridad y privacidad de la información y de los sistemas que le procesan.				
Esquema de Servicio Administrado del MSPI					





2.3

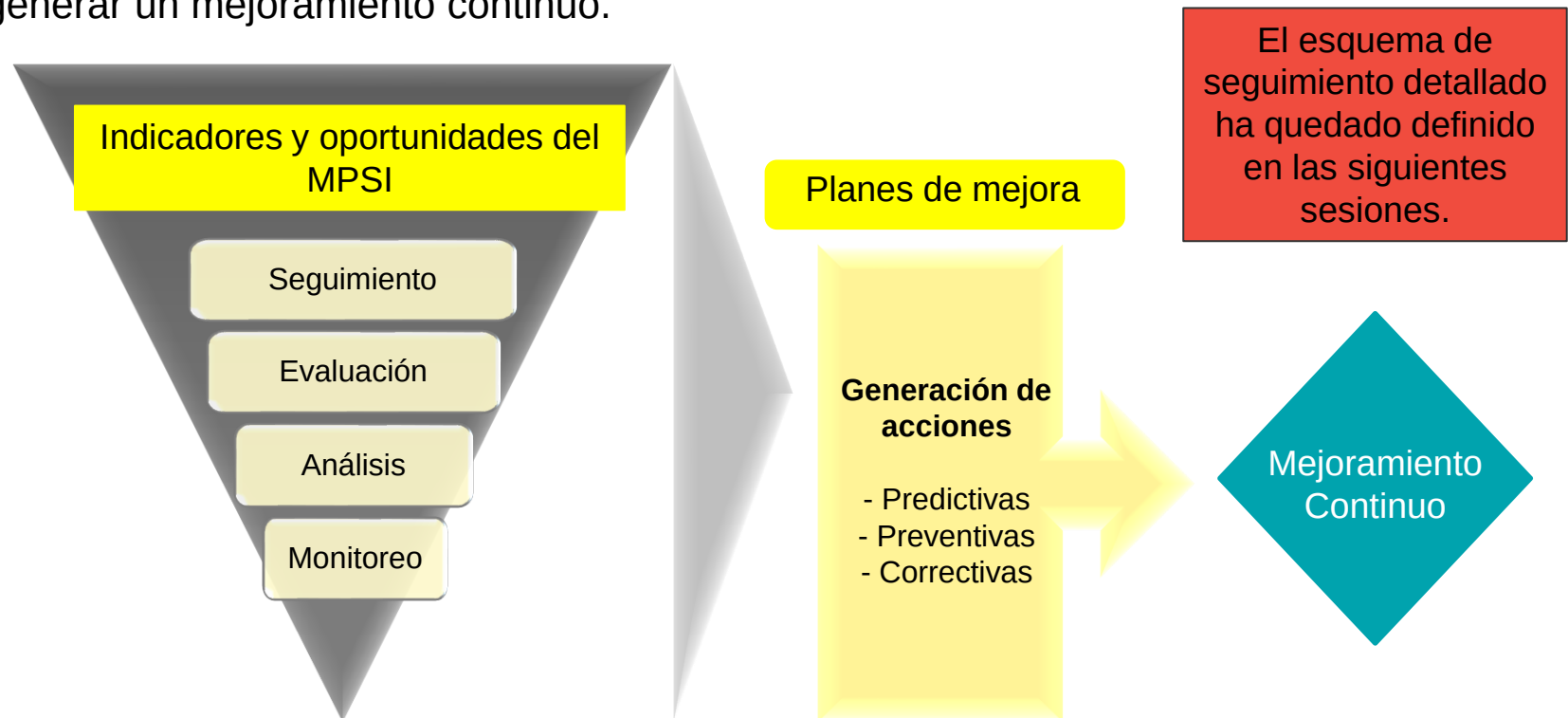
**Plan de mejora continua
del MSPI**

Plan de mejora continua del MSPI

A medida que se desarrolle la implementación y gestión del MSPI, en el Comité de Seguridad **se revisará el avance de cada frente y se identificarán los resultados de manera semestral.**

El comité en sus sesiones identificará en consideración de la metodología la evaluación de desempeño y los indicadores el avance y las oportunidades de mejora en cada frente con el fin de evitar materialización de riesgos.

Finalmente, generará acciones y un plan de acción frente a las brechas identificadas para generar un mejoramiento continuo.





2.4

Seguimiento al plan de tratamiento de riesgos

Seguimiento al plan de tratamiento de riesgos

Definición de riesgos y controles en Seguridad de la información

Ayudando a la entidad a que logre vincular la identificación y análisis de riesgos hacia los temas de la Seguridad de la información, se utilizó el Procedimiento de identificación, valoración del riesgo y controles de CORANTIOQUIA (para mayor detalle ver sesión 1.6) para la identificación de riesgos de seguridad de la información.

El 27 de noviembre de 2019 se realiza el primer Comité de Seguridad de la Información (CSI) en la entidad. El comité se realizó de acuerdo a lo definido en la sesión 1.3 – Roles y responsabilidades, contando con la participación de los involucrados definidos tanto por el área de TI como del resto de la organización. Los asistentes al Comité, aparte del equipo de EY, fue:

Nombres y Apellidos	Dependencia
Yeny Maritza Vallejo	Oficina de Control Interno
Andrea Sierra Uribe	Secretaría General
Miryam Lopez M	Subdirección Administrativa/TH
Ferney Andrés Valdes Tabares	Subdirección Administrativa/TI
Claudia Imelda Henriquez	Subdirección Administrativa/TI
David Betancur Chedraui	Subdirección de Planeación/GIC
Isabel Cano Ramirez	Subdirección de Planeación/GIC
Victor Alfonso Lopez S	Subdirección de Planeación/SGI

Entendiendo que en la Entidad no se tenían identificados riesgos de Seguridad de la información, se identificó como tarea primordial iniciar por dicha definición de acuerdo a la operación y entorno de Corantioquia. Así, durante el Comité de Seguridad de la Información se realizó un ejercicio practico para la identificación de riesgos, basada en la metodología de riesgos ya definida.

Seguimiento al plan de tratamiento de riesgos

Definición de riesgos y controles en Seguridad de la información

Partiendo de un modelo de referencia de riesgos de seguridad de la información, se eligieron 9 riesgos que se consideraron posibles de materializar en la Corporación:

- 1) Pérdida de confidencialidad, integridad o disponibilidad de la información.
- 2) Modificación no autorizada de la información y, sobre los sistemas de información.
- 3) Destrucción o pérdida de la información y/o datos no respaldados.
- 4) Hurto de información por parte de personal interno y/o externo.
- 5) Acceso no autorizado a la información y a los sistemas de información.
- 6) Acceso no autorizado o inapropiado a los centros de datos.
- 7) Utilización de dispositivos de Entrada y/o dispositivos de Salida (E/S) no autorizados.
- 8) Deterioro, daño o sabotaje a la información por parte de personal interno y/o externo.
- 9) Información no disponible por fallas o daños en los sistemas de información, equipos de computo y equipos de telecomunicaciones.

El objetivo de la lista fue generar la discusión durante el Comité de Seguridad de la Información y que entre los interesados se priorizaran y se aplicará la metodología definida

Seguimiento al plan de tratamiento de riesgos

Definición de riesgos y controles en Seguridad de la información

De los 9 riesgos de seguridad de la información presentados, se definieron siguientes 6:

- 1) Accesos no autorizados a la información y/o servicios tecnológicos
- 2) Información no disponible por fallas o daños en los sistemas de información, equipos de computo y equipos de telecomunicaciones.
- 3) Pérdida de equipos de cómputo y medios extraíbles
- 4) Destrucción o pérdida de la información y/o datos no respaldados
- 5) Hurto de información por parte de personal interno y/o externo
- 6) Utilización de dispositivos de Entrada y/o dispositivos de Salida (E/S) no autorizados

Definidos los riesgos a evaluar y continuando con la metodología de riesgos de la Corporación, se procedió a analizar el riesgo bajo las variables establecidas (Probabilidad e Impacto). Para esto, durante el comité se explicó la valoración de riesgos y el criterio que se tiene definido para la calificación de Probabilidad e Impacto.

Seguimiento al plan de tratamiento de riesgos

Calificación de riesgos en Seguridad de la información

El criterio para la calificación de Probabilidad e Impacto fue el siguiente:

Probabilidad

Posibilidad de ocurrencia del riesgo, está puede ser medida con criterios de frecuencia (número de veces en que se ha presentado el riesgo en un período determinado) o por la factibilidad (factores internos o externos que pueden determinar que el riesgo se presente).

1	Rara vez	Ocorre en circunstancias excepcionales. El evento no se ha presentado en los últimos cinco (5) años.
2	Improbable	Puede ocurrir. El evento se presentó al menos 1 vez en los últimos 5 años
3	Posible	Es posible que suceda. El evento se presentó al menos 1 vez en los últimos 2 años.
4	Probable	Es viable que el evento ocurra en la mayoría de los casos. El evento se presentó al menos 1 vez en el último año.
5	Casi Seguro	Se espera que el evento ocurra en la mayoría de las circunstancias. Es muy seguro que se presente. El evento se presentó más de 1 vez al año.

