

ENTIDAD EVALUADA	Corporación para el Desarrollo Sostenible del Urabá - CORPOURABA
FECHAS DE EVALUACIÓN	31/05/2025
CONTACTO	JAIRO AGUDELO - jagudelo@corpouraba.gov.co
ELABORADO POR	JAIRO AGUDELO - jagudelo@corpouraba.gov.co

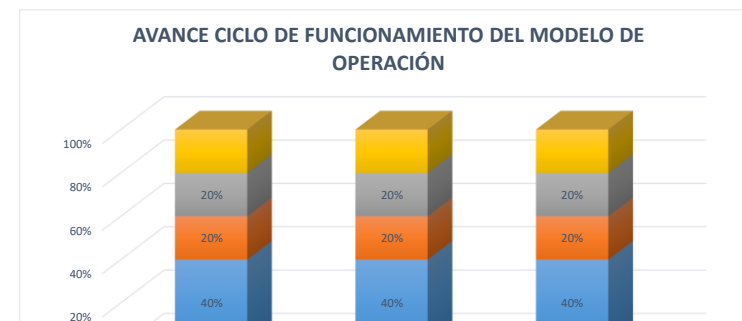
EVALUACIÓN DE EFECTIVIDAD DE CONTROLES - ISO 27001:2013 ANEXO A

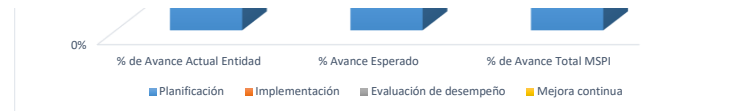
Evaluación de Efectividad de controles				
No.	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	100	95	OPTIMIZADO
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	95	90	OPTIMIZADO
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	100	95	OPTIMIZADO
A.8	GESTIÓN DE ACTIVOS	89	85	OPTIMIZADO
A.9	CONTROL DE ACCESO	99	95	OPTIMIZADO
A.10	CRIPTOGRAFÍA	90	85	OPTIMIZADO
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	95	90	OPTIMIZADO
A.12	SEGURIDAD DE LAS OPERACIONES	91	85	OPTIMIZADO
A.13	SEGURIDAD DE LAS COMUNICACIONES	84	80	OPTIMIZADO
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	83	80	OPTIMIZADO
A.15	RELACIONES CON LOS PROVEEDORES	100	95	OPTIMIZADO
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	83	80	OPTIMIZADO
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	90	85	OPTIMIZADO
A.18	CUMPLIMIENTO	82,5	80	OPTIMIZADO
<b>PROMEDIO EVALUACIÓN DE CONTROLES</b>		<b>92</b>	<b>87</b>	<b>OPTIMIZADO</b>



AVANCE CICLO DE FUNCIONAMIENTO DEL MODELO DE OPERACIÓN (PHVA)

AVANCE PHVA				
Año	COMPONENTE	% de Avance Actual Entidad	% Avance Esperado	% de Avance Total MSPI
2022	Planificación	40%	40%	40%
2022	Implementación	20%	20%	20%
2022	Evaluación de desempeño	20%	20%	20%
2022	Mejora continua	20%	20%	20%
<b>TOTAL</b>				<b>100%</b>





