

	RESOLUCIÓN	Código: GJU-FR-01
		Versión 02
		Página 1 de 2

1000

RESOLUCIÓN 048/24

POR MEDIO DE LA CUAL SE ADOPTA EL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (MSPI)

LA DIRECCIÓN EJECUTIVA SUPLENTE DE LA CORPORACIÓN GILBERTO ECHEVERRI MEJÍA

En uso de sus facultades legales y estatutarias y, en especial por las conferidas en los artículos 35 y 37 de los estatutos y

CONSIDERANDO QUE:

1. Que, la Corporación Gilberto Echeverri Mejía es una asociación mixta sin ánimo de lucro, descentralizada de forma indirecta del orden departamental de Antioquia, perteneciente a la rama del poder ejecutivo, que entre sus asociados están La Fundación EPM, La Gobernación de Antioquia y el Instituto para el Desarrollo de Antioquia-IDEA-. Fue constituida por Acta No. 1, otorgada por la Asamblea de Asociados, en octubre 24 de 2013, por lo tanto, se denomina ENTIDAD ESTATAL, conforme lo establece el literal a) numeral 1 del artículo 2 de la ley 80 de 1993, es así como, en lo relativo a sus actos y contratos, la legislación aplicable es la que rige la contratación administrativa.
2. Que, el objeto de esta es gerenciar la política de acceso y permanencia en la educación superior a través de la promoción, administración, financiación y operación de programas para la educación superior de jóvenes de escasos recursos de estratos 1, 2 y 3 en el Departamento de Antioquia; así como la gestión, promoción y consolidación de mecanismos para la formación en Educación Superior.
3. Que es deber de las entidades salvaguardar la información y velar por un tratamiento adecuado de esta, permitiendo la seguridad de la información en el marco de los postulados consagrados en el Decreto 1078 de 2015 y la Ley 1581 de 2012, Por la cual se dictan disposiciones generales para la protección de datos personales y diagnóstico de seguridad y Privacidad de la información, facilitando un cabal desarrollo de las operaciones de la entidad y que debe ser observado y acatado por los colaboradores de la organización en aras de garantizar la seguridad de la información a la que se tiene acceso en el marco de las actividades y /o funciones realizadas.
4. Que, El objetivo de este plan de implementación es establecer todas las acciones a ejecutar en cada una de las fases del ciclo de operación, así como plasmar las principales evidencias y resultados en cada fase: Diagnóstico, Planificación, Implementación, Evaluación de Desempeño y Mejora Continua.
5. El MSPI se encuentra alineado con el Marco de Referencia de Arquitectura TI, el Modelo Integrado de Planeación y Gestión (MIPG) y La Guía para la Administración del Riesgo y el Diseño Controles en entidades Públicas, este modelo pertenece al habilitador transversal de Seguridad y Privacidad, de la Política de Gobierno Digital y se desarrolla mediante el Documento Maestro del Modelo de Seguridad y Privacidad de la Información y sus guías de orientación.

+ (57) (4) 540 90 40 / 01 8000 413522

Edificio Estación Medellín - Ferrocarril de Antioquia
Carrera 52 n° 43 - 31, Oficinas 204 y 205, Medellín, Antioquia

www.corporaciongilbertoecheverri.gov.co



Fundación epm



	RESOLUCIÓN	Código: GJU-FR-01
		Versión 02
		Página 2 de 2

6. Que, en mérito de lo expuesto, la dirección ejecutiva suplente de la CORPORACIÓN GILBERTO ECHEVERRI MEJÍA

RESUELVE:

ARTÍCULO PRIMERO: Adoptar la versión 1 del Modelo de Seguridad y Privacidad de la Información en la Corporación Gilberto Echeverri Mejía.

ARTÍCULO SEGUNDO: El Modelo de Seguridad y Privacidad de la Información rige a partir de la fecha de su publicación, se divulgará a través del portal institucional, y estará sujeto a actualizaciones en la medida en que se modifiquen o se dicten nuevas disposiciones legales sobre la materia.

Dada en Medellín, el día 20 de agosto de 2024

PUBLIQUESE Y CÚMPLASE



SANDRA PAOLA NOHAVÁ BRAVO
Directora Ejecutiva Suplente

Anexos: Modelo de Seguridad y Privacidad de la Información.

Proyectó: Duver Mario Vasco Velazquez, Profesional Universitario de Oficina TICS

Revisó: Alejandro Hernandez Agudelo, Profesional de la Oficina de Planeación Institucional

Revisó: Jessika Del Carmen Hinestroza Palacios. Profesional especializada de la Oficina Jurídica

Archivar en Resoluciones 2024

CORPORACIÓN GILBERTO ECHEVERRI MEJÍA

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN E IMPLEMENTACIÓN DEL MSPI

**MEDELLIN
2024
VERSION 1**

 **+(57) (4) 540 90 40 / 01 8000 413522**

Edificio Estación Medellín - Ferrocarril de Antioquia
Carrera 52 n° 43 - 31, Oficinas 204 y 205, Medellín, Antioquia

www.corporaciongilbertoecheverri.gov.co



Fundación **epm**

Contenido

1. Introducción.....	3
2. Marco Normativo	3
3. Objetivo General.....	4
4. Alcance.....	4
5. Descripción General del Ciclo de Operación	4
Primera Fase: Diagnóstico	5
Segunda Fase: Planificación.....	18
Tercera Fase: Implementación	21
Cuarta Fase: Evaluación de Desempeño	22
Quinta Fase: Mejora Continua.....	24
Resumen	25

1. Introducción

El modelo de seguridad y privacidad de la información entrega directrices en materia de implementación y adopción de buenas prácticas teniendo como referentes estándares internacionales relacionados con el ciclo de vida de la Seguridad y Privacidad de la Información (Planeación, Implementación Evaluación, Mejora continua), así como el plan de acción para la implementación de dichas políticas definidas y planteadas por el Modelo MSPI.

Si bien la Corporación ya viene adelantando varias actividades respecto a la implementación de acciones del Modelo MSPI, es necesario, hacer un cubrimiento completo en todos los aspectos que define los lineamientos del MinTIC referente a los temas de Seguridad y Privacidad de la Información.

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.

Este documento va dirigido a los funcionarios del área de Tecnología encargados de implementar este tema, funcionarios del resto de áreas que apoyan la implementación, así como los funcionarios tomadores de decisiones dentro de la Corporación que tienen a su cargo la gestión y aprobación de los recursos para tal fin.

2. Marco Normativo

- Constitución Política de Colombia. Artículos 15, 209 y 269.
- Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales.
- Decreto 1377 de 2013. Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
- Ley 1712 de 2014. Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
- Decreto 103 de 2015. Por medio del cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
- Decreto 1078 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- Decreto 1083 de 2015 “Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública”, el cual establece las políticas de Gestión y Desempeño Institucional, entre las que se encuentran las de “11. Gobierno Digital” y “12. Seguridad Digital”.
- CONPES 3854 de 2016. Política Nacional de Seguridad digital.
- Ley 1915 de 2018. Por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos.
- Decreto 612 de 2018. Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.

3. Objetivo General

El objetivo de este plan de implementación es establecer todas las acciones a ejecutar en cada una de las fases del ciclo de operación, así como plasmar las principales evidencias y resultados en cada fase: Diagnóstico, Planificación, Implementación, Evaluación de Desempeño y Mejora Continua.

