Anexo C – Gestión de Indicadores

1. Alcance

El alcance de la gestión de los indicadores para Ícaro S.A.se divide en dos partes:

- Gestión de los indicadores de los controles de seguridad de la ISO/IEC 27002:2013 que aplique su revisión y que necesitan de indicadores para comprobar la aplicación de estas revisiones/comprobaciones.

- Gestión de los indicadores de los objetivos marcados por la dirección de la empresa respecto a la implantación del SGSI.

2. Gestión de indicadores de los controles de seguridad

En la siguiente tabla se muestran los indicadores implementados a realizar para revisar los diferentes controles que aplican de los dominios de la ISO/IEC 27002.

5. Políticas de seguridad de la información					
ID	**Indicador**	**Fórmula de medición**	**Valor objetivo /umbral**	**Frecuencia**	**Control**
IC1	Nº de revisiones de la política de seguridad por parte de la dirección	Revisiones/año	3/1	Anual	5.1.2
6. Organización de la seguridad de la información					
IC2	Verificar si los roles y responsabilidades relativos a seguridad de la información están definidos	(Nº tareas seguridad con responsable / Nº tareas seguridad totales) *100	100% / 80%	Anual	6.1.1
IC3	Revisión de la seguridad en los proyectos	(Nº de proyectos revisados / Total proyectos) * 100	100% / 80%	Semestral	6.1.5
IC4	Revisión de política de teletrabajo	(Nº de proyectos revisados / Total proyectos) * 100	100% / 80%	Anual	6.2.2
7. Seguridad relativa a los recursos humanos					
IC5	Revisiones de antecedentes de nuevo personal contratado	(Nº de revisados / Total nuevos contratados) * 100	100% / 80%	Anual	7.1.1.
IC6	Satisfacción de los cursos de formación relativos a seguridad	(Total valoración cursos) * 10 /Encuestas	90/70	Anual	7.2.2

8. Gestión de activos					
ID	**Indicador**	**Fórmula de medición**	**Valor objetivo /umbral**	**Frecuencia**	**Control**
IC7	Porcentaje del control de activos	(Nº de activos inventariados) / (Total de activos) * 100	100% / 90%	Anual	8.1.1
IC8	Porcentaje de la devolución de los activos	(Nº de activos devueltos) / (Nº de activos que debían devolverse) * 100	100% / 95%	Anual	8.1.4
IC9	Porcentaje de eliminación correcta de soportes	(Nº de soportes eliminados) / (Nº de soportes que debían eliminarse) * 100	100% / 95%	Anual	8.3.2
9. Control de Acceso					
IC10	Porcentaje de accesos no autorizados a la red de la empresa	(Nº de accesos no autorizados) / (Nº total de accesos) * 100	0% / 5%	Mensual	9.1.2
IC11	Eficacia del control de privilegios de empleados	(Nº de empleado con roles correcto) / (Nº total de empleados) *100	100% / 95%	Semestral	9.2.1 9.2.2 9.2.3 9.2.5 9.2.6
IC12	Porcentaje de empleados con privilegios de administrador	((Nº de empleado con privilegios) / (Nº total de empleados) *100)	5% / 10%	Anual	9.4.4
10. Criptografía					
IC13	Eficacia de la política de encriptación de datos sensibles	(Nº de sistemas encriptados) / (Nº de sistemas sensibles) * 100	100% / 95%	Semestral	10.1.1
IC14	Porcentaje de claves de sistemas iguales	(Nº de claves iguales) / (Nº Total de claves) * 100	0% / 5%	Anual	10.1.2
11. Seguridad física y del entorno					
IC15	Eficacia de las medidas de seguridad físicas	(Nº de intrusiones evitadas) / (Nº total de intrusiones) * 100	100% / 95%	Anual	11.1.2 11.1.3
IC16	Revisión de los sistemas contra incendios	(Nº de revisiones) / (Nº objetivo de revisiones) * 100	100% / 95%	Anual	11.1.4
IC17	Revisión de sistemas críticos fuera de áreas seguras	(Nº de sistemas críticos fuera áreas seguras) / (Total sistemas críticos)	0% / 5%	Mensual	11.2.1

