|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **REQUISITO**  **ISO** | **CICLO**  **PROCESO** | **VARIABLE** | **ESTADO**  **ACTUAL** | **CALIFICACIÓN** |
| 4.2.1 | Planear | **ESTABLECIMIENTO Y GESTION SGSI** | | |
| 4.2.1.a | Planear | **ALCANCE Y LIMITES DEL SGSI** | | |
| 4.2.1.a | Planear | ¿Están definidas las características del negocio? |  |  |
| 4.2.1.a | Planear | ¿Están definidos los Objetivos y necesidades de la Organización? |  |  |
| 4.2.1.a | Planear | ¿Está definida la Estructura y recursos en la Organización para implantar SGSI? |  |  |
| 4.2.1.a | Planear | ¿Se han seleccionado las áreas/procesos a involucrar en el SGSI? |  |  |
| 4.2.1.a | Planear | ¿Están definidos los requisitos y expectativas de seguridad? |  |  |
| 4.2.1.a | Planear | ¿Están definidas las actividades, sedes físicas, tecnología a incluir/excluir en el SGSI? |  |  |
| 4.2.1.a | Planear | ¿Se han seleccionado las áreas/procesos a involucrar en el SGSI? |  |  |
| 4.2.1.a | Planear | ¿Están definidos los requisitos y expectativas de seguridad? |  |  |
| 4.2.1.a | Planear | ¿Están definidas las actividades, sedes físicas, tecnología a incluir/excluir en el SGSI? |  |  |
| 4.2.1.a | Planear | ¿Se han estimado los recursos humanos, técnicos y económicos para implantar SGSI? |  |  |
| 4.2.1.a | Planear | ¿Existe un Documento Alcance y Límites SGSI? |  |  |
| 4.2.1.b | Planear | **POLITICA DE SEGURIDAD** | | |
| 4.2.1.b | Planear | ¿Se ha definido una política de seguridad y objetivos globales? |  |  |
| 4.2.1.b | Planear | ¿Existe declaración de la Dirección para el apoyo de objetivos y principios de seguridad? |  |  |
| 4.2.1.b | Planear | ¿Existe una definición de responsabilidades generales y especificas en cada rol? |  |  |
| 4.2.1.b | Planear | ¿Están definidos los activos que se protegen, de quién/qué y por qué? |  |  |
| 4.2.1.b | Planear | ¿Se han establecido los criterios para gestión de riesgos y selección de objetivos de control y controles? |  |  |
| 4.2.1.b | Planear | ¿Se han seleccionado las medidas de seguridad a implementar? |  |  |
| 4.2.1.b | Planear | ¿Se han establecido los criterios de actuación ante incidentes de seguridad? |  |  |
| 4.2.1.b | Planear | ¿Se han establecido los procesos de revisión periódica, ante incidentes de seguridad o ante cambios estructurales en la organización? |  |  |
| 4.2.1.b | Planear | ¿Se ha publicado y aprobado por parte de la Dirección? |  |  |
| 4.2.1.b | Planear | ¿Está disponible para consulta? |  |  |
| 4.2.1.b | Planear | ¿Existe Documento Política de Seguridad? |  |  |
| 4.2.1.a | Planear | **ORGANIZACIÓN DE LA SEGURIDAD** | | |
| 4.2.1.a | Planear | ¿Se ha seleccionado al responsable de la seguridad? |  |  |
| 4.2.1.a | Planear | ¿Se ha nombrado al Comité de Dirección? |  |  |
| 4.2.1.a | Planear | ¿Se ha nombrado al Comité de Gestión? |  |  |
| 4.2.1.a | Planear | ¿Se han tomado medidas frente a terceros para proteger la información? |  |  |
| 4.2.1.a | Planear | ¿Existe Documento Organización de la Seguridad? |  |  |
| 4.2.1.a | Planear | **SENSIBILIZACION Y FORMACION DEL PERSONAL** | | |
| 4.2.1.a | Planear | ¿Existe una campaña para divulgar los avances del SGSI en toda la organización? |  |  |
| 4.2.1.a | Planear | ¿Se ha capacitado al personal encargado de la SGSI para enfrentar sus nuevas actividades? |  |  |
| 4.2.1.a | Planear | ¿Existe Documento sensibilización y formación del personal? |  |  |
| 4.2.1.d | Planear | **IDENTIFICACION DE ACTIVOS** | | |
| 4.2.1.d | Planear | ¿Se ha definido alguna metodología para identificar activos? |  |  |
| 4.2.1.d | Planear | ¿Existe inventario de activos (descripción-localización-propietario-grado de seguridad)? |  |  |