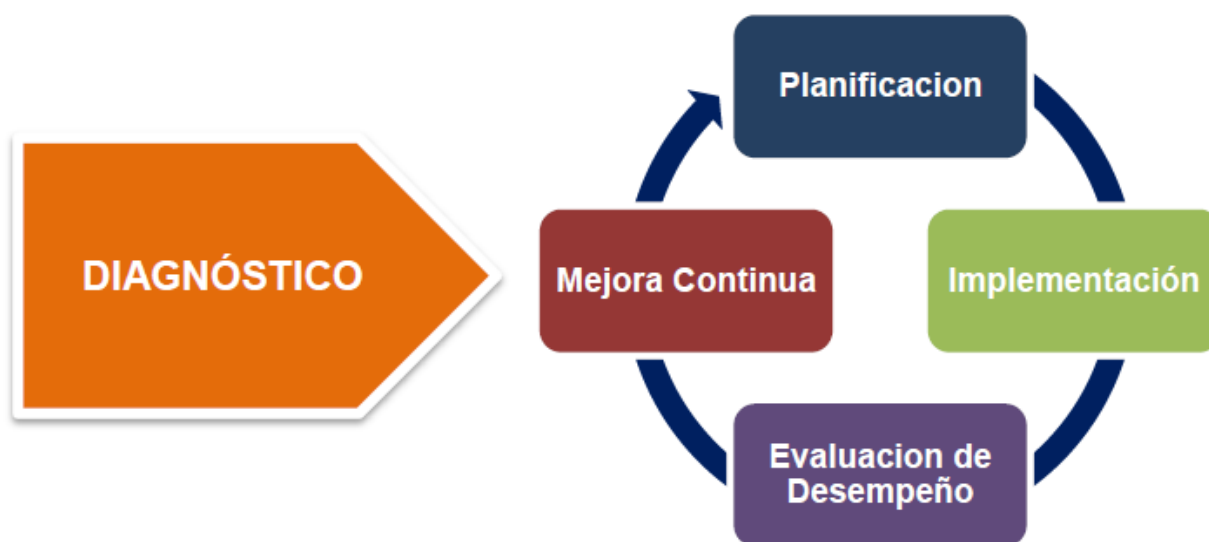
El Modelo de Seguridad y Privacidad de la Información – MSPI, conduce a la preservación de la confidencialidad, integridad, disponibilidad de la información, permitiendo garantizar la privacidad de los datos, mediante la aplicación de un proceso de gestión del riesgo, brindando confianza a las partes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

4. Alcance

El alcance del MSPI permite a la Entidad definir los límites sobre los cuales se implementará la seguridad y privacidad en la Entidad. Este enfoque es por procesos y debe extenderse a toda la Entidad. Para desarrollar el alcance y los límites del Modelo se deben tener en cuenta las siguientes recomendaciones: Procesos que impactan directamente la consecución de objetivos misionales, procesos, servicios, sistemas de información, ubicaciones físicas, terceros relacionados, e interrelaciones del Modelo con otros procesos.

5. Descripción General del Ciclo de Operación

El ciclo de operación del Modelo de Seguridad y Privacidad de la Información comprende cinco (5) etapas o fases, empezando por el Diagnóstico y luego, de forma iterativa, se ejecutan el resto de las fases, como se esquematiza en el siguiente gráfico:



Ciclo de operación del Modelo de Seguridad y Privacidad de la Información - Fuente: Guía del MinTIC

Primera Fase: Diagnóstico

Esta primera fase es muy importante, pues pretende identificar el estado actual de la organización con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información.

En la siguiente tabla se presentan las metas, resultados e instrumentos a utilizar para esta fase de Diagnóstico:

Diagnostico			
Metas	Resultados	Instrumentos MSPI	Alineación MRAE
Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la Entidad.	Diligenciamiento de la herramienta.	Herramienta de diagnóstico.	LI.ES.01 LI.ES.02 LI.GO.01 LI.GO.04 LI.GO.05 LI.GO.07 LI.ST.14
Identificar el nivel de madurez de seguridad y privacidad de la información en la Entidad	Diligenciamiento de la herramienta e identificación del nivel de madurez de la entidad.	Herramienta de diagnóstico	
Identificar vulnerabilidades técnicas y administrativas que sirvan como insumo para la fase de planificación.	Documento con los hallazgos encontrados en las pruebas de vulnerabilidad.	Herramienta de diagnóstico	

Tabla de Metas, resultados e instrumentos de Diagnóstico del MSPI – Fuente: Guía MinTIC

A continuación, se presentan la estructura diligenciada en el “Instrumento de Diagnóstico del Modelo de Seguridad y Privacidad de la Información” provisto por el MinTIC, el cual se almacena como anexo en el archivo de Excel identificado como “**DIAGNOSTICO MPSI-2024**”.

4.1. Evaluación de Efectividad de Controles - ISO 27001:2022 Anexo A

En este componente se muestra el resultado del análisis de brecha frente a los controles del Anexo A, del estándar ISO 27001:2022 en los 14 dominios planteados en la norma:

No.	Evaluación de Efectividad de controles			EVALUACIÓN DE EFECTIVIDAD DE CONTROL
	DOMINIO	Calificación Actual	Calificación Objetivo	
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	80	100	GESTIONADO
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	79	100	GESTIONADO
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	86	100	OPTIMIZADO
A.8	GESTIÓN DE ACTIVOS	69	100	GESTIONADO
A.9	CONTROL DE ACCESO	58	100	EFFECTIVO
A.10	CRIPTOGRAFÍA	40	100	REPETIBLE
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	88	100	OPTIMIZADO
A.12	SEGURIDAD DE LAS OPERACIONES	52	100	EFFECTIVO
A.13	SEGURIDAD DE LAS COMUNICACIONES	39	100	REPETIBLE
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	38	100	REPETIBLE
A.15	RELACIONES CON LOS PROVEEDORES	20	100	INICIAL
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	17	100	INICIAL
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	87	100	OPTIMIZADO
A.18	CUMPLIMIENTO	52,5	100	EFFECTIVO
PROMEDIO EVALUACIÓN DE CONTROLES		58	100	EFFECTIVO

Tabla resultado de la Evaluación

Esta tabla nos indica que, como un dato consolidado, la Corporación Gilberto Echeverri Mejía tiene un promedio de 58% sobre 100%, logrando identificar que de los 14 dominios planteados por la norma ISO 27001:2022, ningún dominio se encuentra cumpliendo al 100%, y el resto de los dominios cuentan con cierto porcentaje de cumplimiento.

Esto nos da los lineamientos para comenzar a identificar áreas por mejorar, planteando diferentes actividades para nivelar los porcentajes a un nivel óptimo.

En la siguiente gráfica, vemos una representación de dicha brecha identificada en los 14 dominios planteados por la norma ISO 27001:2022.

BRECHA ANEXO A ISO 27001:2022



Resultado del análisis de la brecha en la Corporación

4.2. Avance Ciclo de Funcionamiento del Modelo de Operación (PHVA)

Este componente de la hoja consta de una tabla y una gráfica, permite evidenciar el avance en el ciclo del modelo de seguridad definido en el documento MSPI, el cual está alineado con los plazos para la implementación de las actividades que se establecieron para el Manual de Gobierno en Línea, y a través del Decreto 1078 de 2015, en el Título 9, Capítulo 1, Sección 3.

