INFORME DIAGNÓSTICO DE SEGURIDAD RESPECTO A LA ISO 27001:2022

ALCALDÍA CARTAGENA DE INDIAS

DOCUMENTO CONFIDENCIAL

Elaborado por: RED SUMMA

Diciembre 2024

Cartagena

Control de Cambios

Versión	Autor	Fecha	Descripción de la modificación
1	Consultoría	23/12/2024	Versión inicial del documento
1	Apoyo Gerencia Proyecto	23/12/2024	Revisión de calidad
2	Consultoría	27/12/2024	Ajustes al documento de acuerdo con las observaciones y recomendaciones de la ALCALDIA DE CARTAGENA DE INDIAS
2	Apoyo Gerencia Proyecto	27/12/2024	Revisión de calidad
3	Consultoría	30/12/20224	Ajustes al documento de acuerdo con las observaciones y recomendaciones del equipo base
3	Apoyo Gerencia Proyecto	30/12/20224	Revisión de calidad

TABLA DE CONTENIDO

LISTADO DE ILUSTRACIONES

LISTADO DE TABLAS

1. OBJETIVO

Identificar el estado de madurez del Sistema de Gestión de Seguridad de la Información (SGSI), Sistema de Continuidad del trabajo y programa integral de protección de datos personales de la Alcaldia de Cartagena de Indias, evaluando el cumplimiento frente a los requisitos y controles de las normas.

2. ALCANCE

Inicia con la aplicación de la metodología para medir el cumplimiento de los requisitos y controles del Anexo A de la norma NTC - ISO/IEC 27001:2022 de los diferentes procesos de la ALCALDIA DE CARTAGENA DE INDIAS, distribuidos entre las capacidades aplicables y finaliza con la identificación del nivel de madurez del SGSI nivel de madurez de SCN y nivel de madurez de Protección de datos personales PIGPDP.

El alcance incluye los siguientes aspectos de la normativos

- NTC - ISO/IEC 27001:2022:
- NTC – ISO/IEC 22301: 2019
- Ley 1581 del 2012

Requisitos obligatorios (1ª parte de la norma NTC - ISO/IEC 27001:2022)

- 4.Contexto de la Organización
- 5.Liderazgo
- 6.Planificación
- 7. Soporte
- 8. Operación
- 9. Evaluación del Desempeño
- 10. Mejoras

Dominios de Control Anexo A (2ª parte de la norma NTC - ISO/IEC 27001:2022)

- A.5 Controles Organizacionales
- A.6 Controles de Personal
- A.7 Controles Físicos
- A.8 Controles Tecnológicos

3. METODOLOGÍA

Mediante el análisis de brechas se logra determinar cuáles requisitos y controles del Anexo A de la norma NTC - ISO/IEC 27001:2022 están debidamente implementados en la ALCALDIA DE CARTAGENA DE INDIAS y cuáles no; esto con el fin de identificar las acciones necesarias para la implementación de los controles faltantes, actualización de aquellos donde se encuentren debilidades o mejoras de acuerdo con los insumos que brinde la metodología aplicada.

Escala de Valoración de Controles ISO 27001:2022 ANEXO A		
Descripción	Calificación	Criterio
No Aplica	N/A	No aplica.
INEXISTENTE	0	Total falta de cualquier proceso reconocible. La Organización ni siquiera ha reconocido que hay un problema a tratar. No se aplican controles.
INICIAL	20	1) Hay una evidencia de que la Organización ha reconocido que existe un problema y que hay que tratarlo. No hay procesos estandarizados. La implementación de un control depende de cada individuo y es principalmente reactiva. 2) Se cuenta con procedimientos documentados, pero no son conocidos y/o no se aplican.
REPETIBLE	40	Los procesos y los controles siguen un patrón regular. Los procesos se han desarrollado hasta el punto en que diferentes procedimientos son seguidos por diferentes personas. No hay formación ni comunicación formal sobre los procedimientos y estándares. Hay un alto grado de confianza en los conocimientos de cada persona, por eso hay probabilidad de errores.
EFECTIVO	60	Los procesos y los controles se documentan y se comunican. Los controles son efectivos y se aplican casi siempre. Sin embargo, es poco probable la detección de desviaciones, cuando el control no se aplica oportunamente o la forma de aplicarlo no es la indicada.
GESTIONADO	80	Los controles se monitorean y se miden. Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas de acción donde los procesos no estén funcionando eficientemente.
OPTIMIZADO	100	Las buenas prácticas se siguen y automatizan. Los procesos han sido redefinidos hasta el nivel de mejores prácticas, basándose en los resultados de una mejora continua.

Ilustración 1 Metodología de levantamiento del diagnóstico

La información insumo para validar el cumplimiento de cada control, ha sido obtenida mediante las siguientes actividades:

- **Solicitud inicial a la ALCALDIA DE CARTAGENA DE INDIAS de la documentación existente para el cumplimiento de los controles del SGSI:** Se valida mediante lista de chequeo los documentos requisito de la norma o aquellas herramientas que permiten evidenciar el cumplimiento de cada control.
- **Entrevistas con los líderes de los procesos:** se realizaron reuniones para el levantamiento del diagnóstico GAP entre el 16 de diciembre al 20 de diciembre de 2024, donde participaron los siguientes líderes de proceso:

Unidades orgánicas y especialistas entrevistados			
Fecha	**Unidad Orgánica Asignada**	**Cargo**	**Nombre Responsable**
17/12/2024	OAI (Oficina Asesora de Informática)	Profesional especializado	Ingrid Paola Solano Benítez
19/12/2024	OAI (Oficina Asesora de Informática)	Profesional especializado	Ingrid Paola Solano Benítez
		Asesor externo	Carlos Daniel Gómez Padilla
		Asesor externo	Jhonattan Bawin
		Asesor externo	Alexander Carrascal
		Profesional Universitario	Michael Jack Cohen Arteaga
		Asesor externo	Daniela Cabrera
		Profesional Universitario	Miriam C. Orozco Giraldo
20/12/2024	OACD (Oficina Asesora de Control Interno)	Diaz Sabbagh	Tania Rosa
	DATH (Dirección Administrativa de Talento Humano)	Asesor externo	Marlon Andres Matute Yances
		Asesor externo	Melina Ardila
		Profesional especializado	Katherine Díaz Hoyos
	OAI (Oficina Asesora de Informática)	Profesional especializado	Ingrid Paola Solano Benitez
		Asesor externo	Carlos Daniel Gomez Padilla
		Asesor externo	Jhonattan Bawin
		Profesional Universitario	Miriam C. Orozco Giraldo

Tabla 1 Unidades Orgánicas y Especialistas entrevistados

- Análisis de información solicitada: Se realizó el análisis a los documentos compartidos en el repositorio.

Analizando la información anterior, se determina en primera instancia si se encuentra documentada la actividad y el control; adicionalmente, si cumple con los requisitos establecidos en la norma NTC – ISO/IEC 27001:2022. El porcentaje de implementación de cada control se determinó basado en los siguientes criterios:

- Existe evidencia que el control o requisito se ejecuta.
- Existe evidencia que el control o requisito está documentado.
- Existe evidencia que el control cumple con relación a lo que la norma solicita.
- Existe evidencia que el control o requisito se ejecuta acorde a su documentación y es de conocimiento del personal de la ALCALDIA DE CARTAGENA DE INDIAS.

Nota: El análisis GAP no corresponde a una auditoría, por lo tanto, la consultoría depende de las respuestas dadas por las personas entrevistadas, en especial en aquellos casos donde se menciona la forma de ejecutar el control, en los cuales no se solicitará evidencia.

3.1. Definición de niveles y criterios de madurez en seguridad

3.1.1. Valoración de los controles y cláusulas de la ISO 27001: 2022

Para dar un panorama general del cumplimiento tanto para los controles del Anexo A como para las cláusulas de la norma NTC ISO/IEC 27001:2022, se utiliza una escala de valores que indica el nivel de cumplimiento o madurez de cada requisito y control de la norma; a su vez, permite identificar cuales controles se deben trabajar prioritariamente, con base en los porcentajes alcanzados y las preferencias de la entidad para alcanzar el nivel de implementación a corto, mediano o largo plazo; esta escala es la siguiente:

Escala de Valoración de Controles del Anexo A y Cláusulas de la norma NTC ISO/IEC 27001:2022		
Descripción	**Calificación**	**Criterio**
No Aplica	N/A	No aplica.
INEXISTENTE	0%	Total, falta de cualquier proceso reconocible. La Organización ni siquiera ha reconocido que hay un problema a tratar. No se aplican controles.
INICIAL	20%	1) Hay una evidencia de que la Organización ha reconocido que existe un problema y que hay que tratarlo. No hay procesos estandarizados. La implementación de un control depende de cada individuo y es principalmente reactiva. 2) Se cuenta con procedimientos documentados, pero no son conocidos y/o no se aplican.
REPETIBLE	40%	Los procesos y los controles siguen un patrón regular. Los procesos se han desarrollado hasta el punto en que diferentes procedimientos son seguidos por diferentes personas. No hay formación ni comunicación formal sobre los procedimientos y estándares. Hay un alto grado de confianza en los conocimientos de cada persona, por eso hay probabilidad de errores.
EFECTIVO	60%	Los procesos y los controles se documentan y se comunican. Los controles son efectivos y se aplican casi siempre. Sin embargo, es poco probable la detección de desviaciones, cuando el control no se aplica oportunamente o la forma de aplicarlo no es la indicada.
GESTIONADO	80%	Los controles se monitorean y se miden. Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas de acción donde los procesos no estén funcionando eficientemente.
OPTIMIZADO	100%	Las buenas prácticas se siguen y automatizan. Los procesos han sido redefinidos hasta el nivel de mejores prácticas, basándose en los resultados de una mejora continua.