Impacto

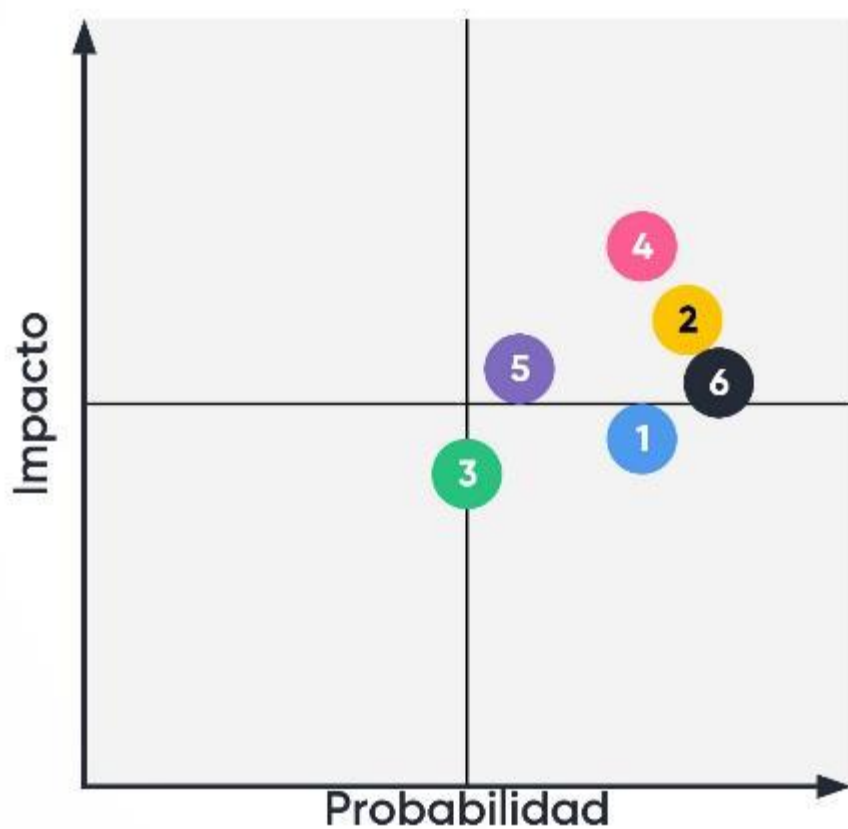
Las consecuencias que puede ocasionar a la Corporación la materialización del riesgo.

1	Moderado	Afectación parcial al proceso y a la corporación. Genera medianas consecuencias para la entidad.
2	Mayor	Impacto negativo para la Corporación. Genera altas consecuencias para la entidad.
3	Catastrófico	Consecuencias desastrosas sobre el sector. Genera consecuencias desastrosas para la entidad.

Seguimiento al plan de tratamiento de riesgos

Calificación de riesgos en Seguridad de la información

Para unificar el criterio de los integrantes del Comité de Seguridad de la Información, se utilizó una herramienta que permitía a cada involucrado calificar los 6 riesgos en probabilidad e impacto, obteniendo el siguiente resultado:



- 1 Accesos no autorizados a la información y/o servicios tecnológicos
- 2 Información no disponible por fallas o daños en los sistemas de información, equipos de cómputo y equipos de telecomunicaciones.
- 3 Pérdida de equipos de cómputo y medios extraíbles
- 4 Destrucción o pérdida de la información y/o datos no respaldados.
- 5 Hurto de información por parte de personal interno y/o externo
- 6 Utilización de dispositivos de Entrada y/o dispositivos de Salida (E/S) no autorizados

Seguimiento al plan de tratamiento de riesgos

Definición de controles

Del resultado obtenido se destacan los riesgos 2, 4, 5 y 6 que se ubicaron en el cuadrante superior derecho, el cual representa los 4 riesgos que tienen mayor criticidad para la Corporación en materia de Seguridad de la Información. Así, el resultado final del ejercicio de identificación de riesgos nos entregó los siguientes riesgos:

- 1) Información no disponible por fallas o daños en los sistemas de información, equipos de computo y equipos de telecomunicaciones.
- 2) Destrucción o pérdida de la información y/o datos no respaldados
- 3) Hurto y fuga de información por parte de personal interno y/o externo
- 4) Utilización de dispositivos de Entrada y/o dispositivos de Salida (E/S) no autorizados

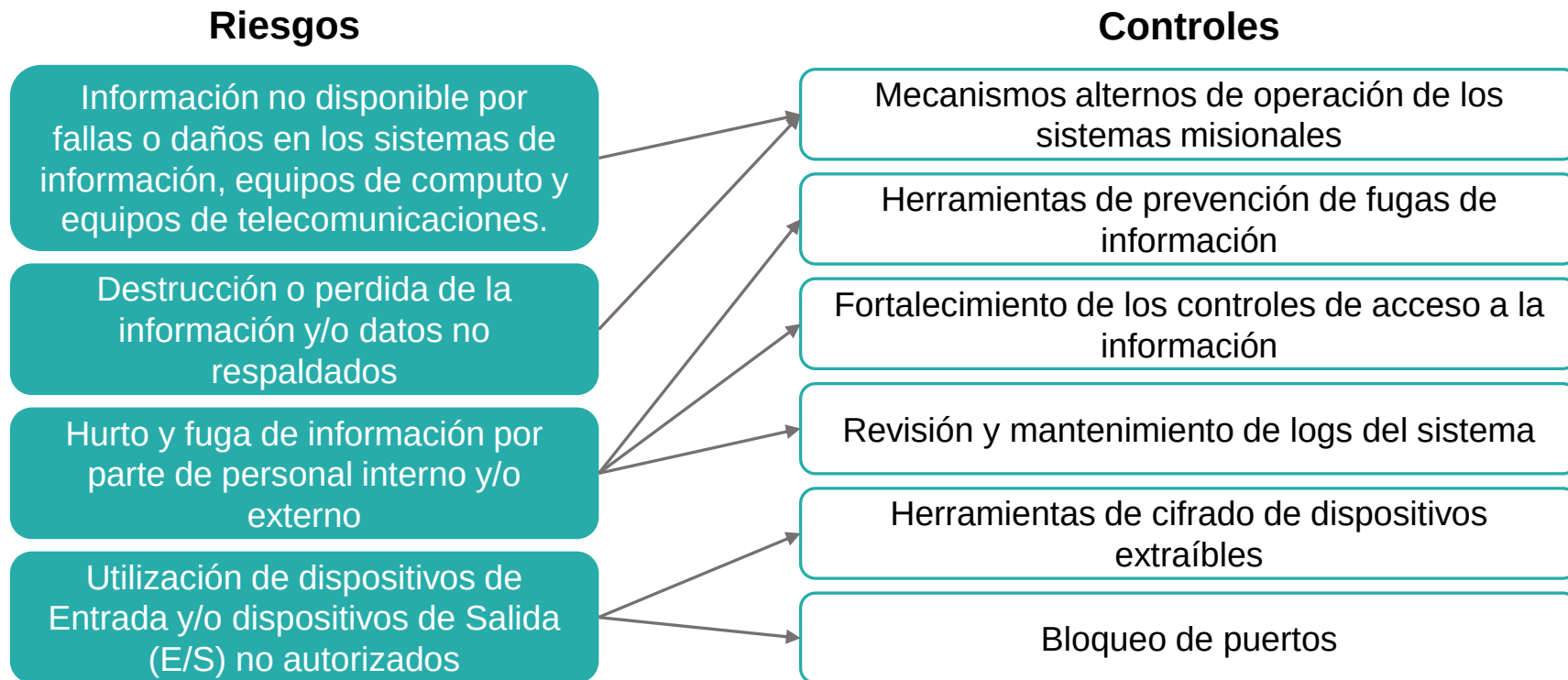
Teniendo identificados y valorados los riesgos, se procedió a definir los controles y los tipos de controles a aplicar a cada riesgo, teniendo en cuenta los 3 tipos de controles definidos en la metodología:

- **Preventivo:** Este tipo de controles intentan evitar la ocurrencia de los riesgos que puedan afectar el cumplimiento de los objetivos
- **Detectivo:** Controles que están diseñados para detectar una situación no deseada, que se corrija y se tomen las acciones correspondientes.
- **Correctivo:** Tipo de control que permite, después de ser detectado el evento no deseado, el restablecimiento de la actividad.

Seguimiento al plan de tratamiento de riesgos

Definición de controles

De esta manera se definieron los controles a implementar para cada riesgo:



Los resultados finales del ejercicio, con sus riesgos y controles definidos se completaron en la Matriz de Riesgos (MT-SG-05) y se encuentran en detalle en el **anexo 5**.