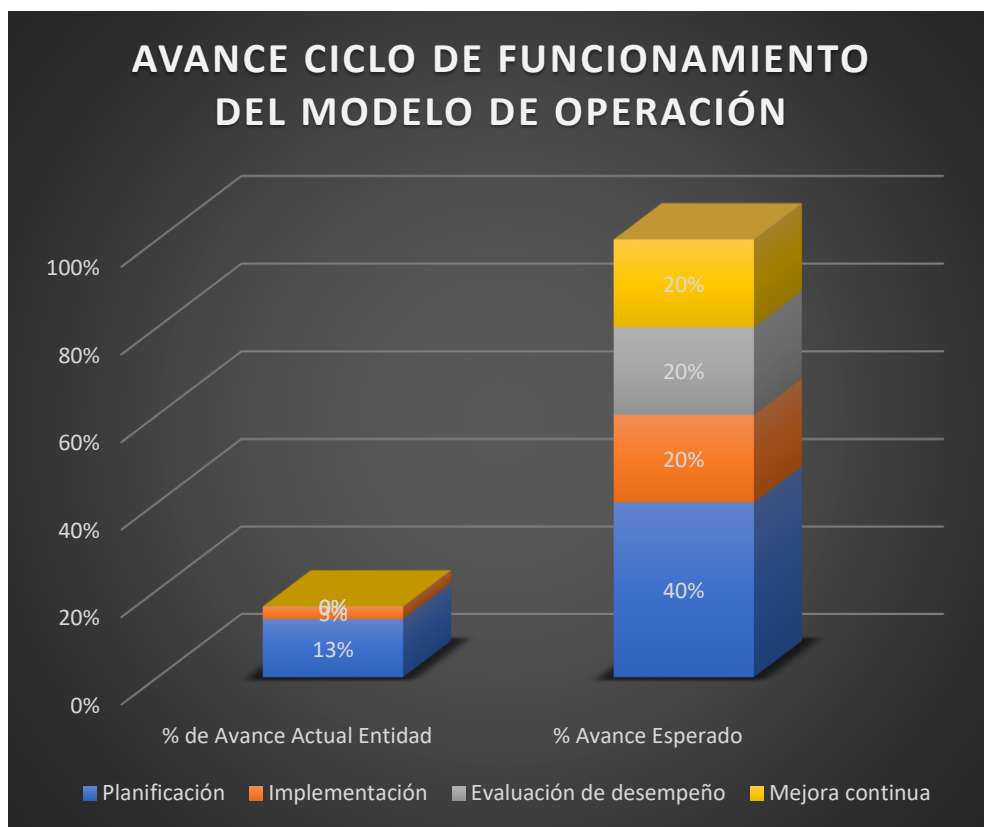
A continuación, se presenta la escala para la valoración en el instrumento de diagnóstico:

Tabla de Escala de Valoración de Controles		
Descripción	Calificación	Criterio
No Aplica	N/A	No aplica.
Inexistente	0	Total falta de cualquier proceso reconocible. La Organización ni siquiera ha reconocido que hay un problema a tratar. No se aplican controles.
Inicial	20	1) Hay una evidencia de que la Organización ha reconocido que existe un problema y que hay que tratarlo. No hay procesos estandarizados. La implementación de un control depende de cada individuo y es principalmente reactiva. 2) Se cuenta con procedimientos documentados pero no son conocidos y/o no se aplican.
Repetible	40	Los procesos y los controles siguen un patrón regular. Los procesos se han desarrollado hasta el punto en que diferentes procedimientos son seguidos por diferentes personas. No hay formación ni comunicación formal sobre los procedimientos y estándares. Hay un alto grado de confianza en los conocimientos de cada persona, por eso hay probabilidad de errores.
Efectivo	60	Los procesos y los controles se documentan y se comunican. Los controles son efectivos y se aplican casi siempre. Sin embargo es poco probable la detección de desviaciones, cuando el control no se aplica oportunamente o la forma de aplicarlo no es la indicada.
Gestionado	80	Los controles se monitorean y se miden. Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas de acción donde los procesos no estén funcionando eficientemente.
Optimizado	100	Las buenas prácticas se siguen y automatizan. Los procesos han sido redefinidos hasta el nivel de mejores prácticas, basándose en los resultados de una mejora continua.

La siguiente tabla presenta el avance porcentual, en años, del ciclo PHVA:

Año	AVANCE PHVA		
	COMPONENTE	% de Avance Actual Entidad	% Avance Esperado
2023	Planificación	13%	40%
2023	Implementación	3%	20%
2023	Evaluación de desempeño	0%	20%
2023	Mejora continua	0%	20%
TOTAL		16%	100%

La gráfica presenta una comparación entre el avance logrado por la entidad, el avance objetivo y el avance total posible. La siguiente gráfica, resume el avance actual de la entidad en el modelo de operación, el cual es del 16%:



4.3. Nivel de Madurez Modelo de Seguridad y Privacidad de la Información

Este componente indica el nivel de madurez en el que se encuentra la entidad evaluada con respecto al Modelo de Seguridad y Privacidad de la Información:

TOTAL DE REQUISITOS CON CALIFICACIONES DE CUMPLIMIENTO	
CRÍTICO	0% a 35%
INTERMEDIO	36% a 70%
SUFICIENTE	71% a 100%

Escala de evaluación

NIVELES DE MADUREZ DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN		NIVEL DE CUMPLIMIENTO
	Inicial	INTERMEDIO
	Repetible	INTERMEDIO
	Definido	INTERMEDIO
	Administrado	CRÍTICO
	Optimizado	CRÍTICO

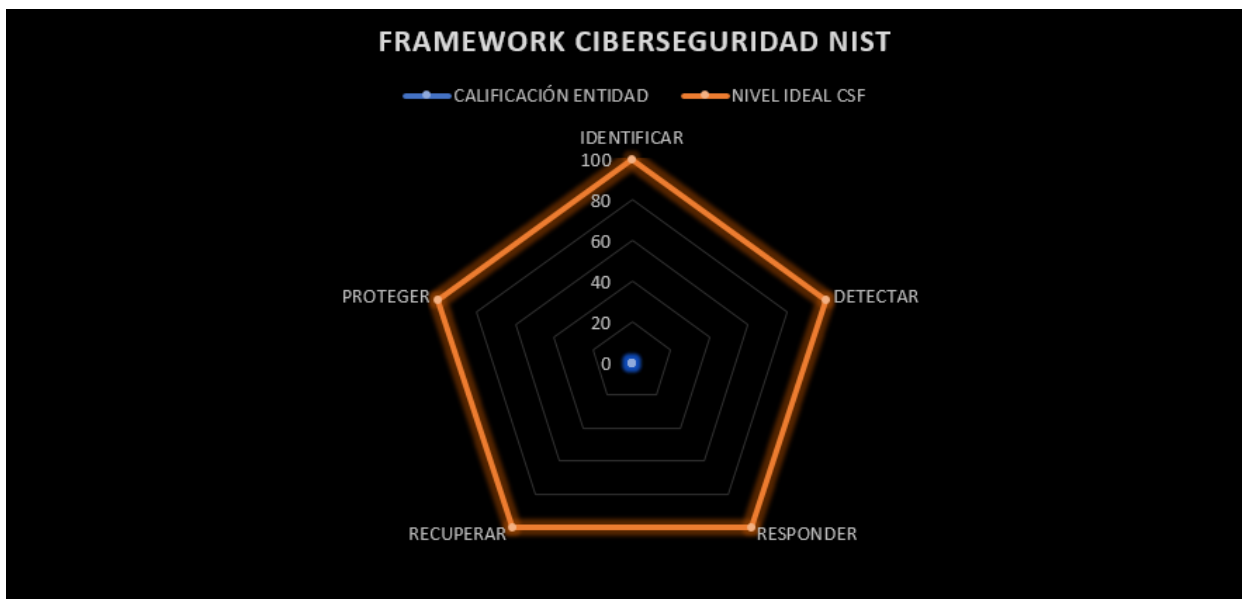
Tabla de resultados del nivel de Madurez

Nivel	Descripción
Inicial	En este nivel se encuentran las entidades, que aún no cuenta con una identificación de activos y gestión de riesgos, que les permita determinar el grado de criticidad de la información, respecto a la seguridad y privacidad de la misma, por lo tanto los controles no están alineados con la preservación de la confidencialidad, integridad, disponibilidad y privacidad de la información
Repetible	En este nivel se encuentran las entidades, en las cuales existen procesos básicos de gestión de la seguridad y privacidad de la información. De igual forma existen controles que permiten detectar posibles incidentes de seguridad, pero no se encuentra gestionados dentro del componente planificación del MSPI.
Definido	En este nivel se encuentran las entidades que tienen documentado, estandarizado y aprobado por la dirección, el modelo de seguridad y privacidad de la información. Todos los controles se encuentran debidamente documentados, aprobados, implementados, probados y actualizados.
Administrado	En este nivel se encuentran las entidades, que cuenten con métricas, indicadores y realizan auditorías al MSPI, recolectando información para establecer la efectividad de los controles.
Optimizado	En este nivel se encuentran las entidades, en donde existe un mejoramiento continuo del MSPI, retroalimentando cualitativamente el modelo.