Tabla 2 Valoración de Cumplimiento de Controles y Cláusulas de la norma ISO

Para determinar el nivel de madurez se establece la eficacia del control o el requisito evaluado durante las entrevistas, así como, la capacidad de cobertura de los mismos dentro de la entidad y sus actividades, dando un porcentaje a cada control para finalmente promediar el cumplimiento total del requisito, dominio o grupo de controles. Para determinar en qué nivel se encuentra cada grupo de controles, una vez obtenido el promedio, se establecen los siguientes rangos porcentuales por cada escala establecida en la metodología de evaluación:

Nivel	Límite Inferior	Límite Superior
Optimizado	81%	100%
Administrado (Gestionado)	61%	80%
Efectivo	41%	60%
Repetible	21%	40%
Inicial	1%	20%
Inexistente	0%	0%

Límites porcentuales de cumplimiento o madurez de los controles y cláusulas del SGSI

3.1.2. Valoración de Madurez del SGSI

En consecuencia con lo anterior, estos niveles son aplicados para validar el ciclo de mejora continua que debe tener todo sistema de gestión; donde se puede determinar cuál es el nivel de cumplimiento de cada control, grupo de controles, requisito o cláusulas de la norma (resultado), y proyectar hasta donde desea llegar la organización, teniendo en cuenta la descripción que se establece a continuación:

Nivel de Cumplimiento	Descripción
INEXISTENTE	En este nivel se encuentran las organizaciones, que aún no tienen en su planificación la implementación de un Sistema de Gestión de Seguridad de la Información, por tanto, no han establecido una política como tampoco han establecido roles y responsabilidades en términos de seguridad.
INICIAL	En este nivel se encuentran las organizaciones, que aún no cuentan con una identificación de activos y gestión de Riesgos, que les permita determinar el grado de criticidad de la información respecto a la seguridad, por tanto, los controles no están alineados con la conservación de la Confidencialidad, Disponibilidad e Integridad de la Información
REPETIBLE	En este nivel se encuentran las organizaciones en las cuales existen procesos básicos de gestión de seguridad de la información, de igual forma cuentan con controles que permiten detectar posibles incidentes en seguridad; pero no se encuentran gestionados de manera adecuada.
EFECTIVO	En este nivel se encuentran las organizaciones que tienen una adecuada documentación, la cual es aprobada por la alta dirección sus procesos están estandarizados y a su vez los controles debidamente documentados, implementados y actualizados. Sin embargo, aún falta llegar a procesos de monitoreo y medición, formalizar algunos controles y lograr la toma de decisiones basados en datos.
GESTIONADO	En este nivel se encuentran las organizaciones que cuentan con métricas, objetivos claros y medibles pues se articulan con los indicadores definidos para el SGSI, se realizan auditorías al SGSI con el fin de establecer una adecuada efectividad en los controles implementados.
OPTIMIZADO	En este nivel se encuentran las organizaciones que cumplen con el ciclo de mejora para el SGSI, donde realizan auditorías a intervalos adecuados, comunican las oportunidades de mejora con todos los colabores y socializan los resultados del SGSI, comunican las lecciones aprendidas de los incidentes de seguridad y actualizan constantemente los objetivos del sistema. Se logra evidenciar el proceso de mejora continua a través del tiempo, tanto en sus componentes documentales, como en el fortalecimiento de controles de seguridad y la articulación con otros sistemas de gestión.

Tabla 3 Niveles de valoración de Madurez del SGSI

4. RESULTADOS

Para la evaluación de los requisitos del numeral 4 al 10 y controles del Anexo A de la norma NTC - ISO/IEC 27001:2022, se diligencia la lista de validación, donde se analiza y evalúa el estado de cumplimiento.

La hoja de verificación de las cláusulas de la norma permite identificar:

- Componente del PHVA asociado a la cláusula
- Numeral y Subnumeral de la cláusula
- Descripción de la cláusula
- Prueba de implementación
- Evidencia aportada o de implementación de la cláusula
- Brecha para identificar que se debe implementar o ajustar
- Columnas de: Nivel de cumplimiento por Subnumeral, porcentaje de cumplimiento del numeral y nivel alcanzado en el componente del PHVA.

La tabla de verificación de cumplimiento de controles, está conformada por cinco (6) columnas que permiten comparar lo requerido por el anexo de la norma con lo establecido actualmente en la ALCALDIA DE CARTAGENA DE INDIAS. Las diferentes columnas indican:

- **Ítem:** Contiene la numeración de los requisitos y controles del Anexo A de la norma NTC- ISO/IEC 27001:2022.
- **Controles y Descripción Anexo A:** contiene el enunciado de los requisitos y controles del Anexo A de la norma NTC- ISO/IEC 27001:2022 a evaluar.
- **Calificación del control:** contiene la calificación de cumplimiento del control.
- **Criterio de Calificación del control:** contiene el criterio de calificación de cumplimiento del control.
- **Evidencia de cumplimiento**: Contiene la explicación de la selección de la respuesta.
- **Observaciones y/o recomendaciones**: se encuentran plasmados los resultados del diagnóstico para cada uno de los requisitos y controles de la norma.

Se define la meta de cumplimiento del 100%, y el objetivo en un 80%, puesto que el propósito es evaluar el nivel de cumplimiento del SGSI implementado actualmente en la ALCALDIA DE CARTAGENA DE INDIAS, frente a los controles y requisitos de la nueva versión de la norma NTC- ISO/IEC 27001: 2022, para iniciar con los procesos de planificación e implementación de los controles inexistentes, y actualización o mejora de los que operan actualmente.

4.1. Resultados evaluación cumplimiento anexo a norma NTC - ISO/IEC 27001:2022

Nivel de Madurez de los controles de seguridad de la información en la ALCALDIA DE CARTAGENA DE INDIAS

Se identifica **un cumplimiento del 45%** encontrándose en un nivel de madurez **EFECTIVO**, puesto que se encuentra en los rangos porcentuales establecidos en la metodología descrita en el numeral 3.1.1. del presente documento; en este nivel se encuentran las organizaciones que tienen una adecuada documentación, la cual

es aprobada por la alta dirección sus procesos están estandarizados y a su vez los controles debidamente documentados, implementados. Sin embargo, aún falta llegar a procesos actualización, monitoreo y medición, formalizar algunos controles y lograr la toma de decisiones basados en datos.

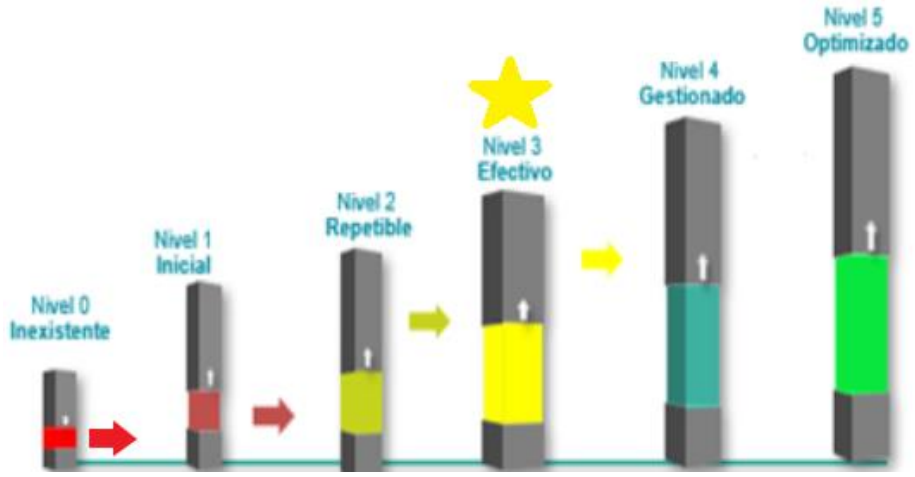

Ilustración 2 *Nivel de Madurez de los controles de seguridad de la información de la ALCALDIA DE CARTAGENA DE INDIAS*

A continuación, podemos observar la tabla y gráfica de resultado hallazgos del nivel de madurez de acuerdo con los dominios del Anexo A de la Norma NTC - ISO/IEC 27001:2022, y seguido a esto la tabla de resultados de los requisitos de la misma:

No.	EVALUACIÓN EFECTIVIDAD DE CONTROLES				
	TEMAS	Calificación Objetivo	Calificación Mínimo Aceptable	Calificación Actual	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
5	CONTROLES ORGANIZACIONALES	100	80	49	EFECTIVO
6	CONTROLES DE PERSONAL	100	80	51	EFECTIVO
7	CONTROLES FÍSICOS	100	80	43	EFECTIVO
8	CONTROLES TECNOLÓGICOS	100	80	37	REPETIBLE
PROMEDIO EVALUACIÓN DE CONTROLES		**100**	**80**	**45**	EFECTIVO

Tabla 3. Resultados de la evaluación del Anexo A de la Norma NTC - ISO/IEC 27001:2022

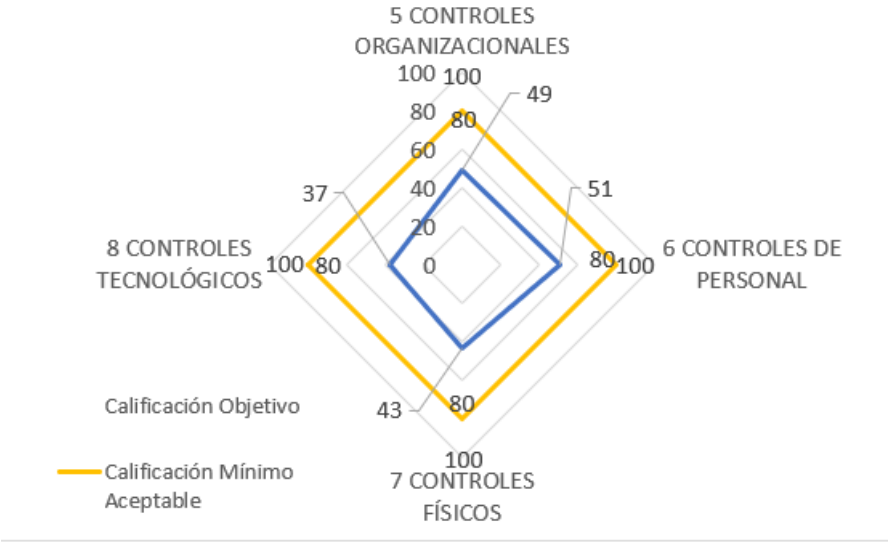

Ilustración 3 Porcentaje de cumplimiento por Dominio de Control

Para la ilustración siguiente, se evidencia el cumplimento por cada requisito de la Norma NTC - ISO/IEC 27001:2022.

