4	**La Organización y su Contexto**
4.1	**Entendiendo la Organización y su contexto**
1.-	¿Están identificados los objetivos del SGS Sistema de Gestión de la Seguridad de la Información?
2.-	¿Se han identificado las cuestiones internas y externas relacionadas con la Seguridad de la Información?
3.-	¿Se han identificado como las partes internas y externas pueden suponer amenazas o riesgos para la seguridad de la Información?
4.2	**Expectativas de las partes interesadas**
1.-	¿Se han identificado las partes interesadas?
2.-	¿Existe un listado de requisitos sobre Seguridad de la Información de las partes interesadas?
3.-	¿Existe un listado de requisitos sobre Seguridad de la Información referente a reglamentos, requisitos legales y requisitos contractuales?
4.3	**Alcance del SGSI**
1.-	¿Se ha determinado el alcance del SGS y se conserva información documentada?
4.4	**SGS Sistema de Gestión de la Seguridad de la información**
1.-	¿El sistema de Gestión de Seguridad de la información SGSI está establecido, implementado y se revisa de forma planificada considerando oportunidades de mejora?
5	**Liderazgo**
5.1	**Liderazgo y compromiso**
1.-	¿Se han establecido objetivos de la Seguridad de la Información acordes con los objetivos del negocio?
2.-	¿La dirección provee de los recursos materiales y humanos necesarios para el cumplimiento de los objetivos del SGSI?
3.-	¿La dirección revisa directamente la eficacia del SGSI para garantizar que se cumplen los objetivos del SGSI?
5.2	**Política de la Seguridad de la Información**
1.-	¿Se ha definido una Política de la Seguridad de la Información?
2.-	¿Se ha establecido un marco que permita el establecimiento de objetivos?
3.-	¿Se ha comunicado la política de la Seguridad de la información a las partes interesadas y a toda la empresa?
4.-	¿Se mantiene información documentada de la política del SGSI y de sus objetivos?
5.3	**Roles y Responsabilidades**

1.-	¿Se han asignado las responsabilidades y autoridades sobre la Seguridad de la Información?
2.-	¿Se han comunicado convenientemente las responsabilidades y autoridades para la Seguridad de la Información?
6	**Planificación**
6.1	**Tratamiento de Riesgos y Oportunidades**
1.-	¿El plan para abordar riesgos y oportunidades considera las expectativas de las partes interesadas en relación a la Seguridad de la Información?
2.-	¿Se identifican y analizan los riesgos mediante un método de evaluación y aceptación de riesgos?
3.-	¿Se ha definido un proceso de tratamiento de riesgos?
4.-	¿Se han establecido criterios para elaborar una declaración de aplicabilidad?
5.-	¿Se mantiene información documentada de los puntos anteriores?
6.2	**Planificación para consecución de objetivos**
1.-	¿Se han establecido objetivos de la Seguridad de la Información medibles y acordes a los objetivos del negocio?
2.-	¿Los objetivos de la Seguridad de la Información están planificados mediante? -Asignación de responsabilidades -Cronograma de ejecución temporal -Método de evaluación
3.-	¿Se han integrado los objetivos de la Seguridad de la Información en los procesos de la organización teniendo en cuenta las funciones principales dentro de la Organización?
7	**Soporte**
7.1	**Recursos**
1.-	¿Se identifican y asignan los recursos necesarios para el SGSI?
7.2	**Competencia**
1.-	¿Se evalúa la competencia en materias de Seguridad de la Información para personas que efectúan tareas que puedan afectar a la seguridad?
2.-	¿Se mantiene información actualizada sobre la competencia del personal?
7.3	**Concienciación**
1.-	¿El personal está involucrado y es consciente de su papel en la Seguridad de la Información?
2.-	¿Existe conciencia de los daños que se pueden producir de no seguir las pautas de la Seguridad de la Información?
7.4	**Comunicación**
1.-	¿Se comunica la política de la Seguridad de la Información con las responsabilidades de cada uno?

2.-	¿Existe un proceso para comunicar las deficiencias o malas prácticas en la seguridad de la Información?
7.5	**Información Documentada**
1.-	¿Se dispone de la documentación requerida por la norma más la requerida por la organización incluyendo? -La política de la Seguridad de la Información y el alcance del Sistema de Gestión -Los procesos principales de la seguridad de la Información -Los Documentos exigidos por la Norma ISO 27001 incluyendo registros -Los Documentos propios de Seguridad de la Información identificados por la empresa (instrucciones técnicas etc.)
2.-	¿Existe un control documental donde se verifica? -Quien publica el documento -Quien lo autoriza y como se revisan -Formatos y Soportes de publicación -Su almacenamiento y protección
3.-	¿Se controlan los documentos de origen externo?
8	**Operación**
8.1	**Control Operacional**
1.-	¿Los procesos de seguridad de la Información están documentados para controlar que se realizan según lo planificado?
2.-	¿Existe un proceso para evaluar los riesgos en la Seguridad de la Información antes de realizar cambios en el Sistema de Gestión o procesos de Seguridad?
3.-	¿Se establecen medidas y planes para mitigar los riesgos en la Seguridad de la Información ante cambios realizados?
4.-	¿Se identifican y controlan los procesos externalizados en cuanto a los riesgos para la Seguridad de la Información?
8.2	**Análisis de riesgos de la Seguridad de la Información**
1.-	¿Se ha establecido un proceso documentado de análisis y evaluación de riesgos para la Seguridad de la Información donde se identifique? -El propietario del riesgo -La importancia del riesgo o nivel de impacto -La probabilidad de ocurrencia
8.3	**Tratamiento de riesgos de la Seguridad de la Información**
1.-	¿Se ha implementado un plan de tratamiento de riesgos dónde? -Los propietarios del riesgo están informados y han aprobado el plan -Se documentan los resultados
2.-	¿Se identifican todos los controles necesarios para mitigar el riesgo justificando su aplicación?
3.-	¿Se documenta el nivel de aplicación de todos los controles a aplicar?

9	**Evaluación del desempeño**
9.1	**Seguimiento y medición**
1.-	¿Se ha establecido un proceso continuo de monitoreo de los aspectos clave de la seguridad de la información teniendo en cuenta los controles para la seguridad de la información?
2.-	¿Se ha establecido un proceso documentado para evaluar los resultados de las mediciones y de que estos resultados son tomados en cuenta por los responsables tanto de los procesos como de la Seguridad de la Información?
9.2	**Auditorías Internas**
1.-	¿Se ha establecido una programación de Auditorías Internas y asignado responsables?
2.-	¿Se ha definido el alcance y los requisitos para el informe de auditoría?
3.-	¿Se consideran acciones correctivas y propuestas de cambio en los informes de auditoría?
9.3	**Informe de Revisión por la Dirección**
1.-	¿Existe una programación para los informes de la dirección y existe constancia de su realización periódica?
2.-	¿Se documentan los resultados de los informes y la dirección se implica tanto en su conocimiento como en la toma de decisiones sobre los aspectos cruciales para el SGSI?
10	**Mejora**
10.1	**No Conformidades y acciones correctivas**
1.-	¿Existe un procedimiento documentado para identificar y registrar las no conformidades y su tratamiento?
2.-	¿Dentro de las acciones correctivas existe una diferenciación entre acciones correctivas sobre la no conformidad y sobre las causas de la misma?
10.2	**Mejora continua**
1.-	¿Existe un proceso para garantizar la mejora continua del SGSI identificando las oportunidades de mejora?