Seguimiento al plan de tratamiento de riesgos

Riesgos y controles por considerar a futuro

Entendiendo la situación actual de la Corporación, en la cual no se contaba con ningún análisis de riesgos en seguridad de la información, ni con ningún control respectivo implementado, se plantea como un buen comienzo los riesgos y controles identificados en el ejercicio anterior. Sin embargo, es clave tener la visión sobre las prácticas líderes, por lo que a continuación se detallan diferentes riesgos y controles que Corantioquia deberá tener en consideración en un futuro cercano:

Riesgo	Control sugerido
Conflictos de segregación de funciones en los sistemas de información e infraestructura tecnológica	1. Definir, aprobar y mantener actualizadas las matrices de segregación de funciones de roles y cargos de todos los sistemas de información e infraestructura de TI y OT. 2. Revisar de manera periódica la segregación de funciones en la configuración de accesos de los sistemas de información de acuerdo con las reglas de segregación definidas. 3. Evaluar la segregación de funciones durante la creación o modificación de usuarios.
Accesos no autorizados a la información y/o servicios tecnológicos	1. Autorizar la creación y/o modificación de usuarios de forma individual o masiva en los sistemas y recursos de TI por parte del responsable establecido en la directriz de gestión de accesos 2. Revisión periódica de privilegios asignados a los usuarios creados en los sistemas de información e infraestructura de TI y OT. 3. Bloquear las cuentas de usuarios internos y contratistas retirados. Notificar los usuarios retirados de la compañía al área de TIC 4. Bloquear de usuarios por inactividad en las cuentas de acceso pasados 30 días de acuerdo con lo definido en la directriz de uso aceptable. 5. Verificar periódicamente los registros de auditoría del sistema de información con el fin de identificar que transacciones críticas, se realizan por los usuarios y roles autorizados

Seguimiento al plan de tratamiento de riesgos

Riesgos y controles por considerar a futuro

Riesgo	Control sugerido
Cambios no autorizados sobre los sistemas de información	1. Gestionar los cambios en los sistemas de información y su infraestructura. 2. Segregar las funciones de los usuarios entre los ambientes de desarrollo, pruebas y producción.
Incumplimiento de los objetivos de negocio y no obtención de beneficios en los proyectos de TI.	1. Aprobar el documento "Project Charter" para los proyectos en fase de preparación. Asimismo, aprobar el inicio y cierre de cada fase del proyecto mediante un acta. 2. Seguimiento al avance del proyecto de TI y al cumplimiento de compromisos del proyecto. 3. Reunión de seguimiento al portafolio de proyectos de TI.
Perdida de la continuidad de la tecnología que soporta procesos críticos del negocio.	Ejecutar pruebas del Plan de Recuperación de Desastres para los sistemas de información, servicios críticos e infraestructura, registrar los resultados de dichas pruebas y definir acciones correctivas en caso de ser necesarias.
Procesamiento y/o configuración inexacta, incompleta y/o no autorizado de datos en los sistemas de información	Revisar los parámetros de seguridad de las aplicaciones y su infraestructura (Sistema Operativo y Bases de datos).
Acceso no autorizado / inapropiado a los equipos en el data center	Aprobar la asignación de accesos al centro de computo
Incumplimiento y/o indisponibilidad en la prestación de los servicios de TI	1. Definir y aprobar de acuerdos de niveles de servicios de TI. 2. Monitorear acuerdos de niveles de servicios de TI 3. Monitorear el desempeño y la capacidad de la infraestructura de TI
Fallas en los equipos	Programar los mantenimientos de equipos de cómputo aprobado por el coordinador de soporte TI Programar los mantenimientos de servidores y equipos de red aprobado por el coordinador de infraestructura



Seguimiento al plan de tratamiento de riesgos

Riesgos y controles por considerar a futuro

Riesgo	Control sugerido
Fallas en los equipos	Programar los mantenimientos de equipos de cómputo aprobado por el coordinador de soporte TI Programar los mantenimientos de servidores y equipos de red aprobado por el coordinador de infraestructura
Inversiones sobre los sistemas de información e infraestructura de TI no alineadas con la estrategia corporativa.	Aprobar los requerimientos de adquisiciones tecnológicas (activos o servicios).
Incumplimiento de la atención de solicitudes de soporte de TI	Registrar, documentar, analizar, solucionar y cerrar de los incidentes, requerimientos o problemas reportados por las áreas de negocio o áreas de apoyo de la compañía.
Falla de controles ambientales y físicos del centro de cómputo.	Verificar que solo el personal autorizado puede ingresar al data center. Además, revisar el cumplimiento del cronograma de mantenimiento de dispositivos de seguridad ambiental e infraestructura según lo definido en la directriz de Acceso a áreas restringidas.
Falta de alineación entre la estrategia de Tecnología de la Información y la de la Compañía	1. Aprobar el plan estratégico de TI y sus modificaciones. 2. Monitorear la ejecución del Plan Estratégico de TI y del avance de sus iniciativas.



Declaración de aplicabilidad

¿Qué es una Declaración de Aplicabilidad?

Una vez que se han definido el tratamiento para los riesgos, la Corporación debe aplicar medidas de seguridad, es decir, decidir de qué manera serán mitigados los riesgos. Es en este punto cuando se desarrolla una Declaración de Aplicabilidad, el documento donde se registran los controles de seguridad que son aplicables (necesarios) y si éstos se encuentran operando o todavía no.

Control	Aplica	Control implementado	Evidencia o registro de implementación
Mecanismos alternos de operación de los sistemas misionales	Si	No	
Herramientas de prevención de fugas de información	Si	No	
Fortalecimiento de los controles de acceso a la información	Si	No	
Revisión y mantenimiento de logs del sistema	Si	No	
Herramientas de cifrado de dispositivos extraíbles	Si	No	
Bloqueo de puertos	Si	No	



2.5

**Indicadores de gestión de
seguridad y privacidad de la
información**

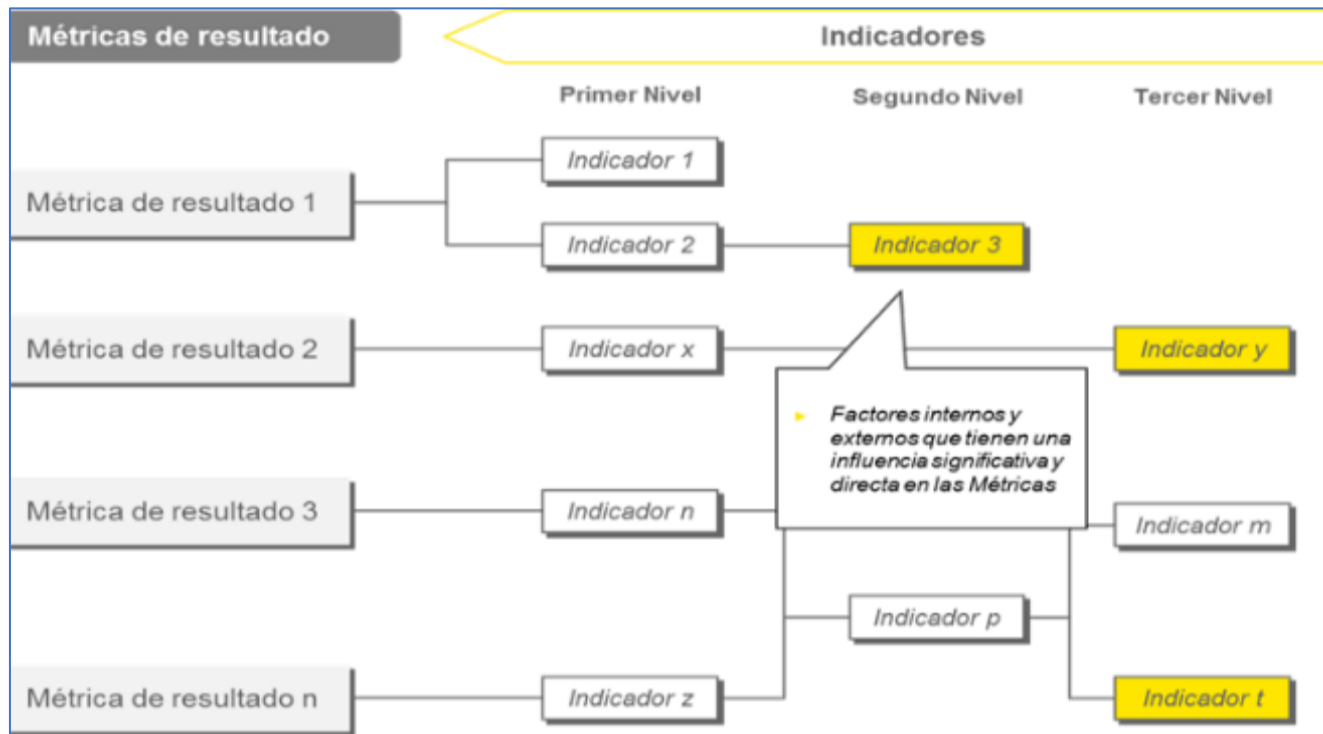
Indicadores de gestión del MSPI

La gestión es el proceso de identificar dimensiones o áreas de valor en la Corporación que deben ser medidas o cuantificadas para soportar el monitoreo, la toma de decisiones y promover comportamientos que permitan lograr los resultados esperados. Un modelo de gestión facilita la planeación y el crecimiento, orienta la innovación y asegura el desempeño de forma sostenible, a través de mecanismos como planear, coordinar, desarrollar, acordar, monitorear y reportar al Modelo de Seguridad y Privacidad de la Información (MSPI) para conservar la efectividad del mismo.

La definición de indicadores o métricas permite a las organizaciones enfocarse en las causas y factores críticos para alcanzar el éxito y reconocer aquello que no se le ha permitido. También permite realizar ajustes en los procesos internos a través del análisis de las metas programadas comparado con los resultados obtenidos.

Indicadores de gestión del MSPI

Para trabajar los indicadores de Corantioquia, se definió el siguiente modelo.



Indicadores de gestión del MSPI

El resultado típico de este modelo es la definición de un árbol de indicadores de gestión que está alineado con la estrategia. El cual inicia con la definición de métricas a nivel operacional y táctico que luego en conjunto permiten tener una visión integral del cumplimiento de la estrategia.

Los indicadores se definen para lograr los siguientes hitos:

1

Identificar los elementos del éxito.

2

Medir los resultados para soportar el cumplimiento y la toma de decisiones.

3

Demostrar resultados para ganar apoyo institucional.

4

Identificar desviaciones para poder corregirlas.

5

Apropiar conocimientos de cómo hacer las cosas correctamente para seguir haciéndolas.

Indicadores de gestión del MSPI

La conformación de los indicadores de seguridad de la información debe partir de los objetivos estratégicos de la Corporación.

