ESTRATEGIA DE PLANIFICACIÓN Y CONTROL OPERACIONAL

MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

ALCALDÍA DEL DISTRITO
DE SANTIAGO DE CALI

2023

COLABORADORES

Nivel Directivo

Equipo Técnico

Departamento Administrativo de Planeación Municipal

Victor Andrés Sandoval
Subdirector de Desarrollo Integral

Adolfo Alfredo Arévalo Barreto
Jhonny Zambrano Zulñiga

Departamento Administrativo de Tecnologías de la Información y las Comunicaciones

Roger González
Subdirector de Tecnología Digital

Cristina Vega Ortíz
Ivan Dario Garzón Fonseca
Lorena Sofia Valderrama Maturana
Rose Marie Reyes Duque

Departamento Administrativo de Desarrollo e Innovación Institucional

Diana Patricia Moreno Cetina
Subdirector de Trámites, Servicios y Gestión Documental

Francisco Javier Millán Hoyos
Jorge Ivan Marmolejo Cardona
Yiminson Solis Estupiñan

Secretaría de Gobierno

Alfagme Sanchez Torres
Jefe de Oficina Asesora de Transparencia

Maria Camila Zemanate Maya
Monica Mesa Marín

Santiago de Cali, julio de 2023

TABLA DE CONTENIDO

INTRODUCCIÓN

El componente de seguridad y privacidad de la información se define como parte integral de la Política de Gobierno Digital, que se establece a través del Decreto Único Reglamentario 1078 de 2015, del sector de Tecnologías de Información y las Comunicaciones. Forma parte del componente de Seguridad y Privacidad de la Información, acorde con las mejores prácticas de seguridad y estándares internacionales las normas ISO 27001 e ISO 31000.

En el ámbito de la misión de la Alcaldía del Distrito de Santiago de Cali y de la implementación de los habilitadores transversales de Gobierno Digital, se debe concebir el Plan de Seguridad y Privacidad de la Información, en el cual, la seguridad se propone ser el marco de la gestión de la organización determinado por las necesidades, objetivos, requisitos, procesos misionales, estratégicos y de apoyo, además del tamaño y estructura de la entidad, y su contexto, de manera que resulte acorde con las características y necesidades institucionales para la preservación de la disponibilidad, confidencialidad e integridad de la información y garantizar la privacidad de los datos, mediante la aplicación de un proceso de gestión del riesgo, que brinde confianza a las partes interesadas gracias a la implementación de controles.

Es por ello que, antes de elaborar el Plan Institucional de Seguridad y Privacidad de la Información, la entidad, por medio de la mesa del MSPI realizó el diagnóstico de nivel de madurez del modelo, que permitió identificar fortalezas y debilidades frente al cumplimiento del mínimo establecido en buenas prácticas de la NTC/IEC 27001. El documento en mención puede ser consultado en el repositorio de Google Drive de productos del MSPI.

En el diagnóstico, se tomó cómo referente el instrumento dispuesto en la caja de herramientas del Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC)[1], del cual se desarrolló el ejercicio de diagnóstico de nivel de madurez del Modelo de Seguridad y Privacidad de la Información - MSPI para la entidad.

Como fue mencionado anteriormente, este trabajo fue elaborado por cuatro organismos que hacen parte del equipo de trabajo o mesa del MSPI, a saber: Subdirección de Tecnología Digital del Departamento de Tecnologías de la Información y las Comunicaciones - Subdirección de Desarrollo Integral del Departamento Administrativo de Planeación - Oficina Asesora de Transparencia de la Secretaría de Gobierno y liderado por la Subdirección de Trámites, Servicios y Gestión Documental del Departamento Administrativo de Desarrollo e Innovación Institucional.

Posteriormente, la mesa del MSPI, elaboró y presenta en este documento la propuesta de Plan de Seguridad y Privacidad de la Información además de los roles y responsabilidades cómo parte integral del cumplimiento del requisito de la norma denominado "*Operación*" que hace parte de la estructura de alto nivel en el ciclo de Deming aplicando la metodología de gestión con los pasos del PHVA, para que sea conocido por la alta dirección de la Alcaldía del Distrito de Santiago de Cali y puedan tomar decisiones frente a la implementación de

[1]Enlace de acceso a la caja de herramientas MINTIC: https://gobiernodigital.mintic.gov.co/portal/Transformate-con-Gobierno-Digital-/Caja-de-herramientas/

controles que permitan fortalecer la seguridad, privacidad de la información y ciberseguridad de los activos de información primarios y secundarios.

1. OBJETIVOS

General

Establecer la estrategia de planificación y control operacional además de roles y responsabilidades del Modelo de Seguridad y Privacidad de la Información (MSPI) de la Alcaldía del Distrito de Santiago de Cali

Específicos

- Verificar resultados del diagnóstico de nivel de madurez del modelo de seguridad y privacidad de la información.
- Elaborar la propuesta de roles y responsabilidades conforme al ciclo de mejora continua (PHVA), teniendo en cuenta los controles establecidos por la NTC/IEC 27001:2013-2022.
- Elaborar la estrategia de planificación y control operacional (requisito 8,1 de la NTC 27001:2022) con las acciones específicas a implementar por la entidad para fortalecer en vigencias futuras el nivel de madurez del MSPI.

2. TÉRMINOS Y DEFINICIONES

Seguridad de la Información: Es la preservación de la confidencialidad, integridad y disponibilidad de la información y consiste en el conjunto de medidas y técnicas utilizadas para salvaguardar los datos que se gestionan dentro de una organización y asegurar que los mismos no salgan del entorno que se ha establecido siendo clave para que las empresas puedan llevar a cabo sus operaciones.

Confidencialidad: Propiedad por la que la información no se pone a disposición o se divulga a personas, entidades o procesos no autorizados.

Integridad: De acuerdo con la NTC ISO/IEC 27001, es la propiedad de salvaguardar la exactitud y estado completo de los activos de información.

Disponibilidad: Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada. La disponibilidad, en el contexto de los sistemas de información se refiere a la capacidad de un usuario para acceder a la información o recursos en una ubicación específica y en el formato correcto.

NTC ISO/IEC 27001 *(Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de seguridad de la información. Requisitos):* Esta norma especifica los requisitos y controles para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información dentro del contexto de la organización. (ISO.ORG, 2022).

Sistema de Gestión de Seguridad de la Información (SGSI) (ISO/IEC 27000:2018): Un Sistema de Gestión para la seguridad de la información consta de una serie de políticas, procedimientos e instrucciones o directrices específicas para cada actividad o sistema de información que persiguen cómo objetivo la protección de los activos de información en una organización.

Modelo de Seguridad y Privacidad de la Información (MSPI): El Modelo de Seguridad y Privacidad de la Información - MSPI, imparte lineamientos a las entidades públicas en materia de implementación y adopción de buenas prácticas, tomando como referencia estándares internacionales (ISO - NIST), con el objetivo de orientar la gestión e implementación adecuada del ciclo de vida de la seguridad de la información (Planeación, Implementación, Evaluación, Mejora Continua), permitiendo habilitar la implementación de la Política de Gobierno Digital. (MINTIC, 2021).

Se desarrolla para que las entidades públicas incorporen la seguridad de la información en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y, en general, en todos los activos de información (primarios y secundarios), con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos.

Niveles de Madurez MSPI: Son aquellos niveles definidos por el líder de la política de Gobierno Digital a nivel nacional (MINTIC), para que las entidades públicas logren identificar el avance o evolución de la seguridad de la información mediante ejercicios de evaluación y diagnóstico de la implementación de los controles establecidos en la NTC 27001. Los niveles son los siguientes:

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 encuentran gestionados dentro del componente de 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.

Figura 1. Niveles de Madurez MSPI - MINTIC

3. METODOLOGÍA

Posterior a la realización del diagnóstico y la identificación del nivel de madurez del MSPI del año 2022, donde fue utilizado el instrumento de evaluación MSPI de MinTIC, archivo en Excel donde entre otros, se especifican en sus pestañas los controles ADMINISTRATIVOS y TÉCNICOS evaluados de la NTC 27001; se continuó con la revisión durante las mesas de trabajo del MSPI, de las columnas "*Cargos*" de las pestañas mencionadas, donde el MINTIC registró de forma genérica un responsable del cumplimiento de cada control.

Después de analizar el registro genérico, se procedió con la recolección de insumos para poder determinar las áreas funcionales que estarían a cargo del cumplimiento de los controles de la norma, y así poder cumplir con un entregable que le permita a la entidad, tener claridad sobre qué hacer y quienes estarían a cargo. Entre los insumos recolectados y revisados están:

- Decreto Extraordinario 411.0.20.0516 de 2016 que determina la estructura de la Administración Central y las funciones de sus dependencias.
- Decreto 4112.010.20.0599 de 12 de octubre de 2018 *Por medio del cual se define el Consejo Superior de Desarrollo Administrativo cómo instancia del Modelo Integrado de Planeación y Gestión MIPG.*
- Decreto 4112.010.20.0664 de 2019 *Por el cual se deroga el Decreto 4112.010.20.0127 de 2018, se realiza un ajuste al equipo de asistencia técnica de Gobierno Digital y se dictan otras disposiciones.*
- Proyecto de Decreto "*Por el cual se conforma el Equipo Técnico de Seguridad de la Información de la Alcaldía del Distrito de Santiago de Cali y se dictan otras*

disposiciones", producto que fue elaborado en reuniones de la mesa transitoria de Arquitectura Empresarial en el 2021.

- Información de los requisitos de los controles establecidos en la norma NTC 27001:2013.

Posteriormente y con el conocimiento de los insumos, se procedió a asignar las áreas o organismos de la administración, cómo responsables para la generación de lineamientos procedimentales y también de aquellas áreas o líderes encargados de implementarlos.

En la asignación, se tuvo en cuenta aquella documentación que es denominada de "alto nivel", que es solicitada por las normas ISO cómo la definición del alcance, diagnóstico, políticas, planes, indicadores, evaluación entre otros, en cumplimiento del ciclo de mejora continua PHVA (Planear - Hacer - Verificar - Actuar), ya que obedece técnicamente a un Sistema de Gestión. Es por ello, que la propuesta de roles y responsabilidades inicia con el ciclo PHVA y posteriormente con aquellos controles procedimentales y técnicos requeridos en la norma.

Después de haber identificado los roles y responsabilidades, se continuó con la propuesta de planificación y control operacional, que hace parte de un requisito de alto nivel en la norma, en este se consolidan las estrategias a desarrollar para preservar la seguridad y privacidad de la información en los activos de la organización.

En el desarrollo de la estrategia de planificación, se identificó en el resultado del diagnóstico de los niveles de madurez definidos por el MINTIC, que la entidad cumple con un resultado SUFICIENTE el nivel inicial y repetible (Nivel 1 y 2) y presenta brechas en los cuatro niveles siguientes, cómo se muestra a continuación:

NIVEL DE CUMPLIMIENTO	BRECHA CONTROLES	PESTAÑA MADUREZ
SUFICIENTE	0	Nivel 1 INICIAL
SUFICIENTE	3	Nivel 2 Gestionado
INTERMEDIO	17	Nivel 3 Definido
CRÍTICO	46	Nivel 4 Gestionado Cuantitativamente
CRÍTICO	59	Nivel 5 Optimizado

Por lo que aparte de considerar las actividades a cumplir en el ciclo PHVA, se consideró el resultado obtenido en los niveles para poder cerrar las debilidades o brechas y para ello se construyó en forma de tabla y con la información obtenida de las RECOMENDACIONES, del diagnóstico, que obedecen a aquellas acciones a cumplir para mejorar los controles, la estrategia de planificación y control operacional, para que la entidad fortalezca y logre seguir escalando en los niveles de madurez definidos a nivel nacional.

4. PROPUESTA DE ROLES Y RESPONSABILIDADES PARA IMPLEMENTAR EL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI)

La mesa técnica del MSPI, realizó la siguiente propuesta de roles y responsabilidades frente a los controles asociados con la NTC/IEC 27001:2013, haciendo distinción entre los controles administrativos y técnicos. Esta propuesta le permitirá a la entidad ajustar y complementar con base conceptual y técnica el documento del proyecto de *"Decreto de Conformación del Equipo Técnico de Seguridad de la Información"*, para que la entidad pueda organizar las responsabilidades y su respectivo cumplimiento de los controles de la norma.

Esta propuesta tuvo cómo insumo el proyecto de Decreto antes mencionado, el Decreto Extraordinario 411.0.20.0516 de 2016 *"Por el cual se determina la estructura de la Administración Central y las funciones de sus dependencias"*, las normas NTC/IEC 27001 - 27002 del año 2013 y su actualización del 2022.