4.4. Calificación frente a Mejores Prácticas en Ciberseguridad (NIST)

En este componente se muestra una tabla con los resultados de comparar la calificación de acuerdo con la escala de evaluación de los controles existentes en la entidad frente a la mejor práctica en Ciberseguridad definida por NIST:

MODELO FRAMEWORK CIBERSEGURIDAD NIST		
Etiquetas de fila	CALIFICACIÓN ENTIDAD	NIVEL IDEAL CSF
IDENTIFICAR	0	100
DETECTAR	0	100
RESPONDER	0	100
RECUPERAR	0	100
PROTEGER	0	100



4.5. Levantamiento de Información

La lista de información a solicitar es todo el conjunto de documentos y/o registros solicitados mediante el anexo 2. Aquí se transfiere la información diligenciada por la entidad en el nombre del documento entregado y las observaciones si aplica.

Adicionalmente, se puede agregar la información, en caso de que se haya avanzado en las fases de Implementación, Evaluación de Desempeño y Mejora Continua.

	INSTRUMENTO DE IDENTIFICACIÓN DE LA LINEA BASE DE SEGURIDAD HOJA LEVANTAMIENTO DE INFORMACIÓN	
	Corporación Gilberto Echeverri Mejía	
DATOS BÁSICOS		
Tipo Entidad	ENTIDAD DE ORDEN TERRITORIAL	
Misión	Somos una entidad para la promoción, administración, financiación y operación de programas de acceso y permanencia a la educación superior en el departamento de Antioquia.	
Análisis de Contexto	La Corporación Gilberto Echeverri Mejía, es una entidad asociativa sin ánimo de lucro, con personería jurídica, de participación mixta, descentralizada de forma indirecta del orden departamental de Antioquia, perteneciente a la rama	
Mapa de Procesos		
Organigrama		
PREGUNTAS		
Que le preocupa a la Entidad en temas de seguridad de la	La protección de la información de los beneficiarios desde el punto de vista de la confidencialidad y la integridad.	
En que nivel de madurez considera que está?	Egestionado cuantitativamente	
En que componente del ciclo PHVA considera que va?	Implementación, Gestión y Mejora Continua	
DATOS E INFORMACIÓN A RECOLECTAR PARA LA EVALUACIÓN		
Lista de información BÁSICA a solicitar		
NO.	NOMBRE DEL DOCUMENTO ENTREGADO	OBSERVACIONES
1	Tipo de entidad (Nacional, Territorial A, Territorial B o C)	TERRITORIAL TIPO A
2	Misión	corporaciongilbertocheverri.gov.co/quienes-somos/
3	Análisis de contexto: La entidad debe determinar los aspectos externos e internos que son necesarios para cumplir su propósito y que afectan su capacidad para lograr los resultados previstos en el MSPI.	
4	Mapa de Procesos	
5	Organigrama de la entidad, detallando el área de seguridad de la información o quien haga sus veces	Estructura orgánica - Corporación Gilberto Echeverri Mejía (corporaciongilbertocheverri.gov.co)

El detalle completo de esta pestaña se encuentra en el archivo anexo (DIAGNOSTICO MSPI-2024.xlsx).

4.6. Áreas Involucradas

Esta hoja pretende involucrar en el proceso de autoevaluación el área o responsable, el tema a tratar y el funcionario que debe apoyar en el desarrollo del tema:

RESPONSABLE / AREA	TEMA	FUNCIONARIO
Control interno	Revisiones de seguridad de la información	Control Interno
	Revisión independiente de la seguridad de la información (agente externo)	
	Cumplimiento con las políticas y normas de seguridad.	
	Auditoría de Seguimiento a Planes de Mejoramiento	
	Revision Documental del MSPI	
CONTRATACION	Selección e investigación de antecedentes	Profesional de Juridica
	Términos y condiciones del empleo	
Responsable de compras y adquisiciones	RELACIONES CON LOS PROVEEDORES	Direccion Ejecutiva
	Seguridad de la información en las relaciones con los proveedores	
	Gestión de la prestación de servicios de proveedores	
Responsable de la continuidad	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	Sistemas
	Continuidad de la seguridad de la información	
	Planificación de la continuidad de la seguridad de la información	
	Implementación de la continuidad de la seguridad de la información	
	Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	
	Redundancias	
	Disponibilidad de instalaciones de procesamiento de información	
Responsable de la seguridad física	SEGURIDAD FÍSICA Y DEL ENTORNO	Administracion edificio ferrocarril
	ÁREAS SEGURAS	
	Perímetro de seguridad física	
	Áreas de despacho y carga	
	Visita al Centro de Computo	

Responsable de SI	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	Sistemas
	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	
	SEGURIDAD DE LOS RECURSOS HUMANOS	
	Antes de asumir el empleo	
	Durante la ejecución del empleo	
	Terminación y cambio de empleo	
	GESTIÓN DE ACTIVOS	
	CUMPLIMIENTO	
	Cumplimiento de requisitos legales y contractuales	
	CONTROL DE ACCESO	
	CRIPTOGRAFÍA	
	SEGURIDAD FÍSICA Y DEL ENTORNO	
	SEGURIDAD DE LAS OPERACIONES	
	PROCEDIMIENTOS OPERACIONALES Y RESPONSABILIDADES	
	Procedimientos de operación documentados	
	Gestión de cambios	
	Gestión de capacidad	
	Separación de los ambientes de desarrollo, pruebas y operación	
	PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS	
	COPIAS DE RESPALDO	
	REGISTRO Y SEGUIMIENTO	
	Registro de eventos	
	Protección de la información de registro	
	Registros del administrador y del operador	
	Sincronización de relojes	
	CONTROL DE SOFTWARE OPERACIONAL	
	Instalación de software en sistemas operativos	
	GESTIÓN DE LA VULNERABILIDAD TÉCNICA	
	Gestión de las vulnerabilidades técnicas	
	Restricciones sobre la instalación de software	
	CONSIDERACIONES SOBRE AUDITORÍAS DE SISTEMAS DE INFORMACIÓN	
	Controles sobre auditorías de sistemas de información	
	SEGURIDAD DE LAS COMUNICACIONES	
	GESTIÓN DE LA SEGURIDAD DE LAS REDES	
	TRANSFERENCIA DE INFORMACIÓN	
	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	
	REQUISITOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN	
	SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y DE SOPORTE	
	DATOS DE PRUEBA	
	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	
	Alcance MSPI (Modelo de Seguridad y Privacidad de la Información)	
	Identificación y valoración de riesgos	
	Tratamiento de riesgos de seguridad de la información	
	Toma de conciencia, educación y formación en la seguridad de la información	
	Planificación y control operacional	
	Implementación del plan de tratamiento de riesgos	
	Indicadores de gestión del MSPI	
	Plan de seguimiento, evaluación y análisis del MSPI	
	Evaluación del plan de tratamiento de riesgos	
	Plan de seguimiento, evaluación y análisis del MSPI	
	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	
	Con 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.	
	La gestión de riesgos tiene en cuenta los riesgos de ciberseguridad	
	Detección de actividades anómalas	
	Respuesta a incidentes de ciberseguridad, planes de recuperación y restauración	

Responsable de TICs	Teletrabajo	Sistemas
	Manejo de medios	
	Derechos de propiedad intelectual.	
	CONTROL DE ACCESO	
	SEGURIDAD DE LAS OPERACIONES	
	PROCEDIMIENTOS OPERACIONALES Y RESPONSABILIDADES	
	COPIAS DE RESPALDO	
	CONTROL DE SOFTWARE OPERACIONAL	
	CONSIDERACIONES SOBRE AUDITORÍAS DE SISTEMAS DE INFORMACIÓN	
	SEGURIDAD DE LAS COMUNICACIONES	
	GESTIÓN DE LA SEGURIDAD DE LAS REDES	
	TRANSFERENCIA DE INFORMACIÓN	
	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	
	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	
	Plan y Estrategia de transición de IPv4 a IPv6	
Implementación del plan de estrategia de transición de IPv4 a IPv6		
Redundancias		

El detalle completo de esta pestaña se encuentra en el archivo anexo (DIAGNOSTICO MSP-2024.xlsx).