| 4.2.1.d | Planear | ¿Están incluidos los activos intangibles (Imagen Organizacional)? |  |  |
| 4.2.1.d | Planear | ¿Se ha determinado el ciclo de vida útil de los activos? |  |  |
| 4.2.1.d | Planear | ¿Existe análisis o árbol de dependencia entre activos? |  |  |
| 4.2.1.d | Planear | ¿Existe Documento Inventario de activos? |  |  |
| 4.2.1.d | Planear | **VALORACION DE ACTIVOS** | | |
| 4.2.1.d | Planear | ¿Existe valoración de activos según la importancia e impacto ante una incidencia basado en CID (cuantitativa y/o cualitativa)? |  |  |
| 4.2.1.d | Planear | ¿Qué Método es empleado para valorar activos (entrevista, encuesta)? |  |  |
| 4.2.1.d | Planear | ¿Existe Documento valoración de activos? |  |  |
| 4.2.1.d | Planear | **IDENTIFICACION DE RIESGOS** | | |
| 4.2.1.d | Planear | ¿Se ha identificado áreas que requieren medidas de seguridad? |  |  |
| 4.2.1.d | Planear | ¿Existe identificación de riesgos y están asociados a los activos inventariados? |  |  |
| 4.2.1.d | Planear | ¿Existe identificación de riesgos asociados a los activos más críticos? |  |  |
| 4.2.1.d | Planear | ¿Hay Amenazas identificadas que afectan los activos inventariados? |  |  |
| 4.2.1.d | Planear | ¿Existe Análisis de vulnerabilidades de los activos inventariados? |  |  |
| 4.2.1.d | Planear | ¿Se conoce el impacto por la ocurrencia de un riesgo? |  |  |
| 4.2.1.d | Planear | ¿Se ha determinado la probabilidad de ocurrencia de un riesgo? |  |  |
| 4.2.1.d | Planear | ¿Este proceso considera los recursos de la organización? |  |  |
| 4.2.1.d | Planear | ¿Existe Análisis de medidas de seguridad ya implantadas? |  |  |
| 4.2.1.d | Planear | ¿Hay Participación de las diversas áreas de la compañía? |  |  |
| 4.2.1.d | Planear | ¿Existe Documento identificación de riesgos? |  |  |
| 4.2.1.c | Planear | **ENFOQUE PARA VALORACION DE RIESGOS** | | |
| 4.2.1.c | Planear | ¿Se ha definido alguna metodología para valorar riesgos? |  |  |
| 4.2.1.c | Planear | ¿Se han estimado los niveles para los riesgos? |  |  |
| 4.2.1.c | Planear | ¿Existe un Documento enfoque para valorar riesgos? |  |  |
| 4.2.1.f | Planear | **GESTION DEL RIESGO** | | |
| 4.2.1.f | Planear | ¿Se han definido acciones frente a los riesgos identificados y valorados? |  |  |
| 4.2.1.f | Planear | ¿Se ha determinado el riesgo residual para cada riesgo identificado y valorado? |  |  |
| 4.2.1.c,e | Planear | ¿Existen criterios definidos para tomar riesgo aceptable? |  |  |
| 4.2.1.f | Planear | ¿Hay Aprobación por dirección para los riesgos aceptable? |  |  |
| 4.2.1.f | Planear | ¿Existe Documento de Aprobación Dirección Gestión de Riesgos? |  |  |
| 4.2.1.h | Planear | ¿Existe Documento de Aprobación Dirección Riesgos residuales? |  |  |
| 4.2.1.f | Planear | ¿Existe Documento matriz de riesgos? |  |  |
| 4.2.1.g | Planear | **SELECCIÓN DE OBJETIVOS DE CONTROL Y CONTROLES** | | |
| 4.2.1.g | Planear | ¿Existe Análisis de controles existentes? |  |  |
| 4.2.1.g | Planear | ¿Existe Análisis y selección de los dominios, objetivos y controles a implantar? |  |  |
| 4.2.1.g | Planear | ¿Se Cumplen los requisitos definidos en procesos de tratamiento de riesgos? |  |  |
| 4.2.1.g | Planear | ¿Se hacen Inversiones en controles proporcionales al impacto del riesgo? |  |  |
| 4.2.1.g | Planear | ¿Existen Controles documentados en procedimientos? |  |  |
| 4.2.1.g | Planear | ¿Hay disponibilidad de recursos para implementar los controles? |  |  |
| 4.2.1.g | Planear | ¿Existe justificación para los objetivos y controles seleccionados y no seleccionados? |  |  |
| 4.2.1.j | Planear | ¿Existe Documento declaración de aplicabilidad? |  |  |
| 4.2.1.i | Planear | **AUTORIZACION PARA IMPLEMENTAR Y OPERAR SGSI** | | |