PHVA del MSPI

ORGANISMO RESPONSABLE	REQUISITOS A IMPLEMENTAR	PHVA
MSPI - PHVA Planear		
Consejo Superior Administrativo Decreto 4112.010.20.0599 de 12 de octubre de 2018	Diagnóstico del MSPI, firmado Alcance MSPI aprobado - Alta Dirección (Modelo de Seguridad y Privacidad de la Información) Conformación del comité de seguridad	Planear
Mesa MSPI - Decreto 0664 de 2019: Subdirección de Trámites, Servicios y Gestión Documental Subdirección de Tecnología Digital Subdirección de Desarrollo Integral Oficina Asesora de Transparencia	Políticas de seguridad y privacidad de la información	Planear
Comité Institucional de Coordinación de Control Interno	Políticas de seguridad y privacidad de la información - Aprobación	Planear
Subdirección de Gestión Organizacional Lider Sistemas de Gestión Decreto Extraordinario No, 411.0.20.0516 de 2016. Art 61 - Numeral 1.	Procedimientos de control documental del MSPI	Planear
Consejo Superior Administrativo Decreto 4112.010.20.0599 de 12 de octubre de 2018	Roles y responsabilidades para la seguridad de la información - Aprobación	Planear
Subdirección de Trámites, Servicios y Gestión documental	Inventario de activos de información	Planear

ORGANISMO RESPONSABLE	REQUISITOS A IMPLEMENTAR	PHVA
Decreto Extraordinario No, 411.0.20.0516 de 2016. Art 62- Numeral 2.		
Consejo Superior Administrativo Decreto 4112.010.20.0599 de 12 de octubre de 2018	Inventario de activos de información - Aprobación	Planear
Subdirección de Gestión Organizacional Lider Sistemas de Gestión Decreto Extraordinario No, 411.0.20.0516 de 2016. Art 61 - Numeral 6.	Identificación y valoración de riesgos - Metodología y capacitación	Planear
Mesa MSPI - Decreto 0664 de 2019: Subdirección de Trámites, Servicios y Gestión Documental Subdirección de Tecnología Digital Subdirección de Desarrollo Integral Oficina Asesora de Transparencia	Declaración de aplicabilidad y el plan de tratamiento de seguridad de la información - formulación	Planear
Subdirección de Gestión Organizacional Lider Sistemas de Gestión Decreto Extraordinario No, 411.0.20.0516 de 2016. Art 61 - Numeral 6.	Declaración de aplicabilidad y el plan de tratamiento de seguridad de la información - Metodología Sistema de Gestión	Planear
Comité Institucional de Coordinación de Control Interno	Tratamiento de riesgos de seguridad de la información - Aprobación	Planear
Subdirección de Gestión de Talento Humano Decreto Extraordinario No, 411.0.20.0516 de 2016. Art 63 - Numeral 15	Toma de conciencia, educación y formación en la seguridad de la información	Planear
Mesa MSPI - Decreto 0664 de 2019: Subdirección de Trámites, Servicios y Gestión Documental Subdirección de Tecnología Digital Subdirección de Desarrollo Integral Oficina Asesora de Transparencia	Planificación y control operacional	Planear
Consejo Superior Administrativo Decreto 4112.010.20.0599 de 12 de octubre de 2018	Planificación y control operacional -Aprobación	Hacer

ORGANISMO RESPONSABLE	REQUISITOS A IMPLEMENTAR	PHVA
MSPI - PHVA Implementación		
Mesa MSPI - Decreto 0664 de 2019: Subdirección de Trámites, Servicios y Gestión Documental Subdirección de Tecnología Digital Subdirección de Desarrollo Integral Oficina Asesora de Transparencia	Planificación y control operacional	Hacer
Líderes de proceso	Implementación de controles	Hacer
Líderes de proceso	Implementación del plan de tratamiento de riesgos	Hacer
Mesa MSPI - Decreto 0664 de 2019: Subdirección de Trámites, Servicios y Gestión Documental Subdirección de Tecnología Digital Subdirección de Desarrollo Integral Oficina Asesora de Transparencia	Indicadores de gestión del MSPI	Hacer
MSPI - PHVA Evaluación de desempeño		
Mesa MSPI - Decreto 0664 de 2019: Subdirección de Trámites, Servicios y Gestión Documental Subdirección de Tecnología Digital Subdirección de Desarrollo Integral Oficina Asesora de Transparencia	Plan de seguimiento, evaluación y análisis del MSPI	Verificar
Departamento Administrativo de Control Interno	Auditoría Interna	Verificar
Líderes de Proceso	Evaluación del plan de tratamiento de riesgos	Verificar
Departamento Administrativo de Control Interno	Evaluación del plan de tratamiento de riesgos	Verificar
MSPI - PHVA Mejora Continua		

ORGANISMO RESPONSABLE	REQUISITOS A IMPLEMENTAR	PHVA
Mesa MSPI - Decreto 0664 de 2019: Subdirección de Trámites, Servicios y Gestión Documental Subdirección de Tecnología Digital Subdirección de Desarrollo Integral Oficina Asesora de Transparencia	Plan de seguimiento, evaluación y análisis del MSPI	Actuar
Líderes de procesos	Toma de acciones correctivas o de mejora	Actuar

CONTROLES

ORGANISMO RESPONSABLE	CONTROL A IMPLEMENTAR	ISO
CICCI - Comité Institucional de Coordinación de Control Interno	Documento de la política de seguridad y privacidad de la Información	A.5.1.1
Departamento Administrativo de Contratación Pública	Gestión de la prestación de servicios de proveedores	A.15.2
	Seguridad de la información en la gestión de proyectos	A.6.1.5
	Seguridad de la información en las relaciones con los proveedores	A.15.1
	Selección e investigación de antecedentes	A.7.1.1
	Terminación o cambio de responsabilidades de empleo	A.7.3.1
	Términos y condiciones del empleo	A.7.1.2
	Acuerdos de confidencialidad o de no divulgación	A.13.2.4
	Acuerdos sobre transferencia de información	A.13.2.2
	Mensajería electrónica	A.13.2.3
	Políticas y procedimientos de transferencia de información	A.13.2.1
	Recolección de evidencia	A.16.1.7
	Uso de información de autenticación secreta	A.9.3.1
Departamento Administrativo de Control Disciplinario Interno	Proceso disciplinario	A.7.2.3
	Recolección de evidencia	A.16.1.7
	Responsabilidades y procedimientos	A.16.1.1
Departamento Administrativo de Control Interno	Revisión independiente de la seguridad de la información	A.18.2.1
Departamento Administrativo de Gestión Jurídica Pública	Derechos de propiedad intelectual.	A.18.1.2
	Identificación de la legislación aplicable y de los requisitos contractuales.	A.18.1.1
	Políticas y procedimientos de transferencia de información	A.13.2.1
	Responsabilidades y procedimientos	A.16.1.1

	Protección de los datos y privacidad de la información relacionada con los datos personales	A.18.1.4
Líderes de proceso	Clasificación de la información	A.8.2.1
	Protección de los datos y privacidad de la información relacionada con los datos personales.	A.18.1.4
	Toma de conciencia, educación y formación en la seguridad de la información	A.7.2.2
	Cumplimiento con las políticas y normas de seguridad.	A.18.2.2
	Devolución de activos	A.8.1.4
	Disponibilidad de instalaciones de procesamiento de información	A.17.2.1
	Disposición de los medios	A.8.3.2
	Etiquetado de la información	A.8.2.2
	Gestión de medios removibles	A.8.3.1
	Implementación de la continuidad de la seguridad de la información	A.17.1.2
	Inventario de activos	A.8.1.1
	Manejo de activos	A.8.2.3
	Planificación de la continuidad de la seguridad de la información	A.17.1.1
	Política para dispositivos móviles	A.6.2.1
	Propiedad de los activos	A.8.1.2
	Responsabilidades de la dirección	A.7.2.1
	Revisión de cumplimiento técnico.	A.18.2.3
	Revisión y evaluación	A.5.1.2
	Selección e investigación de antecedentes	A.7.1.1
	Separación de deberes / tareas	A.6.1.2
	Teletrabajo	A.6.2.2
	Términos y condiciones del empleo	A.7.1.2
	Uso aceptable de los activos	A.8.1.3
	Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	A.17.1.3
	Roles y responsabilidades para la seguridad de la información	A.6.1.1
	Suministro de acceso de usuarios	A.9.2.2
	Acceso a redes y a servicios en red	A.9.1.2
	Acuerdos de confidencialidad o de no divulgación	A.13.2.4
	Acuerdos sobre transferencia de información	A.13.2.2
	Ambiente de desarrollo seguro	A.14.2.6
	Análisis y especificación de requisitos de seguridad de la información	A.14.1.1
	Aprendizaje obtenido de los incidentes de seguridad de la información	A.16.1.6

	Áreas de despacho y carga	A.11.1.6
	Controles contra códigos maliciosos	A.12.2.1
	Controles de redes	A.13.1.1
	Controles físicos de entrada	A.11.1.2
	Controles sobre auditorías de sistemas de información	A.12.7.1
	Desarrollo contratado externamente	A.14.2.7
	Disposición segura o reutilización de equipos	A.11.2.7
	Equipos de usuario desatendidos	A.11.2.8
	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	A.16.1.4
	Gestión de cambios	A.12.1.2
	Gestión de capacidad	A.12.1.3
	Gestión de derechos de acceso privilegiado	A.9.2.3
	Gestión de información de autenticación secreta de usuarios	A.9.2.4
	Gestión de las vulnerabilidades técnicas	A.12.6.1
	Gestión de llaves	A.10.1.2
	Instalación de software en sistemas operativos	A.12.5.1
	Mantenimiento de equipos	A.11.2.4
	Mensajería electrónica	A.13.2.3
	Perímetro de seguridad física	A.11.1.1
	Política de desarrollo seguro	A.14.2.1
	Política de escritorio limpio y pantalla limpia	A.11.2.9
	Políticas y procedimientos de transferencia de información	A.13.2.1
	Principios de construcción de sistemas seguros	A.14.2.5
	Procedimiento de ingreso seguro	A.9.4.2
	Procedimientos de control de cambios en sistemas	A.14.2.2
	Protección contra amenazas externas y ambientales	A.11.1.4
	Protección de datos de prueba	A.14.3.1
	Protección de la información de registro	A.12.4.2
	Protección de transacciones de los servicios de las aplicaciones	A.14.1.3
	Prueba de aceptación de sistemas	A.14.2.9
	Pruebas de seguridad de sistemas	A.14.2.8
	Registro de eventos	A.12.4.1
	Registro y cancelación del registro de usuarios	A.9.2.1
	Registros del administrador y del operador	A.12.4.3
	Reporte de debilidades de seguridad de la información	A.16.1.3
	Reporte de eventos de seguridad de la información	A.16.1.2
	Respaldo de la información	A.12.3.1

	Responsabilidades y procedimientos	A.16.1.1
	Respuesta a incidentes de seguridad de la información	A.16.1.5
	Restricción de acceso a la información	A.9.4.1
	Restricciones en los cambios a los paquetes de software	A.14.2.4
	Restricciones sobre la instalación de software	A.12.6.2
	Retiro de activos	A.11.2.5
	Retiro o ajuste de los derechos de acceso	A.9.2.6
	Revisión de los derechos de acceso de usuarios	A.9.2.5
	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	A.14.2.3
	Seguridad de equipos y activos fuera de las instalaciones	A.11.2.6
	Seguridad de los servicios de red	A.13.1.2
	Seguridad de oficinas, recintos e instalaciones	A.11.1.3
	Seguridad de servicios de las aplicaciones en redes públicas	A.14.1.2
	Seguridad del cableado	A.11.2.3
	Separación de los ambientes de desarrollo, pruebas y operación	A.12.1.4
	Servicios de suministro	A.11.2.2
	Sincronización de relojes	A.12.4.4
	Sistema de gestión de contraseñas	A.9.4.3
	Trabajo en áreas seguras	A.11.1.5
	Ubicación y protección de los equipos	A.11.2.1
	Uso de información de autenticación secreta	A.9.3.1
Líderes de proceso segunda línea de defensa	Roles y responsabilidades para la seguridad de la información	A.6.1.1
Mesa MSPI - Decreto 0664 de 2019: Subdirección de Trámites, Servicios y Gestión Documental Subdirección de Tecnología Digital Subdirección de Desarrollo Integral Oficina Asesora de Transparencia	Contacto con las autoridades.	A.6.1.3
	Planificación de la continuidad de la seguridad de la información	A.17.1.1
	Protección de los datos y privacidad de la información relacionada con los datos personales	A.18.1.4
Oficina Asesora de Transparencia	Procedimientos de operación documentados	A.12.1.1
	Responsabilidades y procedimientos	A.16.1.1
Oficina de Comunicaciones	Contacto con grupos de interés especiales	A.6.1.4
	Aprendizaje obtenido de los incidentes de seguridad de la información	A.16.1.6
	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	A.16.1.4

	Políticas y procedimientos de transferencia de información	A.13.2.1
	Responsabilidades y procedimientos	A.16.1.1
	Respuesta a incidentes de seguridad de la información	A.16.1.5
Secretaría de Gestión del Riesgo de Emergencia y Desastres	Disponibilidad de instalaciones de procesamiento de información	A.17.2.1
	Implementación de la continuidad de la seguridad de la información	A.17.1.2
	Planificación de la continuidad de la seguridad de la información	A.17.1.1
	Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	A.17.1.3
	Protección contra amenazas externas y ambientales	A.11.1.4
Subdirección de Desarrollo Integral	Seguridad de la información en la gestión de proyectos	A.6.1.5
	Protección de los datos y privacidad de la información relacionada con los datos personales.	A.18.1.4
	Aprendizaje obtenido de los incidentes de seguridad de la información	A.16.1.6
	Disposición segura o reutilización de equipos	A.11.2.7
	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	A.16.1.4
	Políticas y procedimientos de transferencia de información	A.13.2.1
	Procedimientos de operación documentados	A.12.1.1
	Recolección de evidencia	A.16.1.7
	Responsabilidades y procedimientos	A.16.1.1
	Respuesta a incidentes de seguridad de la información	A.16.1.5
Subdirección de Gestión Estratégica del Talento Humano	Contacto con grupos de interés especiales	A.6.1.4
	Selección e investigación de antecedentes	A.7.1.1
	Separación de deberes / tareas	A.6.1.2
	Teletrabajo	A.6.2.2
	Terminación o cambio de responsabilidades de empleo	A.7.3.1
	Términos y condiciones del empleo	A.7.1.2
	Toma de conciencia, educación y formación en la seguridad de la información	A.7.2.2
	Recolección de evidencia	A.16.1.7
	Uso de información de autenticación secreta	A.9.3.1
	Acuerdos de confidencialidad o de no divulgación	A.13.2.4
	Acuerdos sobre transferencia de información	A.13.2.2
	Mensajería electrónica	A.13.2.3
	Políticas y procedimientos de transferencia de información	A.13.2.1
Subdirección de Gestión Organizacional	Contacto con las autoridades.	A.6.1.3

