

DEFINIDO		Puntaje Obtenido
Planificación y control operacional.		
<i>Divulgación de las políticas de seguridad y privacidad de la información.</i>		
1	¿Se ejecutan los planes de toma de conciencia, comunicación y divulgación, de las políticas de seguridad y privacidad de la información y están, aprobados por la alta Dirección?	10
<i>El comité directivo divulga, las medidas de seguridad y privacidad de la información que deberán ser tomadas para la conservación de la información.</i>		
1	¿Se han implementado 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?	10
Plan de tratamiento del riesgo		
<i>Lista de chequeo de requerimientos de seguridad</i>		
1	¿Existencia del listado de requerimientos sobre la seguridad de la información en proyectos?.	15
<i>Elaboración del plan de tratamiento del riesgo (quién, cómo y cuándo)</i>		
1	¿Se tiene un plan de acción definido en función de los diversos controles definidos por la DdA (Declaración de Aplicabilidad)?	10
2	¿Se tiene una descripción de las tareas a realizar para la ejecución de los controles que lo necesiten o de las tareas de administración del SGSI?	10
3	¿Se tiene una descripción del personal requerido con experiencia, habilidades, funciones, dentro del plan de acción para el tratamiento de riesgos de seguridad?	10
<i>Implementación de controles</i>		
1	¿Se han Implementado los controles seleccionados para la gestión de riesgos de seguridad de la información con priorización de acciones evaluación de opciones de control recomendadas facilidad/efectividad, Costo/ beneficio y asignación de responsabilidades?	7
2	¿Se aplica el protocolo de controles preventivos y detectivos (políticas de seguridad, procedimientos, metodologías, seguridad del personal, física y ambiental) en el tratamiento de riesgos de seguridad de la información?.	7
3	¿Se establecen los indicadores de gestión pertinentes que permitan medir eficacia de los controles de seguridad de la información?	8
4	¿Se incluye un plan de contingencia para la gestión de riesgos de seguridad de la información?	8
<i>Seguimiento</i>		
1	Se tienen Instrumentos diseñados para hacer el seguimiento.	15
2	Se reconoce la importancia de ampliar los planes de continuidad del negocio a otros procesos, pero aún no se pueden incluir ni trabajar con ellos.	15
Gestión de recursos y procedimientos implementados para la asignación de recursos financieros		
<i>Asignación del presupuesto para Seguridad de la Información.</i>		
1	¿Se genera la documentación de la asignación del presupuesto de seguridad como % del presupuesto de TI?	20
Gestión de recursos y procedimientos implementados para la asignación de recursos humanos		

<i>Perfiles y experiencia del personal (descripción) para cada rol o función.</i>		
1	¿Se genera la documentación de perfiles para cada función en materia de seguridad de la información?	20
<i>Inventario de habilidades del personal disponible (experiencia existente).</i>		
1	¿Se genera la documentación del inventario de habilidades del personal?	0
<i>Procedimientos para la asignación del personal según las funciones.</i>		
1	¿Se genera la documentación de procedimientos de asignación de personal?	20
<i>Procedimientos para la contratación del personal</i>		
1	¿Se genera la documentación del proceso de contratación?	20
<i>Implementación del plan y estrategia de transición de IPv4 a IPv6.</i>		
1	¿Se posee la implementación del plan y estrategia de transición de IPv4 a IPv6?	20
Total de calificación para nivel Definido		225

De acuerdo con la escala de madurez establecida por MINTIC el estado de implementación del SGSI en el MADR a 30 de junio de 2017, tiene un **nivel definido** con calificación **INTERMEDIO**

225

Indicador de eficacia en la implementación del SGSI

215 x 100

245

92%