### NIVEL DE MADUREZ MODELO SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

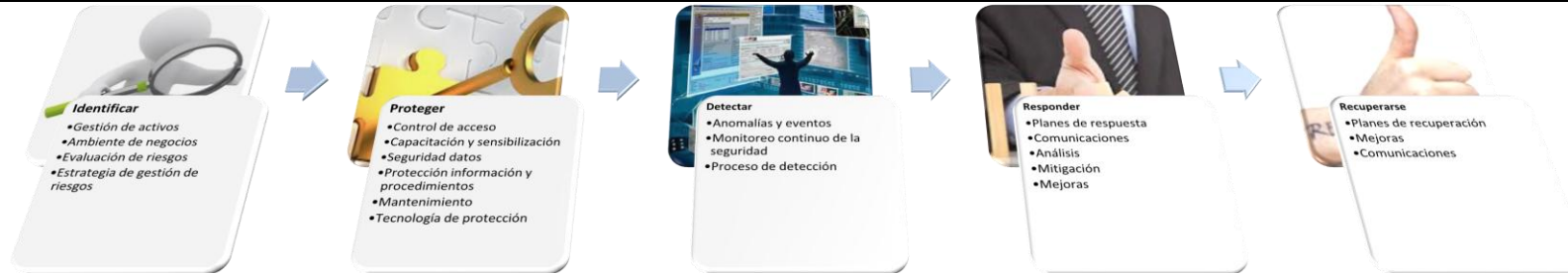
NIVELES DE MADUREZ DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

	NIVEL DE CUMPLIMIENTO
Inicial	SUFICIENTE
Repetible	SUFICIENTE
Definido	SUFICIENTE
Administrado	SUFICIENTE
Optimizado	SUFICIENTE

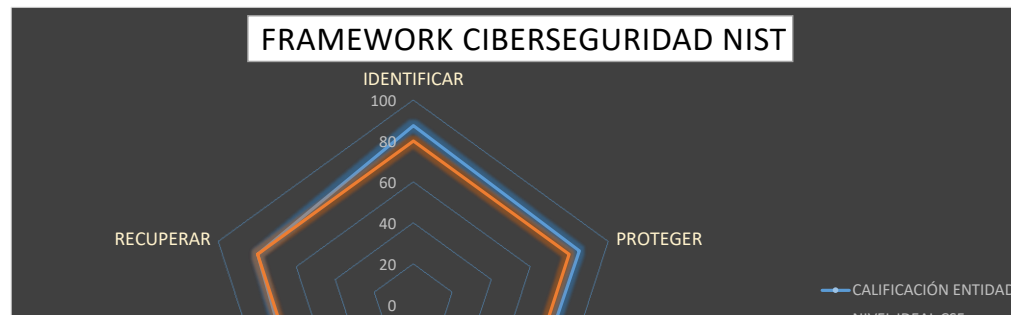
Nivel	Descripción
<b>Inicial</b>	En este nivel se encuentran las entidades, que aún no cuenta con una identificación de activos y gestión de riesgos, que les permita determinar el grado de criticidad de la información, respecto a la seguridad y privacidad de la misma, por lo tanto los controles no están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

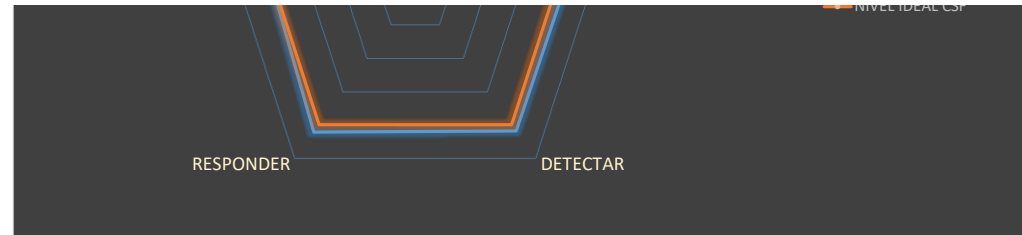
TOTAL DE REQUISITOS CON CALIFICACIONES DE CUMPLIMIENTO	
CRÍTICO	0% a 35%
INTERMEDIO	36% a 70%
SUFICIENTE	71% a 100%

### CALIFICACIÓN FRENTE A MEJORES PRÁCTICAS EN CIBERSEGURIDAD (NIST)



MODELO FRAMEWORK CIBERSEGURIDAD NIST		
Etiquetas de fila	CALIFICACIÓN ENTIDAD	NIVEL IDEAL CSF
IDENTIFICAR	88	80
PROTEGER	85	80
DETECTAR	84	80
RESPONDER	84	80
RECUPERAR	80	80