4.7. Pruebas Administrativas

Estas pruebas están orientadas a los temas de seguridad de la información que no están directamente relacionadas con las áreas tecnológicas de la entidad, y contemplan entre otras cosas la evaluación, implementación, revisión y mejoras de la Política de Seguridad de la Información:

		INSTRUMENTO DE IDENTIFICACIÓN DE LA LINEA BASE DE SEGURIDAD ADMINISTRATIVA Y TÉCNICA PARA EL AVANTAJAMIENTO DE INFORMACIÓN										
Corporación Gilberto Echeverri Mejía												
ID. ITEM	CARGO	ITEM	DESCRIPCIÓN	ISO	MSH	CIBERSEG URIDAD	PRUEBA	EVIDENCIA	BRECHA	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN	
POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN												
AD-1	Responsable de SI	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	Orientación de la dirección para gestión de la seguridad de la información	A.5	Componente planificación y modelo de madurez nivel gestionado					80		
AD-1.1	Responsable de SI	Documento de la política de seguridad y privacidad de la información	Se debe definir un conjunto de políticas para la seguridad de la información aprobadas por la dirección, publicadas y comunicadas a los empleados y a las partes externas pertinentes	A.5.1.1	Componente planificación y modelo de madurez inicial	ID GV-1	¿Se tiene la política de seguridad de la información de la seguridad media? ¿Se definen los objetivos, alcances de las políticas de SI en su estructura alineada con la estrategia y plan de la entidad? ¿SI fue debidamente aprobada y socializada al menos de nivel superior la alta dirección? Responde si la política: ¿Se vive que en seguridad de la información? ¿SI el asignador de las responsabilidades generales y específicas para la gestión de la seguridad de la información, están definidos. ¿El proceso para manejar las desviaciones y las acciones?			80		
AD-1.2	Responsable de SI	Revisión y evaluación	Las políticas para seguridad de la información se debían revisar a intervalos planificados o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continua.	A.5.1.2	componente planificación		Indague sobre los responsables designados para monitorear por la dirección para determinar si cumplen o mejor las políticas. Para la calificación tenga en cuenta que: ¿SI se empezaron a definir las políticas de seguridad y privacidad de la información basadas en el Plan de Seguridad y Privacidad de la Información, están en (2)? ¿SI se iniciaron o aprobaron las políticas de seguridad, privacidad de la información, están en (2)?			80		
RESPONSABILIDADES Y ORGANIZACIÓN SEGURIDAD INFORMACIÓN												
A2	Responsable de SI	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	Marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización	A.6						79		
AD-2.1	Responsable de SI	Organización Interna	Marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización	A.6.1	Componente planificación y modelo de madurez gestionado					68		
							Para revisar la brecha a la NIST y verificación de los roles y					

El detalle completo de esta pestaña se encuentra en el archivo anexo (DIAGNOSTICO MPS-2024.xlsx).

4.8. Pruebas Técnicas

Esta hoja incluye la evaluación de controles y requisitos: Los controles y requisitos evaluados están asociados los dominios A9, A10, A11, A12, A13, A14 y A16, a los requisitos del MSPI, Gobierno en Línea y mejores prácticas en ciberseguridad.

INSTRUMENTO DE IDENTIFICACIÓN DE LA LÍNEA BASE DE SEGURIDAD ADMINISTRATIVA Y TÉCNICA HOJA LEVANTAMIENTO DE INFORMACIÓN								
Corporación Gilberto Echeverri Mejía								
ID/ITEM	CARGO	ITEM	DESCRIPCIÓN	ISO	MSPI	CIBERSEGURIDAD	PRUEBA	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001
CONTROL DE ACCESO								
T.1	Responsable de SI/Responsable de TICs	CONTROL DE ACCESO		A.9	Componente planificación y modelo de madurez nivel gestionado			58
T.1.1	Responsable de SI	REQUISITOS DEL NEGOCIO PARA CONTROL DE ACCESO	Se debe limitar el acceso a información y a instalaciones de procesamiento de información.	A.9.1	Modelo de madurez definido			70
T.1.1.1	Responsable de SI	Política de control de acceso	Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.	A.9.1.1		PR.D5-5	Revisar que la política contenga lo siguiente: a) los requisitos de seguridad para las aplicaciones del negocio; b) las políticas para la divulgación y autorización de la información, y los niveles de seguridad de la información y de clasificación de la información; c) la coherencia entre los derechos de acceso y las políticas de clasificación de información de los sistemas y redes; d) la legislación pertinente y cualquier obligación contractual concerniente a la limitación del acceso a datos o servicios; e) la gestión de los derechos de acceso en un entorno distribuido y en red, que reconozca todos los tipos de conexiones disponibles; f) la separación de los roles de control de acceso, (solicitud de acceso, autorización de acceso, administración del acceso); g) los requisitos para la autorización formal de las solicitudes de acceso; h) los requisitos para la revisión periódica de los derechos de acceso; i) el retiro de los derechos de acceso; j) el ingreso de los registros de todos los eventos significativos concernientes al uso y gestión de identificación de los usuarios, e información de autenticación secreta, en el archivo permanente; k) los roles de acceso privilegiado;	80
T.1.1.2	Responsable de TICs	Acceso a redes y a servicios en red.	Se debe permitir acceso de los usuarios a la red y a los servicios de red, para los que han sido.	A.9.1.2		PR.AC-4 PR.D5-5	Revisar la política relacionada con el uso de redes y de servicios de red y verificar que incluya: a) las redes y servicios de red a los que se permite el acceso; b) los procedimientos de autorización para determinar a quién se permite el acceso a qué redes y servicios de red; c) los controles y procedimientos de gestión para proteger el acceso a las conexiones de red y a los servicios de red;	60

El detalle completo de esta pestaña se encuentra en el archivo anexo (DIAGNOSTICO MSPI-2024.xlsx).

4.9. Avance PHVA

A través del diligenciamiento y la formulación de esta hoja se determina el nivel de cumplimiento de acuerdo al ciclo PHVA del modelo de seguridad MSPI, el ciclo evaluado incluye cuatro (4) componentes Planificación, Implementación, Gestión y Mejora Continua.

		INSTRUMENTO DE IDENTIFICACIÓN DE LA LÍNEA BASE DE SEGURIDAD ADMINISTRATIVA Y TÉCNICA HOJA LEVANTAMIENTO DE INFORMACIÓN					
		Corporación Gilberto Echeverri Mejía					
COMPONENTE	ID	CARGO	ITEM	DESCRIPCIÓN	PRUEBA	CIBERSEGURIDAD	MSPI
	P.1	Responsable SI	Alcance MSPI (Modelo de Seguridad y Privacidad de la Información)	Se debe determinar los límites y la aplicabilidad del SGSI para establecer su alcance.	Solicite el documento del alcance que debe estar aprobado, socializado al interior de la Entidad, por la alta dirección. Determine si en la definición del alcance se considerará: 1) Aspectos internos y externos referidos en el 4.1.1: La Entidad debe determinar los aspectos externos e internos que son necesarios para cumplir su propósito y que afectan su capacidad para lograr los resultados previstos en el SGSI. Nota. La terminación de estos aspectos hace referencia a establecer el contexto interno y externo de la empresa, referencia a la norma ISO 31000:2009 en el apartado 5.3. 2) Los requisitos referidos en 4.2.1: a. Se debe determinar las partes interesadas que son pertinentes al SGSI. b. Se debe determinar los requisitos de las partes interesadas. Nota. Los requisitos pueden incluir los requisitos legales y de reglamentación y las obligaciones contractuales. 3) Las interfaces y dependencias entre las actividades realizadas y las que realizan otras entidades del gobierno nacional o entidades exteriores		componente planificación
					Solicite la política de seguridad de la información de la entidad y evalúe:		

El detalle completo de esta pestaña se encuentra en el archivo anexo (DIAGNOSTICO MSPI-2024.xlsx).

