

Anexo D – Procedimiento de revisión por la dirección

1. Alcance

El proceso de revisión alcanzará a todo el dominio de SGSI, ya que se trata de una revisión global para la evaluación de la correcta función e implantación del mismo.

2. Frecuencia

La primera revisión del SGSI por parte de la dirección se llevará a cabo a los SEIS MESES desde su implantación. Posteriormente las revisiones se realizarán ANUALMENTE.

3. Entradas de la revisión

- Resultados de las revisiones anteriores del SGSI (Si las hubo)
- Resultados de los indicadores del SGSI
- No conformidades de las anteriores auditorías internas (Si la hubo)
- Resultado de la auditoría interna
- Estado de las medidas correctivas y preventivas
- Vulnerabilidades y amenazas no gestionadas adecuadamente
- Cambios en la organización que afectan al SGSI
- Feedback de los clientes relacionado con la seguridad de la información
- Sugerencias del personal de la empresa respecto a temas de la seguridad de la información

4. Procedimiento

- Comprobación de que el personal conoce las normas de seguridad
- Realización de un informe por parte del responsable de seguridad

- Evaluación de las incidencias ocurridas, de las amenazas y de las vulnerabilidades
- Actualización de las políticas de seguridad y resto de documentación
- Actualización de los indicadores
- Revisión minuciosa de las auditorías.

5. Salidas

- Modificación de los procedimientos que así se hayan justificado
- Actualización de la evaluación del tratamiento de riesgos
- Inclusión de nuevos controles y modificación de los que lo requieran
- Mejora de la efectividad y eficacia del SGSI.