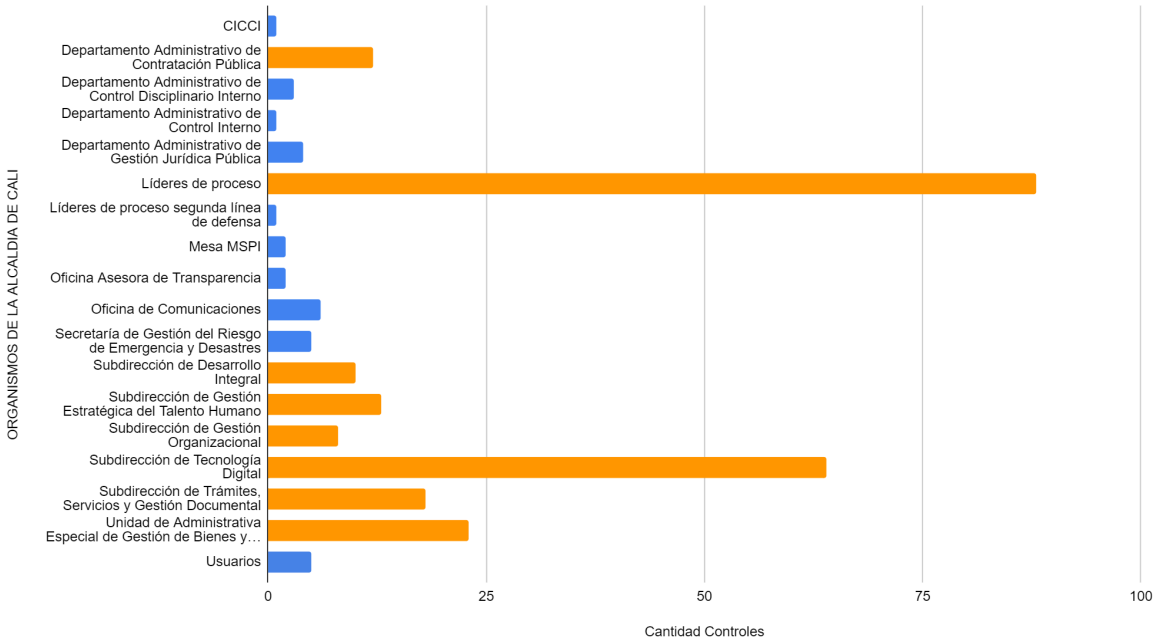
	Documento de la política de seguridad y privacidad de la Información	A.5.1.1
	Revisión y evaluación	A.5.1.2
	Roles y responsabilidades para la seguridad de la información	A.6.1.1
	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	A.16.1.4
	Gestión de cambios	A.12.1.2
	Reporte de debilidades de seguridad de la información	A.16.1.3
	Reporte de eventos de seguridad de la información	A.16.1.2
Subdirección de Tecnología Digital	Disponibilidad de instalaciones de procesamiento de información	A.17.2.1
	Disposición de los medios	A.8.3.2
	Gestión de medios removibles	A.8.3.1
	Manejo de activos	A.8.2.3
	Política para dispositivos móviles	A.6.2.1
	Reglamentación de controles criptográficos.	A.18.1.5
	Revisión de cumplimiento técnico.	A.18.2.3
	Separación de deberes / tareas	A.6.1.2
	Teletrabajo	A.6.2.2
	Acceso a redes y a servicios en red	A.9.1.2
	Ambiente de desarrollo seguro	A.14.2.6
	Análisis y especificación de requisitos de seguridad de la información	A.14.1.1
	Aprendizaje obtenido de los incidentes de seguridad de la información	A.16.1.6
	Control de acceso a códigos fuente de programas	A.9.4.5
	Controles contra códigos maliciosos	A.12.2.1
	Controles de redes	A.13.1.1
	Controles sobre auditorías de sistemas de información	A.12.7.1
	Desarrollo contratado externamente	A.14.2.7
	Disposición segura o reutilización de equipos	A.11.2.7
	Equipos de usuario desatendidos	A.11.2.8
	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	A.16.1.4
	Gestión de capacidad	A.12.1.3
	Gestión de información de autenticación secreta de usuarios	A.9.2.4
	Gestión de las vulnerabilidades técnicas	A.12.6.1
	Gestión de llaves	A.10.1.2
	Instalación de software en sistemas operativos	A.12.5.1
	Mantenimiento de equipos	A.11.2.4
	Mensajería electrónica	A.13.2.3

	Política de control de acceso	A.9.1.1
	Política de desarrollo seguro	A.14.2.1
	Política de escritorio limpio y pantalla limpia	A.11.2.9
	Política sobre el uso de controles criptográficos	A.10.1.1
	Políticas y procedimientos de transferencia de información	A.13.2.1
	Principios de construcción de sistemas seguros	A.14.2.5
	Procedimiento de ingreso seguro	A.9.4.2
	Procedimientos de control de cambios en sistemas	A.14.2.2
	Procedimientos de operación documentados	A.12.1.1
	Protección contra amenazas externas y ambientales	A.11.1.4
	Protección de datos de prueba	A.14.3.1
	Protección de la información de registro	A.12.4.2
	Protección de transacciones de los servicios de las aplicaciones	A.14.1.3
	Prueba de aceptación de sistemas	A.14.2.9
	Pruebas de seguridad de sistemas	A.14.2.8
	Recolección de evidencia	A.16.1.7
	Registro de eventos	A.12.4.1
	Registros del administrador y del operador	A.12.4.3
	Respaldo de la información	A.12.3.1
	Responsabilidades y procedimientos	A.16.1.1
	Respuesta a incidentes de seguridad de la información	A.16.1.5
	Restricción de acceso a la información	A.9.4.1
	Restricciones en los cambios a los paquetes de software	A.14.2.4
	Restricciones sobre la instalación de software	A.12.6.2
	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	A.14.2.3
	Seguridad de equipos y activos fuera de las instalaciones	A.11.2.6
	Seguridad de los servicios de red	A.13.1.2
	Seguridad de servicios de las aplicaciones en redes públicas	A.14.1.2
	Seguridad del cableado	A.11.2.3
	Separación de los ambientes de desarrollo, pruebas y operación	A.12.1.4
	Separación en las redes	A.13.1.3
	Servicios de suministro	A.11.2.2
	Sincronización de relojes	A.12.4.4
	Sistema de gestión de contraseñas	A.9.4.3
	Uso de información de autenticación secreta	A.9.3.1

	Uso de programas utilitarios privilegiados	A.9.4.4
Subdirección de Trámites, Servicios y Gestión Documental	Clasificación de la información	A.8.2.1
	Etiquetado de la información	A.8.2.2
	Inventario de activos	A.8.1.1
	Manejo de activos	A.8.2.3
	Protección de registros.	A.18.1.3
	Aprendizaje obtenido de los incidentes de seguridad de la información	A.16.1.6
	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	A.16.1.4
	Política de control de acceso	A.9.1.1
	Política de escritorio limpio y pantalla limpia	A.11.2.9
	Política sobre el uso de controles criptográficos	A.10.1.1
	Políticas y procedimientos de transferencia de información	A.13.2.1
	Procedimientos de operación documentados	A.12.1.1
	Protección contra amenazas externas y ambientales	A.11.1.4
	Recolección de evidencia	A.16.1.7
	Respaldo de la información	A.12.3.1
	Responsabilidades y procedimientos	A.16.1.1
	Respuesta a incidentes de seguridad de la información	A.16.1.5
	Retiro de activos	A.11.2.5
Unidad Administrativa Especial de Gestión de Bienes y Servicios	Devolución de activos	A.8.1.4
	Disposición de los medios	A.8.3.2
	Gestión de la prestación de servicios de proveedores	A.15.2
	Política para dispositivos móviles	A.6.2.1
	Seguridad de la información en las relaciones con los proveedores	A.15.1
	Teletrabajo	A.6.2.2
	Transferencia de medios físicos	A.8.3.3
	Áreas de despacho y carga	A.11.1.6
	Controles físicos de entrada	A.11.1.2
	Disposición segura o reutilización de equipos	A.11.2.7
	Gestión de información de autenticación secreta de usuarios	A.9.2.4
	Mantenimiento de equipos	A.11.2.4
	Perímetro de seguridad física	A.11.1.1
	Política de control de acceso	A.9.1.1
	Políticas y procedimientos de transferencia de información	A.13.2.1
	Protección contra amenazas externas y ambientales	A.11.1.4
	Recolección de evidencia	A.16.1.7

	Retiro de activos	A.11.2.5
	Seguridad de equipos y activos fuera de las instalaciones	A.11.2.6
	Seguridad de oficinas, recintos e instalaciones	A.11.1.3
	Servicios de suministro	A.11.2.2
	Trabajo en áreas seguras	A.11.1.5
	Ubicación y protección de los equipos	A.11.2.1
Usuarios	Política para dispositivos móviles	A.6.2.1
	Equipos de usuario desatendidos	A.11.2.8
	Reporte de eventos de seguridad de la información	A.16.1.2
	Mensajería electrónica	A.13.2.3
	Política de escritorio limpio y pantalla limpia	A.11.2.9
	Uso de información de autenticación secreta	A.9.3.1

A continuación se presenta en la gráfica aquellos organismos resaltados que tienen a cargo mayor cantidad de controles, siendo los líderes de procesos en conjunto con los usuarios, los encargados de implementar a nivel operativo los controles que han sido diseñados por aquellos organismos que generan lineamientos (segunda línea de defensa) y aquellos que en el marco de seguridad y privacidad de la información es necesaria su participación.



5. PROPUESTA DE PLANIFICACIÓN Y CONTROL OPERACIONAL

Para lograr el cumplimiento de los diferentes niveles, de acuerdo a lo identificado en la pestaña madurez del diagnóstico elaborado, se debe mantener la aplicación de los controles existentes y fortalecer la implementación de los controles de acuerdo a los niveles del modelo *y* el ciclo *PHVA del MSPI - controles de la norma ISO IEC 27001 anexo A - controles de Ciberseguridad MSPI.* A continuación se presentan los controles del ciclo de

mejora continua y posteriormente se distinguen los niveles del modelo y las recomendaciones o requerimientos a implementar para que la entidad continúe avanzando en los niveles de cumplimiento.

PHVA del MSPI

PHVA	ITEM	RECOMENDACIONES
Planear	Alcance MSPI (Modelo de Seguridad y Privacidad de la Información)	Determinar los límites y la aplicabilidad del SGSI para establecer el alcance. Establecer el alcance conforme al resultado de la matriz de nivel de madurez del MSPI y los recursos disponibles para la implementación del SGSI. Aprobar el alcance por la alta dirección y socializar al interior de la Entidad. Evaluar la conveniencia de realizar un ejercicio de arquitectura empresarial para llevar a cabo la implementación del MSPI
	Políticas de seguridad y privacidad de la información	Articular la Política de seguridad y privacidad de la información de la entidad al proceso estratégico Planeación institucional. Complementar la política de seguridad de la información teniendo en cuenta la aplicación de controles de seguridad de la información no tecnológicos como los de Seguridad física y del entorno, procesos de ingreso y salida del personal, capacitaciones, cumplimiento normativo, gestión de datos, etc. Articular la Política de seguridad de la información de la entidad a los sistemas integrados de planeación y gestión
	Procedimientos de control documental del MSPI	Articular los requisitos del MSPI y/o SGSI al Sistema integrado de planeación de gestión actual. Complementar en los requisitos de análisis de contexto, definición del alcance, partes interesadas y documentación levantada para el cumplimiento de la norma de gestión de calidad, y sistemas integrados de gestión con los requisitos relacionados con la Seguridad y Privacidad de la Información.
	Roles y responsabilidades para la seguridad de la información	Definir y aprobar los roles y responsabilidades frente a la implementación del Sistema de Gestión de Seguridad de la Información (SGSI), así como la responsabilidad frente a la seguridad de la información y activos relacionados en todos los cargos y partes interesadas.
	Inventario de activos	Fortalecer la implementación del inventario de activos de información de la entidad y su relación con la seguridad de la información en la entidad. Ajustar la frecuencia de revisión de la matriz de activos de información en el procedimiento.
	Identificación y valoración de riesgos	Fortalecer el conocimiento e implementación de la metodología de riesgos de seguridad de la información en la entidad. Realizar la actualización de las herramientas de gestión del riesgo y capacitar en su aplicación.