1

Estratégicos

Este tipo de indicador está relacionado directamente con el impacto que ha generado la gestión del gobierno de seguridad de la información con los objetivos que se desean cumplir a mediano y largo plazo.

2

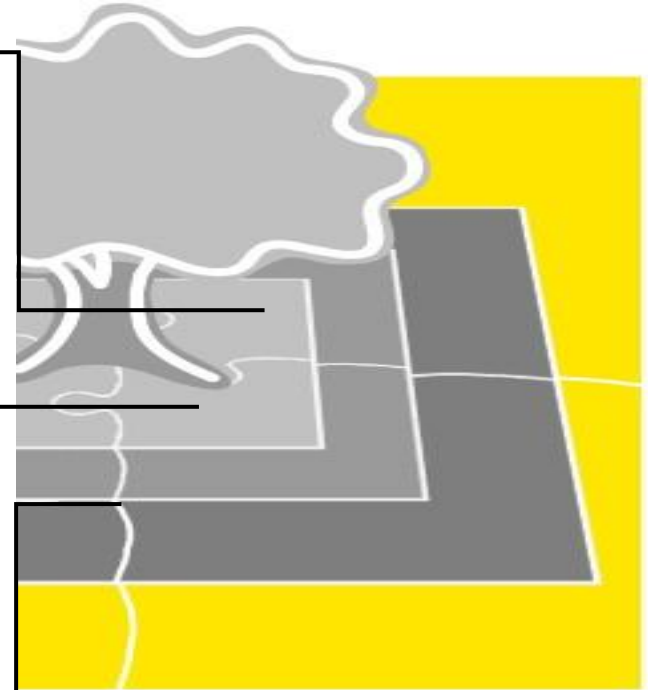
Tácticos

Los indicadores de este tipo están encaminados a medir todas las acciones deseadas que se deben lograr como resultado directo de la aplicación de una estrategia de gestión apoyada en las áreas de la compañía.

3

Operacionales

Con este tipo de indicadores se desea monitorear el cumplimiento de acciones específicas y controles a los que se comprometió cada área en la compañía.



Indicadores de gestión del MSPI

La elaboración de los indicadores debe ir acompañada de un análisis integral que permita establecer el nivel de desempeño esperado por medio de criterios como: objetividad, disponibilidad de información, costo-beneficio de la obtención de información, benchmarking internacional, entre otros.

A continuación, se relacionan los criterios para la construcción de indicadores:

- ▶ **Objetividad:** los indicadores deben reflejar hechos y no opiniones. También deben basarse en un análisis constante de las leyes, regímenes y prácticas.
- ▶ **Comparabilidad:** la metodología de medición para un indicador debe ser fácilmente replicable en las diferentes áreas de la compañía.
- ▶ **Procesabilidad:** los indicadores deben medir aspectos de las políticas y del entorno regulatorio que permitan desarrollar procedimientos claros.
- ▶ **Neutralidad:** los indicadores deben profundizar e indagar características del entorno deseado de la compañía.
- ▶ **Disponibilidad:** la información para la elaboración del indicador debe estar disponible.
- ▶ **Rentabilidad:** la recolección de la información para la elaboración del indicador debe tener un costo razonable.

Indicadores de gestión del MSPI

A continuación, se mencionan y describen los atributos que deben evaluarse para actualizar o construir indicadores que sean viables de implementar e impulsen la gestión y sostenibilidad del Modelo de Seguridad y Privacidad de la Información:

- ▶ **Datos de entrada para la medición del indicador:** mide la disponibilidad de la información requerida para medir el indicador.
- ▶ **Medición del indicador:** determina el grado automatización del cálculo del indicador (manual, semiautomático o automático)
- ▶ **Características de los resultados del indicador:** mide cualidades y aspectos a contemplar al momento de analizar los resultados.
- ▶ **Características del diseño del indicador:** evalúa si el diseño del indicador en términos de frecuencia y costo-beneficio es adecuado para la compañía.

Indicadores de gestión del MSPI

Finalmente, luego de realizar el ejercicio en Corantioquia se definieron los siguientes indicadores:

Indicador	Descripción	Observación
Cumplimiento del plan de entrenamiento	Mide el avance en el cumplimiento del plan de entrenamiento y capacitaciones	% de avance real / % de avance esperado
Seguimiento a comités	Mide el número de comités realizados versus la frecuencia de comités definidos	Número de comités realizados en el periodo* / número de comités definidos por periodo
Efectividad en la respuesta a incidentes	Respuesta eficiente de incidentes	Número de incidentes reportados / Número de incidentes resueltos
Tiempo invertido en incidentes	Tiempo invertido en la solución del incidente.	Número de horas invertidas en incidentes de protección de datos / Número de horas de trabajo semanales
Cumplimiento del plan de sensibilización y comunicaciones	Mide el avance en el cumplimiento del plan de sensibilización de usuario y comunicaciones	% de avance real / % de avance esperado
Cumplimiento de la implementación de iniciativas del MSPI	Mide el avance en el cumplimiento de las iniciativas definidas en el MSPI	% de avance real / % de avance esperado



2.6

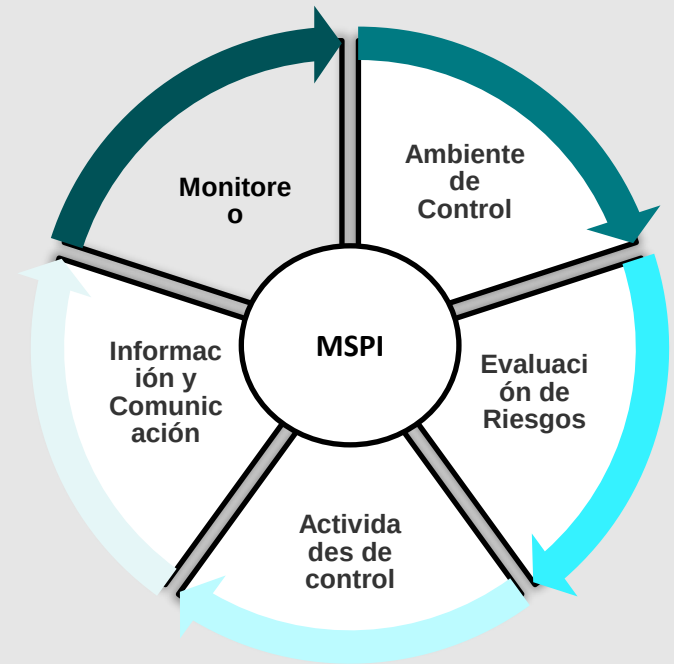
Programa de auditoría al MSPI

Programa de auditoría al MPSI

Las actividades sobre las cuales Corantioquia debe realizar las auditorías de seguridad de la información y que deben ser transversales al Plan Anual de Auditoría son:

- ▶ Alineación de actividades acordes con las estrategias corporativas.
- ▶ Incoherencia, Falta y/o redundancia de controles en procesos.
- ▶ Sobre cobertura en los procesos.
- ▶ Riesgos no estimados ni cubiertos.

Focalización: El enfoque de Auditoría al MPSI ayuda a focalizar esfuerzos para alinear, identificar incoherencias, redundancias o falta de coberturas, monitorear riesgos críticos, entre otros. El resultado debe proporcionar recomendaciones de valor a los responsables del Sistema de Gestión de Seguridad de la Información SGSI, mediante el Comité de Seguridad de la Información CSI.

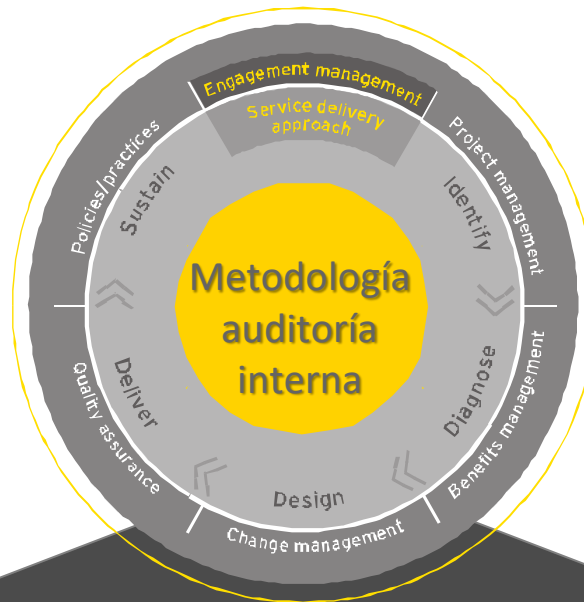


Programa de auditoría al MPSI

Enfoque metodológico de auditoría del MPSI

Creación y medición de valor

Esta metodología es diseñada para conducir un impacto de valor en CORANTIOQUIA.



Metodología – Conocimiento – Tecnología

Establecer protocolos de compromiso

Desarrollar estrategia con el MPSI

Identificación riesgos, controles prácticas líderes

Desarrollar el plan de auditoría

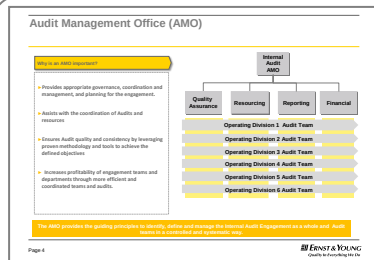
Ejecutar

Comunicar los resultados

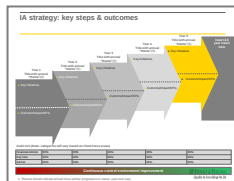
Impacto medible

Programa de auditoría al MPSI

La alineación a la estrategia de la organización y de los procesos a través de cada paso del ciclo de auditoría:



Establecer protocolos comunicación, seguimiento y reporte de avances.