REQUISITOS NTC ISO/IEC 27001:2022		
COMPONENTE	**% de Avance Actual Entidad**	**% Avance Esperado**
4. Contexto de la organización	55%	80,0%
5. Liderazgo	53%	80,0%
6. Planificación	36%	80,0%
7. Apoyo	28%	80,0%
8. Operación	47%	80,0%
9. Evaluación del desempeño	53%	80,0%
10. Mejora	50%	80,0%

Tabla 4 Resultados de la evaluación de los requisitos de la Norma ISO/IEC 27001:2022

A continuación, se evidencia el cumplimento en porcentaje por cada requisito de la Norma ISO/IEC 27001:2022.

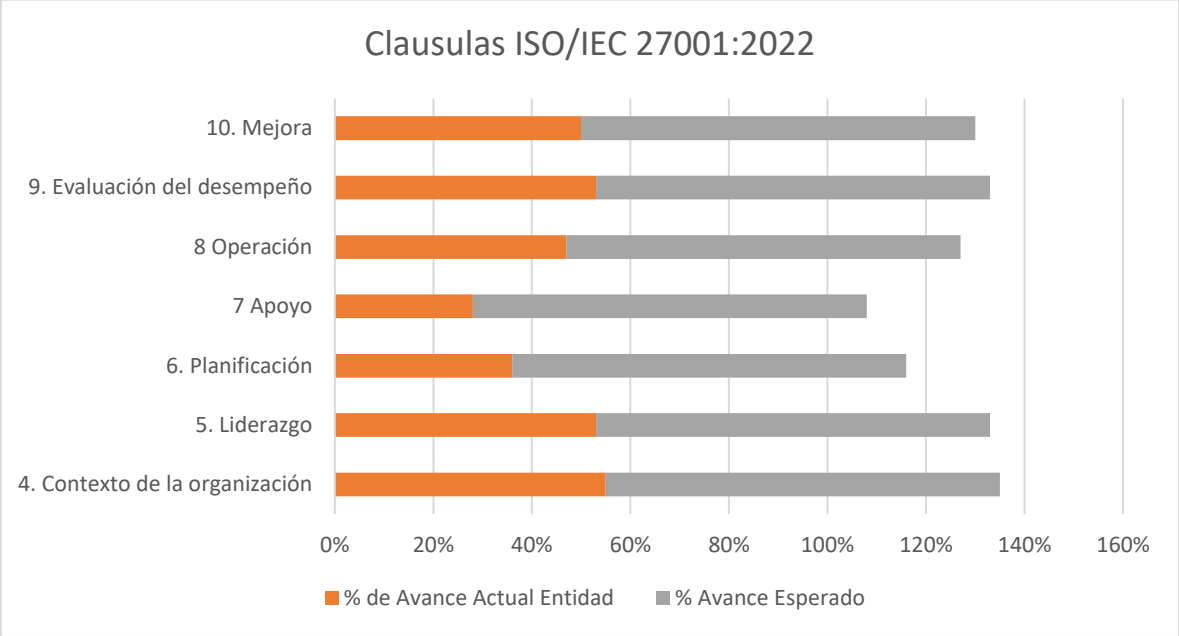

Ilustración 4 Porcentaje de cumplimiento Clausulas

Con respecto a la escala y niveles para establecer el cumplimiento del sistema con el ciclo PHVA, en la siguiente tabla y grafica se indican los porcentajes para cada etapa y su nivel avance esperado:

Año	AVANCE PHVA		
	COMPONENTE	**% de Avance Actual Entidad**	**% Avance Esperado**
2024	**Planificación**	19%	40%
	Implementación	7%	20%
	Evaluación de desempeño	10%	20%
	Mejora continua	10%	20%
TOTAL		**46%**	100%

Tabla 5 Avance del SGSI de la ALCALDIA DE CARTAGENA DE INDIAS frente al ciclo PHVA

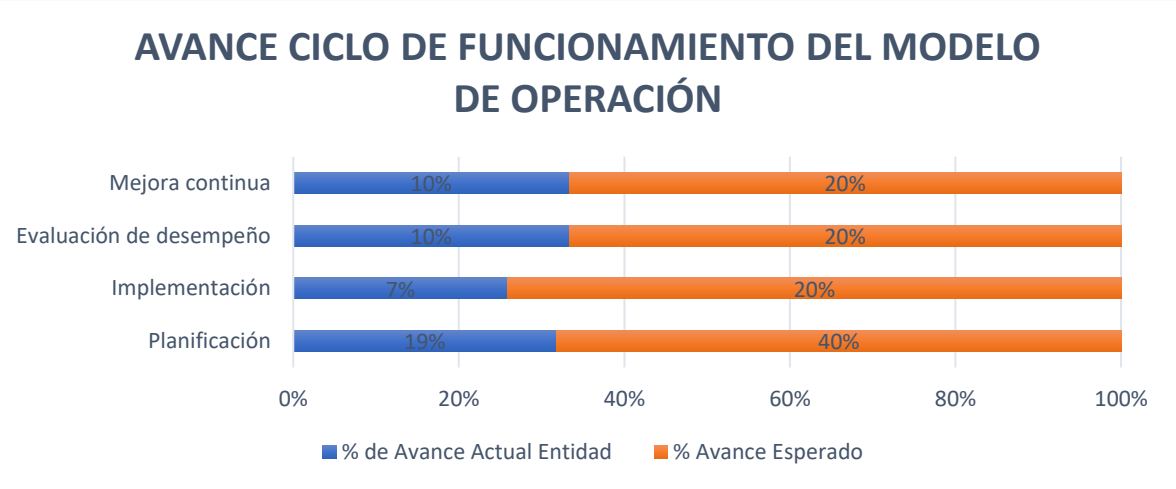

Ilustración 5 Porcentaje de cumplimiento Avance Ciclo Modelo Operación

A continuación, se presentan las ilustraciones que evidencian el nivel de cumplimiento de los controles en comparación con el nivel objetivo, esperado y actual. Los resultados detallan el grado de implementación de los controles organizacionales en la ALCALDÍA DE CARTAGENA DE INDIAS.

	INSTRUMENTO DE DIAGNÓSTICO DEL CUMPLIMIENTO DE CONTROLES ISO/IEC 27001:2022 ANEXO A		
Controles	**Detalles**	**Nivel de cumplimiento Control**	**Escala**
37	**CONTROLES ORGANIZACIONALES**		
5.1	Políticas para la seguridad de la información	80	GESTIONADO
5.2	Roles y responsabilidades en seguridad de la información	60	EFECTIVO
5.3	Segregación de funciones	40	REPETIBLE
5.4	Responsabilidades de la dirección	60	EFECTIVO
5.5	Contacto con autoridades	80	GESTIONADO
5.6	Contacto con grupos especiales de interés	40	REPETIBLE
5.7	Inteligencia de amenazas	50	EFECTIVO
5.8	Seguridad de la información en la gestión de proyectos	40	REPETIBLE
5.9	Inventario de información y otros activos asociados	40	REPETIBLE
5.1	Uso aceptable de la información y otros activos asociados	60	EFECTIVO
5.11	Devolución de activos	80	GESTIONADO
5.12	Clasificación de la información	80	GESTIONADO
5.13	Etiquetado de la información	60	EFECTIVO
5.14	Transferencia de información	60	EFECTIVO
5.15	Control de acceso	73	GESTIONADO
5.16	Gestión de identidades	60	EFECTIVO
5.17	Información de autenticación	80	GESTIONADO
5.18	Derechos de acceso	56	EFECTIVO
5.19	Seguridad de la información en las relaciones con los proveedores	27	REPETIBLE
5.20	Abordar la seguridad de la información dentro de los acuerdos con proveedores	40	REPETIBLE
5.21	Gestión de la seguridad de la información en la cadena de suministro de las tecnologías de la información y comunicación (TIC)	20	INICIAL

5.22	Seguimiento. revisión y gestión de cambios en servicios de proveedores	20	INICIAL
5.23	Seguridad de la información en el uso de servicios en la nube	60	EFECTIVO
5.24	Planificación y preparación de la gestión de incidentes de seguridad de la información	58	EFECTIVO
5.25	Evaluación y decisión sobre eventos de seguridad de la información	60	EFECTIVO
5.26	Respuesta a incidentes de seguridad de la información	33	REPETIBLE
5.27	Aprendizaje de los incidentes de seguridad de la información	20	INICIAL
5.28	Recolección de evidencia	20	INICIAL
5.29	Seguridad de la información durante una interrupción	20	INICIAL
5.30	Preparación de las TIC para la continuidad del negocio	20	INICIAL
5.31	Requisitos legales. estatutarios. regulatorios y contractuales	60	EFECTIVO
5.32	Derechos de propiedad intelectual	40	REPETIBLE
5.33	Protección de registros	40	REPETIBLE
5.34	Privacidad y protección de la información de identificación personal (IIP)	60	EFECTIVO
5.35	Revisión independiente de la seguridad de la información	40	REPETIBLE
5.36	Cumplimiento con políticas. reglas y normas de seguridad de la información	40	REPETIBLE
5.37	Procedimientos operativos documentados	40	REPETIBLE

Tabla 6 Controles del grupo A.5 – Controles Organizacionales

Se define como:

- **Nivel objetivo** – 100
- **Nivel Esperado** – 80
- **Atención prioritaria**: Se abracan todos los controles, puesto que es el propósito del contrato

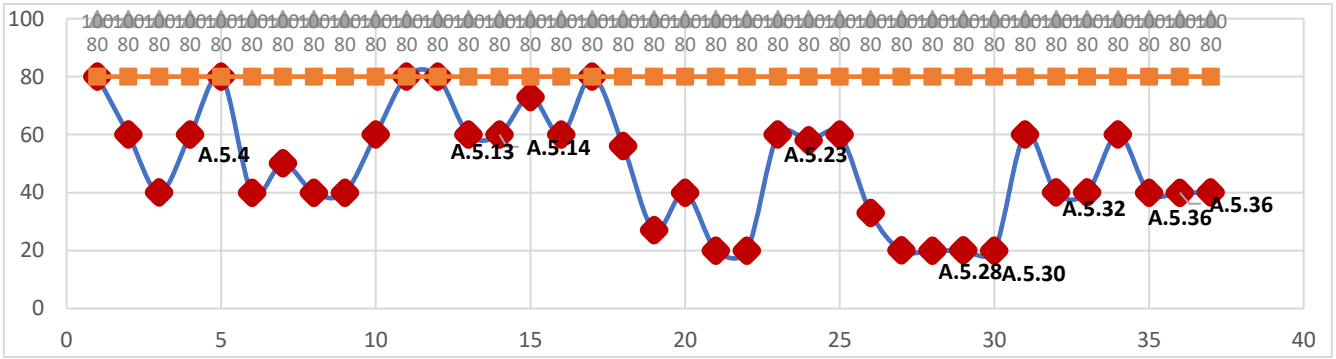

Ilustración 6 Porcentaje de cumplimiento dominio controles organizacionales frente al objetivo y la meta

Es necesario aclarar que los controles del dominio A.5 se encuentran entre los niveles 20 y 40; sin embargo, la priorización depende del cronograma de trabajo establecido para el desarrollo del contrato.

Los siguientes controles se encuentran en los niveles más bajos de implementación, entre inicial y repetible (0 al 40):

Controles	Detalles	Nivel de cumplimiento Control	Escala
37	**CONTROLES ORGANIZACIONALES**		
5.3	Segregación de funciones	40	REPETIBLE
5.6	Contacto con grupos especiales de interés	40	REPETIBLE
5.8	Seguridad de la información en la gestión de proyectos	40	REPETIBLE

5.9	Inventario de información y otros activos asociados	40	REPETIBLE
5.19	Seguridad de la información en las relaciones con los proveedores	27	REPETIBLE
5.20	Abordar la seguridad de la información dentro de los acuerdos con proveedores	40	REPETIBLE
5.21	Gestión de la seguridad de la información en la cadena de suministro de las tecnologías de la información y comunicación (TIC)	20	INICIAL
5.22	Seguimiento. revisión y gestión de cambios en servicios de proveedores	20	INICIAL
5.26	Respuesta a incidentes de seguridad de la información	33	REPETIBLE
5.27	Aprendizaje de los incidentes de seguridad de la información	20	INICIAL
5.28	Recolección de evidencia	20	INICIAL
5.29	Seguridad de la información durante una interrupción	20	INICIAL
5.30	Preparación de las TIC para la continuidad del negocio	20	INICIAL
5.32	Derechos de propiedad intelectual	40	REPETIBLE
5.33	Protección de registros	40	REPETIBLE
5.35	Revisión independiente de la seguridad de la información	40	REPETIBLE
5.36	Cumplimiento con políticas. reglas y normas de seguridad de la información	40	REPETIBLE
5.37	Procedimientos operativos documentados	40	REPETIBLE

Tabla 7 *Controles del grupo A.5 con los niveles más bajos de implementación*

Los controles de personal tienen un porcentaje promedio de implementación de 38, sin embargo, seis (06) de estos, se encuentran en niveles entre 20 y 40.

Controles	Detalles	Nivel de cumplimiento Control	Escala
8	**CONTROLES DE PERSONAL**		
6.1	Selección	100	OPTIMIZADO
6.2	Términos y condiciones del empleo	28	REPETIBLE
6.3	Toma de conciencia. educación y entrenamiento sobre la seguridad de la información	40	REPETIBLE
6.4	Proceso disciplinario	40	REPETIBLE
6.5	Responsabilidades después del cese o cambio de empleo	80	GESTIONADO
6.6	Acuerdos de confidencialidad o no divulgación	40	REPETIBLE
6.7	Trabajo remoto	40	REPETIBLE
6.8	Reporte de eventos de seguridad de la información	40	REPETIBLE

Tabla 8 Controles del grupo A.6 – Controles de Personal

Se define como:

- **Nivel objetivo** – 100
- **Nivel Esperado** – 80
- **Atención prioritaria**: Se abracan todos los controles, puesto que es el propósito del contrato

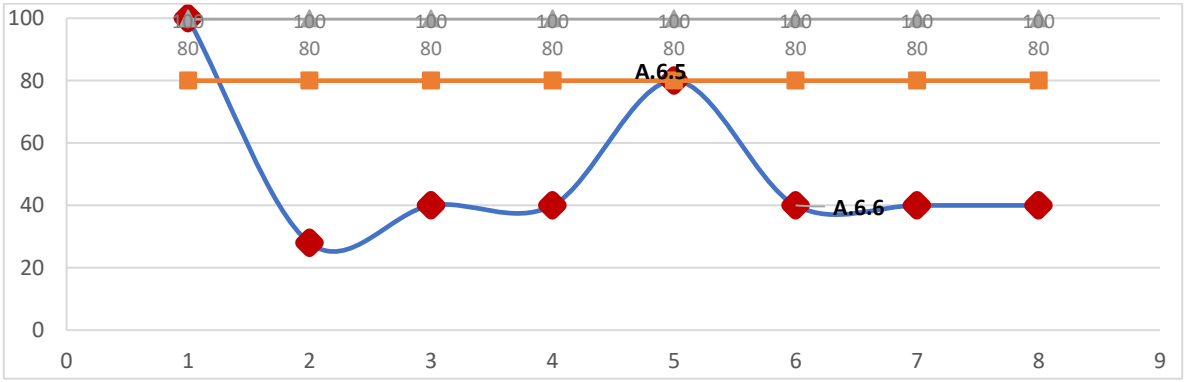

Ilustración 7 Porcentaje de cumplimiento dominio controles personal frente al objetivo y la meta

Los controles del dominio A.6 con los niveles más bajos de implementación son:

Controles	Detalles	Nivel de cumplimiento Control	Escala
8	**CONTROLES DE PERSONAL**		
6.2	Términos y condiciones del empleo	**28**	REPETIBLE
6.3	Toma de conciencia. educación y entrenamiento sobre la seguridad de la información	**40**	REPETIBLE
6.4	Proceso disciplinario	**40**	REPETIBLE
6.6	Acuerdos de confidencialidad o no divulgación	**40**	REPETIBLE
6.7	Trabajo remoto	**40**	REPETIBLE
6.8	Reporte de eventos de seguridad de la información	**40**	REPETIBLE

Tabla 9 *Controles del grupo A.6 con los niveles más bajos de implementación*

En lo que respecta a los resultados de los controles del dominio A.7, se tiene:

Controles	Detalles	Nivel de cumplimiento Control	Escala
14	**CONTROLES FÍSICOS**		
7.1	Perímetros de seguridad física	**40**	REPETIBLE
7.2	Ingreso físico	**20**	INICIAL
7.3	Asegurar oficinas. salas e instalaciones	**40**	REPETIBLE
7.4	Supervisión de la seguridad física	**60**	EFECTIVO
7.5	Protección contra amenazas físicas y ambientales	**60**	EFECTIVO
7.6	Trabajo en áreas seguras	**20**	INICIAL
7.7	Escritorio y pantalla limpios	**60**	EFECTIVO
7.8	Ubicación y protección de los equipos	**40**	REPETIBLE
7.9	Seguridad de los activos fuera de las instalaciones	**40**	REPETIBLE
7.1	Medios de almacenamiento	**40**	REPETIBLE
7.11	Servicios de suministro de apoyo	**40**	REPETIBLE
7.12	Seguridad del cableado	**20**	INICIAL
7.13	Mantenimiento de equipos	**80**	GESTIONADO
7.14	Eliminación segura o reutilización de equipos	**40**	REPETIBLE

Tabla 10 Controles del grupo A.7 – Controles Físicos

Se define como:

- **Nivel objetivo** – 100
- **Nivel Esperado** – 80
- **Atención prioritaria**: Se abracan todos los controles, puesto que es el propósito del contrato

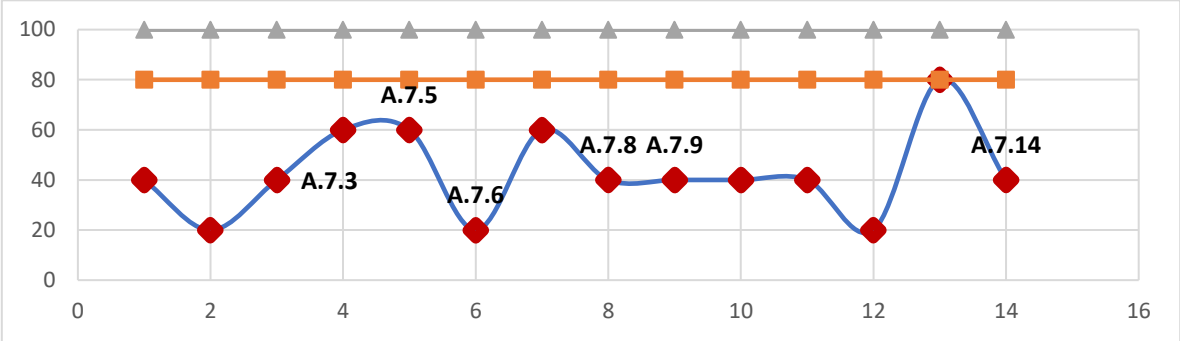

Ilustración 8 Porcentaje de cumplimiento dominio controles físicos frente al objetivo y la meta