PHVA	ITEM	RECOMENDACIONES
		Implementar el módulo de riesgos en el sistema DARUMA, con el fin de automatizar los reportes y facilitar el análisis de riesgos basado en los datos del sistema.
	Tratamiento de riesgos de seguridad de la información	Determinar el plan de tratamiento de riesgos de seguridad de la información, evaluando las opciones apropiadas para tratar los riesgos, según los resultados de la evaluación de riesgos de los activos de información. Implementar el plan de tratamiento de riesgos y las medidas necesarias para mitigar la materialización de las amenazas que afecten la seguridad de la información de la entidad de acuerdo a los controles del Anexo A de la norma ISO 27001 vigente Definir la declaración de aplicabilidad como parte del Sistema Integrado de Planeación y Gestión registrando los controles de la norma ISO 27001 que no se aplicarán, con su justificación. Aprobar la declaración de aplicabilidad y el plan de tratamiento de seguridad de la información por la Alta Dirección.
	Toma de conciencia, educación y formación en la seguridad de la información	Incluir en el plan de capacitaciones de la entidad, capacitaciones permanentes de seguridad de la información. Determinar un plan de sensibilización en los procesos de inducción y reinducción tanto para personal de planta cómo contratistas. Establecer lineamientos para que se realice toma de conciencia, educación y formación en los organismos de acuerdo al manejo de la información específica y la seguridad de la información.
Implementación	Planificación y control operacional	Elaborar la estrategia de planificación y control operacional teniendo en cuenta los demás instrumentos existentes en la entidad (activos de información, metodología de gestión de riesgos, diagnóstico de nivel de madurez MSPI), además del compromiso de líderes de procesos en la implementación de aquellos controles necesarios. Cómo resultado se ha generado para la entidad esta propuesta de planificación, esta debe ser aprobada por el nivel directivo e implementada por los organismos cómo se ha detallado en el apartado de Roles y Responsabilidades de este documento.
	Implementación de controles	Cumplir con esta estrategia y los niveles de madurez que se presentan a continuación permitirá avanzar en la implementación de los controles del Anexo A de la NTC 27001:2013-2022. Cada vez que se mejore en los controles se recomienda estar actualizando específicamente la calificación en la herramienta de diagnóstico para conocer la mejora del modelo a través de los años, partiendo de la línea base de 54 sobre 100.
	Implementación del plan de tratamiento de riesgos	Actualizar los tratamientos de riesgos de seguridad de la información por proceso una vez se determine desde el MSPI la aplicabilidad del plan de tratamiento de riesgos de seguridad y privacidad de la información. El plan de tratamiento de los riesgos se debe construir con el resultado de los mapas de riesgos de proceso y estos a su vez con la gestión de activos primarios y secundarios valorados cómo críticos.

PHVA	ITEM	RECOMENDACIONES
	Indicadores de gestión del MSPI	Elaborar un plan institucional que permita implementar el MSPI en la entidad conforme a las brechas encontradas en el diagnóstico y a partir del plan, generar indicadores de gestión del modelo.
Evaluación de desempeño	Plan de seguimiento, evaluación y análisis del MSPI	Socializar los resultados del diagnóstico con los involucrados y responsables de implementar acciones o estrategias recomendadas resultado de este ejercicio. La socialización debe ser constante para lograr la eficacia en desarrollo de proyectos que impulsen el modelo. Realizar seguimiento, evaluación y análisis del MSPI. Generar informes del desempeño de la operación del MSPI, según los resultados de los planes de trabajo e indicadores formulados para el Modelo.
	Auditoría Interna	Evaluar el establecimiento de controles para la seguridad de la información y su efectividad, siguiendo la metodología establecida. Se deben establecer auditorías al MSPI tomando cómo referencia la normativa vigente y los controles establecidos en la NTC/IEC 27001:2022 para conocer el nivel de cumplimiento de la entidad frente a los controles.
	Evaluación del plan de tratamiento de riesgos	Realizar evaluaciones al plan de tratamiento de riesgos por parte de los líderes de proceso y por nivel independiente cómo el Departamento Administrativo de Control Interno que permitan establecer mejoras a las herramientas de control. Además se recomienda la digitalización o automatización de la gestión de riesgos.
Mejora Continua	Plan de seguimiento, evaluación y análisis del MSPI	Realizar el análisis de los resultados consolidados del plan de trabajo, auditorías y efectividad del plan de tratamiento. Establecer acciones de mejora de acuerdo al análisis de los resultados y requerimientos de la entidad. Generar y mantener actualizado el plan institucional para la implementación del MSPI en la entidad.
	Auditoría Interna	Establecer auditorías que permitan evaluar la implementación del MSPI y los controles SPI, teniendo en cuenta el alcance o declaración de aplicabilidad.

CONTROLES POR NIVELES DEL MSPI

NIVEL	ISO 27001 ANEXO A	RECOMENDACIONES
Nivel 2 Gestionado	R8 T.7.1.1 Responsabilidades y procedimientos 2013: A.16.1.1 2022 5.24	Evaluar la capacidad de la entidad para la resolución de incidentes si es posible resolverlos por sí misma o requiere la colaboración de terceros, conservación de registros de incidencias, comunicación de incidencias al personal pertinente, registro de acciones y resultados, cierre del incidente y análisis de causas. Implementar y comunicar procedimientos de respuesta a incidentes de seguridad a todas las partes interesadas. Establecer responsabilidades, controles y procedimientos relacionados con la seguridad de la información de acuerdo a la estructura, capacidad y competencia de la entidad.

NIVEL	ISO 27001 ANEXO A	RECOMENDACIONES
		Establecer responsables para la gestión de incidentes que garanticen que se desarrollen los procedimientos para gestionar los incidentes. Definir las responsabilidades del personal contratado frente a la colaboración para el reporte y la respuesta de incidentes de seguridad de la información. Documentar un procedimiento de gestión de incidentes en la entidad, donde se establezca las responsabilidades, controles y procesos en cuanto a la seguridad y privacidad de la información, lo anterior de acuerdo a la estructura y competencias de la entidad. Comunicar a todas las partes interesadas los procedimientos relacionados con la gestión de los incidentes de seguridad y privacidad de la información.
Nivel 2 Gestionado	R8 T7.1.4 - Evaluación de eventos de seguridad de la información y decisiones sobre ellos 2013: A.16.1.4 2022: 5.25	Establecer criterios de priorización de incidentes con base en la criticidad del sistema, servicio, usuario, etc. determinar los actores a realizar y registrar la evaluación de incidentes para revisar la prioridad de los mismos para analizar los parámetros de calidad en resolución y clasificación, tener en cuenta el impacto del incidente y la rapidez con que se debe corregir la situación en su priorización. Implementar el procedimiento de gestión de incidentes de seguridad de la información en la entidad, de acuerdo a las responsabilidades, controles y procesos de acuerdo a la estructura y competencias de la entidad.
Nivel 2 Gestionado	R10 R9 Madurez. Aprobación de la alta dirección, documentada y firmada, para la Implementación del Modelo de Seguridad y Privacidad de la Información.	Se debe documentar el alcance (declaración de aplicabilidad), complementar el análisis de contexto, documentación de cumplimiento normativo, conforme a los numerales de la norma.
Nivel 2 Gestionado	R12 T7.1.2. Eventos de seguridad de la información 2013: A.16.1.2 2022: 6.8 Reporte de eventos de seguridad de la información	Establecer un mecanismo de comunicación que permita al personal informar de los eventos de seguridad y privacidad de la información identificados o supuestos de forma oportuna a través de canales apropiados. Establecer un procedimiento de reporte de eventos de seguridad y privacidad de la información Capacitar al recurso humano en el procedimiento y los mecanismos de notificación de eventos determinados. Concientizar al personal de la entidad frente a la responsabilidad de informar los eventos de seguridad y privacidad de la información de manera rápida para lograr prevenir o minimizar los efectos de los incidentes de seguridad de la información.

NIVEL	ISO 27001 ANEXO A	RECOMENDACIONES
Nivel 3 Definido	AD.5.1.1 Planificación de la continuidad de la seguridad de la información 2013:A.17.1.1 2022: 5.29	Actualizar el plan de continuidad del negocio de acuerdo a los nuevos escenarios que se puedan presentar incluyendo los riesgos que se puedan presentar y las alternativas de solución,además de sus pruebas de los tiempos establecidos de recuperación. Establecer estrategias de comunicación frecuente del Plan de Continuidad del Negocio. Se recomienda la documentación de “Primeros Auxilios en Documentos de Archivos" y la elaboración del “Plan de Atención de Emergencias y Atención de Desastres en los Archivos” para cubrir la gestión documental y garantizar la continuidad de la documentación física.
Nivel 3 Definido	AD.2.1.1 Roles y responsabilidades para la seguridad de la información 2023:A.6.1.12022:5 .2	Definir claramente los roles y responsabilidades frente al Sistema de Seguridad y Privacidad de la Información (SGSI) estableciendo compromisos para la protección de los activos, niveles de autorización y la asignación de recursos que permitan la implementación del sistema. Aprobar los roles y responsabilidades y establecer el plan operacional para la implementación del SGSI. De conformidad con las buenas prácticas para implementar el sistema de gestión de seguridad de la información, garantizar la efectividad y objetividad frente al cumplimiento de los controles, la entidad debe analizar la viabilidad de que exista el Oficial de Seguridad de la Información siendo este el profesional responsable de alinear las iniciativas de seguridad con los objetivos misionales, garantizando que los bienes y las tecnologías de la información están adecuadamente protegidos.
Nivel 3 Definido	AD.2.1.2 Separación de deberes / tareas 2013: A.6.1.2 2022: 5.3	Fortalecer el conocimiento frente a la importancia de establecer las segregación de funciones adecuadas, enfocadas a la seguridad de la información. Documentar los lineamientos a tener en cuenta para la realización de segregación de funciones del recurso humano de la entidad en relación con la seguridad de la información. Implementar la automatización y/o el uso de herramientas que permitan agilizar el proceso de revisiones periódicas de rastros de auditoría.
Nivel 3 Definido	AD.2.1.3 Contacto con las autoridades. 2013: A.6.1.3 2022: 5.5	Documentar un procedimiento específico a aplicar en caso que en la entidad ocurran violaciones a la seguridad de la información y/o a la seguridad informática, al igual que a la privacidad de la información. Definir las responsabilidades frente a la implementación del control teniendo en cuenta la objetividad e independencia de la operación
Nivel 3 Definido	AD.2.1.4 Contacto con grupos de interés especiales. 2013: A.6.1.4 2022: 5.6	Determinar responsabilidades frente a la implementación del control e Implementar el proyecto de procedimiento planteado en evidencias, a parte los beneficios de convenios que tiene la entidad con Microsoft - Oracle - AWS, con el fin de que los responsables de seguridad de la información en los organismos o personas que tengan a cargo activos relevantes puedan ser concienciados y educados en seguridad de la información e informática.

NIVEL	ISO 27001 ANEXO A	RECOMENDACIONES
		Establecer y mantener contacto institucional con grupos de interés cómo asociaciones profesionales en seguridad de la información para el asesoramiento especializado.
Nivel 3 Definido	AD.2.1.5 Seguridad de la información en la gestión de proyectos 2013:A.6.1.5 2022: A.5.8	Se recomienda que el Departamento Administrativo de Planeación y el Departamento Administrativo de Contratación Pública se articulen para generar un lineamiento en la entidad frente a la inclusión de seguridad y privacidad de la información durante el ciclo de vida de los proyectos, independientemente de su complejidad, tamaño, duración, disciplina o área de aplicación (por ejemplo un proyecto para un proceso de negocio principal, TIC, gestión de instalaciones u otros procesos de soporte). Analizar y determinar los requisitos y requerimientos que deben cumplir los proveedores que manejen información crítica para los procesos, la inclusión de certificaciones en seguridad de la información para poder contratar con la entidad y así garantizar el buen manejo de los activos por parte de terceros. Este lineamiento debería contemplar al menos: ● Activos primarios y secundarios gestionados en el proyecto, es decir, qué información está involucrada física o digital y sus soportes tecnológicos. ● Los riesgos de seguridad de la información sean evaluados y tratados desde una fase temprana y periódica durante el ciclo de vida del proyecto. ● Identificación de requisitos de seguridad de la información alineados con la NTC/IEC 27001. ● Las responsabilidades y autoridades de seguridad de la información pertinentes para el proyecto. ● El cumplimiento del entorno reglamentario y contractual en el que va a operar el proyecto.
Nivel 3 Definido	AD.3.3.1 Terminación o cambio de responsabilidades de empleo 2013:A.7.3.1 2022:6.5	Establecer un lineamientos frente a la creación de acuerdos de confidencialidad.
Nivel 3 Definido	T.1.2.6 Retiro o ajuste de los derechos de acceso 2013: A.9.2.6 2022: 5.18 (Eliminación o ajuste de los derechos de acceso)	Realizar registros del monitoreo de la revisión de los derechos de acceso a la información y a los activos asociados con instalaciones de procesamiento de información.