4.10. Madurez MSPI

En la hoja de madurez MSPI, se identifican cada uno de los requisitos para cumplir los niveles de madurez definidos en el MSPI. Estos requisitos en su mayoría han sido previamente evaluados en las hojas Administrativas, Técnicas y PHVA.

 INSTRUMENTO DE IDENTIFICACIÓN DE LA LÍNEA BASE DE SEGURIDAD ADMINISTRATIVA Y TÉCNICA HOJA LEVANTAMIENTO DE INFORMACIÓN Corporación Gilberto Echeverri Mejía											
ID REQUISITO	CARGO	REQUISITO	HOJA	ELEMENTO	CLASIFICACIÓN OBTENIDA	NIVEL 1 INICIAL	CUMPLIMIENTO NIVEL INICIAL	NIVEL 2 GESTIONADO	CUMPLIMIENTO NIVEL GESTIONADO	NIVEL 3 DEFINIDO	CUMPLIMIENTO NIVEL DEFINIDO
R1	n/a	1) Si se identifican en forma general los activos de información de la Entidad 2) Si se cuenta con un inventario de activos de información física y lógica de toda la entidad, documentado y firmado por la alta dirección 3) Si se revisa y monitorean periódicamente los activos de información de la entidad	Administrativas	AD 4.1.1	80	100	MEJOR	100	MEJOR	100	MEJOR
R2	n/a	Se clasifican los activos de información lógicos y físicos de la Entidad.	Administrativas	AD 4.2.1	100	100	CUMPLE	100	CUMPLE	100	CUMPLE
R3	n/a	1. Si los funcionarios de la Entidad no tienen conciencia de la seguridad y privacidad de la información y se han diseñado programas para los funcionarios de conciencia y comunicación, de las políticas de seguridad y privacidad de la información, están en 20. 2. Si se observa en los funcionarios una conciencia de seguridad y privacidad de la información y los planes de toma de conciencia y comunicación, de las políticas de seguridad y privacidad de la información, están aprobados y documentados, por la alta Dirección, están en 40. 3. Si se han ejecutado los planes de toma de conciencia, comunicación y divulgación, de las políticas de seguridad y privacidad de la información, aprobados por la alta Dirección, están en 60.	Administrativas	AD 3.2.2	60	60	CUMPLE	60	CUMPLE	80	MEJOR
R4	n/a	Existencia de la necesidad de implementar el Modelo de Seguridad y Privacidad de la información, para definir políticas, procesos y procedimientos claros para dar una respuesta proactiva a las amenazas que se presenten	PHVA	P.1	0	20	MEJOR	40	MEJOR	60	MEJOR
			Administrativas	AD 1.1	60	20	MEJOR	40	MEJOR	60	CUMPLE
			PHVA	P.4	60	20	MEJOR	40	MEJOR	60	CUMPLE

El detalle completo de esta pestaña se encuentra en el archivo anexo (DIAGNOSTICO MSPI-2024.xlsx).

4.11. Ciberseguridad

En esta hoja se pretende determinar cómo se encuentra la entidad frente a las mejores prácticas en ciberseguridad definidas por el NIST, con miras a ir realizando un diagnóstico frente a los lineamientos de la política de ciberseguridad y ciberdefensa definidos en el documento Conpes 3701 y el Conpes 3854.

		FTIC-LP-09-15 INSTRUMENTO DE IDENTIFICACIÓN DE LA LINEA BASE DE SEGURIDAD ADMINISTRATIVA Y TÉCNICA HOJA LEVANTAMIENTO DE INFORMACIÓN			Corporación Gilberto Echeverri Mejía		
FUNCIÓN NIST	SUBCATEGORÍA NIST	CONTROL ANEXO A ISO 27001	CARGO	REQUISITO	HOJA	CALIFICACIÓN	FUNCION CSF
DETECTAR	DE.AE-1, DE.AE-3, DE.AE-4, DE.AE-5	n/a	Responsable de SI	La detección de actividades anómalas se realiza oportunamente y se entiende el impacto potencial de los eventos: 1) Se establece y gestiona una línea base de las operaciones de red, los flujos de datos esperados para usuarios y sistemas. 2) Se agregan y correlacionan datos de evento de múltiples fuentes y sensores. 3) Se determina el impacto de los eventos 4) Se han establecido los umbrales de alerta de los incidentes.	n/a	80	DETECTAR
DETECTAR	DE.AE-1	n/a	Responsable de SI	La efectividad de las tecnologías de protección se comparte con las partes autorizadas y apropiadas.	n/a	80	DETECTAR
IDENTIFICAR	ID.BE-2	n/a	Responsable de SI	La entidad conoce su papel dentro del estado Colombiano, identifica y comunica a las partes interesadas la infraestructura crítica.	n/a	60	IDENTIFICAR
IDENTIFICAR	ID.GV-4	n/a	Responsable de SI	La entidad tiene en cuenta los riesgos de ciberseguridad.	n/a	60	IDENTIFICAR
RESPONDER	RS.CO-4, RS.CO-5	n/a	Responsable de SI	Las actividades de respuesta son coordinadas con las partes interesadas tanto internas como externas, según sea apropiado, para incluir soporte externo de entidades o agencias estatales o legales.: 1) Los planes de respuesta a incidentes están coordinados con las partes interesadas de manera consistente. 2) De manera voluntaria se comparte información con partes interesadas externas para alcanzar una conciencia más amplia de la situación de ciberseguridad.	n/a	80	RESPONDER
RECUPERAR	RC.CO-1, RC.CO-2, RC.CO-3	n/a	Responsable de SI	Las actividades de restauración son coordinadas con las partes internas y externas, como los centros de coordinación, proveedores de servicios de Internet, los dueños de los sistemas atacados, las víctimas, otros CSIRT, y proveedores.: 1) Se gestionan las comunicaciones hacia el público. 2) Se procura la no afectación de la reputación o la reparación de la misma. 3) Las actividades de recuperación son comunicadas a las partes interesadas internas y a los grupos de gerentes y directores.	n/a	80	RECUPERAR
IDENTIFICAR	ID.RA-3	n/a	Responsable de SI	Las amenazas internas y externas son identificadas y documentadas.	n/a	20	IDENTIFICAR
RESPONDER	RS.IM-2	n/a	Responsable de SI	Las estrategias de respuesta se actualizan	n/a	60	RESPONDER
IDENTIFICAR	ID.BE-3	n/a	Responsable de SI	Las prioridades relacionadas con la misión, objetivos y actividades de la Entidad son establecidas y comunicadas.	n/a	80	IDENTIFICAR
IDENTIFICAR	ID.RA-4	n/a	Responsable de SI	Los impactos potenciales en la entidad y su probabilidad son identificados	n/a	80	IDENTIFICAR
RECUPERAR	RC.IM-1, RC.IM-2	n/a	Responsable de SI	Los planes de recuperación y los procesos son mejorados incorporando las lecciones aprendidas para actividades futuras: 1) Los planes de recuperación incorporan las lecciones aprendidas. 2) Las estrategias de recuperación son actualizadas.	n/a	100	RECUPERAR
PROTEGER	PR.IP-7	n/a	Responsable de SI	Los procesos de protección son continuamente mejorados	n/a	60	PROTEGER
DETECTAR	DE.CM-1, DE.CM-2, DE.CM-7	n/a	Responsable de SI	Los sistemas de información y los activos son monitoreados a intervalos discretos para identificar los eventos de ciberseguridad y verificar la efectividad de las medidas de protección: 1) La red es monitoreada para detectar eventos potenciales de ciberseguridad. 2) El ambiente físico es monitoreado para detectar eventos potenciales de ciberseguridad. 3) Se monitorea en búsqueda de eventos como personal no autorizado, u otros eventos relacionados con conexiones, dispositivos y software.	n/a	60	DETECTAR

El detalle completo de esta pestaña se encuentra en el archivo anexo (DIAGNOSTICO MSPI-2024.xlsx).