11. Seguridad física y del entorno					
ID	**Indicador**	**Fórmula de medición**	**Valor objetivo /umbral**	**Frecuencia**	**Control**
IC18	Eficacia del sistema de suministro continuo de electricidad del CPD	(Nº de equipos que sufren apagado) / (Total de los equipos) * 100	0% / 5%	Anual	11.2.2
IC19	Eficacia del ciclo de parcheado de los sistemas	(Nº de sistemas con último parche) / (Nº total de sistemas) * 100	100% / 95%	Semestral	11.2.4 12.5.1
12. Seguridad de las operaciones					
IC20	Sistemas fuera de su zona de red	(Nº de sistemas fuera de su zona de red) / (Nº de sistemas) * 100	0% / 2%	Mensual	12.1.4 13.1.3
IC21	Sistemas sin antivirus que lo precisen	(Nº de sistemas sin antivirus) / (Nº de sistemas que precisan antivirus) * 100	0% / 2%	Mensual	12.2.1
IC22	Eficacia del antivirus corporativo	(Nº de amenazas detectadas) / (Nº de amenazas) * 100	100% / 98%	Trimestral	12.2.1
IC23	Eficacia del sistema de backup de sistema Sirio	(Nº de backup satisfactorios) / (Número de Backup) * 100	100% / 95%	Mensual	12.3.1
IC24	Accesos no autorizados a los registros del sistema Sirio	(Nº de accesos no autorizados) / (Total de accesos) * 100	0% / 2%	Mensual	12.4.2
IC25	Snapshot disponibles en el tiempo de las MV del sistema sirio	Nº Snapshot / MV	4/2	Semanal	12.5.1
IC26	Eficacia del sistema de control de vulnerabilidades	(Vulnerabilidades convertidas en amenazas) / (Nº de vulnerabilidades) * 100	0% / 1%	Semestral	12.6.1
IC27	Instalación de software no permitido en equipos de empleados	(Equipos con software compliance) / (Nº de equipos) * 100	100% / 95%	Anual	12.6.2
IC28	Cumplimiento de calendario de auditorías internas de sistemas	(Auditoría realizadas) / (Auditorías planificadas) * 100	100% / 95%	Anual	12.7.1 18.2.1
13. Seguridad de las comunicaciones					

13. Seguridad de las comunicaciones					
ID	**Indicador**	**Fórmula de medición**	**Valor objetivo /umbral**	**Frecuencia**	**Control**
IC29	Eficacia de los equipos de seguridad de red	(Nº de acceso a la red no permitidos) / (Nº de accesos) * 100	0% / 2%	Mensual	13.1.2
IC30	Cumplimiento de los acuerdos de intercambio de información	Nº de filtraciones	0 / 2	Anual	13.2.2 13.2.4
14. Adquisición, desarrollo y mantenimiento de los sistemas de información					
IC31	Eficacia de los test de seguridad de software	(Nº de aplicaciones liberadas sin fallos de seguridad / (Aplicaciones liberadas) * 100	100% / 98%	Anual	14.2.1 14.2.8 14.2.9
IC32	Cumplimiento del control de cambios en entornos de desarrollo	(Cambios registrados) / (Nº de cambios) * 100	100% / 98%	Trimestral	14.2.2
IC33	Cumplimiento de comprobación de los sistemas tras parcheado en Sirio	(Sistemas comprobados) / (Sistemas parcheados) * 100	100% / 95%	Semestral	14.2.3
15. Relación con proveedores					
IC34	Acceso a los sistemas del sistema Sirio por personal subcontratado	Nº de accesos sin autorización	0/1	Mensual	15.1.2
IC35	Cumplimiento sistemas de seguridad en el entorno de desarrollo contratado a un proveedor externo	Nº de intrusiones	0/1	Anual	15.1.3
IC36	Indisponibilidad del entorno de desarrollo contratado a un proveedor externo	Veces de indisponibilidad del servicio	1/3	Anual	15.2.1
16. Gestión de incidentes de seguridad de la información					
IC37	Nº de notificación de debilidades	Nº de notificaciones de debilidades	0/1	Mensual	16.1.2 16.1.3
IC38	Eficacia de sistema de respuesta a incidentes	(Nº de incidentes resueltos <= 4h) / (Nº de incidentes) *100	100% / 95%	Anual	16.1.5

17. Seguridad física y del entorno					
ID	**Indicador**	**Fórmula de medición**	**Valor objetivo /umbral**	**Frecuencia**	**Control**
IC39	Operatividad de los procesos que forman parte del plan de continuidad de negocio	(Nº de procesos que funcionan correctamente) / (Nº de procesos) * 100	100% / 95%	Anual	17.1.2
IC40	Porcentaje de sistemas críticos redundados	(Nº de sistemas críticos redundados) / (Nº de sistemas críticos) * 100	100% / 95%	Anual	17.2.1
18. Cumplimiento					
IC41	Fallos en cumplimiento legislativo	(Nº Incumplimientos de obligaciones legales) / (Nº de obligaciones legales)	0% / 5%	Anual	18.1.1
IC42	Perdida de registros de los sistemas	(Nº de registros perdidos) / (Nº de registros totales)	0% / 5%	Trimestral	18.1.3
IC43	Verificación de ejecución de auditorias	(Nº de auditorías realizadas) / (Nº de auditorías planeadas) *100	100% / 80%	Anual	18.2.1
IC44	Revisión independiente de la seguridad de la información	Nº de revisiones año	100%/90%	Anual	18.2.1
IC45	Cumplimiento de las políticas de seguridad	Nº de infracciones	0/5	Anual	18.2.2

3. Gestión de los indicadores de los objetivos marcados por la dirección de la empresa respecto al SGSI

ID	Indicador	Fórmula de medición	Valor objetivo /umbral	Frecuencia
IO1	Incremento del número de clientes	(Nuevos clientes) / (Clientes año anterior) * 100	20% / 10%	Anual
IO2	Resultado encuesta satisfacción clientes	(Suma resultado encuesta clientes) / (Nº de clientes encuestados) * 10	90/70	Anual
IO3	Costes derivados de incidentes de seguridad	Costes en €	<1000€ / 6000€	Anual
IO4	Incremento de beneficios	(Beneficios año actuales) / (Beneficios año anterior) *100	6% / 3%	Anual