NIVEL	ISO 27001 ANEXO A	RECOMENDACIONES
Nivel 3 Definido	T.1.3.1 Uso de información de autenticación secreta. 2013: A.9.3.1 2022: 5.17	Sensibilizar frente al uso y creación de las contraseñas siguiendo buenas prácticas. Difundir buenas prácticas de contraseñas, en articulación con el proceso de comunicaciones.
Nivel 3 Definido	T.3.2 Seguridad física y ambiental de los equipos T.3.2.1 Ubicación y protección de los equipos 2013: A.11.2.1 2022: 7.8	Realizar la documentación del control cómo lineamiento para que los organismos que cuenten con debilidad se puedan fortalecer en la ubicación de equipos de modo que se minimice el acceso. Reiterar la definición del concepto de áreas seguras en la entidad. Documentar lineamiento para aquellas áreas de información crítica, directrices sobre consumir alimentos, fumar en cercanía a instalaciones de procesamiento. Realizar el seguimiento a las condiciones ambientales cómo temperatura, humedad que puedan afectar las instalaciones de procesamiento. En general, es importante que la entidad implemente medidas para proteger sus activos de información ante fallos eléctricos. y si ya están implementadas, documentarlas y socializarlas, revisar periódicamente de acuerdo a un plan de mantenimiento y verificar su correcto funcionamiento, ya que se ha evidenciado que no hay respuesta oportuna en casos de fallos de energía eléctrica, estas medidas pueden incluir UPS, protectores de sobretensión, copias de seguridad regulares, sistemas de protección contra incendios y mantener los equipos en un entorno controlado. Gestión de residuos: contar con un plan de gestión de residuos adecuado, para evitar la acumulación de desechos que puedan convertirse en focos de contaminación y peligros para los equipos. Los residuos electrónicos deben ser manejados adecuadamente para su posterior tratamiento y disposición final.
Nivel 3 Definido	T3.2.2 Servicios de suministro 2013: A.11.2.2 2022: 7.12	Realizar el cuidado o mantenimiento de los equipos y redes de suministro, conforme a especificaciones de fabricantes y buenas prácticas, conservando los registros de su ejecución. Generar por parte de la Unidad Administrativa Especial de Gestión de Bienes y Servicios - UAEGBS un lineamiento y regla de buen uso de equipos y redes de suministro en la entidad, para que los organismos implementen actividades que permitan dar cumplimiento a este control, según su independencia tecnológica y financiera. Realizar una revisión de todas las áreas de la entidad, verificando y documentando el estado en que se encuentran con el fin de analizar y tomar decisiones frente a las mejoras de condiciones físicas que permitan la eficaz seguridad de la información a nivel de entidad. Documentar los esquemas de servicios de suministro y redes de la entidad. En cuanto a la protección de energía eléctrica, los equipos deben estar conectados a sistemas de suministro eléctrico estables y seguros, que

NIVEL	ISO 27001 ANEXO A	RECOMENDACIONES
		eviten interrupciones y daños en caso de fluctuaciones de energía, cortes de luz o sobrecargas eléctricas. Realizar seguimiento a los cortes de energía e internet de forma anual, estableciendo indicadores que permitan analizar su comportamiento e identificar requerimientos relacionados para su mejoramiento continuo.
Nivel 3 Definido	T.3.2.3 Seguridad en el cableado 2013: A.11.2.3 2022: 7.12	Establecer lineamientos de directrices de seguridad para el cableado a nivel de toda la entidad, además de revisión periódica conforme la certificación de cableado se va actualizando. Documentar la infraestructura de red que existe en la entidad, su topología o mapas físicos/lógicos de red, organismo por organismo, quien es el responsable del mantenimiento de esta infraestructura, verificar si está o no certificada, si está actualizada, qué dispositivos están obsoletos. etc. Determinar en qué casos es necesario el uso de cables blindados: Los cables blindados pueden ayudar a reducir la interferencia electromagnética (EMI) y la interferencia de radiofrecuencia (RFI) que pueden afectar a los datos que se transmiten a través del cable. Estos cables tienen una capa metálica que los envuelve para bloquear las señales externas. Establecer cuando es necesario la instalación de conductos o canalizaciones: Los conductos o canalizaciones pueden proteger los cables de daños físicos, como cortes, golpes, abrasiones y exposición a elementos ambientales. También pueden ayudar a prevenir la interferencia electromagnética y de radiofrecuencia. Además, se recomienda realizar pruebas de penetración: Las pruebas de penetración pueden ayudar a identificar vulnerabilidades en el cableado y en los sistemas conectados. Estas pruebas pueden simular ataques para determinar la resistencia del sistema y las medidas de seguridad implementadas.
Nivel 3 Definido	T.3.2.4 Mantenimiento de equipos 2013: A.11.2.4 2022: 7.13	Se recomienda documentar, planear y ejecutar el mantenimiento preventivo de los activos secundarios de información (hardware), garantizando que se cumplan las recomendaciones del fabricante, que el mantenimiento o actualización sea realizado por personal calificado para ello. Asegurar que la información sensible en los equipos sea protegida durante todo el mantenimiento, si es el caso establecer el retiro de la misma si se requiere. Tener en cuenta los requisitos de mantenimiento, equipamiento y seguridad para el cumplimiento de pólizas de seguro
Nivel 3 Definido	T.3.2.5 Retiro de activos 2013: A.11.2.5 2022: 7.10	Fortalecer los controles, en cuanto la realización de revisiones de activos salientes y entrantes por parte del encargado de seguridad en el ingreso y salida de las instalaciones, solicitando la documentación e inspeccionando el correspondiente activo saliente y entrante. Automatizar el registro de ingresos y salidas de activos de información

NIVEL	ISO 27001 ANEXO A	RECOMENDACIONES
Nivel 3 Definido	T.3.2.6 Seguridad de equipos y activos fuera de las instalaciones 2013: A.11.2.6 2022: 7.9	Documentar en el Manual de Bienes muebles e Inmuebles, la responsabilidad de cada organismo frente a sus activos de información. Mantener el registro de la custodia de activos que salen de la organización y las medidas de seguridad aplicadas en la información si aplica. Procedimentar el teletrabajo o trabajo en casa, además de la gestión de riesgos para aquellas plazas a ser objeto de teletrabajo y su posterior implementación de controles.
Nivel 3 Definido	T.3.2.7 Disposición segura o reutilización de equipos 2013: A.11.2.7 2022: 7.14	Fortalecer la verificación de la eliminación de la información de todos los medios de almacenamiento por parte del organismo en los equipos que solicita dar de baja. Incluir por parte de la Unidad de Administrativa Especial de Bienes y Servicios en la información requerida para dar de baja equipos tecnológicos, la obligatoriedad de la certificación de la eliminación segura de la información en los activos entregados por el organismo.
Nivel 3 Definido	T.3.2.8 Equipos de usuario desatendidos 2013: A.11.2.8 2022: 8.1	Implementar en todos los sistemas de información de la entidad, controles de cierre de sesión automática cuando estén desatendidos. Sensibilizar al personal frente a los peligros de los equipos desatendidos. Además se recomienda, que en campañas de concienciación se socialice con el recurso humano sobre la importancia del bloqueo y cierre de sesión de aplicaciones que ya no se necesiten.
Nivel 3 Definido	T.3.2.9 Política de escritorio limpio y pantalla limpia 2013: A.11.2.9 2022: 7.7	Fortalecer los lineamientos documentados referente a pantalla y escritorio limpio para que contengan explícitamente los requerimientos del control en la política de seguridad de la información.
Nivel 3 Definido	T.5.1.1 Controles de redes 2013: A.13.1.1 2022: 8.20	Implementar instrumentos de registro que permita tener la trazabilidad de la gestión y controles para proteger la información en sistemas y aplicaciones. Realizar la separación de funciones de gestión/operación en las redes con las actividades del control de las mismas. Establecer controles para la implementación de redes inalámbricas.
Nivel 3 Definido	T.5.1.2 Seguridad de los servicios de red 2013: A.13.1.2 2022: 8.21	Documentar procedimiento para restringir el acceso a servicios o aplicaciones de red y para verificar constantemente los parámetros técnicos requeridos para la conexión segura con los servicios de red de acuerdo con las reglas de conexión de seguridad.
Nivel 3 Definido	T.5.1.3 Separación en las redes 2013: A.13.1.3 2022: 8.22	Diseñar, e implementar el mapa de redes de la alcaldía de Cali. Se debe tener en cuenta el organismo que hace la conexión, servidores que acceso, inventario de direcciones IP, activos conectados, protocolos de enrutamiento, segmentos de red, dominios, flujos de tráfico.

NIVEL	ISO 27001 ANEXO A	RECOMENDACIONES
Nivel 3 Definido	T.6.3.1 Protección de datos de prueba 2013: A.14.3.1 2022: 8.33	Contar con un repositorio de evidencias resultado de lo gestionado en los ambientes de desarrollo y pruebas, además del cumplimiento de los requisitos que verifican los supervisores de contrato a cargo de los diferentes Sistemas de Información. Además se recomienda lo siguiente: ● Establecer réplicas de producción en dichos ambientes (p.e. dos o tres veces al año). ● Administración de los ambientes de desarrollo seguro con usuario, roles y perfil. ● Repositorio de resultado de las pruebas funcionales realizadas. ● Generación adecuada de ejecutables para la puesta en producción. ● Garantizar backup de los fuentes del ambiente de desarrollo.
Nivel 3 Definido	T.7.1.3 Reporte de debilidades de seguridad de la información 2013: A.16.1.3 2022: 6.8	Establecer lineamientos frente al reporte de incidentes, resaltando la identificación de posibles debilidades del sistema que sean detectados en los sistemas o servicios. Concientizar a los usuarios en la responsabilidad de observar y reportar cualquier debilidad de seguridad de la información observada o sospechada, acatando el procedimiento de reporte de incidentes.
Nivel 3 Definido	T.7.1.7 Recolección de evidencia. 2013: A.16.1.7 2022: 5.28	Establecer un procedimiento interno para tratar información documentada como evidencia relacionada con los eventos de seguridad de la información, donde se establezcan las responsabilidades, controles y procesos para asegurar la información relacionada con incidentes de seguridad de la información que permita conservar los derechos dea acceso, inicios y cierres de sesión, identificaciones, estado de dispositivos, redes, sistemas al igual que evidencia de reuniones informativas, documentación de responsabilidades y funciones de seguridad de la información, lo anterior de acuerdo a la estructura y competencias en la entidad. Contar con herramientas automáticas que permitan correlacionar eventos al igual que sistemas de almacenamiento y preservación de registros, logs o información de auditoría.
Nivel 3 Definido	AD.7.1 Seguridad de la información en las relaciones con los proveedores 2013: A.15.1.1 2022: No aplica.	Validar conocimiento de la política de seguridad y acuerdo de confidencialidad con los proveedores y sus terceros. Establecer bitácoras (manuales o digitales) de registro como evidencias de ingreso de los proveedores en los diferentes sitios de la entidad (físico o virtual). Realizar seguimiento periódico del cumplimiento de los dos puntos anteriores. Revisar modelos de responsabilidad compartida para implementar con los proveedores de servicio incluyendo servicios de informática en nube. Establecer lineamiento en el proceso de Gestión Contractual, donde se establezca el uso de herramientas de seguimiento a los riesgos de seguridad de la información que se puedan generar durante la ejecución de proyectos, para dar cumplimiento a las cláusulas generales.

NIVEL	ISO 27001 ANEXO A	RECOMENDACIONES
Nivel 3 Definido	AD.7.2 Gestión de la prestación de servicios de proveedores. 2013: A.15.2 2022: No aplica.	Establecer en los contratos, cláusulas contractuales que incluyan la gestión de seguridad de la información con los contratistas y proveedores de servicios. Programar visitas o revisiones para verificar la implementación de controles de seguridad de la información y su efectividad.
Nivel 4 Gestionado Cuantitativamente	AD.4.2.1 Clasificación de la información. 2013: A.8.2.1 2022: A.5.12	Establecer políticas claras sobre cómo se debe clasificar la información y quién tiene acceso a ella Capacitar a los empleados sobre la importancia de clasificar la información y cómo hacerlo correctamente de conformidad con el resultado de la matriz de activos de información. Utilizar tecnologías modernas y adecuadas para proteger la información confidencial. Supervisar la gestión de la información, especialmente la información confidencial y sensible para garantizar que se estén cumpliendo los requisitos de seguridad
Nivel 4 Gestionado Cuantitativamente	AD.3.2.2 Toma de conciencia, educación y formación en la seguridad de la información 2013:A.7.2.2 - 2022: 6.3	Establecer en el proceso de inducción y reinducción de personal capacitaciones en seguridad de la información de obligatorio cumplimiento, y capacitaciones específicas de acuerdo a los activos de información primarios y secundarios según el cargo, generando conciencia, a través de la educación y formación, lo que permite transformar la cultura en seguridad de la información en toda la organización Establecer el plan de comunicación, sensibilización y capacitación de seguridad de la información y conservar los registros de aprobación por la Alta Dirección, con los respectivos soportes de implementación, revisión y actualización. Al redactar el programa de sensibilización, es importante no solo centrarse en el qué y el cómo llevarlo a cabo, sino también en el objetivo del mismo. Es importante que el personal comprenda el objetivo de la seguridad de la información y el efecto potencial, positivo o negativo, en la organización, resultado de su comportamiento frente a la seguridad de la información.
Nivel 4 Gestionado Cuantitativamente	P1. PHVA 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 en la Entidad.	Definir el alcance establecido conforme al resultado de la matriz de nivel de madurez del MSPI y los recursos disponibles para la implementación del SGSI. Declaración de Aplicabilidad. Complementar en la documentación de análisis de requisitos de la iso 9001, los aspectos relacionados con seguridad de la información (contexto, alcance, partes interesadas, información documentada, etc) para articular el Modelo de Seguridad y Privacidad de la Información - MSPI en los sistemas integrados de gestión de acuerdo al MIPG.