Los controles del dominio A.7 con los niveles más bajos de implementación son:

Controles	Detalles	Nivel de cumplimiento Control	Escala
14	**CONTROLES FÍSICOS**		
7.1	Perímetros de seguridad física	**40**	REPETIBLE
7.2	Ingreso físico	**20**	INICIAL
7.3	Asegurar oficinas. salas e instalaciones	**40**	REPETIBLE
7.6	Trabajo en áreas seguras	**20**	INICIAL
7.8	Ubicación y protección de los equipos	**40**	REPETIBLE
7.9	Seguridad de los activos fuera de las instalaciones	**40**	REPETIBLE
7.1	Medios de almacenamiento	**40**	REPETIBLE
7.11	Servicios de suministro de apoyo	**40**	REPETIBLE
7.12	Seguridad del cableado	**20**	INICIAL
7.14	Eliminación segura o reutilización de equipos	**40**	REPETIBLE

Tabla 11 *Controles del grupo A.7 con los niveles más bajos de implementación*

Por su parte, los controles tecnológicos obtuvieron los siguientes resultados:

INSTRUMENTO DE DIAGNÓSTICO DEL CUMPLIMIENTO DE CONTROLES ISO/IEC 27001:2022 ANEXO A			
Controles	**Detalles**	**Nivel de cumplimiento Control**	**Escala**

34	CONTROLES TECNOLÓGICOS		
8.1	Dispositivos terminales del usuario	47	EFECTIVO
8.2	Derechos de acceso privilegiados	70	GESTIONADO
8.3	Restricción de acceso a la información	60	EFECTIVO
8.4	Acceso al código fuente	20	INICIAL
8.5	Autenticación segura	60	EFECTIVO
8.6	Gestión de capacidad	40	REPETIBLE
8.7	Protección contra programas maliciosos (malware)	43	EFECTIVO
8.8	Gestión de vulnerabilidades técnicas	40	REPETIBLE
8.9	Gestión de la configuración	40	REPETIBLE
8.1	Eliminación de información	20	INICIAL
8.11	Enmascaramiento de datos	20	INICIAL
8.12	Prevención de fuga de datos	40	REPETIBLE
8.13	Copia de seguridad de la información	40	REPETIBLE
8.14	Redundancia de las instalaciones de procesamiento de información	40	REPETIBLE
8.15	Registro	20	INICIAL
8.16	Actividades de monitoreo	40	REPETIBLE
8.17	Sincronización de reloj	80	GESTIONADO
8.18	Uso de programas de utilidad privilegiados	47	EFECTIVO
8.19	Instalación de software en sistemas operativos	43	EFECTIVO
8.2	Seguridad de redes	40	REPETIBLE
8.21	Seguridad de servicios de red	40	REPETIBLE
8.22	Segregación de redes	20	INICIAL
8.23	Filtrado de la web	80	GESTIONADO
8.24	Uso de criptografía	5	INICIAL
8.25	Ciclo de vida de desarrollo seguro	40	REPETIBLE
8.26	Requisitos de seguridad de la aplicación	3	INICIAL
8.27	Arquitectura de sistemas seguros y principios de ingeniería	7	INICIAL
8.28	Codificación segura	40	REPETIBLE
8.29	Pruebas de seguridad en desarrollo y aceptación.	40	REPETIBLE
8.3	Desarrollo subcontratado	26	REPETIBLE
8.31	Separación de los entornos de desarrollo. prueba y producción	40	REPETIBLE
8.32	Gestión de cambios	40	REPETIBLE
8.33	Información de las pruebas	40	REPETIBLE
8.34	Protección de los sistemas de información durante las pruebas de auditoría	0	INEXISTENTE

Tabla 12 Controles del grupo A.8 – Controles Tecnológicos

Se define como:

- **Nivel objetivo** – 100
- **Nivel Esperado** – 80
- **Atención prioritaria**: Se abracan todos los controles, puesto que es el propósito del contrato

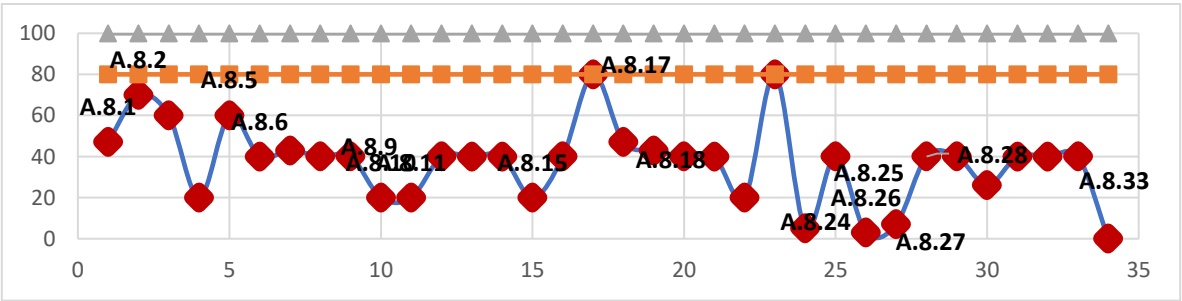

Ilustración 9 *Porcentaje de cumplimiento dominio controles tecnológicos frente al objetivo y la meta*

Los controles del dominio A.8 con los niveles más bajos de implementación son:

Controles	Detalles	Nivel de cumplimiento Control	Escala
34	**CONTROLES TECNOLÓGICOS**		
8.4	Acceso al código fuente	20	INICIAL
8.6	Gestión de capacidad	40	REPETIBLE
8.8	Gestión de vulnerabilidades técnicas	40	REPETIBLE
8.9	Gestión de la configuración	40	REPETIBLE
8.1	Eliminación de información	20	INICIAL
8.11	Enmascaramiento de datos	20	INICIAL
8.12	Prevención de fuga de datos	40	REPETIBLE
8.13	Copia de seguridad de la información	40	REPETIBLE
8.14	Redundancia de las instalaciones de procesamiento de información	40	REPETIBLE
8.15	Registro	20	INICIAL
8.16	Actividades de monitoreo	40	REPETIBLE
8.2	Seguridad de redes	40	REPETIBLE
8.21	Seguridad de servicios de red	40	REPETIBLE
8.22	Segregación de redes	20	INICIAL
8.24	Uso de criptografía	5	INICIAL
8.25	Ciclo de vida de desarrollo seguro	40	REPETIBLE
8.26	Requisitos de seguridad de la aplicación	3	INICIAL
8.27	Arquitectura de sistemas seguros y principios de ingeniería	7	INICIAL
8.28	Codificación segura	40	REPETIBLE
8.29	Pruebas de seguridad en desarrollo y aceptación.	40	REPETIBLE
8.3	Desarrollo subcontratado	26	REPETIBLE
8.31	Separación de los entornos de desarrollo. prueba y producción	40	REPETIBLE
8.32	Gestión de cambios	40	REPETIBLE
8.33	Información de las pruebas	40	REPETIBLE
8.34	Protección de los sistemas de información durante las pruebas de auditoría	0	INEXISTENTE

Tabla 13 Controles del grupo A.7 con los niveles más bajos de implementación

4.2. Resultado detallado del diagnóstico de los requisitos y el anexo A norma NTC - ISO/IEC 27001:2022

El detalle de los resultados para cada control y requisito de la norma se encuentran en el Anexo No 1 Matriz de Diagnostico GAP – ISO 27001 2022 ALCALDIA DE CARTAGENA DE INDIAS (VF). Con sus recomendaciones para el cumplimiento de una implementación y Acciones prioritarias recomendadas para la mejora continua por dominios de control T5, T6, T7 y T8 y Ciclo PHVA.

4.3. Resultados detallados del diagnóstico de los requisitos para el Sistema de Continuidad del Negocio de acuerdo a norma NTC – ISO 23301: 2019

El presente documento tiene como objetivo evaluar el estado actual del Plan de Continuidad del Negocio (BCP) de la ALCALDÍA DE CARTAGENA DE INDIAS frente a la norma ISO 22301:2019. Este análisis abarca la revisión de la documentación existente compartida, la evaluación del Análisis de impacto (BIA), evaluación de

los riesgos (RIA) y el plan de crisis. El propósito es identificar las fortalezas, debilidades y áreas por mejorar para garantizar que el BCP este alineado a los objetivos estratégicos del negocio.

Objetivo: Identificar el estado actual del Plan de Continuidad del Negocio (BCP) de la ALCALDÍA DE CARTAGENA DE INDIAS, basado en la norma ISO/IEC 22301:2019 que garantice el adecuado funcionamiento del modelo de operación por procesos de la entidad.

Alcance del diagnóstico: El análisis estará limitado a la revisión de la información proporcionada por la ALCALDÍA DE CARTAGENA DE INDIAS sobre su sistema de continuidad del negocio actual y se evaluará el nivel de madurez organizacional en la gestión de la continuidad del negocio verificando la alineación con los requisitos de la norma ISO 22301:2019.

Metodología: Mediante el análisis de brechas se logra determinar cuáles requisitos y controles de la norma están debidamente implementados en la ALCALDIA DE CARTAGENA DE INDIAS y cuáles no; esto con el fin de identificar las acciones necesarias para la implementación de los controles faltantes, actualización de aquellos donde se encuentren debilidades o mejoras de acuerdo con los insumos que brinde la metodología aplicada

Revisión Documental: Se revisaron los documentos actuales de la organización, tales como políticas, procedimientos, planes de continuidad del negocio, planes de respuestas a incidentes, evaluaciones de riesgo entre otros.