| 4.2.1.i | Planear | ¿Existe Documento de aprobación por dirección para implementar y operar el SGSI? |  |  |
| 4.2.1 | Planear | **GESTION DE LA CONTINUIDAD DEL NEGOCIO (PCN)** | | |
| 4.2.1 | Planear | ¿Están identificados los procesos críticos a recuperar progresivamente? |  |  |
| 4.2.1 | Planear | ¿Existe PCN extraído de gestión de riesgos críticos? |  |  |
| 4.2.1 | Planear | ¿Se ha puesto a prueba el PCN (cuánto es el tiempo de recuperación mínimo, los ANS se conservan)? |  |  |
| 4.2.1 | Planear | ¿Existe comité de emergencia para solucionar las crisis? |  |  |
| 4.2.1 | Planear | ¿Existen procedimientos (relacionados a cada situación) establecidos para aplicar en las crisis (indica acciones y sugerencias)? |  |  |
| 4.2.1 | Planear | ¿Los procedimientos han sido divulgados y puestos a prueba? |  |  |
| 4.2.1 | Planear | ¿Existen registros que documentan la reacción ante la crisis y su respectivo análisis? |  |  |
| 4.2.1 | Planear | Fases PCN: Definición del proyecto (alcance y objetivos de peor escenario)  -Análisis de impacto (riesgos, impacto económico)  -Selección de estrategias (recursos-salvaguardas a usar)  - Desarrollo  -Pruebas periódicas y mantenimiento |  |  |
| 4.2.2 | Hacer | **IMPLEMENTACION Y OPERACIÓN SGSI** | | |
| 4.2.2.a,b | Hacer | **PLAN DE TRATAMIENTO DE RIESGOS** | | |
| 4.2.2.a,b | Hacer | ¿Existe guía de ejecución del plan para tratamiento de riesgos? |  |  |
| 4.2.2.h | Hacer | ¿Se han definido Procedimientos y controles adicionales para detectar y reaccionar ante incidentes de seguridad en esta fase? |  |  |
| 4.2.2.a,b | Hacer | ¿Existe documento informe de plan para tratamiento de riesgos? |  |  |
| 4.2.2.c | Hacer | **IMPLANTACION DE CONTROLES** | | |
| 4.2.2.c | Hacer | ¿Se han definido los responsables de los controles técnicos? |  |  |
| 4.2.2.c | Hacer | ¿Se han definido los responsables de los controles administrativos? |  |  |
| 4.2.2.d | Hacer | ¿Se han definido los indicadores para cada control implantado? |  |  |
| 4.2.2.d | Hacer | ¿Existe un método para medir la eficacia de los controles implantados? |  |  |
| 4.2.2.h | Hacer | ¿Se han implantado controles adicionales ante incidentes de seguridad detectados en esta fase? |  |  |
| 4.2.2.e | Hacer | ¿Se ha hecho sensibilización y divulgación? |  |  |
| 4.2.2.c | Hacer + Dominios  1-15 | ¿Existen los procedimientos de los controles del anexo A, correspondientes a 133 controles? |  |  |
| 4.2.3 | Verificar | **SEGUIMIENTO Y REVISION SGSI** | | |
| 4.2.3 | Verificar | **PROCEDIMIENTOS SEGUMIENTO Y REVISION** | | |
| 4.2.3.a,c | Verificar | ¿Se hace un análisis periódico de indicadores y su eficacia? |  |  |
| 4.2.3.b,e | Verificar | ¿Se realizan auditorías internas/externas al sistema? |  |  |
| 4.2.3.b,e | Verificar | ¿Se hace revisión por Dirección de las auditorias? |  |  |
| 4.2.3.a | Verificar | ¿Se hace revisión por Dirección del informe Comité de Gestión? |  |  |
| 4.2.3.a | Verificar | ¿Se hace revisión por Dirección del informe Responsable Seguridad? |  |  |
| 4.2.3.d | Verificar | ¿Se hace revisión periódica por Dirección de valoración de riesgos, riesgo residual, riesgo aceptable? |  |  |
| 4.2.3.b,e | Verificar | ¿Existe un documento auditorías internas? |  |  |
| 4.2.3.a,b, c,d,e | Verificar | ¿Existe un documento de revisión por dirección? |  |  |
| 4.2.4 | Actuar | **MANTENIMIENTO Y MEJORA SGSI** | | |
| 4.2.4.a,b | Actuar | ¿Se ejecutan acciones correctivas, preventivas, mejora? |  |  |
| 4.2.4.a,b | Actuar | ¿Se hace la actualización de riesgos y controles? |  |  |
| 4.2.4.d | Actuar | ¿Se hace la medición de eficacia de acciones implementadas? |  |  |
| 4.2.4.c | Actuar | ¿Existe un documento informe de ejecución de acciones correctivas-preventivas? |  |  |