Identificación de Controles y Riesgos claves del MSPI, así como Prácticas líderes del programa.

Audit Response Category	Audit Response
'Standard' Audits	1 Health Check/Diagnostic
	2 'Standard' Sample Testing Audit
	3 Project/Program Monitoring
	4 Pre-implementation Review
	5 Post-implementation Review
	6 Compliance Audit
Risk and Control Framework Reviews	7 Risk Interviews/Verbal Advice
	8 Project Management Framework
	9 Control Process Overview
	10 Control Framework Review
	11 End-to-End Process Audit
'Complex' Audits	12 Deep Dive
	13 Investigation
Education	14 Integrity Audits
	15 Business Coaching/Education

Realizar entendimiento del programa y crear plan de auditoria interna basado en riesgos, controles claves y prácticas líderes.

Ejecutar el plan de auditoría, seleccionar muestras, documentar pepes de trabajo

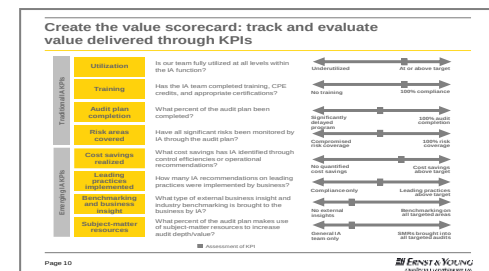


Validación de resultados y elaboración de informes



Comunicar a los interesados los resultados de la auditoría

Estructuración del valor medible de planes de acción y mejoras al MSPI



Desarrollar una estrategia y objetivos en relación al MSPI, relación con la estrategia de la Corporación y objetivos del proceso. Está será informada y definida por el Comité Institucional Coordinador del Sistema del Control Interno -CICSCI

Programa de auditoría al MPSI

La metodología del programa de auditoría interna al MSPI nos lleva a desarrollar una función de auditoría que busca la alineación con la estrategia de CORANTIOQUIA y, enfocarse en los principales riesgos; lo que conlleva a priorizar el trabajo en lo mas importante para la Corporación.

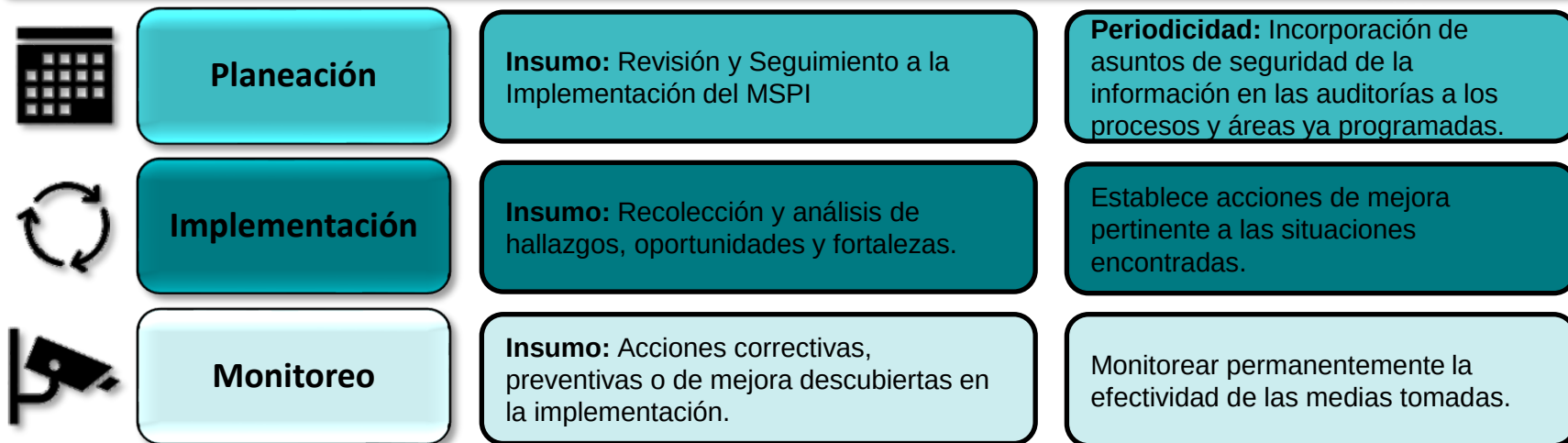


Programa de auditoría al MPSI

La auditoría al MPSI deberá hacerse bajo los lineamientos de la Norma Técnica Colombiana NTC-ISO/IEC 27001 y las disposiciones del MINTIC.

Para lo cual el(la) auditor(a) deberá tener amplios conocimientos (preferible certificación en la norma) y aplicar principios de integridad, veracidad y exactitud, imparcialidad, confidencialidad, independencia y enfoque sistémico. Ello con el fin de salvaguardar confiabilidad, objetividad, pertinencia y suficiencia de la información y la seguridad de la misma.

Proceso de auditoría al MPSI en CORANTIOQUIA



Programa de Auditoría al MSPI

Objetivos de la Auditoría en materia de Seguridad de Información:

- Confirmar los avances respecto a la implementación y desarrollo del modelo de seguridad de información en los diferentes procesos de la organización.
- Validar la efectividad en la implementación de los controles y procedimientos.
- Evidenciar el cumplimiento de la protección de los activos de información de la Corporación.



Temas que se deben auditar de seguridad y privacidad de la información.

Políticas, controles y procedimientos de seguridad de la información
Seguridad de la información en el talento humano
Gestión de activos de información
Controles de acceso
Cifrado
Seguridad perimetral
Seguridad de los procesos
Seguridad de las comunicaciones
Adquisición, desarrollo y mantenimiento de sistemas de información
Mantenimiento de equipos de cómputo y equipo de telecomunicaciones
Relación con terceros y proveedores
Gestión de incidentes de seguridad de la información y, continuidad del negocio



2.7

**Comunicaciones y
capacitaciones**

Comunicaciones y capacitaciones

La implementación del Modelo de Privacidad y Seguridad de la Información (MPSI) en Corantioquia requiere diferentes necesidades de formación asociadas a la normatividad, políticas y procedimientos requeridos en la compañía.

El objetivo de los Planes de formación y Comunicaciones es definir los distintos aspectos relevantes para atender las necesidades de aprendizaje e información en los servidores públicos de Corantioquia.



Comunicaciones y capacitaciones

La formación y las comunicaciones juegan un papel crítico en el éxito del Modelo de Privacidad y Seguridad de la Información (MPSI) en Corantioquia y la adopción de los cambios generados por éste.

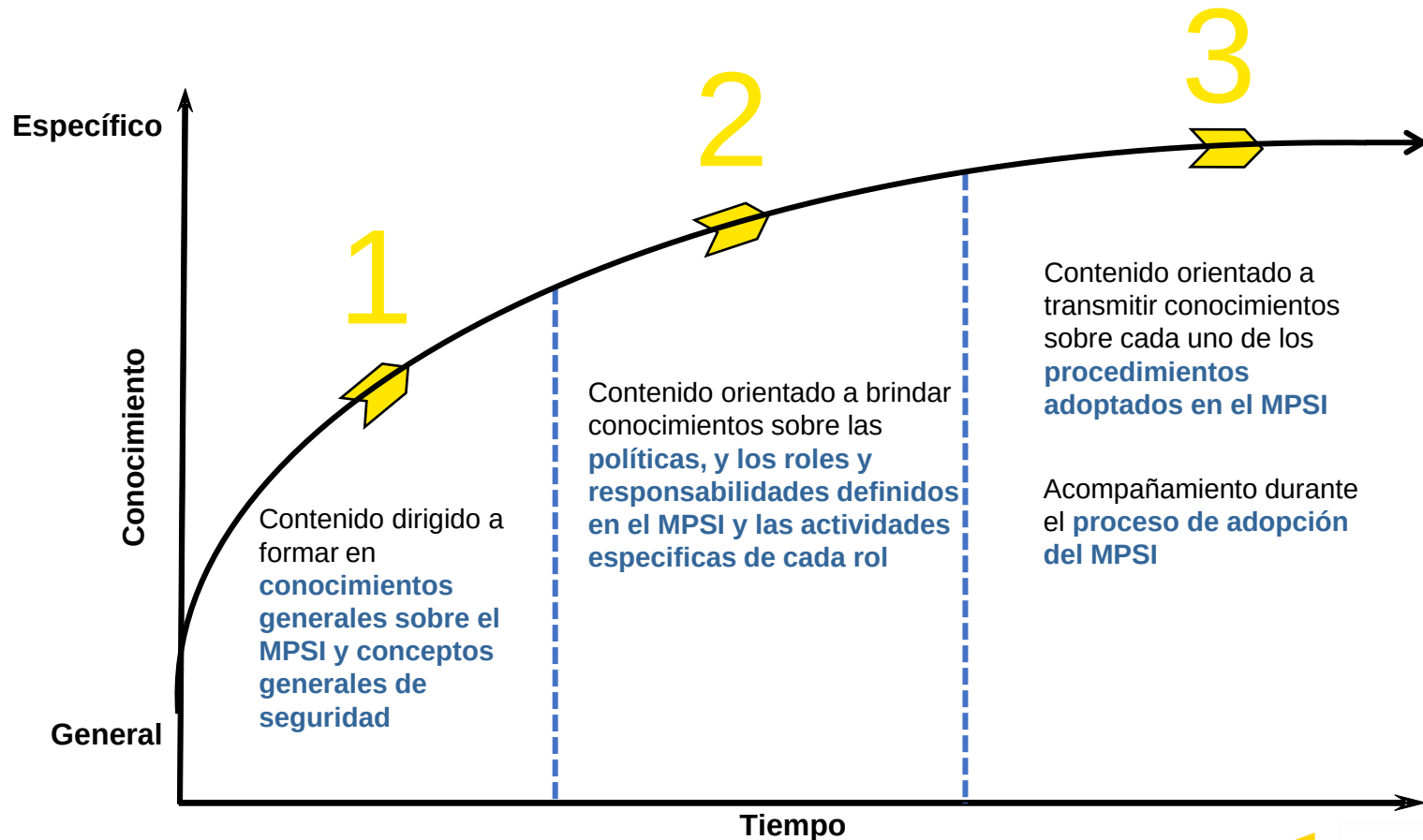
Los principios fundamentales en los cuales se enmarcarán los planes de formación y de comunicaciones del programa son:

