

Anexo B

Estado de Implementación ISO 27001

| Sección | Requerimientos ISO 27001 | Estado | Nivel de Madurez | Madurez numeral |
|------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|-------------|------------------|-----------------|
| 4 | Contexto de la organización | | | |
| 4.1 | Comprensión de la organización y de su contexto | | | |
| 4.1 | Determinar las cuestiones externas e internas que son pertinentes para su propósito y que afecten su capacidad para lograr los resultados previstos | Inicial | 2 | 1,6 |
| 4.2 | Comprensión de las necesidades y expectativas de las partes interesadas | | | |
| 4.2 (a) | Identificar las partes interesadas incluyendo leyes aplicables, regulaciones, contratos, etc. | Inicial | 2 | |
| 4.2 (b) | Determinar los requerimientos y obligaciones relevantes de seguridad de la información | Inexistente | 0 | |
| 4.3 | Determinación del alcance del SGSI | | | |
| 4.3 | Determinar y documentar el alcance del SGSI | Inicial | 2 | |
| 4.4 | SGSI | | | |
| 4.4 | Establecer, implementar, mantener y mejorar de forma continua el SGSI acorde al estándar | Inicial | 2 | |
| 5 | Liderazgo | | | |
| 5.1 | Liderazgo y compromiso | | | |
| 5.1 | La administración debe demostrar liderazgo y compromiso por el SGSI | Repetible | 4 | 2,0 |
| 5.2 | Política | | | |
| 5.2 | Documentar la Política de Seguridad de la Información | Inexistente | 0 | |
| 5.3 | Roles, responsabilidades y autoridades en la organización | | | |
| 5.3 | Asignar y comunicar los roles y responsabilidades de seguridad de la información | Inicial | 2 | |
| 6 | Planificación | | | |
| 6.1 | Acciones para tratar los riesgos y oportunidades | | | |
| 6.1.1 | Diseñar el SGSI para satisfacer los requerimientos, tratando riesgos e identificando oportunidades | Inicial | 2 | |
| 6.1.2 | Definir e implementar un proceso de análisis de riesgos de seguridad de la información | Inicial | 2 | |

| | | | | |
|------------|-----------------------------------------------------------------------------------------------------------------------------|-------------|---|-----|
| 6.1.3 | Documentar e implementar un proceso de tratamiento de riesgos de seguridad de la información | Inexistente | 0 | 1 |
| 6.2 | Objetivos de seguridad de la información y planificación para su consecución | | | |
| 6.2 | Establecer y documentar los planes y objetivos de la seguridad de la información | Inexistente | 0 | |
| 7 | Soporte | | | |
| 7.1 | Recursos | | | |
| 7.1 | Determinar y asignar los recursos necesarios para el SGSI | Inicial | 2 | 2,6 |
| 7.2 | Competencia | | | |
| 7.2 | Determinar, documentar hacer disponibles las competencias necesarias | Inicial | 2 | |
| 7.3 | Concienciación | | | |
| 7.3 | Implementar un programa de concienciación de seguridad | Inicial | 2 | |
| 7.4 | Comunicación | | | |
| 7.4 | Determinar la necesidades de comunicación internas y externas relacionadas al SGSI | Desconocido | 0 | |
| 7.5 | Información documentada | | | |
| 7.5.1 | Proveer documentación requerida por el estandar más la requerida por la organización (Registros de información documentada) | Inicial | 2 | |
| 7.5.2 | Proveer un titulo, autor, formato consistente, revisión y aprobación a los documentos | Repetible | 4 | |
| 7.5.3 | Mantener un control adecuado de la documentación | Definido | 6 | |
| 8 | Operación | | | |
| 8.1 | Planificación y control operacional | | | |
| 8.1 | Planificar, implementar, controlar y documentar el proceso de gestion de riesgos del SGSI (Tratamiento de riesgos) | Inicial | 2 | 0,7 |
| 8.2 | Apreciación de los riesgos de seguridad de la información | | | |
| 8.2 | Evaluar y documentar los riesgos de seguridad regularment y cuando hay cambios | Inexistente | 0 | |
| 8.3 | Tratamiento de los riesgos de seguridad de la información | | | |
| 8.3 | Implementar un plan de tratamiento de riesgos y documentar los resultados | Desconocido | 0 | |

| | | | | |
|-------------|---------------------------------------------------------------------------------------------------------------------|--------------------|----------|------------|
| 9 | Evaluación del desempeño | | | |
| 9.1 | Seguimiento, medición, análisis y evaluación | | | |
| 9.1 | Realizar un seguimiento, medición, análisis y evaluación del SGSI y los controles | Inicial | 2 | 0,7 |
| 9.2 | Auditoría interna | | | |
| 9.2 | Planificar y realizar una auditoria interna del SGSI | Desconocido | 0 | |
| 9.3 | Revisión por la dirección | | | |
| 9.3 | La administración realiza una revision periodica del SGSI | Inexistente | 0 | |
| 10 | Mejora | | | |
| 10.1 | No conformidad y acciones correctivas | | | |
| 10.1 | Identificar, arreglar y reaccionar ante no conformidades para evitar su recurrencia documentando todas las acciones | Inicial | 2 | 2 |
| 10.2 | Mejora continua | | | |
| 10.2 | Mejora continua del SGSI | Inicial | 2 | |

CLAUSULAS

| | | | | |
|-----------|------------------------------------|------------|-----------|----------|
| 4 | CONTEXTO DE LA ORGANIZACIÓN | 1,6 | 10 | 8 |
| 5 | LIDERAZGO | 2,0 | 10 | 8 |
| 6 | PLANIFICACIÓN | 1,0 | 10 | 8 |
| 7 | SOPORTE | 2,9 | 10 | 8 |
| 8 | OPERACIÓN | 0,7 | 10 | 8 |
| 9 | EVALUACIÓN DE DESEMPEÑO | 0,7 | 10 | 8 |
| 10 | MEJORA | 2,0 | 10 | 8 |

Promedio

1,56

Valoración cmm - gestión sgsi