Entrevista y análisis de brechas: Se llevo a cabo una entrevista con una persona clave en la gestión de la continuidad del negocio. Durante la entrevista, se formularon preguntas basadas en las cláusulas regulatorias de la norma ISO 22301:2019, con el fin de evaluar el cumplimiento y madurez de los procesos. De acuerdo con la siguiente tabla:

El entrevistado califica a juicio de experto, la ubicación de su cumplimiento. En la siguiente tabla mostramos como se va a cuantificar los resultados de esta evaluación.

Escala de Valoración de Controles del Anexo A y Cláusulas de la norma NTC ISO/IEC 27001:2022		
Descripción	**Calificación**	**Criterio**
No Aplica	N/A	No aplica.
INEXISTENTE	0%	Total falta de cualquier proceso reconocible. La Organización ni siquiera ha reconocido que hay un problema a tratar. No se aplican controles.
INICIAL	20%	1) Hay una evidencia de que la Organización ha reconocido que existe un problema y que hay que tratarlo. No hay procesos estandarizados. La implementación de un control depende de cada individuo y es principalmente reactiva. 2) Se cuenta con procedimientos documentados, pero no son conocidos y/o no se aplican.
REPETIBLE	40%	Los procesos y los controles siguen un patrón regular. Los procesos se han desarrollado hasta el punto en que diferentes procedimientos son seguidos por diferentes personas. No hay formación ni comunicación formal sobre los procedimientos y estándares. Hay un alto grado de confianza en los conocimientos de cada persona, por eso hay probabilidad de errores.
EFECTIVO	60%	Los procesos y los controles se documentan y se comunican. Los controles son efectivos y se aplican casi siempre. Sin embargo, es poco probable la detección de desviaciones, cuando el control no se aplica oportunamente o la forma de aplicarlo no es la indicada.
GESTIONADO	80%	Los controles se monitorean y se miden. Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas de acción donde los procesos no estén funcionando eficientemente.

Escala de Valoración de Controles del Anexo A y Cláusulas de la norma NTC ISO/IEC 27001:2022		
Descripción	**Calificación**	**Criterio**
OPTIMIZADO	100%	Las buenas prácticas se siguen y automatizan. Los procesos han sido redefinidos hasta el nivel de mejores prácticas, basándose en los resultados de una mejora continua.

Valoración de Cumplimiento de Controles y Cláusulas de la norma ISO

Nivel de Cumplimiento	Límite Inferior	Limite Superior
OPTIMIZADO	81%	100%
GESTIONADO	61%	80%
EFECTIVO	41%	60%
REPETIBLE	21%	40%
INICIAL	1%	20%
INEXISTENTE	0%	0%

Limites porcentuales de cumplimiento

Requisitos obligatorios (Clausulas Parte de la norma ISO/IEC 22301:2019)

4- Contexto de la organización.
5- Liderazgo y compromiso
6-Planificación
7-Apoyo
8-Operación
9-Evaluacion de desempeño
10-Mejora Continua

Matriz de madurez y Análisis GAP - Entrevistas

Esta matriz se calculó con la información de 23 preguntas realizadas en la entrevista, donde cada pregunta tenía una escala de respuesta de 0 a 100 y basándose en estas, se realizó el promedio y se ubicó en el nivel de cumplimiento correspondiente.

Clausula	Requisito ISO 22301:2019	Descripción	Estado Actual	Calificación actual	Nivel Ideal
C4	**Contexto de la organización**	Comprender las necesidades y expectativas de las partes interesadas y los riesgos y oportunidades que puedan impactar la continuidad.	Repetible	24%	80%
C5	**Liderazgo y Compromiso**	Compromiso y liderazgo de la alta dirección en la implementación y mantenimiento del SGCN.	Repetible	40%	80%

C6	**Planificación**	Establecimiento de objetivos y planificación de acciones para abordar riesgos y oportunidades. Esto incluye planificar como alcanzar los objetivos y asegurar sostenibilidad.	Inicial	12%	80%
C7	**Apoyo**	Recursos, competencia y comunicación. Garantizar que los recursos necesarios estén disponibles y que el personal este capacitado y sensibilizado.	Repetible	40%	80%
C8	**Operación**	Planificación operativa para responder a incidentes que interrumpan las operaciones, con planes de recuperación específicos para funciones críticas.	Efectivo	60%	80%
C9	**Evaluación del Rendimiento**	Monitoreo, medición, análisis y evaluación, incluidas auditorías internas y revisiones periódicas para garantizar su efectividad.	Inicial	20%	80%
C10	**Mejora Continua**	Mejorar el SGNC con base en los resultados de las auditorias, análisis, desempeño y revisiones de la dirección.	Efectivo	60%	80%
Promedio			Repetible	37%	

Tabla 15 Resultados evaluación cumplimiento plan de continuidad

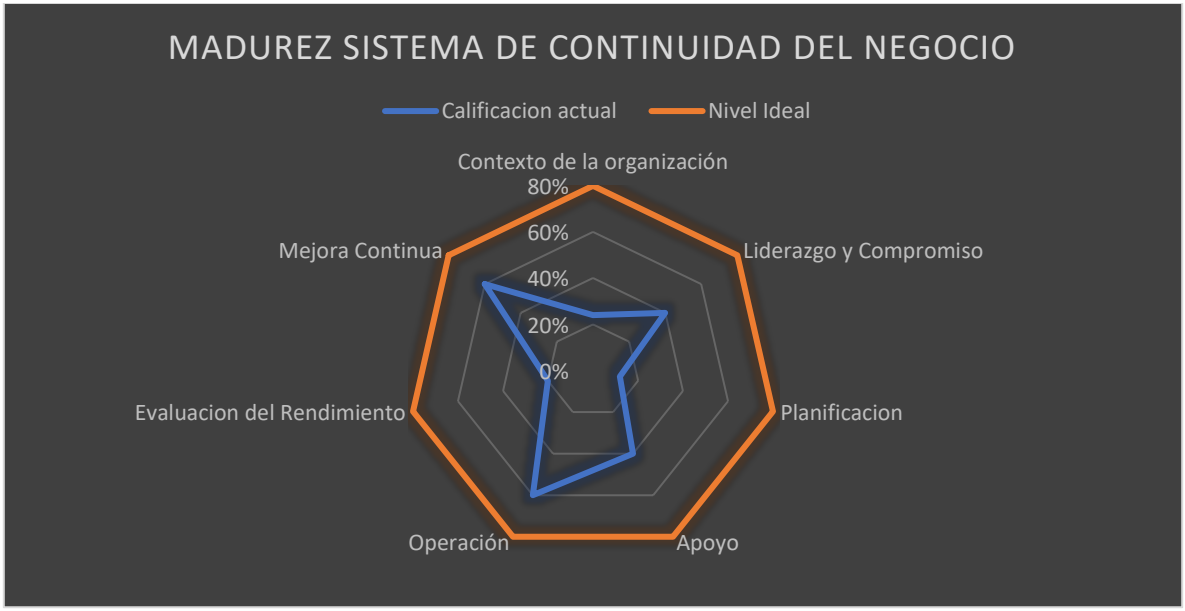

Ilustración 10 *Porcentaje de cumplimiento por dominio ISO: 22301:2019*

Se ha identificado un nivel de madurez REPETIBLE, con un **cumplimiento del 37%,** en línea con los valores porcentuales establecidos en este documento. En este nivel, las organizaciones cuentan con un proceso básico para la continuidad del negocio basado en los acuerdos de niveles de servicios (ANS) contratados con proveedores y terceros; sin embargo, dicho proceso no está estandarizado ni formalizado. La documentación relacionada es limitada, se encuentra desactualizada y carece de revisiones periódicas que garanticen su vigencia y efectividad.

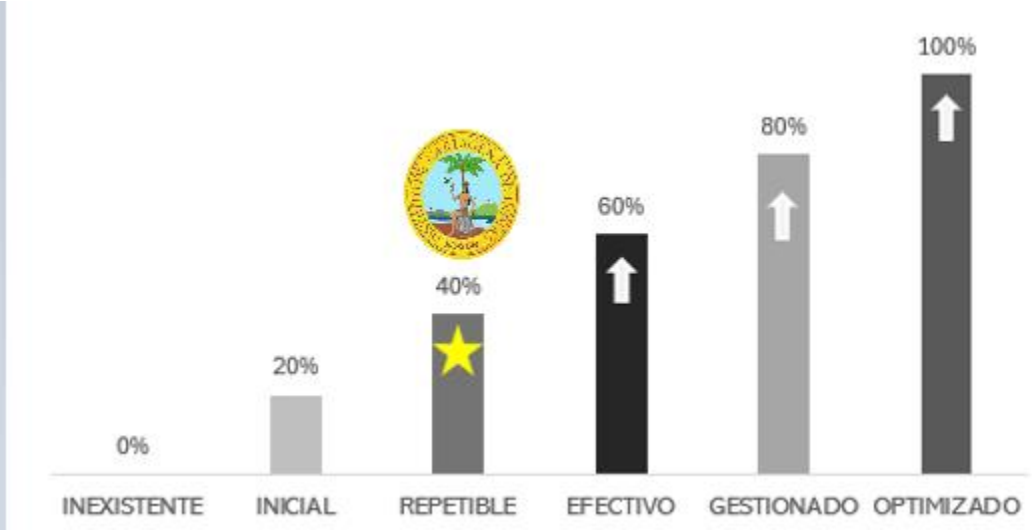

Ilustración 10 *Nivel de madurez SCN*

Hallazgos encontrados en el análisis del BCP

- Documentación clave desactualizada: Se evidencia que en general el BIA, RIA y BCP no ha sido revisado, ni actualizado en los últimos años, lo que genera riesgos de no continuidad en los procesos críticos de la organización.
- Necesidad de mayor compromiso: La alta dirección no ha revisado ni actualizado la política de continuidad, lo que genera falta de alineación entre los objetivos estratégicos y el plan de continuidad.