1. La formación y comunicación será **proactiva y clara**
2. Se priorizarán los **canales de comunicación cara a cara** antes que cualquier otra forma de comunicación
3. La formación y comunicados deberán **ser relevantes e interesantes** para la audiencia
4. Se utilizarán **diferentes métodos de formación** (instructor, coaching, terceros)
5. Se **confirmará la comprensión de los contenidos** impartidos a las distintas audiencias en los programas de formación



Contenido de la formación y las comunicaciones

Hemos definido 3 grupos de contenido que se cubrirán durante la ejecución de los planes de formación y comunicaciones, y una fase de acompañamiento mientras en Corantioquia se alcanza el conocimiento requerido por el Modelo de Privacidad y Seguridad de la Información (MPSI):





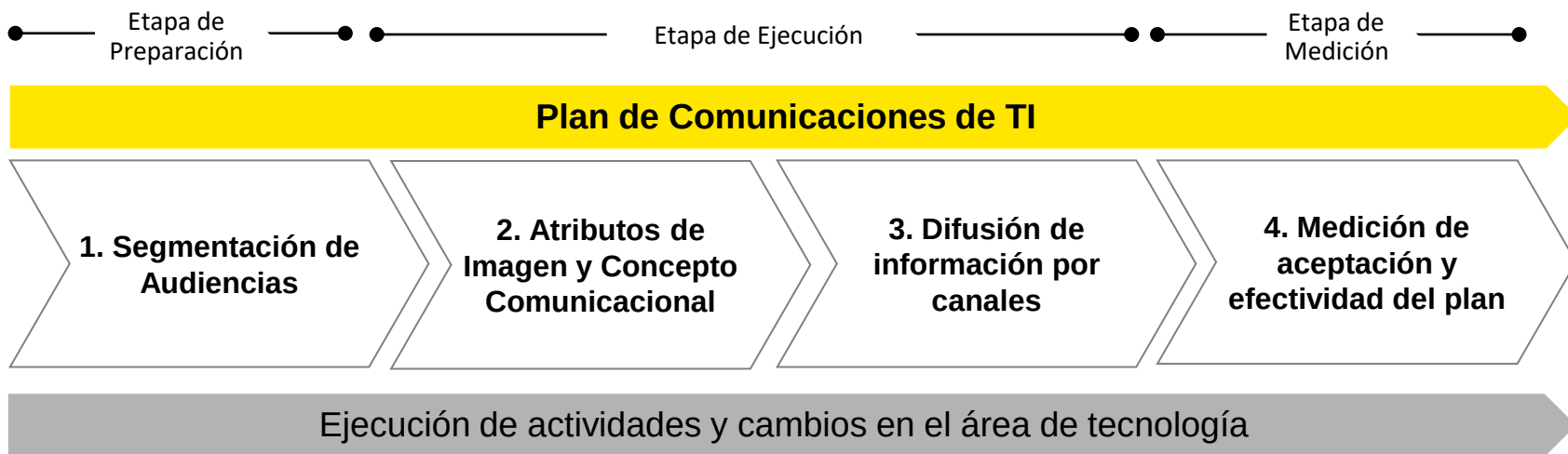
2.7.1

**Plan de comunicaciones de
Seguridad de la información
(integrado con el plan de TIC)**

Plan de comunicaciones

Crear un marco de acción y lineamientos para el manejo de las comunicaciones internas de la corporación generadas desde el área de TI, con el propósito de lograr coherencia, consistencia y congruencia a fin de asegurar su efectividad e impacto en cada una de las audiencias.

La metodología de comunicaciones de TICs será aplicada para comunicar los asuntos propios de Seguridad de la Información



Plan de comunicaciones

En un taller realizado con el equipo de tecnología, hemos definido como vectores de comunicaciones los siguientes asuntos en materia de seguridad de la información:



Planificados	Orientaciones sobre el uso de los equipos y manejo seguro de la información Divulgación de políticas y directrices Prevencciones de seguridad informática Tips de seguridad de informática Ethical hacking Riesgos identificados
Por demanda	Incidentes de seguridad

Plan de comunicaciones

Se identifica la necesidad de comunicar a los funcionarios de la corporación los lineamientos establecidos en la corporación para la protección de la información y en materia de Seguridad de la información.

Eje Temático	Audiencias					DIVULGACIÓN		Mes propuesto	Canales
	Directora y subdirectores	Coordinadores	Usuarios de aplicaciones	Funcionarios de TI	Todos los funcionarios	Usuarios externos	Una vez / Actualización		
							Periódica		
Frente de trabajo: Seguridad de la información									
Orientaciones sobre el uso de los equipos y manejo seguro de la información				X			X	Mensual	Correo electrónico e intranet
Divulgación de políticas y directrices				X			X	Mensual	Correo electrónico
Tips de seguridad informática				X			X	Mensual	Correo electrónico y cartelera
Prevenciones de seguridad informática				X			X	Mensual	Correo electrónico y redes sociales
Ethical hacking				X			X	Mensual	Correo electrónico
Riesgo identificados				X			X	Mensual	Correo electrónico
Incidentes de seguridad	X			X		X		Demanda	Correo electrónico y telefónico



2.7.2

Plan de formación de Seguridad de la información

Plan de formación

El objetivo principal del programa de formación es proporcionar la educación adecuada, a las personas adecuadas, en el momento adecuado, con el fin de permitir a los usuarios finales: adquirir las habilidades y conocimientos necesarios para dominar todos los lineamientos y directrices en materia de seguridad de la información. A continuación se presentan algunos principios de alto nivel en la implementación de la metodología de formación:

Principios típicos	Tácticas (cómo vamos a lograr los principios de entrenamiento)
Implementar formación justo a tiempo	▶ Los usuarios finales serán comunicados al respecto de los beneficios del uso adecuado de la información.
Competencia y capacidad	▶ La formación se estructura de tal manera que los usuarios puedan entender los principales asuntos de Seguridad de la Información y el impacto en la corporación. La capacitación abordará el ¿Por qué? ¿Qué? y ¿Cómo? Preguntas: ¿Por qué estamos haciendo esto? ¿Qué cubre este proceso? ¿Cómo completo esta actividad?
Crear usuarios autosuficientes	▶ Proporcionar a los usuarios los conocimientos necesarios para un tratamiento adecuado y administración de la seguridad de la información.
Desarrollar y garantizar altos estándares de calidad para todo el material de formación	▶ Todos los materiales de formación, incluyendo esquemas de cursos, serán sometidas a un proceso de control de calidad que implica el visto bueno por el equipo de Talento Humano de la corporación que se encargará de dictar y los cursos de Seguridad de la información. ▶ Desarrollar materiales de capacitación que son escalables para soportar actualizaciones y actividades de Seguridad de la Información.
Formación	▶ Los usuarios de las capacitaciones serán evaluados sobre el contenido de la formación y sobre el aprendizaje recibido.

Plan de formación

1

Generalidades sobre la Seguridad de la información

Contenido:

1. ¿Qué es seguridad de la información? (pilares)
2. Importancia para la entidad (no temas regulatorios)
3. ¿Quién es quién en el mundo de la ciberseguridad?
4. ¿Qué es ingeniería social?
5. ¿Cuáles son los tipos de ataques de ingeniería social?
6. ¿Cómo funciona un ataque de ingeniería social?
7. Caso de ejemplo de ataque
8. ¿Cómo protegerse de un ataque?

¿A quien va dirigido?

Todo el equipo de Corantioquia

Periodicidad

Anual o al ingreso de un colaborador

Evaluación

Sobre los temas se realizara una evaluación con preguntas que medirán la efectividad del plan de formación.

Plan de formación

2 Tratamiento y administración del MPSI

Contenido:

1. Seguridad de la información (según los temas críticos que sean requeridos para la administración del MPSI).

¿A quien va dirigido?

Equipo encargado de la administración del MPSI y que se encuentran en el comité de Seguridad de la Información

Periodicidad

Anual

Evaluación

Sobre los temas se realizara una evaluación con preguntas que medirán la efectividad del plan de formación.



3

**Administración
del MSPI**

Administración del MSPI

Detalles del servicio

Finalizada la construcción e implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) de CORANTIOQUIA, el servicio administrado de seguridad y privacidad de la información le permitirá a la Corporación gestionar el modelo implementado y, que así, se realice un seguimiento continuo a la Seguridad de la información.

Para garantizar la adecuada gestión de seguridad de la información, la Corporación debe incorporar Servicios tercerizados de la administración de seguridad y privacidad de la información.