Segunda Fase: Planificación


 +(57) (4) 540 90 40 / 01 8000 413522

Edificio Estación Medellín - Ferrocarril de Antioquia
 Carrera 52 n° 43 - 31, Oficinas 204 y 205, Medellín, Antioquia
www.corporaciongilbertocheverri.gov.co



Fundación epm



Para el desarrollo de esta fase la Corporación utilizó los resultados de la etapa de Diagnóstico y procedió a elaborar el plan de seguridad y privacidad de la información, alineado con el objetivo misional de la entidad, con el propósito de definir las acciones a implementar a nivel de seguridad y privacidad de la información.

El alcance del MSPI permite a la Corporación, definir los límites sobre los cuales se implementará la seguridad y privacidad en la entidad.

Esta etapa tiene los siguientes entregables:

5.1. Política de seguridad y privacidad de la información

La Política de Seguridad y Privacidad de la información está contenida en un documento de alto nivel que incluye la voluntad de la Alta Dirección de la Corporación, para apoyar la implementación del Modelo de Seguridad y Privacidad de la Información.

La política debe contener una declaración general por parte de la administración, donde se especifique sus objetivos, alcance, nivel de cumplimiento.

En la Corporación Gilberto Echeverri Mejía, esta política es establecida mediante el acto administrativo No. 072-2023, en la cual se adoptó la segunda versión del manual de políticas de seguridad de la información para la Corporación Gilberto Echeverri Mejía.

5.2. Procedimientos de Seguridad de la Información

La Corporación cuenta con diferentes guías y procedimientos para gestionar la seguridad de la información en cada uno de los procesos definidos en la entidad. Dentro de los que se destacan las siguientes políticas:

Política de recursos compartidos: Esta política define los diferentes tipos de recursos compartidos que se usan en la Corporación y la forma como se deben gestionar.

Política de manejo de las cuentas de correo: Esta política define el tratamiento y uso de las cuentas de correo de los usuarios de la Corporación que se tienen almacenadas en la plataforma de la nube de Microsoft Office 365.

Política de respaldo de usuarios salientes: Esta política define todos los lineamientos del tratamiento de un usuario que sale o se retira de la Corporación.

5.3. Roles y Responsabilidades de Seguridad y Privacidad de la Información

Mediante el acto administrativo No. 072-2023, se estableció en la corporación, los roles y responsabilidades de seguridad de la información en los diferentes niveles administrativos, a saber:

ROL	RESPONSABLE(S)
Oficial de Protección de Datos	Profesional Universitario Oficina TIC
Responsable de la seguridad de la Base de Datos de Empleados Activos	Base de Datos Física: subdirección de Proyectos Base de Datos sistematizada: Profesional universitario Oficina TIC
Responsable de la seguridad de la Base de Datos de los Becarios	Base de Datos Física: subdirección Proyectos Base de Datos sistematizada: Profesional universitario Oficina TIC
Responsable de la seguridad de la Base de Datos de la Junta Directiva	Base de Datos Física: dirección ejecutiva Base de Datos sistematizada: NO APLICA
Responsable de la seguridad de la Base de Datos de Contratistas y Proveedores Activos e Inactivos	Base de Datos Física: Subdirección Administrativa y Financiera Base de Datos sistematizada: Profesional universitario Oficina TIC
Responsable de la seguridad de la Base de Datos de Corporados	Base de Datos Física: dirección ejecutiva Base de Datos sistematizada: NO APLICA
Responsable de la seguridad de la Base de Datos de Postulantes Becarios	Base de Datos Física: NO APLICA Base de Datos sistematizada: Profesional universitario Oficina TIC
Responsable de la seguridad de la Base de Datos de Capacitaciones y Eventos	Base de Datos Física: subdirección de proyectos Base de Datos sistematizada: Profesional universitario Oficina TIC
Responsable de la seguridad de la Base de Datos de Empleados Inactivos	Base de Datos Física: subdirección Administrativa y Financiera Base de Datos sistematizada: Profesional universitario Oficina TIC
Responsable de la seguridad de la Base de Datos de Aliados Estratégicos	Base de Datos Física: subdirección Administrativa y Financiera Base de Datos sistematizada: subdirección Administrativa y Financiera

5.4. Inventario de activos de información

La Corporación desarrolló una metodología de gestión de activos que le permitió generar un inventario de activos de información a partir de su identificación, clasificación y registro en el catálogo de activos de información

Los lineamientos base para la metodología definida, se establecen en la definición del subproceso "**GT102 Gestión de Información**", del área de Tecnología de la Corporación.

Mediante el acto administrativo No:072, se adoptó los instrumentos de gestión de la información pública de la Corporación Gilberto Echeverri Mejía, los cuales se detallan a continuación:

Registro de Activos de Información.



+ (57) (4) 540 90 40 / 01 8000 413522

Edificio Estación Medellín - Ferrocarril de Antioquia
Carrera 52 n° 43 - 31, Oficinas 204 y 205, Medellín, Antioquia

www.corporaciongilbertoecheverri.gov.co



Fundación **epm**



GOBERNACIÓN DE ANTIOQUIA
República de Colombia

Índice de Información clasificada y reservada.
Esquema de Publicación de Información.

5.5. Identificación, Valoración y Tratamiento de Riesgos

Para este ítem, la Entidad debe definir una metodología de gestión del riesgo enfocada a procesos, que le permita identificar, evaluar, tratar y dar seguimiento a los riesgos de seguridad de la información a los que estén expuestos los activos, es por ello que el grupo interdisciplinario definido en la Corporación, identificó y consignó todos los riesgos en el documento llamado “*Matriz de Riesgos.xlsx*”, en el cual se define toda la metodología a seguir para el tratamiento de los riesgos, desde su identificación, causas y consecuencias, así como el plan para evitarlos o mitigarlos en caso que los riesgos ocurran.

5.6. Plan de Comunicaciones

En el documento del “Plan Estratégico de TI 2023 – PETI” de la Corporación, en las secciones “**7.6 Plan de capacitaciones 2023**”, se detallan las temáticas, objetivos, responsables, grupos de interés y público objetivo, así como los contenidos para la capacitación referentes a Seguridad y Privacidad de la Información.

Así mismo, en este mismo documento, en la sección “**8.6. Implementar estrategia**”, se detallan las actividades referentes a la sensibilización en los temas de Seguridad y Privacidad de la Información.

5.8. Plan de transición de IPv4 a IPv6

La Corporación cuenta con el plan de Transición del protocolo Ipv4 a Ipv6, el cual está consignado en el documento “ESTADO TRANSICION IPV4 A IPV6.doc”, donde se detallan todas las actividades a seguir, divididas en cuatro fases.

Fase 0. Diagnóstico.

Fase 1. Diagnóstico de la Situación Actual.

Fase 2. Desarrollo del Plan de implementación.

Fase 3. Desarrollo del Plan de implementación.

Tercera Fase: Implementación

Esta fase le permite a la Corporación la implementación de la planificación realizada en la fase anterior.