Acciones prioritarias recomendadas para la mejora continua

1. Actualización de la documentación: Se deben actualizar todos los documentos del SGCN e incluir procesos críticos actuales, nuevas amenazas y dependencias relevantes.

2. Establecer metodologías: Se deberá establecer metodologías para el análisis del BIA, RIA, cálculo del RTO, RPO y BCP de acuerdo con la norma ISO 22301:2019.

3. Realizar un Análisis de Impacto en el Negocio (BIA): Identificar y evaluar los procesos críticos, los tiempos máximos tolerables de interrupción (RTO) y los recursos necesarios para su recuperación.

4. Evaluación de Riesgos: Analizar los riesgos que pueden interrumpir las operaciones críticas, identificando las vulnerabilidades y las posibles amenazas, para implementar controles y estrategias de mitigación.

5. Diseño y desarrollo del BCP: Establecer procedimientos y estrategias detalladas para responder a interrupciones, asegurando la continuidad de los procesos críticos y la recuperación en los plazos definidos.
6. Definir roles y responsabilidades: Designar un equipo de gestión de continuidad del negocio, con funciones y responsabilidades claramente definidas para la implementación y ejecución del BCP.
7. Establecer un plan de comunicación: Diseñar estrategias para informar y coordinarse con las partes interesadas internas y externas durante una interrupción, asegurando el flujo continuo de información.
8. Capacitación y concienciación: Entrenar regularmente al personal clave en los procedimientos del BCP, fomentando una cultura organizacional orientada a la continuidad del negocio.
9. Pruebas y simulacros: Realizar pruebas periódicas del BCP para evaluar su efectividad y capacidad de respuesta ante escenarios de crisis, identificando y corrigiendo posibles fallos.
10. Revisión y mejora continua: Actualizar y ajustar el BCP con base en los resultados de las pruebas, cambios organizacionales, nuevas amenazas identificadas y lecciones aprendidas de incidentes anteriores.
11. Integración con otros sistemas de gestión: Alinear el BCP con otros sistemas de gestión de la organización, como la gestión de riesgos, seguridad de la información y calidad, para una mayor efectividad.
12. Establecer plan de sensibilización: Crear un programa de capacitaciones enfocado en el Plan de Continuidad del Negocio para los procesos críticos y sus lideres responsables.
13. Alineación con la dirección: Involucrar a la alta dirección en la revisión, verificación y aprobación de los documentos elaborados para el plan de continuidad del negocio.

Es crucial que la organización adopte un enfoque más preventivo en la gestión de su plan de continuidad del negocio, además, es necesario ampliar el alcance del plan para incluir todos los procesos críticos de la organización.

Al implementar estas medidas, la organización incrementará su capacidad de respuesta frente a interrupciones cumpliendo así con los estándares establecidos en la norma ISO 22301:2019.

4.4. Resultados detallados del diagnóstico de los requisitos para el programa integral de protección de datos personales PIGDP

El cumplimiento de la Ley 1581 de 2012, conocida como la Ley de Protección de Datos Personales, es un imperativo para las empresas del Estado en Colombia, dado su papel como garantes de la transparencia, la ética pública y la confianza ciudadana. Esta normativa establece el marco jurídico para el adecuado tratamiento de los datos personales, asegurando la protección de los derechos fundamentales a la privacidad, la intimidad y el buen nombre de los ciudadanos.

Para LA ALCALDÍA DE CARTAGENA DE INDIAS, cumplir con la Ley 1581 no solo implica apegarse a los estándares legales, sino también fortalecer la confianza de la ciudadanía al garantizar que la información suministrada será manejada con responsabilidad, confidencialidad y seguridad. Además, permite prevenir riesgos legales, sanciones económicas y daños reputacionales que podrían afectar la credibilidad y la legitimidad de la institución.

En un contexto donde la tecnología y la digitalización son fundamentales para la prestación de servicios públicos, la gestión ética y segura de los datos personales se convierte en un pilar esencial para fomentar la eficiencia, proteger los derechos de los titulares y promover una relación sólida y transparente entre el Estado y la sociedad. Cumplir con esta ley no es solo una obligación, sino un compromiso con la protección de la información personal en beneficio de todos los ciudadanos.

El presente documento tiene como objetivo evaluar el estado actual de Programa integral de gestión de protección de datos personales de la ALCALDÍA DE CARTAGENA DE INDIAS frente a la ley 1581 del 2012. Este análisis abarca la revisión de la documentación existente en la web https://www.cartagena.gov.co/nuevas-politicas-sitio con el fin de identificar las acciones necesarias para la implementación de los controles faltantes, actualización de aquellos donde se encuentren debilidades o mejoras de acuerdo con los insumos que brinde la metodología aplicada.

Objetivo: Identificar el estado actual del Programa integral de gestión protección de datos PIGPD de la ALCALDÍA DE CARTAGENA DE INDIAS, basado en la ley 1581 del 2012.

Alcance del diagnóstico: El análisis estará limitado a la revisión de la información proporcionada por la ALCALDÍA DE CARTAGENA DE INDIAS sobre su programa integral de gestión de protección de datos personales.

Revisión Documental: Se revisaron los documentos actuales de la organización, tales como políticas, procedimientos.

Entrevista y análisis de brechas: Se llevo a cabo una entrevista con una persona clave en la organización. Durante la entrevista, se formularon preguntas basadas en las PIGPDP cláusulas regulatorias de la norma ISO 22301:2019, con el fin de evaluar el cumplimiento y madurez de los procesos. De acuerdo con la siguiente tabla:

El entrevistado califica a juicio de experto, la ubicación de su cumplimiento. En la siguiente tabla mostramos como se va a cuantificar los resultados de esta evaluación.

Nivel de Madurez del cumplimiento de PIGPDP en la ALCALDIA DE CARTAGENA DE INDIAS

El análisis del nivel de madurez en el cumplimiento de la Ley 1581 de 2012 indica que la organización se encuentra en un nivel EFECTIVO, con un **cumplimiento del 50%,** según los rangos establecidos en la metodología descrita en el numeral 3.1.1. Este nivel refleja una adecuada documentación aprobada por la alta dirección, procesos estandarizados y controles debidamente documentados, implementados, pero no actualizados. No obstante, se identifican oportunidades de mejora en áreas clave como el monitoreo y la

medición de los procesos, la formalización de algunos controles pendientes y la incorporación de un enfoque basado en datos para la toma de decisiones estratégicas

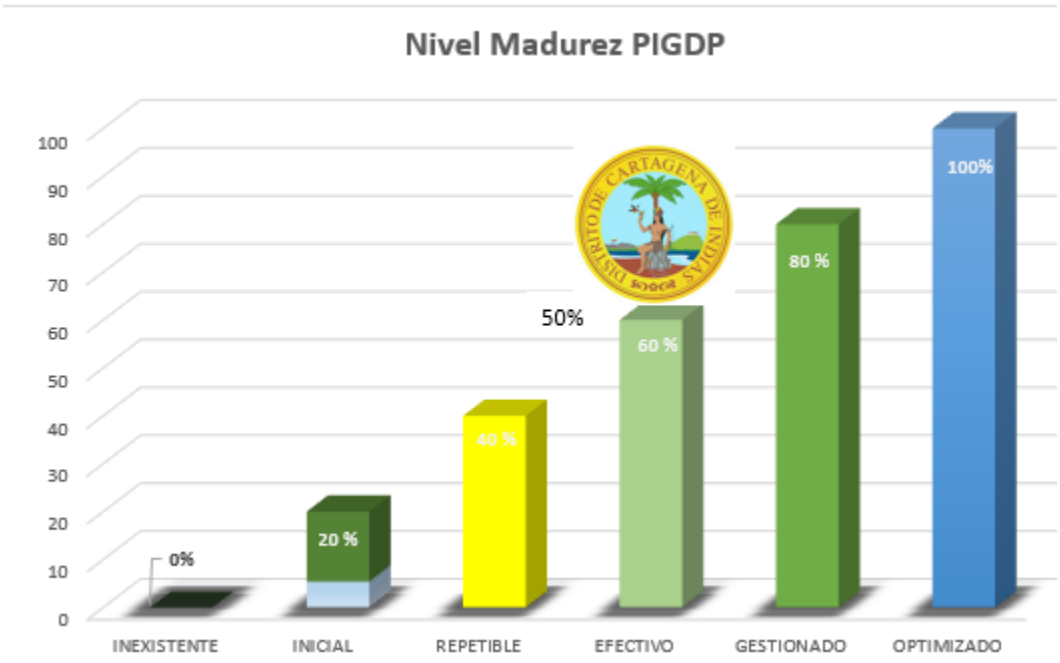

Ilustración 11 *Nivel de madurez PIGPD*

Resultado detallado del diagnóstico de Programa integral de gestión datos personales Ley 1581 del 2012

Hallazgos encontrados en el análisis del PIGPD

- La política podría ser un documento formal, pero no estar implementada en los procesos operativos.
- Ausencia de mecanismos de control y monitoreo para garantizar que la política se cumpla.
- Falta de un inventario o registro de las bases de datos personales tratadas por la organización, incluyendo su finalidad, ubicación y responsables del tratamiento.
- No se han realizado evaluaciones de impacto relacionadas con la protección de datos personales (PIA/DPIA) para identificar riesgos en el tratamiento de datos.
- No existe evidencia de programas de formación o sensibilización del personal en relación con la protección de datos personales y las implicaciones legales.

- No se han formalizado acuerdos de protección de datos con terceros encargados del tratamiento de datos personales, como proveedores.

- No se implementan controles técnicos y organizativos para garantizar la seguridad de los datos personales (por ejemplo, encriptación, controles de acceso, auditorías de sistemas).

- La organización no ha designado a un responsable de protección de datos o no se evidencia su rol activo dentro de la implementación de la política.
- No se han definido procedimientos para responder a incidentes relacionados con la fuga o mal manejo de datos personales, ni mecanismos de notificación a las autoridades competentes o a los titulares.