¿Qué es un Servicio Administrado de Seguridad de la Información?

Los Servicios administrados de seguridad de la información se encargan de realizar un seguimiento y analizar la actividad en servidores, redes, puntos finales, sitios web, aplicaciones, bases de datos y otros sistemas, buscando actividades particulares y anómalas que puedan ser indicativas de un incidente o compromiso de seguridad en la organización.

En resumen, el servicio es responsable de garantizar que los posibles incidentes de seguridad se identifiquen, analicen, defiendan, investiguen e informen correctamente.



Administración del MSPI

Modelo optimo de servicio

Entendiendo la necesidad de Corantioquia de poseer un Servicio administrado de Seguridad de la información, la discusión siguiente es encontrar el modelo más optimo, para lo cual se presentan dos alternativas: modelo interno y modelo tercerizado.

	Interno	Tercerizado
Ventajas	• Equipo propio • Personalización a medida • Almacenamiento interno de logs	• Disponibilidad inmediata • Menor inversión inicial y a largo plazo • Expertise en todos los sectores • Mayor flexibilidad y escalabilidad • Equipo especializado (ahorro en personal)
Desventajas	• Implantación a largo plazo • Mayor inversión total que incluye infraestructura, personal y espacio físico • Dificultad para el calculo del ROI • Dificultad para retener talento	• Conocimiento no específico de la empresa (pero sí del sector) • Almacenamiento no local de logs

Luego del análisis realizado específicamente para Corantioquia y entendiendo las capacidades operacionales de la entidad, se define que el modelo más optimo es el de un servicio tercerizado, toda vez que no existe capacidad instalada para los servicios administrados del MSPI.

¿Cuáles son los objetivos que tiene el Servicio?

- Incrementar la capacidad de vigilancia y detección de amenazas en las actividades diarias de los sistemas de información y comunicaciones de Corantioquia.
- Analizar los ataques o posibles amenazas.
- Recuperar información perdida o dañada que Corantioquia haya podido tener por consecuencia de dichos ataques.
- Mejorar la capacidad de respuesta ante cualquier ataque.

A través de la vigilancia y análisis realizados, se utilizan procesos estratégicos y metodologías para construir y mantener las líneas de defensas de seguridad de la información. Estos procedimientos deberían incorporar las siguiente iniciativas:

Servicio tercerizado

Detección y respuesta a amenazas desde la infraestructura tecnológica

Gestión de la exposición a amenazas a través de pruebas de vulnerabilidad

Gestión de la exposición a amenazas con enfoque desde las personas

Detección y respuesta a amenazas desde la infraestructura tecnológica

El alcance del servicio de detección y respuesta a amenazas debería incluir al menos:

- Monitoreo 24x7x365 a la infraestructura tecnológica
- Análisis de tráfico de red
- Detección automatizada basada en anomalías
- Bloqueo de ataques
- Monitoreo de activos de alto valor
- Detección de ataques dirigidos
- Detección de robo de datos
- Caza proactiva de amenaza
- Investigación y reacción a incidentes
- Contención y respuesta de incidentes
- Análisis IOC (Indicadores de Compromiso)
- Análisis de Malware
- Gestión de la exposición a amenazas a través de pruebas de vulnerabilidad

Gestión de la exposición a amenazas a través de pruebas de vulnerabilidad

El alcance del servicio gestión de la exposición a amenazas a través de pruebas de vulnerabilidad debería incluir:

- Escaneo de vulnerabilidad
- Reporte de vulnerabilidad
- Gestión de vulnerabilidades
- Revisión de código de aplicación
- Pruebas de penetración
- Configuración de líneas de base y escaneo
- Orquestación y remediación de amenazas
- Soporte de mitigación de riesgos
- Cyber Threat Intelligence
- Cyber CERT Notificación

Gestión de la exposición a amenazas con enfoque desde las personas

El alcance del servicio gestión de la exposición a amenazas con enfoque desde las personas debería incluir:

- Pruebas de Phishing por correo electrónico
- Pruebas de Vishing (Llamadas telefónicas)
- Pruebas de escritorio limpio
- Pruebas de equipos desatendidos
- Pruebas de seguridad física
- Recomendaciones para el cierre de las brechas de seguridad identificadas
- Campañas de concientización que refuercen las vulnerabilidades identificadas

Administración del MSPI

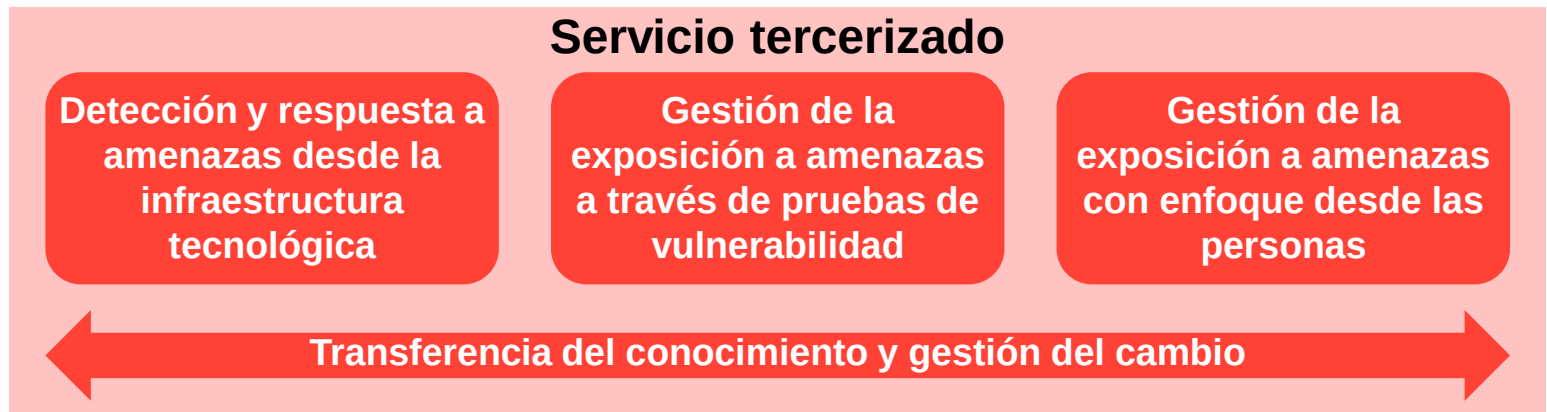
Niveles de servicio / Variables del acuerdo

Niveles de servicio

El servicio administrado de seguridad de la información debe manejar, como mínimo, los siguientes ANS (Acuerdos de Nivel de Servicio):

Incidentes de seguridad críticos	Cualquier hora
Incidentes de seguridad NO críticos	Cualquier hora
Auditoría de vulnerabilidades	Horario laboral
Notificación de alerta temprana	Horario laboral
Gestión de vulnerabilidades	Cualquier hora

Variables del acuerdo



De acuerdo a nuestras referencias en el mercado y con información sobre entidades públicas en SECOP (EDU, IDEA y Plaza Mayor), los costos aproximados son:

\$50.000.000
Valor mensual
Recomendado realizar permanentemente

\$30.000.000
Valor mensual
Recomendado realizar 2 veces al año

\$25.000.000
Valor mensual
Recomendado realizar 2 veces al año



Bibliografía

Bibliografía

- [1] Sophos Ltd. (2019). El rompecabezas imposible de la ciberseguridad. Disponible en: <https://www.sophos.com/es-es/medialibrary/Gated-Assets/white-papers/sophos-impossible-puzzle-of-cybersecurity-wp.pdf>
- [2] El Tiempo (2018). WhatsApp, el más utilizado por los cibercriminales en Colombia. Disponible en: <https://www.eltiempo.com/tecnosfera/novedades-tecnologia/whatsapp-es-la-plataforma-mas-utilizada-por-cibercriminales-en-colombia-303592>
- [3] El Tiempo (2019). Colombia sufrió 42 billones de intentos de ciberataques en 3 meses. Disponible en: <https://www.eltiempo.com/tecnosfera/novedades-tecnologia/colombia-sufrio-42-billones-de-intentos-de-ciberataques-en-3-meses-413666>
- [4] El Espectador (2019). ¿Puede un “hacker” dejar sin luz a Colombia?. Disponible en: <https://www.elespectador.com/tecnologia/puede-un-hacker-dejar-sin-luz-colombia-articulo-821696>
- [5] La Republica (2019). Colombia fue uno de los países con más ataques cibernéticos el año pasado. Disponible en: <https://www.larepublica.co/empresas/colombia-fue-uno-de-los-paises-con-mas-ataques-ciberneticos-el-ano-pasado-2887401>
- [6] El Tiempo (2019). En 2019 se reportaron más de 28.000 casos de ciberataques en Colombia. Disponible en: <https://www.eltiempo.com/tecnosfera/novedades-tecnologia/reporte-de-ciberataques-en-colombia-2019-de-policia-nacional-y-ccit-428790>
- [7] El Tiempo (2018). El sector privado es el más perjudicado por ‘ransomware’. Disponible en: <https://www.eltiempo.com/tecnosfera/novedades-tecnologia/el-sector-privado-es-el-mas-perjudicado-por-ransomware-259090>
- [8] El Tiempo (2017). En Colombia hay 12 empresas afectadas por ciberataque mundial. Disponible en: <https://www.eltiempo.com/tecnosfera/novedades-tecnologia/numero-de-empresas-afectadas-en-colombia-por-ciberataque-mundial-103550>