Corporación para el Desarrollo Sostenible del Urabá - CORPOURABA

ID REQUISITO	CARGO	REQUISITO	HOJA	ELEMENTO	CALIFICACIÓN OBTENIDA	NIVEL 1 INICIAL	CUMPLIMIENTO NIVEL INICIAL	NIVEL 2 GESTIONADO	CUMPLIMIENTO NIVEL GESTIONADO	NIVEL 3 DEFINIDO	CUMPLIMIENTO NIVEL DEFINIDO	NIVEL 4 GESTIONADO CUANTITATIVAMENTE	CUMPLIMIENTO NIVEL 4 GESTIONADO CUANTITATIVAMENTE	NIVEL 5 OPTIMEADO	CUMPLIMIENTO NIVEL 5 OPTIMIZADO
R1	n/a	1) Si se identifican en forma general los activos de información de la Entidad, están en 40. 2) Si se cuenta con un inventario de activos de información física y lógica de toda la entidad, documentado y firmado por la alta dirección, están en 60. 3) Si se revisa y monitorean periódicamente los activos de información de la entidad, están en 80.	Administrativas	AD.4.1.1	100	40	MAYOR	60	MAYOR	60	MAYOR	80	MAYOR	100	CUMPLE
R2	n/a	Se clasifican los activos de información lógicos y físicos de la Entidad.	Administrativas	AD.4.2.1	100	20	MAYOR	40	MAYOR	60	MAYOR	80	MAYOR	100	CUMPLE
R3	n/a	1. Si los funcionarios de la Entidad no tienen conciencia de la seguridad y privacidad de la información y se han diseñado programas para los funcionarios de conciencia y comunicación, de las políticas de seguridad y privacidad de la información, están en 20. 2. Si se observa en los funcionarios una conciencia de seguridad y privacidad de la información y los planes de toma de conciencia y comunicación, de las políticas de seguridad y privacidad de la información, están aprobados y documentados, por la alta Dirección, están en 40. 3. Si se han ejecutado los planes de toma de conciencia, comunicación y divulgación, de las políticas de seguridad y privacidad de la información, aprobados por la alta Dirección, están en 60.	Administrativas	AD.3.2.2	100	20	MAYOR	40	MAYOR	60	MAYOR	80	MAYOR	100	CUMPLE
R4	n/a	Existe la necesidad de implementar el Modelo de Seguridad y Privacidad de la información, para definir políticas, procesos y procedimientos claros para dar una respuesta proactiva a las amenazas que se presenten en la Entidad.	PHVA Administrativas PHVA	P.1 AD.1.1 P.4	100 100 100	20 20 20	MAYOR MAYOR MAYOR	40 40 40	MAYOR MAYOR MAYOR	60 60 60	MAYOR MAYOR MAYOR	80 80 80	MAYOR MAYOR MAYOR	100 100 100	CUMPLE CUMPLE CUMPLE
R5	Responsable de SI	1. Si se tratan temas de seguridad y privacidad de la información en los comités del modelo integrado de gestión, colócase 20 2. Los temas de seguridad de la información se tratan en los comités directivos interdisciplinarios de la Entidad, con regularidad, colócase 40	Madurez	R5	60	20	MAYOR	40	MAYOR	60	CUMPLE	80	MENOR	100	MENOR
R6	n/a	1. Si se empiezan a definir las políticas de seguridad y privacidad de la información basada en el Modelo de Seguridad y Privacidad de la Información, están en 20. 2. Si se revisan y se aprueban las políticas de seguridad y privacidad de la información, están en 40. 3. Si se divulgan las políticas de seguridad y privacidad de la información, están en 60.	Administrativas	AD.1.1	100	20	MAYOR	40	MAYOR	60	MAYOR	80	MAYOR	100	CUMPLE
R7	n/a	Establecer y documentar el alcance, límites, política, procedimientos, roles y responsabilidades y del Modelo de Seguridad y Privacidad de la Información.	PHVA	P.1	100	60	MAYOR	60	MAYOR	60	MAYOR	80	MAYOR	100	CUMPLE
