ANEXO 2

El futuro digital es de todos | Gobierno de Colombia MinTIC

INSTRUMENTO DE IDENTIFICACIÓN DE LA LINEA BASE DE SEGURIDAD
HOJA PORTADA

+MásTIC MejorPaís

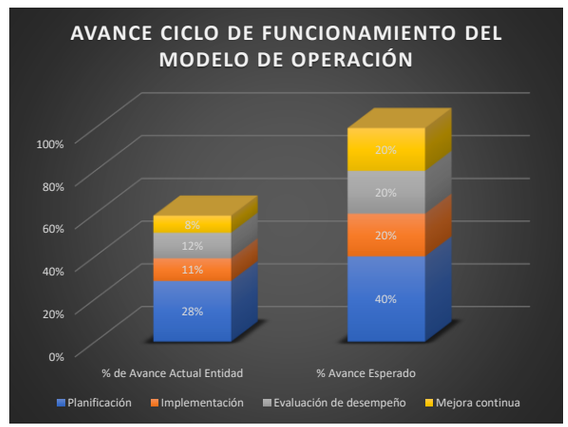
ENTIDAD EVALUADA	GOBERNACIÓN DEL ARCHIPIÉLAGO DE SAN ANDRÉS, PROVIDENCIA Y SANTA CATALINA
FECHAS DE EVALUACIÓN	20/08/2021
CONTACTO	Claudia Mendoza - cmendoza@sanandres.gov.co
ELABORADO POR	Jonathan Marin - jmarin@sanandres.gov.co

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

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	80	100	GESTIONADO
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	86	100	OPTIMIZADO
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	96	100	OPTIMIZADO
A.8	GESTIÓN DE ACTIVOS	69	100	GESTIONADO
A.9	CONTROL DE ACCESO	51	100	EFECTIVO
A.10	CRIPTOGRAFÍA	30	100	REPETIBLE
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	53	100	EFECTIVO
A.12	SEGURIDAD DE LAS OPERACIONES	37	100	REPETIBLE
A.13	SEGURIDAD DE LAS COMUNICACIONES	63	100	GESTIONADO
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	17	100	INICIAL
A.15	RELACIONES CON LOS PROVEEDORES	30	100	REPETIBLE
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	31	100	REPETIBLE
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	54	100	EFECTIVO
A.18	CUMPLIMIENTO	37,5	100	REPETIBLE
PROMEDIO EVALUACIÓN DE CONTROLES		52	100	EFECTIVO

AVANCE CICLO DE FUNCIONAMIENTO DEL MODELO DE OPERACIÓN (PHVA)

Año	AVANCE PHVA		
	COMPONENTE	% de Avance Actual Entidad	% Avance Esperado
2020	Planificación	28%	40%
	Implementación	11%	20%
	Evaluación de desempeño	12%	20%
	Mejora continua	8%	20%
TOTAL		59%	100%



NIVEL DE MADUREZ MODELO SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

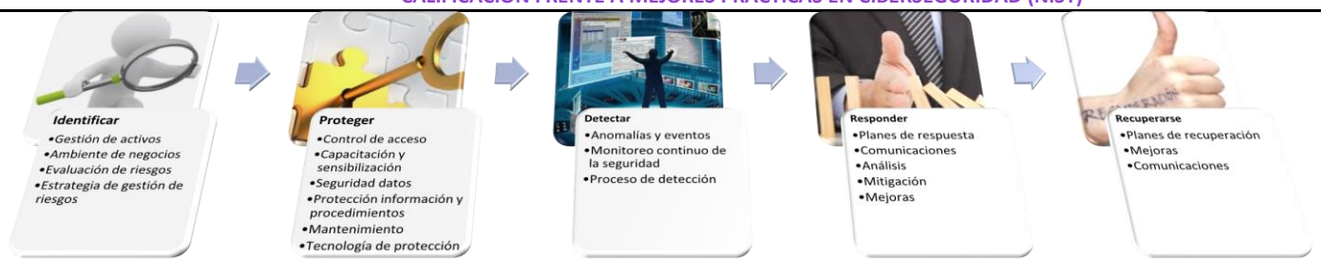
NIVELES DE MADUREZ DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

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

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 procesos básicos de gestión de la seguridad y privacidad de la información. De igual forma existen controles que permiten detectar posibles incidentes de seguridad, pero no se encuentra gestionados dentro del componente planificación del MSPI.
Definido	En este nivel se encuentran las entidades que tienen documentado, estandarizado y aprobado por la dirección, el modelo de seguridad y privacidad de la información. Todos los controles se encuentran debidamente documentados, aprobados, implementados, probados y actualizados.
Administrado	En este nivel se encuentran las entidades, que cuenten con métricas, indicadores y realizan auditorías al MSPI, recolectando información para establecer la efectividad de los controles.
Optimizado	En este nivel se encuentran las entidades, en donde existe un mejoramiento continuo del MSPI, retroalimentando cualitativamente el modelo.

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	55	100
DETECTAR	26	100
RESPONDER	19	100
RECUPERAR	33	100
PROTEGER	35	100