NIVEL	ISO 27001 ANEXO A	RECOMENDACIONES
Nivel 4 Gestionado Cuantitativamente	P4 Roles y responsabilidades para la seguridad de la información	Definir y aprobar los roles y responsabilidades específicas frente al Sistema de Seguridad y Privacidad de la Información (SGSI).
Nivel 4 Gestionado Cuantitativamente	AD.4.1.1 Inventario de Activos A.8.1.1 Inventario de activos	Concientizar al nivel directivo y equipos técnicos a su cargo de utilizar la matriz de activos de información cómo insumo para realizar la gestión de riesgos, con el propósito de implementar medidas de seguridad y protección adecuadas para cada tipo de activo identificado cómo crítico, con controles cómo como la encriptación de datos, controles de acceso y respaldo de información entre otros, utilizando el catálogo de controles del Anexo A NTC/IEC 27001:2022 y su guía de implementación NTC 27002:2022. Fortalecer el liderazgo y compromiso de la alta dirección con respecto a la implementación de la matriz de activos de información para asegurar la integración de los requisitos del sistema de gestión en los procesos de la organización. Continuar con las revisiones de calidad de los datos registrados y las capacitaciones sobre el uso y la importancia de la identificación y actualización de activos de información por parte del área líder del procedimiento de Gestión Documental.
Nivel 4 Gestionado Cuantitativamente	AD.4.1 Responsabilidad de los activos AD 4.1.3 Uso aceptable de los activos de activos 2013:A.8.1.3 2022: 5.10	Documentar las reglas de uso aceptable de activos de información tomando cómo referencia la criticidad de los activos primarios y secundarios. Realizar una evaluación de riesgos para identificar todas las posibles reglas para el uso aceptable de información y activos asociados con información y documentarlas en un manual de políticas. Establecer un programa de capacitación y concientización para el recurso humano sobre las políticas de uso aceptable de información y activos asociados con información.
Nivel 4 Gestionado Cuantitativamente	AD.4.1 Responsabilidad de los activos AD.4.1.4 Devolución de activos 2013:A.8.1.4 2022: 5.11	Establecer un proceso formal para la entrega de activos de la organización al comienzo de cualquier empleo, contrato o acuerdo. Educar y concienciar a los empleados o contratistas sobre la importancia de devolver todos los activos de la organización al final de su período de empleo o contrato. Mantener una lista actualizada de todos los activos de la organización y asegurarse de que se actualice regularmente.
Nivel 4 Gestionado Cuantitativamente	AD.2.2 Dispositivos Móviles y Teletrabajo AD.2.2.1 Política para dispositivos móviles	Implementar los requerimientos para la protección de información en los dispositivos móviles como son: Los requisitos de la protección física, pólizas, etc. Controles de protección lógica. controles de acceso, biométricos, entre otros.

NIVEL	ISO 27001 ANEXO A	RECOMENDACIONES
	2013: A.6.2.1 2022: 8.1	Actualizar las versiones de software de dispositivos móviles y el procedimiento de revisiones de actualización para la aplicación de parches de seguridad. Monitorear el cumplimiento de la protección contra software malicioso mediante el uso de antivirus.
Nivel 4 Gestionado Cuantitativamente	AD.2.2 Dispositivos Móviles y Teletrabajo AD.2.2.2 Teletrabajo 2013: A.6.2.2 2022: 6.7	Continuar con el diseño del modelo de teletrabajo para la Alcaldía por parte de la Subdirección de Gestión Estratégica del Talento Humano teniendo en cuenta la determinación de la(s) política(s) respectiva(s) y del establecimiento de los controles de seguridad de la información respectivos. Determinar claramente el manejo y control de los equipos de la entidad y de los equipos de propiedad privada que serán utilizados para el teletrabajo. la clasificación de la información a la cual puede acceder y mantener, así como sistemas y servicios internos autorizados, así como los métodos y requisitos de seguridad, respaldo y continuidad.
Nivel 4 Gestionado Cuantitativamente	T.4.3 Copias de seguridad T.4.3.1 Respaldo de la información 2013: A.12.3.1 2022: 8.13 (Copia de seguridad de la información).	Definir las situaciones en las que la confidencialidad tiene importancia y las copias de respaldo deben estar protegidas por medio de encriptación de acuerdo al resultado de una gestión de riesgo, tomando cómo referencia la valoración de activos. Contar con herramientas automáticas que permitan realizar la administración de las copias de respaldo (programación, realización, registro, etiquetado, custodia, almacenamiento y restauración)
Nivel 4 Gestionado Cuantitativamente	T.4.6 Gestión de la vulnerabilidad técnica T.4.6.1 Gestión de las vulnerabilidades técnicas 2013: A.12.6.1 2022: 8.8	Realizar la implementación del procedimiento Gestión de vulnerabilidades. Elaborar de manera semestral un informe de vulnerabilidades identificadas, atendidas y necesidades a mediano y largo plazo que la entidad deberá suplir. Realizar la suscripción a canales de información donde los diferentes equipos de trabajo puedan conocer las vulnerabilidades existentes y comunicarlas al interior de la entidad al personal pertinente
Nivel 4 Gestionado Cuantitativamente	AD.3.1 Antes de asumir el empleo AD.3.1.1 Selección e investigación de antecedentes 2013: A.7.1.1 2022: 6.1	Fortalecer el procedimiento de selección de personal tanto de planta cómo contratista, frente al manejo de activos críticos en la entidad con la inclusión de verificaciones adicionales que permitan asegurar la confiabilidad de las personas que van a ser responsables de activos críticos primarios o secundarios. Realizar el mantenimiento de los sistemas de información que son utilizados para el manejo de la información de Historias Laborales. Estandarizar el uso de formatos o acuerdos de confidencialidad en la entidad por parte del Departamento Administrativo de Contratación Pública, para que los diferentes organismos utilicen el formato en casos necesarios cuando los prestadores de servicio custodien o tengan acceso activos críticos para la entidad.

NIVEL	ISO 27001 ANEXO A	RECOMENDACIONES
Nivel 4 Gestionado Cuantitativamente	AD 3.1 Antes de asumir el empleo AD.3.1.2 Términos y condiciones del empleo 2023:A.7.1.2 2022: 6.2	Establecer específicamente en ambas modalidades de contratación las responsabilidades del compromiso de seguridad de la información de acuerdo con la gestión de activos. Aclarar y precisar los siguientes puntos: Acuerdos de confidencialidad o no divulgación que el personal a que se dé acceso a información confidencial debería firmar antes de que se le dé acceso a la información y otros activos asociados. Responsabilidades y derechos legales (por ejemplo, respecto a las leyes de derechos de autor o la legislación sobre protección de datos). Acciones a tomar si el personal ignora los requisitos de seguridad de la organización. Asegurar que el personal comprenda y acepte los términos y condiciones relativos a la seguridad de la información.
Nivel 4 Gestionado Cuantitativamente	AD.3.2 Durante la ejecución del empleo AD.3.2.1 Responsabilidades de la dirección. 2013:A.7.2.1 2022:5.4	Documentar en procesos de inducción y reinducción aquellos módulos que concienticen a contratistas y personal de planta frente a la gestión de los activos primarios y secundarios a su cargo. Incluir en el PIC, capacitaciones por parte de la entidad en articulación con proveedores (Universidades, entes certificadores), la seguridad de la información e informática para mejorar las habilidades y concientizar sobre el uso de activos en las diferentes dependencias de la Alcaldía. Elaborar procedimientos de denuncias anónimas específicas frente a la seguridad informática y de información. Incluir en plataforma de capacitación(inducción) el conocimiento específico sobre las políticas de seguridad y privacidad de la información
Nivel 4 Gestionado Cuantitativamente	AD.3.2 Durante la ejecución del empleo AD.3.2.2 Toma de conciencia, educación y formación en la seguridad de la información 2013:A.7.2.2 2022:6.3	Establecer en el proceso de inducción y reinducción de personal capacitaciones en seguridad de la información de obligatorio cumplimiento, y capacitaciones específicas de acuerdo a los activos de información primarios y secundarios según el cargo, generando conciencia, a través de la educación y formación, lo que permite transformar la cultura en seguridad de la información en toda la organización. Establecer el plan de comunicación, sensibilización y capacitación de seguridad de la información y conservar los registros de aprobación por la Alta Dirección, con los respectivos soportes de implementación, revisión y actualización. Al redactar el programa de sensibilización, es importante no solo centrarse en el qué y el cómo llevarlo a cabo, sino también en el objetivo del mismo. Es importante que el personal comprenda el objetivo de la seguridad de la información y el efecto potencial, positivo o negativo, en la organización, resultado de su comportamiento frente a la seguridad de la información.

NIVEL	ISO 27001 ANEXO A	RECOMENDACIONES
Nivel 4 Gestionado Cuantitativamente	AD.3.2 Durante la ejecución del empleo AD.3.2.3 Proceso disciplinario 2013:A.7.2.3 2022:6.4	Se recomienda establecer una ruta específica para violaciones en seguridad de la información, además de la sensibilización de implicaciones legales.
Nivel 4 Gestionado Cuantitativamente	T.1.1 Requisitos de negocio para el control de accesos. T.1.1.1 Política de control de acceso 2013: A.9.1.1 2022: 5.15 (Control de acceso).	Revisar los temas relacionados en las brechas y si aplica Incluir en la política de Seguridad de la Información Establecer el seguimiento al cumplimiento de las políticas de Seguridad de la Información.
Nivel 4 Gestionado Cuantitativamente	T.4.1 Responsabilidades y procedimientos de operación T.4.1.2 Gestión de cambios 2013: A.12.1.2 2022: 8.3.2	Fortalecer la documentación de Gestión de Cambios de acuerdo a los requerimientos del control. Crear el comité de control de cambios Llevar a cabo análisis del impacto y de gestión de riesgo cada vez que ocurran cambios que puedan afectar la seguridad de la información.
Nivel 4 Gestionado Cuantitativamente	T.4.1 Responsabilidades y procedimientos de operación T.4.1.3 Gestión de capacidad 2013: A.12.1.3 2022: 8.6	Fortalecer procedimentalmente la gestión de la demanda de capacidad que incluya los siguientes controles: a) Eliminar datos obsoletos (espacio en disco); b) Realizar cierre definitivo de aplicaciones, sistemas, bases de datos o ambientes; c) Optimizar cronogramas y procesos de lotes; d) Optimizar las consultas de bases de datos o lógicas de las aplicaciones; e) Realizar una negación o restricción de ancho de banda a servicios ávidos de recursos, si estos no son críticos para el negocio (por ejemplo, video en tiempo real). Realizar la proyección de la capacidad y el manejo de los costos de los servicios en la nube.
Nivel 4 Gestionado Cuantitativamente	T.5.2 TRANSFERENCIA DE INFORMACIÓN T.5.2.1 Políticas y procedimientos de transferencia de información 2013: A.13.2.1 2022: 5.14	Documentar reglas, procedimientos y acuerdos para la transferencia de información por medios físicos, verbales y electrónicos. Determinar la utilización de técnicas criptográficas, realizar mapa criptográfico por aplicación. Utilizar diccionarios de datos para la clasificación de la información. Realizar convenios de tratamiento de información con empleados, prestadores de servicios y contratistas. Implementar el modelo CRUD de datos de la Organización (las bases de datos y sistemas de gestión de información).

NIVEL	ISO 27001 ANEXO A	RECOMENDACIONES
		Incluir dentro del formato de protección y autorización del uso de la información implementación de controles y restricciones asociadas a las instalaciones de comunicación. Implementar una política de utilización y borrado de la información para máquinas FAX, PBX y demás contestadoras, que puedan alojar información grabada, teniendo en cuenta que la utilización de este tipo de activos de información tiende a desaparecer. Elaborar el procedimiento para asegurar trazabilidad en las transferencias Adoptar los mecanismos para el uso de un sistema de etiquetado acordado para información sensible o crítica, que asegure que el significado de la etiqueta se entiende de inmediato, y que la información está protegida apropiadamente. Establecer el cronograma de trabajo con el Departamento Administrativo de Planeación - SDI, DADII Subdirección de Trámites Servicios y Gestión Documental, DATIC, Gestión Jurídica y el Comité de Arquitectura Empresarial para generar de manera conjunta los lineamientos y mecanismos para el marcado de información confidencial
Nivel 4 Gestionado Cuantitativamente	T.6.1 REQUISITOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN T.6.1.1 Análisis y especificación de requisitos de seguridad de la información. 2013: A.14.1.1 2022: 5.8 SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE PROYECTOS	Garantizar que los riesgos de seguridad de la información se aborden en la gestión de proyectos a lo largo de su ciclo de vida. Detallar los requisitos para la seguridad de la información en las especificaciones de las condiciones para sistemas de información adicional a las funcionalidades requeridas para el desarrollo o compras de aplicaciones teniendo en cuenta su impacto en la entidad Implementar en los nuevos sistemas de información el módulo de usuario, roles y perfiles garantizando la trazabilidad, no repudio, auditoría, detección de fallos, etc , y la articulación con los sistemas de la organización especialmente aquellos de control como el Directorio Activo. Establecer controles de seguridad específicos con desarrollos o compras de aplicaciones a terceros como validación del producto, homologaciones y aceptación de productos que no vulneren la seguridad de los sistemas. Garantizar la actualización y el mantenimiento continuo de los Sistemas de información que se encuentran operando.
Nivel 4 Gestionado Cuantitativamente	T.6.2 SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y DE SOPORTE T.6.2.2 Procedimientos de control de cambios en sistemas 2013: A.14.2.2 2022: 8.32	Institucionalizar el comité de cambios tecnológicos y de información. Implementar y/o actualizar el procedimiento de gestión del cambio para su divulgación e implementación de cambios en las instalaciones y sistemas de procesamiento de información. Validar la herramienta mesa de ayuda MARI para el registro de la gestión de los cambios tecnológicos y de información de la entidad