Bibliografía

- [9] Ministerio de Tecnologías de la Información y Comunicaciones. (26, Mayo 2015). Decreto Número 1078. Disponible en: https://www.mintic.gov.co/portal/604/articles-9528_documento.pdf
- [10] Congreso de Colombia. (25, Mayo 2019). Ley Número 1955. Disponible en: <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=93970>
- [11] Ministerio de Tecnologías de la Información y Comunicaciones. (14, Junio 2018). Decreto Número 1008. Disponible en: https://www.mintic.gov.co/portal/604/articles-74903_documento.pdf
- [12] Ministerio de Tecnologías de la Información y Comunicaciones. (4, Abril 2018). Decreto Número 612. Disponible en: <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=85742>
- [13] Ministerio de Tecnologías de la Información y Comunicaciones. (11, Septiembre 2017). Decreto Número 1499. Disponible en: <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=83433>
- [14] Ministerio de Tecnologías de la Información y Comunicaciones. (25, Agosto 2017). Decreto Número 1413. Disponible en: https://www.mintic.gov.co/portal/604/articles-59399_documento.pdf
- [15] Congreso de Colombia. (5, Julio 2015). Ley Estatutaria Número 1757. Disponible en: <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=65335>
- [16] Ministerio de Tecnologías de la Información y Comunicaciones. (31, Diciembre 2015). Resolución Número 3564. Disponible en: <https://mintic.gov.co/portal/inicio/14476:Resolucion-3564-del-31-de-diciembre-de-2015>
- [17] Departamento Administrativo de la Presidencia de la República. (26, Mayo 2015). Decreto Reglamentario Único 1081. Disponible en: <http://wp.presidencia.gov.co/sitios/normativa/dapre/Normativa/Decreto-1081-2015.pdf>
- [18] Ministerio de Tecnologías de la Información y Comunicaciones. (26, Mayo 2015). Decreto Número 1083. Disponible en: <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=62866>

Bibliografía

- [19] Ministerio de Tecnologías de la Información y Comunicaciones. (12, Diciembre 2014). Decreto Número 2573. Disponible en: https://www.mintic.gov.co/portal/604/articles-14673_documento.pdf
- [20] Congreso de la República. (6, Marzo 2014). Ley Número 1712. Disponible en: <https://www.mintic.gov.co/portal/inicio/7147:Ley-1712-de-2014>
- [21] Congreso de Colombia. (27, Febrero 2013). Ley Estatutaria Número 1618. Disponible en: <https://discapacidadcolombia.com/phocadownloadpap/LEGISLACION/LEY%20ESTATUTARIA%201618%20DE%202013.pdf>
- [22] Ministerio de Comercio, Industria y Turismo. (2, Noviembre 2012). Decreto Número 2364. Disponible en: <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=50583>
- [23] Congreso de la República. (17, Octubre 2012). Ley Estatutaria Número 1581. Disponible en: http://www.defensoria.gov.co/public/Normograma%202013_html/Normas/Ley_1581_2012.pdf
- [24] ICONTEC (Consejo Directivo). (15, Junio 2012). NTC Número 5854. Disponible en: https://intranet.meta.gov.co/secciones_archivos/334-35445.pdf
- [25] Departamento Administrativo de la Función Pública. (10, Enero 2012). Decreto Número 019. Disponible en: <http://wsp.presidencia.gov.co/Normativa/Decretos/2012/Documents/Enero/10/Dec1910012012.pdf>
- [26] Ministerio de Tecnologías de la Información y Comunicaciones. (21, Diciembre 2012). Decreto Número 2693. Disponible en: https://mintic.gov.co/portal/604/articles-3586_documento.pdf
- [27] Ministerio del Interior y de Justicia. (28, Enero 2010). Decreto Número 235. Disponible en: <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=38743>

Bibliografía

- [28] Ministerio de Tecnologías de la Información y Comunicaciones. (30, Julio 2009). Ley Número 1341. Disponible en: https://www.mintic.gov.co/portal/604/articles-3707_documento.pdf
- [29] Ministerio de Tecnologías de la Información y Comunicaciones. (5, enero 2009). Ley Número 1273. Disponible en: https://www.mintic.gov.co/portal/604/articles-3705_documento.pdf
- [30] Procuraduría General de la Nación. (4, Septiembre 2008). Circular Número 058. Disponible: https://www.mintic.gov.co/portal/604/articles-3518_documento.pdf
- [31] Ministerio de Tecnologías de la Información y Comunicaciones. (14, Abril 2008). Decreto Número 1151. Disponible en: https://www.mintic.gov.co/portal/604/articles-3643_documento.pdf
- [32] Congreso de la República. (31, Diciembre 2008). Ley estatutaria Número 1266. Disponible en: <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34488>
- [33] Departamento Administrativo de la Función Pública (2015). Guía para la gestión del riesgo de corrupción. Disponible en: http://www.funcionpublica.gov.co/eva/admon/files/empresas/ZW1wcmVzYV83Ng==/archivos/1461159134_5808c334fdf5c054b27c28ada33880f8.pdf
- [34] Departamento Administrativo de la Función Pública, (2018). Guía para la gestión del riesgo y diseño de controles, en entidades públicas. Disponible en: <http://www.funcionpublica.gov.co/-/consulta-publica-de-la-cartilla-de-gestion-de-riesgos-y-controles>
- [35] Ministerio de Tecnologías de la Información y Comunicaciones (). Guía de gestión de riesgos. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf



A1

Apéndice 1: Glosario

Glosario

- ▶ **Activo de información.** Toda aquella información (información financiera, datos personales, entre otros) que reside en medio electrónico o físico que tiene un significado y valor para la Compañía y, por ende, necesita ser protegida. Los activos de información incluyen la información estructurada y no estructurada que se encuentre presente en forma impresa, escrita en papel, transmitida por cualquier medio electrónico, almacenada electrónicamente en equipos de cómputo, memorias, dispositivos móviles, cintas o cualquier medio magnético u óptico, etc.
- ▶ **Amenazas.** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la Compañía.
- ▶ **Autorización.** Consentimiento previo, expreso e informado del titular para llevar a cabo el tratamiento de datos personales.
- ▶ **Clasificación de la información.** Proceso que permite determinar cualitativamente el valor o la criticidad de un activo de información para Corantioquia, en cuanto a su confidencialidad, integridad y disponibilidad. Tiene como objetivo identificar mecanismos de control necesarios que permitan asegurar los activos de información. Los activos de información se pueden clasificar de la siguiente forma: Público, de uso interno, confidencial y secreto.
- ▶ **Confidencialidad.** Principio que busca asegurar que la información de la entidad sea accedida solo por personal que tiene una necesidad legítima para la realización de sus funciones, con el fin de prevenir el uso o divulgación de la misma en forma no autorizada.

Glosario

- ▶ **Contenedor de la información.** Cualquier plataforma tecnológica o lugar físico que almacena, procesa, transmite o transporta un activo de información por cualquier lapso de tiempo o propósito.
- ▶ **Custodio de la información.** Encargado de proteger un activo de información durante su registro, procesamiento, transmisión, transporte y almacenamiento, mediante la implementación, mantenimiento y sostenibilidad de los controles sugeridos por el propietario de la Información en los contenedores del activo de información. Para el ejercicio de clasificación de activos de información, en la etapa de la elaboración del inventario de los mismos, se deben tener en cuenta todos los posibles custodios y por ende, deben ser relacionados en la matriz o documento donde se realice el inventario de activos de información.
- ▶ **Disponibilidad.** Principio que busca asegurar que la información esté disponible cuando sea requerido por los procesos de Corantioquia.
- ▶ **Información confidencial.** Información de uso exclusivo por parte de usuarios claramente identificados y autorizados dentro de la entidad. La divulgación no autorizada de este tipo de información conlleva impactos severos en la operación, reputación de Corantioquia, desventaja competitiva y daños patrimoniales, o podría llegar a ser utilizada por personal no autorizado para fines particulares, entre otros.

Glosario

- ▶ **Incidente de seguridad.** Evento adverso dentro del sistema interno de recursos tecnológicos que compromete la confidencialidad, integridad, disponibilidad, la legalidad y confiabilidad de la información. Puede ser causado mediante la presencia de alguna vulnerabilidad, intento o amenaza de romper los mecanismos de seguridad existentes.
- ▶ **Integridad.** Principio que busca asegurar que la información esté protegida contra modificaciones no autorizadas para garantizar su consistencia, exactitud y completitud.
- ▶ **Proceso.** Grupo de actividades relacionadas de manera lógica que, cuando se llevan a cabo, utilizan los recursos de la entidad para lograr resultados definitivos o transformar elementos de entrada, a través de una serie de actividades, en un producto o servicio.
- ▶ **Propietario del activo (o de la información).** Funcionario encargado de identificar y establecer el alcance y valor o criticidad de un activo de información, los requerimientos de seguridad del mismo y la comunicación de éstos a los custodios del activo de información.
- ▶ **Riesgo.** Hecho, acción o una omisión que puede afectar en forma adversa a la organización.
- ▶ **Usuario.** Colaborador, contratista o tercero que tiene acceso a los activos de información personal.

Glosario

- ▶ **Valor de la información.** Expectativa o estimación cualitativa que hace la entidad sobre la capacidad que tiene un activo de información de satisfacer la operación de los procesos de la Compañía.
- ▶ **Vulnerabilidad.** Debilidad asociada al contenedor de un activo de información y que puede ser explotada para materializar un riesgo, causando incidentes no deseados que pueden dar lugar a la pérdida de confidencialidad, integridad o disponibilidad de los activos de información y datos personales.