R8	n/a	Determinar el impacto que generan los eventos que atenten contra la integridad, disponibilidad y confidencialidad de la información de la Entidad.	Técnicas	T.7.1.4	80	20	MAYOR	40	MAYOR	60	MAYOR	60	MAYOR	80	CUMPLE
<b>DE MADUREZ INICIAL</b>					<b>940</b>	<b>260</b>	<b>CUMPLE</b>	<b>440</b>	<b>CUMPLE</b>	<b>600</b>	<b>CUMPLE</b>	<b>780</b>	<b>MENOR</b>	<b>980</b>	<b>MENOR</b>
R9	Responsable de SI	Con base en el inventario de activos de información clasificado, se establece la caracterización de cada uno de los sistemas de información.	Madurez	R9	60	N/A	N/A	40	MAYOR	60	CUMPLE	80	MENOR	100	MENOR
R10	n/a	Aprobación de la alta dirección, documentada y firmada, para la implementación del Modelo de Seguridad y Privacidad de la Información.	Madurez	R9	100	N/A	N/A	60	MAYOR	60	MAYOR	80	MAYOR	100	CUMPLE
R11	n/a	Identificar los riesgos asociados con la información, físicos, lógicos, identificando sus vulnerabilidades y amenazas.	PHVA	P.6	100	N/A	N/A	40	MAYOR	60	MAYOR	80	MAYOR	100	CUMPLE
R12	n/a	1) Si se elaboran informes de TODOS los incidentes de seguridad y privacidad de la información, TODOS están documentados e incluidos en el plan de mejoramiento continuo. Se definen los controles y medidas necesarias para disminuir los incidentes y prevenir su ocurrencia en el futuro, están en 40. 2) Si los controles y medidas identificados para disminuir los incidentes fueron implementados, están en 60.	Técnicas	T.7.1.2	100	N/A	N/A	40	MAYOR	60	MAYOR	80	MAYOR	100	CUMPLE
R13	n/a	1. Si se cuentan con procedimientos que indican a los funcionarios como manejar la información y los activos de información en forma segura. Se tienen documentados los controles físicos y lógicos que se han definido en la Entidad, con los cuales se busca preservar la seguridad y privacidad de la información, aprobado por la alta Dirección, están en 40. 2. Si se han divulgado e implementado los controles físicos y lógicos que use han definido en la entidad, con los cuales se busca preservar la seguridad y privacidad de la información, están en 60.	Administrativas	AD.4.1	100	N/A	N/A	40	MAYOR	60	MAYOR	80	MAYOR	100	CUMPLE
R14	n/a	Si existen planes de continuidad del negocio que contemplen los procesos críticos de la Entidad que garanticen la continuidad de los mismos. Se documentan y protegen adecuadamente los planes de continuidad del negocio de la Entidad, este de estar documentado y firmado, por la alta Dirección, están en 40. Si se reconoce la importancia de ampliar los planes de continuidad del negocio a otros procesos, pero aun no se pueden incluir ni trabajar con ellos, están en 60.	Administrativas	AD.5.1.1	100	N/A	N/A	40	MAYOR	60	MAYOR	80	MAYOR	100	CUMPLE
R15	n/a	Los roles de seguridad y privacidad de la información están bien definidos y se lleva un registro de las actividades de cada uno.	Administrativas	AD.2.1	100	N/A	N/A	40	MAYOR	60	MAYOR	80	MAYOR	100	CUMPLE
R16	n/a	Dispositivos para movilidad y teletrabajo	Administrativas	AD.2.2	90	N/A	N/A	40	MAYOR	60	MAYOR	80	MAYOR	100	MENOR
R17	n/a	Protección contra código malicioso	Técnicas	T.4.2	100	N/A	N/A	40	MAYOR	60	MAYOR	80	MAYOR	100	CUMPLE