NIVEL	ISO 27001 ANEXO A	RECOMENDACIONES
Nivel 4 Gestionado Cuantitativamente	AD.5.1.2 Implementación de la continuidad de la seguridad de la información. 2013:A.17.1.2 2022: 5.29 (Seguridad de la información durante una interrupción)	Ajustar el Manual de Funciones de acuerdo a la necesidad de la Seguridad de la Información en la entidad y definir responsabilidades del nivel directivo frente a los controles de la NTC 27001. Así mismo incluir dentro de los ejercicios de planificación de la entidad (corto, mediano, largo plazo), la seguridad de la información de acuerdo a responsabilidades definidas, para asegurar la existencia del personal de planta, prestadores de servicio y elementos necesarios para operar la seguridad de la información e informática. Crear un mecanismo de seguimiento o control para garantizar la divulgación de los lineamientos impartidos por DATIC al interior de cada organismo, esto podría evaluarse dentro de las visitas trimestrales del líder CTO a cada organismo Actualizar el capítulo de gestión de incidentes que se encuentra en el procedimiento administración de la operación MAGT04.04.02.G007. Sensibilizar en los comités tecnológicos operativos la actualización de las políticas de operación y seguridad y privacidad de la información. Realizar la actualización del plan de continuidad del negocio en servidores TI. Actualizar el Plan de Continuidad del Negocio de la entidad, en sus procedimientos de respuesta, recuperación que especifique como la entidad gestionará un evento contingente y mantendrá su seguridad de la información de acuerdo con la realidad y tiempos, Realizar pruebas de su funcionamiento mediante simulacros.
Nivel 4 Gestionado Cuantitativamente	P.8 PHVA Tratamiento de riesgos de seguridad de la información	Realizar la actualización de las herramientas de gestión del riesgo y capacitar en su aplicación. Determinar el plan de tratamiento de riesgos de seguridad de la información, evaluando las opciones apropiadas para tratar los riesgos, según los resultados de la evaluación de riesgos de los activos de información. Implementar el plan de tratamiento de riesgos y las medidas necesarias para mitigar la materialización de las amenazas que afecten la seguridad de la información de la entidad de acuerdo a los controles del Anexo A de la norma ISO 27001 vigente Definir la declaración de aplicabilidad como parte del Sistema Integrado de Planeación y Gestión registrando los controles de la norma ISO 27001 que no se aplicarán, con su justificación. Aprobar la declaración de aplicabilidad y el plan de tratamiento de seguridad de la información por la Alta Dirección.
Nivel 4 Gestionado Cuantitativamente	I.4 Implementación PHVA Indicadores de gestión del MSPI	Se recomienda elaborar un plan institucional que permita implementar el MSPI en la entidad conforme a los requisitos establecidos y el alcance definido, teniendo en cuenta las brechas encontradas en el diagnóstico y las recomendaciones

NIVEL	ISO 27001 ANEXO A	RECOMENDACIONES
		Establecer Indicadores de gestión y cumplimiento del MSPI definidos, revisados y aprobados por la Alta Dirección.
Nivel 4 Gestionado Cuantitativamente	E1.Evaluación del desempeño PHVA. Plan de seguimiento, evaluación y análisis del MSPI	Se recomienda socializar los resultados del diagnóstico con los involucrados y responsables de implementar acciones o estrategias recomendadas resultado de este ejercicio. Establecer el Plan de seguimiento para evaluar el desempeño y eficacia del MSPI a través de instrumentos que permitan determinar la efectividad de su implantación.
Nivel 4 Gestionado Cuantitativamente	M1.Mejora continua PHVA. Plan de seguimiento, evaluación y análisis del MSPI	Se recomienda evaluar y analizar los resultados del plan del MSPI periódicamente, y tomar acciones de mejora oportunamente con el fin de implementar la mejora continua
Nivel 4 Gestionado Cuantitativamente	T.7.1.6 Aprendizaje obtenido de los incidentes de seguridad de la información. 2013: A.16.1.6 2022: A.5.27	Documentar un procedimiento de gestión de incidentes en la entidad, donde se establezca las responsabilidades, controles y procesos en cuanto a la seguridad de la información, lo anterior de acuerdo a la estructura y competencias de la entidad. Cuantificar y monitorear los tipos, cantidad y costos de los incidentes de seguridad producidos. Establecer controles que permitan mantener una base de conocimientos sobre los incidentes como fuente de información para resolución de futuros incidentes y mejora de la seguridad de la información, cantidad de incidentes, tipología, costo de la resolución, impacto y solución aplicada, para el análisis, toma de decisiones y mejora de la seguridad. Establecer un plan de capacitación para el personal encargado de los incidentes de seguridad de la información.
Nivel 4 Gestionado Cuantitativamente	T.6.2.8 Pruebas de seguridad de sistemas 2013: A.14.2.8 2022: 8.29	Definir e implementar las pruebas de seguridad de la información en el ciclo de vida del desarrollo de las aplicaciones o códigos y validar que se cumplen en el entorno de producción. Garantizar que las pruebas al sistema o componentes sean confiables y permitan identificar vulnerabilidades existentes en el entorno de la organización, proporcionando un entorno de prueba que coincida con el entorno de producción de destino. Tener ambiente de desarrollo y pruebas seguros para los SI o aplicaciones críticas del organismo Establecer réplicas de producción en dichos ambientes (p.e. dos o tres veces al año) Administrar los ambientes de desarrollo seguro con usuario, roles y perfil Contar con repositorio de resultados de las pruebas funcionales realizadas. Realizar una generación adecuada de ejecutables para la puesta en producción. Garantizar backup de los fuentes del ambiente de desarrollo

NIVEL	ISO 27001 ANEXO A	RECOMENDACIONES
Nivel 4 Gestionado Cuantitativamente	T.7.1.5 Respuesta a incidentes de seguridad de la información 2013: A.16.1.5 2022: 5.26	Documentar un procedimiento de gestión de incidentes con definición clara de responsabilidades, controles y procesos de acuerdo a la estructura, capacidad y competencia de la entidad. Determinar los responsables de gestionar los incidentes de seguridad. Capacitar al recurso humano encargado de gestionar los incidentes de seguridad de la información, garantizando su competencia y actualización del conocimiento.
Nivel 4 Gestionado Cuantitativamente	T.1.4 CONTROL DE ACCESO A SISTEMAS Y APLICACIONES T.1.4.1 Restricción de acceso a la información 2013: A.9.4.1 2022: 8.3	Afianzar cumplimiento de los lineamientos de seguridad de la información en sistemas y aplicaciones de la Alcaldía. Fortalecer los acuerdos de confidencialidad con las partes interesadas pertinentes Implementar herramientas de prevención de pérdida de datos - DLP para proteger la información que está en modo digital. Dar lineamientos para contratar y administrar los accesos al servicio de la nube - AWS
Nivel 4 Gestionado Cuantitativamente	T.1.4 CONTROL DE ACCESO A SISTEMAS Y APLICACIONES T.1.4.3 Sistema de gestión de contraseñas 2013:A.9.4.3 2022:5.17	Concientizar a los usuarios acerca de la importancia del buen uso de la contraseña. Validar la gestión de contraseñas en las aplicaciones y/o servicios.de los diferentes organismos. Validar las integraciones con el Directorio Activo. Implementar una herramienta o gestor de contraseñas y accesos para los sistemas y servicios digitales de la entidad.
Nivel 4 Gestionado Cuantitativamente	T.1.4 CONTROL DE ACCESO A SISTEMAS Y APLICACIONES T.1.4.4 Uso de programas utilitarios privilegiados 2013: A.9.4.4 2022: 8.18	Documentar el establecimiento de las directrices para el uso de programas utilitarios con la capacidad de anular los controles de sistemas y de aplicaciones (parches, diagnósticos, antivirus, desfragmentadores, copias de seguridad, herramientas de red, etc), de cardo a la guia de la ISO 27002
Nivel 4 Gestionado Cuantitativamente	T.2.1 CONTROLES CRIPTOGRÁFICOS T.2.1.1 Política sobre el uso de controles criptográficos 2013: A.10.1.1 2022: 8.24	Revisar la pertinencia de establecer políticas de seguridad de la información, direccionadas a establecer el enfoque de la dirección con relación al uso de controles criptográficos en toda la organización, incluyendo los principios generales bajo los cuales se deben proteger la información del negocio. Realizar una valoración de riesgos, que identifique el nivel de protección requerida, teniendo en cuenta el tipo, fortaleza y calidad del algoritmo de encriptación requerido y al utilizar la encriptación para la protección de información transportada por dispositivos de encriptación móviles o removibles, o a través de líneas de comunicación y gestionar llaves para la recuperación de información encriptada.

NIVEL	ISO 27001 ANEXO A	RECOMENDACIONES
		Establecer roles y responsabilidades en la implementación de la política y la gestión de llaves criptográficas. Documentar las normas que se van a adoptar para la implementación efectiva en los procesos, definiendo el impacto de usar información encriptada y el cumplimiento de requisitos legales, reglamentarios y contractuales, entre otros relacionados con la criptografía.
Nivel 4 Gestionado Cuantitativamente	T.2.1 CONTROLES CRIPTOGRÁFICOS T.2.1.2 Gestión de llaves 2013: A.10.1.2 2022: 8.24	Fortalecer el establecimiento y documentación de procesos seguros para la gestión de llaves en la entidad, así como la existencia de registros frente a su aplicación, monitoreo y actualización frecuente.
Nivel 4 Gestionado Cuantitativamente	T.4.4 REGISTRO Y SEGUIMIENTO T.4.4.1 Registro de eventos 2013: A.12.4.1 2022: 8.15	Garantizar que los sistemas cuenten con el registro oportuno de actividades, excepciones, fallas y otros eventos relevantes que permitan generar evidencia, asegurar la integridad de la información, prevenir acceso no autorizado, identificar eventos que puedan provocar incidentes de seguridad de la información y respaldar investigaciones. Implementar herramientas correlacionadoras de eventos, que permitan la detección de eventos y faciliten el análisis de los mismos para la toma de decisiones, establecimiento e implementación de controles. Documentar los controles implementados y los resultados de la revisión regular de los eventos, así como determinar los informes que se deben generar para tener control y la revisión de los mismos por parte de la Alta Dirección para toma de decisiones pertinentes y oportunas. Implementar una política específica de registro, revisión y análisis de eventos
Nivel 4 Gestionado Cuantitativamente	T.4.4 REGISTRO Y SEGUIMIENTO T.4.4.2. Protección de la información de registro 2013: A.12.4.2 2022: 8.15	Documentar procedimientos y controles para proteger la información de registros (logs) contra cambios no autorizados y contra problemas de registro, con el establecimiento de revisión periódica de eventos que permitan detectar o evitar fallas o sobreescritura. Evaluar la asignación de roles, y determinar la segregación de funciones.
Nivel 4 Gestionado Cuantitativamente	T.4.4 REGISTRO Y SEGUIMIENTO T.4.4.3. Registros del administrador y del operador 2013: A.12.4.3 2022: 8.15	Elaborar la documentación del requerimiento, con los puntos críticos de control para contar con la evidencia de la revisión periódica de eventos. Validar el registro de actividades por parte de operadores y administradores y los alcances de los permisos de los roles específicos especialmente los privilegios de administración. Generar un cronograma de evaluación por organismos y sistemas de información con el fin de garantizar una revisión en su totalidad a todas las dependencias de la Alcaldía
Nivel 4 Gestionado	T.4.7 CONSIDERACIONES SOBRE AUDITORÍAS DE	Establecer lineamientos frente a realización de pruebas técnicas de auditoría y actividades de aseguramiento que se desarrollen con el fin de

NIVEL	ISO 27001 ANEXO A	RECOMENDACIONES
Cuantitativamente	SISTEMAS DE INFORMACIÓN T.4.7.1 Controles sobre auditorías de sistemas de información 2013: A.12.7.1 2022: 8.34	evaluar los sistemas operativos en cada ambiente (prueba, desarrollo y operación). Evaluar la pertinencia de establecer la realización de auditorías técnicas a los sistemas y documentar la toma de decisión según los resultados obtenidos
Nivel 4 Gestionado Cuantitativamente	AD.6.1 Cumplimiento de requisitos legales y contractuales AD.6.1.4 Protección de los datos y privacidad de la información relacionada con los datos personales 2013: A.18.1.4 2022: 5.34	Actualizar la política de tratamiento de datos personales, desarrollar herramienta que permita realizar el respectivo seguimiento de la misma e incluir procedimiento en el sistema de gestión que permita desarrollar el gobierno de datos. Establecer controles para el cumplimiento de la legislación vigente en materia de protección de Datos personales Sensibilizar continuamente la política de tratamiento de datos personales y verificar la actualización normativa de la misma. Fortalecer la visibilidad del tratamiento de datos en el portal web, listados de asistencia de reuniones, pagos y servicios en general de los procesos de la entidad
Nivel 4 Gestionado Cuantitativamente	AD.6.1 Cumplimiento de requisitos legales y contractuales AD.6.1.5 Reglamentación de controles criptográficos 2013:A.18.1.5 2022:5.31	Identificar la normativa vigente relacionada con controles criptográficos en uso, verificando el cumplimiento por ejemplo Ley 2069 de 2020, “Por medio de la cual se impulsa el emprendimiento en Colombia”, en su artículo 18, le ordena al Gobierno nacional reglamentar el uso de la firma electrónica y digital, para promover su uso teniendo en cuenta las nuevas tecnologías e importancia de la digitalización. Revisar la implementación de herramientas de cifrado como el Bitlocker a nivel estaciones o equipos identificados como activos de información críticos móviles o de uso compartido.
Nivel 5 optimizado	T.4.1 Responsabilidades y procedimientos de operación T.4.1.1 Procedimientos de operación documentados 2013: A.12.1.1 2022: 5.37	Establecer lineamientos sobre el manejo de medios y elementos de salida, como el uso de papelería especial o la gestión de elementos de salida de información confidencial, incluidos procedimientos para la disposición segura de elementos de salida de trabajos fallidos. Además de documentar lineamiento de seguimiento a logs, donde se establezca el análisis a los mismos y la presentación de informes para la toma de decisiones.
Nivel 5 Optimizado	T.1.1.2 - A.9.1.2 Acceso a redes y a servicios en red	Revisar en la política de seguridad de la información el registro específico del 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;

