**Lista de verificación para la implementación de ISO 27001**

|  |  |  |  |
| --- | --- | --- | --- |
| **Fases de implementación** | **Tareas** | **Documentos del Paquete de Documentos que se utilizarán** | **Hecho** |
| *Obtener apoyo de la dirección* | Investigar qué beneficios de ISO 27001 serían aplicables a su organización | - |  |
| Presentar los beneficios a la dirección y obtener su compromiso | - |  |
| Obtener la aprobación formal para comenzar la planificación del proyecto | - |  |
|  |  |  |
| *Prepararse para su proyecto* | Escribir procedimiento para el control de documentos | 01 – Procedimiento para el control de documentos y registros |  |
| Instruir a su equipo de proyecto | - |  |
| Redactar el plan del proyecto, incluida la definición del gerente del proyecto, el equipo del proyecto, el promotor del proyecto, los recursos necesarios y los hitos | 02 – Plan de proyecto |  |
| Definir qué partes interesadas deben estar informadas sobre cada paso del proyecto | - |  |
| Organizar reunión de lanzamiento | - |  |
|  |  |  |
| *Identificar requisitos* | Definir el procedimiento para la identificación de las partes interesadas | 03 – Procedimiento para la identificación de requisitos |  |
| Identificar los requisitos de las partes interesadas | 03.1 – Lista de requisitos legales, normativos, contractuales y de otra índole |  |
|  |  |  |
| *Definir el alcance, la intención de gestión y las responsabilidades* | Redactar el Documento de alcance del SGSI | 04 – Documento de alcance del SGSI |  |
| Redactar la Política de seguridad de la información | 05 – Política de seguridad de la información |  |
| Decidir sobre los objetivos de seguridad de la información | 05 – Política de seguridad de la información |  |
|  |  |  |
| *Realizar la gestión de riesgos* | Desarrollar la metodología de evaluación de riesgos | 06 – Metodología de evaluación y tratamiento de riesgos |  |
| Realizar evaluación de riesgos | 06.1 – Cuadro de evaluación de riesgos |  |
| Realizar tratamiento de riesgos | 06.2 – Cuadro de tratamiento de riesgos |  |
| Redactar el informe de evaluación y tratamiento de riesgos | 06.3 – Informe sobre la evaluación y tratamiento de riesgos |  |
|  |  |  |
| *Desarrollar el perfil de seguridad de su organización y plan de acción sobre cómo lograrlo* | Desarrollar la Declaración de aplicabilidad | 07 – Declaración de aplicabilidad |  |
| Aceptar los riesgos residuales | 07 – Declaración de aplicabilidad |  |
| Desarrollar el Plan de tratamiento de riesgos | 08 – Plan de tratamiento de riesgos |  |
|  |  |  |
| *Implementar los controles* | Implementar todos los controles definidos en el Plan de tratamiento de riesgos | Documentos en la carpeta 09\_Anexo\_A\_Controles\_de\_seguridad |  |
| Mantener registros de implementación | Para los documentos del SGSI, esto es visible a través del historial de versiones de un documento; para el software, esto podría ser un registro sobre su prueba y lanzamiento. |  |
|  |  |  |
| *Realizar programas de formación y concienciación* | Realizar concienciaciones para todos los empleados que carecen de las habilidades requeridas | 10 – Plan de formación y concienciación |  |
| Realizar programas de concienciación para todos los empleados y terceros que tengan un rol en su SGSI | 10 – Plan de formación y concienciación |  |
|  |  |  |
| *Implementar procedimientos de gestión* | Escribir procedimiento para la auditoría interna | 11 – Procedimiento para auditoría interna |  |
| Desarrollar el programa de auditoría | 11.1 – Programa anual de auditoría interna |  |
| Definir qué medidas se van a realizar en relación con los objetivos del SGSI y de los controles | 12.1 – Informe de medición |  |
| Identificar las fuentes de información que se utilizarán en la revisión por la dirección | 12.2 – Actas de revisión de la gerencia |  |
| Escribir el procedimiento para la acción correctiva | 13 – Procedimiento para la acción correctiva |  |
|  |  |  |
| *Operar el SGSI* | Mantener todos los registros requeridos por sus propias políticas y procedimientos | Diversos registros que se crean debido a los documentos del SGSI, por ejemplo, registro de copias de seguridad (del software de copias de seguridad), Lista completa de requisitos legales, reglamentarios y contractuales, etc. |  |
| Realizar acciones correctivas según sea necesario como consecuencia de las mejoras necesarias en la operación del SGSI | 13.1 – Formulario de acción correctiva |  |
|  |  |  |
| *Supervisar y medir el SGSI* | Asegurarse de monitorear todos sus sistemas | Registros de seguimiento definidos en cada documento implementado, por ejemplo, número de incidentes, número de errores en un sistema en particular, etc. |  |
| Medir si ha alcanzado los objetivos fijados para su SGSI y para sus controles | 12.1 –Informe de medición |  |
|  |  |  |
| *Realizar una auditoria interna* | Realizar auditoría/s interna/s | 11.3 – Lista de verificación de auditoría interna |  |
| Escribir un informe de auditoría interna | 11.2 – Informe de auditoría interna |  |
| Realizar acciones correctivas como consecuencia de las no-conformidades encontradas durante la auditoría interna | 13.1 – Formulario de acción correctiva |  |
|  |  |  |
| *Realizar la revisión por la dirección* | Realizar revisión por la dirección | - |  |
| Mantener registros de la revisión por la dirección | 12.2 – Actas de revisión por la dirección |  |
| Realizar acciones correctivas como consecuencia de las mejoras identificadas durante la revisión por la dirección | 13.1 – Formulario de acción correctiva |  |
|  |  |  |
| *Auditoría de certificación* | Obtener propuestas de varios organismos de certificación | - |  |
| Seleccionar el organismo de certificación | - |  |
| Auditoría de certificación de etapa 1 | - |  |
| Auditoría de certificación de etapa 2 | - |  |
| Visitas de vigilancia | - |  |
|  |  |  |