A continuación, se presenta la tabla de metas y resultados para esta etapa, tomada de la guía del MinTIC:

Implementación			
Metas	Resultados	Instrumentos	
		MSPI	MRAE
Planificación y Control Operacional.	Documento con la estrategia de planificación y control operacional, revisado y aprobado por la alta Dirección.	Documento con el plan de tratamiento de riesgos. Documento con la declaración de aplicabilidad.	LI.ES.09 LI.ES.10 LI.GO.04 LI.GO.09 LI.GO.10 LI.GO.14 LI.GO.15 LI.INF.09 LI.INF.10 LI.INF.11 LI.INF.14 LI.INF.15 LI.SIS.22 LI.SIS.23 LI.ST.05 LI.ST.06 LI.ST.09 LI.ST.10 LI.ST.12
Implementación del plan de tratamiento de riesgos.	Informe de la ejecución del plan de tratamiento de riesgos aprobado por el dueño de cada proceso.	Documento con la declaración de aplicabilidad. Documento con el plan de tratamiento de riesgos.	
Indicadores De Gestión.	Documento con la descripción de los indicadores de gestión de seguridad y privacidad de la información.	Guía No 9 - Indicadores de Gestión SI.	
Plan de Transición de IPv4 a IPv6	Documento con las estrategias del plan de implementación de IPv6 en la entidad, aprobado por la Oficina de TI.	Documento con el Plan de diagnóstico para la transición de IPv4 a IPv6. Guía No 20 - Transición de IPv4 a IPv6 para Colombia. Guía No 19 – Aseguramiento del Protocolo IPv6.	LI.ST.13 LI.UA.01

Tabla de Metas y Resultados de la fase de Implementación – Fuente: Guía MinTIC

La Corporación ha iniciado con este proceso, construyendo el documento de tratamiento de riesgos de la Entidad, donde se ha consignado en una matriz todos los riesgos identificados en las diferentes áreas y procesos de la Corporación, así como las causas, consecuencias y las acciones para prevenirlos o para mitigarlos en caso de que se materialicen.

El documento “*Mapa riesgos 2023.xlsm*”, consigna toda la metodología a seguir para el tratamiento de los riesgos.

Así mismo, se cuenta con el plan de Transición del protocolo Ipv4 a Ipv6, el cual está consignado en el documento “ESTADO TRANSICION IPV4 A IPV6.doc”.

En la siguiente sección se detallan los indicadores de evaluación de desempeño y gestión para medir la implementación del modelo de seguridad y privacidad de la información en la Corporación.

Cuarta Fase: Evaluación de Desempeño

El proceso de seguimiento y monitoreo del MSPI se hace con base a los resultados que arrojan los indicadores de la seguridad de la información propuestos para verificación de la efectividad, la eficiencia y la eficacia de las acciones implementadas.

Para el caso de la Corporación, se definieron los siguientes indicadores:

INDICADOR No. 1	Cumplimiento de las Políticas de Seguridad de la Información de la Corporación
ALCANCE:	Indicador que mide el cumplimiento de las políticas de seguridad de la información
OBJETIVO:	Identificar el nivel de estructuración de los procesos de la entidad orientados a la seguridad de la información
TIPO DE INDICADOR:	Indicador de Cumplimiento
PERIODICIDAD:	Anual
DESCRIPCION DE VARIABLES	FORMULAS
VAR01: ¿La entidad ha definido una política general de seguridad de la información?	VAR01 ó VAR02 ó VAR03 = 1 (si se logra la evidencia) VAR01 ó VAR02 ó VAR03 = 0 (si no se evidencia)
VAR02: ¿La entidad ha definido roles y responsabilidades con el fin de cumplir las políticas de seguridad de la información?	
VAR03: ¿La entidad cumple con los requisitos legales y contractuales con respecto al manejo de la información?	
META	
CUMPLE: 1	NO CUMPLE: 0

INDICADOR No. 2	Identificación de lineamientos de Seguridad en la Corporación
DEFINICION:	Grado de la seguridad de la información y de los equipos de cómputo
OBJETIVO:	Medir el nivel de preparación del recurso humano y su apropiación en cuanto a la seguridad de la información y los equipos de cómputo
TIPO DE INDICADOR:	Indicador de Cumplimiento
PERIODICIDAD:	Anual
DESCRIPCION DE VARIABLES	FORMULAS
VAR04: ¿La entidad ha definido lineamientos de trabajo a través del responsable de seguridad para que sus funcionarios cumplan las políticas de seguridad y evalúa periódicamente su pertinencia?	VAR04 ó VAR05 = 1 (si se logra la evidencia) VAR04 ó VAR05 = 0 (si no se evidencia)
VAR05: ¿La entidad ha definido lineamientos en cuanto a la protección de las instalaciones	

físicas, equipos de cómputo y su entorno para evitar accesos no autorizados y minimizar riesgos de la información de la entidad?	
META	
CUMPLE: 1	NO CUMPLE: 0
INDICADOR No. 3	Porcentaje de implementación de controles de seguridad
DEFINICION:	Grado de avance en la implementación de controles de seguridad
OBJETIVO:	Identificar el grado de avance en la implementación de controles de seguridad
TIPO DE INDICADOR:	Indicador de gestion
PERIODICIDAD:	Annual
DESCRIPCION DE VARIABLES	FORMULAS
VAR06: número de controles implementados	(VAR06 / VAR07) * 100
VAR07: número de controles que se planearon implementar	
META	
MINIMA: 75% A 80%	SATISFACTORIA: 81% A 90%
91% A 100%	SOBRESALIENTE:

Quinta Fase: Mejora Continua

En esta fase la Corporación debe consolidar los resultados obtenidos de la fase de Evaluación de Desempeño, para diseñar el plan de mejoramiento continuo de seguridad y privacidad de la información.

Para lograr lo anterior, se debe tener la siguiente información:

Resultados de la ejecución del plan de seguimiento para alimentar los indicadores de gestión.

Resultados del plan de ejecución de auditorías y revisiones independientes al MSPI.

Utilizando los insumos anteriores, la Corporación puede efectuar los ajustes necesarios y tendrán como resultado un plan de mejoramiento y un plan de comunicaciones de mejora continua, revisados y aprobados por la Alta Dirección de la entidad.

9. Acciones de Hacking Ético

En el documento “**Mapa riesgos 2024.xlsm**”, se establecen las acciones mínimas recomendadas para ejecutar para evaluar la eficacia de la implementación del modelo de seguridad respecto a las diferentes vulnerabilidades que se puedan presentar en la Corporación.

El resultado de estas actividades permite desarrollar planes de mitigación para las vulnerabilidades encontradas.

Resumen

Esta tabla nos indica que, como un dato consolidado, la Corporación Gilberto Echeverri Mejía tiene un promedio de 58% sobre 100%, logrando identificar que de los 14 dominios planteados por la norma ISO 27001:2022, ningún dominio se encuentra cumpliendo al 100%, y el resto de los dominios cuentan con cierto porcentaje de cumplimiento.

Lo anterior nos da los lineamientos para comenzar a identificar áreas por mejorar, planteando diferentes actividades para nivelar los porcentajes a un nivel óptimo. Por lo cual se le solicita a recurso económico para el próximo año a la subdirección administrativa y financiera; para así poder iniciar los indicadores que se encuentran en cero y mejorar indicadores de seguridad digital

El nivel de madurez de implementación del estándar ISO 27001:2022, se encuentra en Repetible con un 20%.

En cada uno de los anexos que se presentan a continuación se contemplan planes de acción para mitigar las brechas identificadas tanto en las cláusulas mandatorias como en los objetivos de control del Anexo A del estándar ISO 27001:2022.

Se debe realizar el análisis de vulnerabilidad de red de la corporación, mediante Acciones de Hacking Ético, para de esta forma determinar las acciones a tomaren la red de la corporación



DUVER MARIO VASCO VELASQUEZ
Profesional universitario Oficina TIC