NIVEL	ISO 27001 ANEXO A	RECOMENDACIONES
		d) los medios usados para acceder a las redes y servicios de red (uso de VPN o redes inalámbricas); e) los requisitos de autenticación de usuarios para acceder a diversos servicios de red; f) el seguimiento del uso de servicios de red. Lo anterior permite conocer en tiempo real el uso que se le da al servicio y poder mitigar riesgos a los que está expuesto el recurso humano en el internet.
Nivel 5 Optimizado	T.1.2.1 - A.9.2.1 Registro y cancelación del registro de usuarios	Contar con registros del monitoreo o seguimiento de la aplicación de lo siguiente: b) deshabilitar o retirar inmediatamente las identificaciones de los usuarios que han dejado la organización; c) identificar y eliminar o deshabilitar periódicamente las identificaciones de usuario redundantes; d) asegurar que las identificaciones de usuario redundantes no se asignen a otros usuarios. Además, concientizar a los delegados CTO sobre la importancia de la implementación efectiva del procedimiento dispuesto para ello.
Nivel 5 Optimizado	T.1.2.2 - A.9.2.2 Suministro de acceso de usuarios	Contar con registros del monitoreo o seguimiento de la aplicación de los ítems: e) Adaptar los derechos de acceso de usuarios que han cambiado de roles o de empleo, y retirar o bloquear inmediatamente los derechos de acceso de los usuarios que han dejado la organización. f) Revisar periódicamente los derechos de acceso con los propietarios de los sistemas de información o servicios.
Nivel 5 Optimizado	T.1.2.3 - A.9.2.3 Gestión de derechos de acceso privilegiado	Fortalecer el control administrativo para cumplir con el seguimiento a este control técnico que incluya los seguimientos planteados en las brechas. Establecer políticas específicas de seguridad de la información relacionadas con el acceso privilegiado, monitoreo y seguimiento así como registros de la aplicación.
Nivel 5 Optimizado	T.1.4.2 - A.9.4.2 Procedimiento de ingreso seguro	Todos los sistemas de información deben tener activa la funcionalidad de restricciones de tiempo, requerimiento de conexión).
Nivel 5 Optimizado	T.1.4.5 - A.9.4.5 Control de acceso a códigos fuente de programas.	Construir registros o reportes de la entrega, seguimiento o monitoreo de la gestión realizada.
Nivel 5 Optimizado	T.4.1.4 - A.12.1.4 Separación de los ambientes de desarrollo, pruebas y operación	Recomendación de mejora continua conforme a lecciones aprendidas de la ejecución del lineamiento documentado.
Nivel 5 Optimizado	T.4.2.1 - A.12.2.1 Controles contra códigos maliciosos	Revisar e investigar periódicamente y de manera formal la presencia de archivos o códigos maliciosos, de enmiendas y/o desviaciones en el comportamiento de la red realizadas por estos. Disponer de entornos de prueba destinados a obtener resultados controlados e identificar posibles

NIVEL	ISO 27001 ANEXO A	RECOMENDACIONES
		impactos catastróficos, cómo secuestro de información (ransomware) u otro tipo de materialización de riesgos derivado de código malicioso. Disponer de registros que permitan evidenciar el tratamiento y mejora de los controles frente a la gestión del riesgo relacionados con códigos maliciosos.
Nivel 5 Optimizado	T.4.4.4 - A.12.4.4 Sincronización de relojes	Documentar la manera en que se realiza la sincronización de los sistemas de información con una fuente de información y establecer un informe de seguimiento aleatorio a los sistemas de información cómo verificación de su cumplimiento.
Nivel 5 Optimizado	T.4.5.1 - A.12.5.1 Instalación de software en sistemas operativos	Documentar el monitoreo al cumplimiento de los requisitos del control, con indicadores que permitan mejorar los resultados, además de contar con la documentación de estrategias que permitan conservar un estado anterior antes de implementar cambios en los sistemas de información con el fin de tener un punto de restauración.
Nivel 5 Optimizado	T.5.2.3 - A.13.2.3 Mensajería electrónica	Generar de manera conjunta los lineamientos para el manejo de firma electrónica y mensajería electrónica Subdirección de Trámites, servicios y Gestión Documental, Departamento Administrativo de Planeación - SDI y DATIC. Realizar el análisis jurídico frente al cumplimiento normativo del uso de las firmas electrónicas en la entidad. Se debe formular cómo política de operación el uso de medios de comunicación internos oficiales, cómo el uso del chat de Google Workspace.
Nivel 5 Optimizado	T.6.1.2 - A.14.1.2 Seguridad de servicios de las aplicaciones en redes públicas.	Fortalecer la política para la implementación de certificados de seguridad. Elaborar cronogramas de fechas de vencimiento de los certificados digitales para su renovación oportuna. Asegurar la continuidad del soporte por parte de los proveedores de los dispositivos de infraestructura y redes, así como, su mantenimiento y actualización.
Nivel 5 Optimizado	T.6.1.3 - A.14.1.3 Protección de transacciones de los servicios de las aplicaciones	Documentar los lineamientos frente a las transacciones de información en los servicios y el uso de firmas electrónicas para la trazabilidad y no repudio en los mismos.
Nivel 5 Optimizado	T.6.2.1 - A.14.2.1 Política de desarrollo seguro	Establecer puntos de control para garantizar en el diseño e implementación del Sistema de Información la aplicación de los lineamientos de la guía de desarrollo GUÍA PARA EL DESARROLLO E IMPLEMENTACIÓN DE SISTEMAS DE INFORMACIÓN - V4 CÓDIGO:MAGT04.04.01.P002.G001. https://sig.cali.gov.co/app.php/staff/document/viewPublic?index=1191 Implementar una herramienta de repositorio de información que permita mantener organizados y actualizados los entregables de los sistemas de información. Ejemplos: https://git-scm.com/ https://docs.github.com/
Nivel 5 Optimizado	AD.1.1 - A.5.1.1 Documento de la política de seguridad y privacidad de la Información	Vincular el documento Política de Seguridad de la Información como documento estratégico de compromiso de la alta gerencia frente a la implementación de la seguridad de la información en la entidad al proceso estratégico de Planeación Institucional y a los Sistemas de Gestión, con una estructura que soporte su implementación y mejora continua. Complementar la política de seguridad de la información con políticas de

NIVEL	ISO 27001 ANEXO A	RECOMENDACIONES
		seguridad referentes a controles propios de los organismos participantes y de los identificados de acuerdo a su competencia, la propuesta de roles y responsabilidades del Sistema de Gestión se encuentra en el numeral 8 del presente documento. Articular la Política de seguridad de la información de la entidad a los sistemas integrados de planeación y gestión
Nivel 5 Optimizado	AD.5.2.1 - A.17.2.1 Disponibilidad de instalaciones de procesamiento de información	Garantizar la renovación y prestación de los servicios de mantenimiento eléctrico, ups, aire acondicionados, etc. y el soporte técnico por parte de los proveedores de equipos de infraestructura tecnológica del Datacenter.
Nivel 5 Optimizado	AD.6.1.1 - A.18.1.1 Identificación de la legislación aplicable y de los requisitos contractuales.	Crear el normograma para el MSPI cómo sistema de gestión para que los responsables de los diferentes procesos garanticen su cumplimiento. Lo anterior, se debe realizar con el apoyo jurídico del Departamento Administrativo de Gestión Jurídica Pública, la identificación de la normativa (requisitos externos, incluidos legales, estatutarios, reglamentarios o contractuales que deben tenerse en cuenta) aplicable a la seguridad y privacidad de la información. Esta identificación debe tener en cuenta cuando: a) Se desarrollan políticas y procedimientos de seguridad de la información. b) Se diseñan, aplican o modifican los controles de seguridad de la información c) Se clasifica la información y otros activos asociados como parte del proceso para establecer requisitos de seguridad de la información para necesidades internas o acuerdos con proveedores. d) Se determinan los procesos junto con las funciones y responsabilidades relacionadas con la seguridad de la información e) Se determinan los requisitos contractuales de los proveedores pertinentes para la organización y el alcance del suministro de productos y servicios. Tomar en consideración el cumplimiento de normativa de los países pertinentes, si la organización realiza negocios en o con otros países, transfiere información y/o utiliza productos/servicios en los que las leyes y normativas pueden afectar el manejo de la información de la organización.
Nivel 5 Optimizado	AD.6.1.2 - A.18.1.2 Derechos de propiedad intelectual.	Identificar en la pirámide documental, los documentos metodológicos, guías, instructivos, protocolos,, especificaciones técnicas, manuales, catálogos, bibliográficos - de investigación - diagnósticos entre otros, en los cuales sea requisito el registro de citas directas o indirectas de propiedad intelectual según las normas APA - NTC 1486, para estandarizar la creación de textos en la entidad y disminuir posibles violaciones a derechos de autor. Se recomienda el uso de software que permita analizar e identificar violaciones a la propiedad intelectual, para textos escritos, audios, videos, imágenes y sean utilizados por la entidad.

NIVEL	ISO 27001 ANEXO A	RECOMENDACIONES
		Hacer seguimiento al cumplimiento de los derechos de autor con herramientas que permitan automatizar el proceso, al igual que en el registro de la información.
Nivel 5 Optimizado	AD.6.1.3 - A.18.1.3 Protección de registros.	Continuar con el proceso de actualización de TRD y TVD por cada proceso de la entidad. Validar que se están recolectando los logs necesarios o relevantes para administrar la seguridad de la información en los sistemas de la entidad (logs del sistema y logs de programas y aplicaciones) Documentar el proceso para la gestión de logs con relación al almacenamiento, ubicación y custodia.
Nivel 5 Optimizado	AD.6.2.1 - A.18.2.1 Revisión independiente de la seguridad de la información	Enfocar auditorías específicas a la seguridad de la información, tomando cómo referencia los controles establecidos en la NTC/IEC 27001:2022, con el fin de generar valor para la organización concientizando a las diferentes áreas de la importancia de la seguridad de la información en los procesos, además de prepararla para una futura certificación en la norma ante entidades certificadoras.
Nivel 5 Optimizado	AD.6.2.2 - A.18.2.2 Cumplimiento con las políticas y normas de seguridad.	Realizar inclusión de la normatividad de seguridad de la información a nivel de procesos. Automatizar las herramientas de control lideradas por la Subdirección de Gestión Organizacional (SGO) y su consolidación en la entidad. Complementar la política de seguridad de la información, con políticas específicas de los controles de la norma que involucren a los demás organismos, con el fin de evidenciar el cumplimiento de la misma.
Nivel 5 Optimizado	R9-MADUREZ	Con base en el inventario de activos de información clasificados, se establece la caracterización de cada uno de los sistemas de información.
Nivel 5 Optimizado	T.1.2.4 - A.9.2.4 Gestión de información de autenticación secreta de usuarios.	Fortalecer el control administrativo de Gestión de contraseñas en la entidad, la declaratoria para mantener confidencial la información de autenticación secreta del personal, como también realizar la documentación de algunos controles y su seguimiento por medio de registros para garantizar el cumplimiento por parte de los delegados CTO de los organismos.
Nivel 5 Optimizado	T.1.2.5- A.9.2.5 Retiro o ajuste de los derechos de acceso	Se recomienda realizar un procedimiento en control administrativo para la revisión de los usuarios registrados (usuarios en vacaciones, retirados, traslados etc).
Nivel 5 Optimizado	R55 - AD.5.1.3 - A.17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	Realizar en un ambiente de pruebas la restauración de un backup para validar el funcionamiento correcto y tomar las evidencias pertinentes y actualizar y realizar pruebas al Plan de Continuidad del Negocio.

NUEVOS CONTROLES NORMA VERSIÓN 2022

NIVEL	ISO 27001 ANEXO A	RECOMENDACIONES
Nivel 3 Definido	27001:2022 5.7 Inteligencia sobre amenazas	Adquirir la Guía Técnica Colombiana GTC-ISO/IEC 27002:2022 Realizar la revisión de los documentos metodológicos que hacen referencia a la norma 27001 y su anexo A y la pertinencia de su actualización. Dar lineamientos frente a la revisión del cumplimiento de los nuevos controles y los cambios normativos, durante en la transición de la aplicación de los mismos en los documentos guía del MinTIC. Implementar una estrategia que permita actualizar los conocimientos del recurso humano encargado de la implementación del MSPI y la seguridad y privacidad de la información en la entidad.
	5.23 Seguridad de la información para el uso de servicios en la nube	
	5.30 Preparación de las TIC para la continuidad de la actividad	
	7.4 Monitoreo de la seguridad Física	
	8.9 Gestión de la configuración	
	8.10 Eliminación de la información	
	8.11 Enmascaramiento de datos	
	8.12 prevención de fuga de datos	
	8.16 Actividades de monitoreo	
	8.23 Filtrado Web	
	8.28 Codificación segura	