ISO 27001

Estrategia, Cumplimiento y Resiliencia Organizacional

Institut de Física Corpuscular (IFIC)

Presentación para el Comité de Artemisa. 19 de Junio del 2026

Auditoría: 07 y 08 de Julio

1. DEFINICIÓN DEL CONCEPTO

Marco Global de Seguridad

La norma **ISO 27001** establece los requisitos para el Sistema de Gestión de Seguridad de la Información (SGSI). No es un proyecto técnico, sino un **proceso de gestión estratégico**.

La Tríada de la Seguridad

Confidencialidad: Solo acceso autorizado.

Integridad: Datos exactos y sin alteraciones.

Disponibilidad: Acceso cuando se requiera.

2. ELEMENTOS CLAVE

Mejora Continua

Uso del ciclo PDCA (Planificar, Hacer, Verificar, Actuar) para la evolución del sistema.

Controles Anexo A

Conjunto de 93 controles específicos (Organizativos, Personas, Físicos y Tecnológicos).

Liderazgo

Compromiso obligatorio de la Alta Dirección en la aprobación y recursos del SGSI.

3. POLÍTICA DE SEGURIDAD

Es el **documento maestro** que define la dirección y el compromiso del IFIC con la protección de sus activos científicos y datos.

- Declara los principios de seguridad.
- Define el marco para objetivos SMART.
- Es comunicada a todo el personal y usuarios dentro del alcance de Artemisa.

5. OBJETIVOS DE SEGURIDAD

IFIC INSTITUT DE FÍSICA CORPUSCULAR

Disponibilidad

Garantizar un tiempo de actividad del 99.9% en servicios de cálculo crítico.

Cultura

Formar al 100% de la plantilla en buenas prácticas de ciberseguridad anual.

Resiliencia

Reducir el tiempo de respuesta ante incidentes críticos en un 25%.

"Lo que no se puede medir, no se puede mejorar."

5. OBJETIVOS DE SEGURIDAD 2026

- Mantenimiento de la certificación de la ISO 27001
- Mejora de la infraestructura tecnológica de la organización
- Mejora de plataforma de inteligencia de amenazas.

6. ANÁLISIS DE RIESGOS

INSTITUT DE FÍSICA CORPUSCULAR

Metodología

Evaluamos amenazas sobre nuestros activos críticos para determinar su nivel de riesgo:

$$\text{Riesgo} = \text{Probabilidad} \times \text{Impacto}$$

Aceptación

Dirección decide el nivel de riesgo residual aceptable tras aplicar controles.

Likelihood						
Almost Certain (>1 in 10)	5	Medium 5	High 10	Extreme 15	Catastrophic 20	Catastrophic 25
Likely (1 in 20)	4	Low 4	Medium 8	High 12	Extreme 16	Catastrophic 20
Occasional (1 in 200)	3	Low 3	Medium 6	High 9	High 12	Extreme 15
Unlikely (1 in 2000)	2	Very Low 2	Low 4	Medium 6	Medium 8	High 10
Rare (<1 in 10000)	1	Very Low 1	Very Low 2	Low 3	Low 4	Medium 5

#	Failure Mode	CAUSE of Failure	LIKELIHOOD	EFFECT of Failure	IMPACT	RISK SCORE
1	Motor overheating	Overuse or poor ventilation	2	Motor failure, bike stops functioning	4	8
2	Battery overcharge	Faulty charging system	2	Battery explosion or failure	5	10
3	Brake pad wear	Normal wear and tear	5	Reduced stopping ability, increased stopping distance	4	20
4	Frame crack	Poor material quality or stress points	2	Structural failure, rider injury	5	10
5	Low battery capacity	Poor battery quality or aging	4	Shorter ride distance	3	12
6	Display malfunction	Faulty wiring or water ingress	3	Loss of speed and battery status information	2	6
7	Sensor failure	Sensor damage or wiring issues	2	Pedal assist stops working, reducing ease of riding	3	6
8	Gets muddy	Rides in mud	1	Becomes unpleasant to look at	1	1
9						-
10						-
11						-
12						-
13						-
14						-

7. REVISIÓN POR DIRECCIÓN

Entradas (Inputs)

Resultados de auditorías internas/externas.

Estado de los objetivos de seguridad.

Desempeño de los procesos de seguridad.

Retroalimentación de partes interesadas.

Salidas (Outputs)

- Decisiones sobre mejora continua.
- Aprobación de cambios en el SGSI.
- Necesidades de recursos y presupuesto.
- Aprobación del Análisis de Riesgos.

¿Preguntas?

Hacia un IFIC más seguro y resiliente.

---

www.ific.uv.es

Responsable de Seguridad de la Información