Acciones prioritarias recomendadas para la mejora continua

1. Diseñar y aplicar formatos de consentimiento explícito, informando claramente a los titulares sobre la finalidad del tratamiento y los derechos que les asisten.

2. Implementar mecanismos para almacenar y rastrear los consentimientos otorgados.

3. Crear procedimientos accesibles para que los titulares ejerzan sus derechos de acceso, rectificación, cancelación y oposición.

4. Designar personal o un equipo encargado de gestionar estas solicitudes dentro de los plazos legales establecidos.

5. Realizar análisis de impacto en privacidad para identificar riesgos asociados al tratamiento de datos personales y establecer medidas de mitigación.

6. Desarrollar programas regulares de formación en protección de datos para todo el personal.

7. Incluir sesiones específicas para roles críticos, como el equipo de TI, marketing y recursos humanos.

8. Revisar contratos con terceros que manejan datos personales, asegurando que incluyan cláusulas de protección de datos conforme a la normativa aplicable.

9. Supervisar el cumplimiento de estas cláusulas por parte de los encargados.

10. Implementar controles técnicos como encriptación, autenticación de usuarios, y firewalls.

11. Realizar auditorías periódicas de los sistemas que manejan datos personales para identificar y corregir vulnerabilidades.

12. Designación de un responsable de Protección de Datos

4.5. Resultados por función del NIST CSF ((Identify, Protect, Detect, Respond, Recover) y del MSPI (Planificación, Ejecución, Monitoreo y Revisión y Mejora Continua).

El marco de controles NIST (National Institute of Standards and Technology) se ha consolidado como una guía esencial para fortalecer la ciberseguridad de las organizaciones, proporcionando un enfoque sistemático para identificar, proteger, detectar, responder y recuperar frente a amenazas y vulnerabilidades. Adoptar este marco es especialmente relevante, considerando el creciente panorama de riesgos asociados al uso de tecnologías digitales y la necesidad de cumplir con normativas locales como la Ley 1581 de 2012 sobre protección de datos personales y la Ley 1273 de 2009 sobre delitos informáticos.

El NIST ayuda a alinear las estrategias de seguridad con estándares internacionales, mejorando la resiliencia organizacional y garantizando la continuidad operativa en un entorno cada vez más globalizado. Este marco no solo permite gestionar riesgos de forma proactiva, sino que también impulsa la confianza de clientes, socios y otras partes interesadas, posicionando a las empresas colombianas como actores confiables en un mercado altamente competitivo y conectado.

Objetivo: Identificar el estado actual del cumplimiento de los controles de seguridad enfocado el Security Framework del NIST (NIST CSF).

Alcance del diagnóstico: Controles de seguridad implementados en el MSPI de la ALCALDÍA DE CARTAGENA DE INDIAS

Metodología: Mediante el análisis de brechas se logra determinar cuáles requisitos y controles de la norma están debidamente implementados en la ALCALDIA DE CARTAGENA DE INDIAS y cuáles no; esto con el fin de identificar las acciones necesarias para la implementación de los controles faltantes, actualización de aquellos donde se encuentren debilidades o mejoras de acuerdo con los insumos que brinde la metodología aplicada

Revisión Documental: Se revisaron los documentos actuales de la organización, tales como políticas, procedimientos, planes de continuidad del negocio, planes de respuestas a incidentes, evaluaciones de riesgo entre otros.

Entrevista y análisis de brechas: Se llevo a cabo una entrevista con una persona clave en la gestión de la continuidad del negocio. Durante la entrevista, se formularon preguntas basadas en las cláusulas regulatorias de la norma ISO 27002:2022, con el fin de evaluar el cumplimiento y madurez de los controles de seguridad vs la madures en la integración del marco Security Framework del NIST (NIST CSF).

MODELO FRAMEWORK CIBERSEGURIDAD NIST		
Etiquetas de fila	CALIFICACIÓN ENTIDAD	NIVEL IDEAL CSF
IDENTIFICAR	37,31	100

DETECTAR	38,06	100
RESPONDER	36,66	100
RECUPERAR	24,3	100
PROTEGER	45,77	100

Tabla 16 Resultados evaluación cumplimiento NIST Vs MSPI

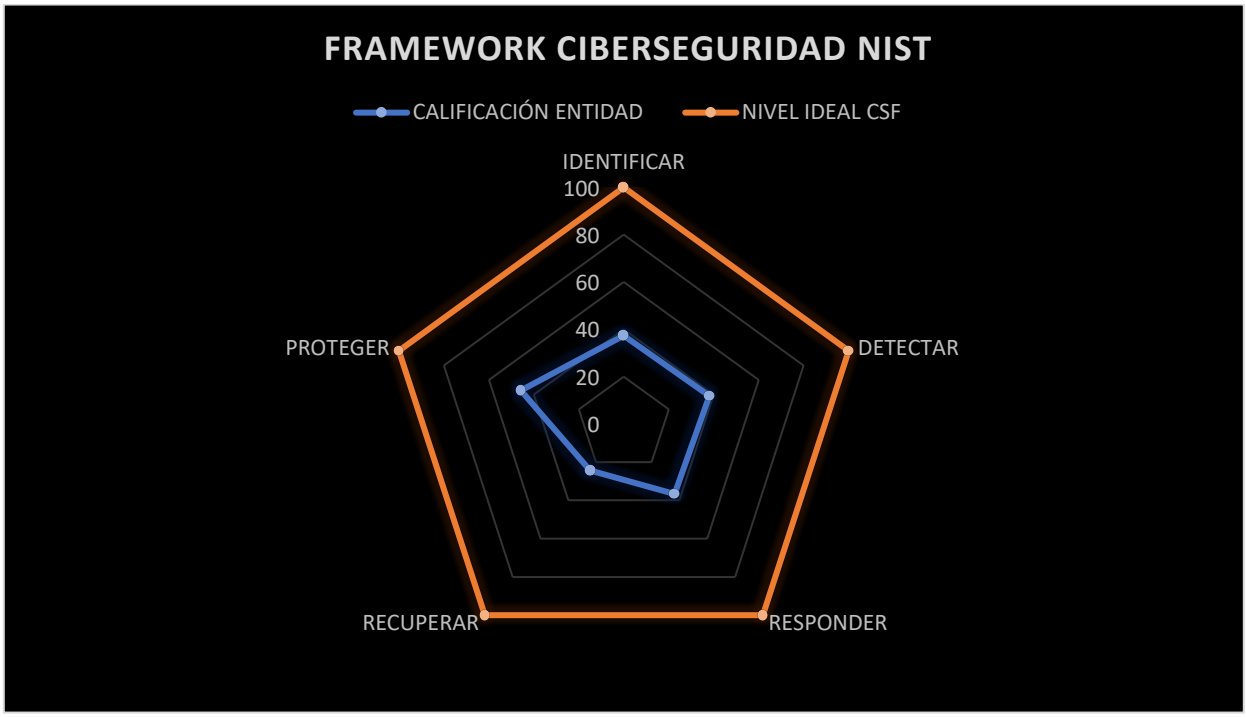

Ilustración 12 *Cumplimiento Framework NIST*

Hallazgos encontrados en el análisis del NIST

Identificar (37,31)

- Falta de un inventario completo de activos críticos y dependencias de sistemas.
- Riesgos de seguridad no están completamente documentados o evaluados.

Detectar (38,06)

- Falencias en la implementación de mecanismos robustos para monitorear y detectar amenazas en tiempo real.

- Insuficiencia en sistemas de alerta temprana y herramientas de monitoreo continuo.

Responder (36,66)

- Procedimientos de respuesta a incidentes no formalizados ni probados regularmente.
- Comunicación ineficiente durante los eventos de seguridad, lo que retrasa la mitigación.

Recuperar (24,3)

- Capacidad limitada para restaurar sistemas y datos tras incidentes críticos, reflejando una baja preparación en recuperación.
- Falta de pruebas regulares en planes de recuperación y continuidad operativa.

Proteger (45,77)

- Aunque la puntuación más alta, aún persisten áreas de mejora en controles de acceso, protección de datos sensibles y capacitación al personal.

Acciones prioritarias recomendadas para la mejora continua

Para Identificar:

- Crear y mantener un inventario actualizado de activos críticos, clasificados por prioridad y riesgos asociados.
- Realizar evaluaciones regulares de riesgos y actualizar los registros de amenazas potenciales.

Para Detectar:

- Implementar herramientas avanzadas de monitoreo como SIEM (Gestión de Eventos e Información de Seguridad) para la detección proactiva.
- Establecer un equipo de respuesta ante incidentes que esté capacitado en detección y análisis de amenazas.

Para Responder:

- Formalizar y documentar un plan de respuesta a incidentes, con roles y responsabilidades claramente definidos.
- Realizar simulaciones periódicas para garantizar que los procedimientos sean eficaces y conocidos por los equipos.

Para Recuperar:

- Desarrollar y probar regularmente planes de recuperación ante desastres (DRP) y continuidad de negocio (BCP).
- Implementar redundancia en sistemas críticos y realizar copias de seguridad automatizadas, seguras y frecuentes.

Para Proteger:

- Reforzar las políticas de control de acceso mediante la autenticación multifactorial (MFA) y gestión de privilegios.
- Capacitar continuamente al personal en ciberseguridad, con énfasis en la prevención de ataques como phishing.

Los resultados sugerencias para reforzar cada control T8 y requisito de la norma se presentan en el Anexo No. 1, 'Matriz de Diagnóstico GAP - ISO 27001 2022 Alcaldía de Cartagena de Indias'. Este anexo incluye recomendaciones para el mejoramiento en el cumplimiento y acciones prioritarias sugeridas para la mejora continua. Estas acciones fortalecerán los niveles de ciberseguridad de la organización, alineándolos con los principios del marco NIST y mejorando su resiliencia frente a amenazas.

JOSE ALEJANDRO CHAMORRO L
Lider de Proyecto REDSUMMA