Binter

Implantación Part-IS

Caminando juntos

Público

Volamos por ti

Binter

Contexto y situación de partida

Volamos por ti

17
empresas

36
años de trayectoria

250
vuelos cada día

42
aviones en nuestra flota

+2.600
personas en el equipo

https://www.bintercanarias.com/es/corporativo/sistema-binter

Binter

Operadores

Mantenimiento

Producción

Diseño

Handling

Tecnología

Formación

Servicios generales

https://www.bintercanarias.com/es/corporativo/sistema-binter

Binter

SGSI con una elevada madurez. 10 años “de maduración”. Certificado ISO 27001 en 2015.

Certificación en el Esquema Nacional de Seguridad en el año 2020 en categoría media y en 2024 en categoría alta.

Las organizaciones dentro del alcance de nuestro SGSI **compartimos** **estructuras organizativas**, **políticas**, **procesos**, **procedimientos de seguridad de la información** e **infraestructuras** tecnológicas.

La responsabilidad sobre las TIC y la seguridad de la información, recae sobre el equipo de Atlantis Tecnología.

Hay una **gestión única y homogénea** de la seguridad de la información.

Hay **un único responsable de seguridad de la información** para todas las empresas.

El SGSI ha evolucionado con el Sistema Binter y siempre según el principio de mejora continua.

SGSI adaptado para el cumplimiento de **múltiples requisitos** (27001, NIS, ENS, AVSEC) y ahora Part-IS.

Múltiples organizaciones con múltiples aprobaciones que comparten SGSI. Dos autoridades.

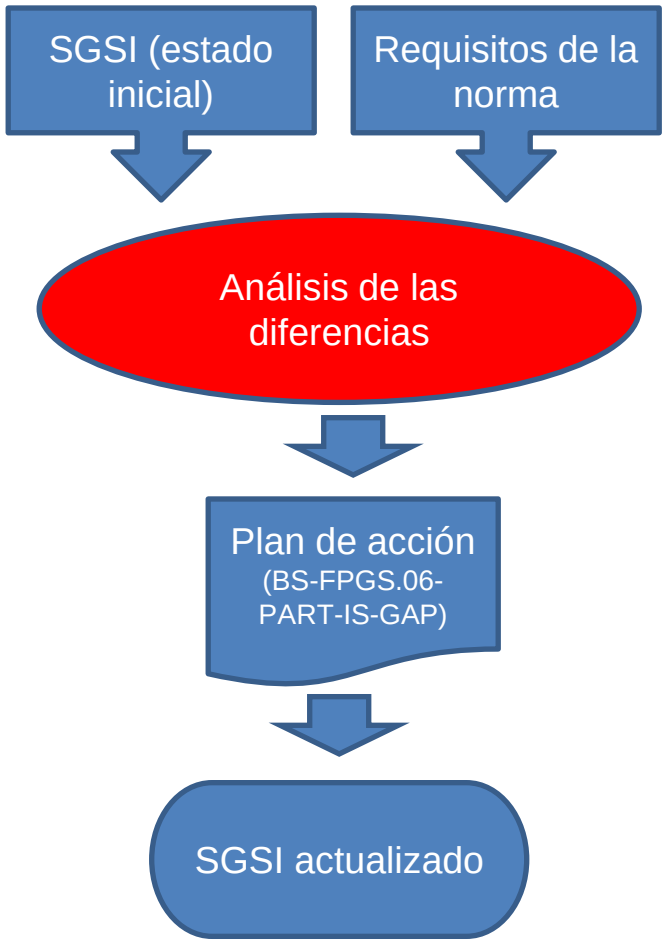
Binter

Binter

El camino

Volamos por ti

Primer paso: Análisis de Gap



- Se identificaron 17 acciones para adecuar el SGSI a Part-IS.
- Principal problema: nueva norma en proceso de “puesta en marcha”. Sin referencias. Sin ejemplos de aplicación. Sin criterios de aplicación totalmente definidos.

Proyecto Piloto con AESA

Iniciado en diciembre de 2024 y con final previsto inicialmente para abril o mayo del 2025 (aunque finalmente se cerró en septiembre 2025).

El proceso de implantación de cualquier norma nueva suele estar lleno de dudas e incertidumbres.

Permitió hacer parte del camino junto a la autoridad, **compartiendo dudas y aprendizajes**.

Fue un **catalizador importante** que nos permitió avanzar con mayor seguridad.

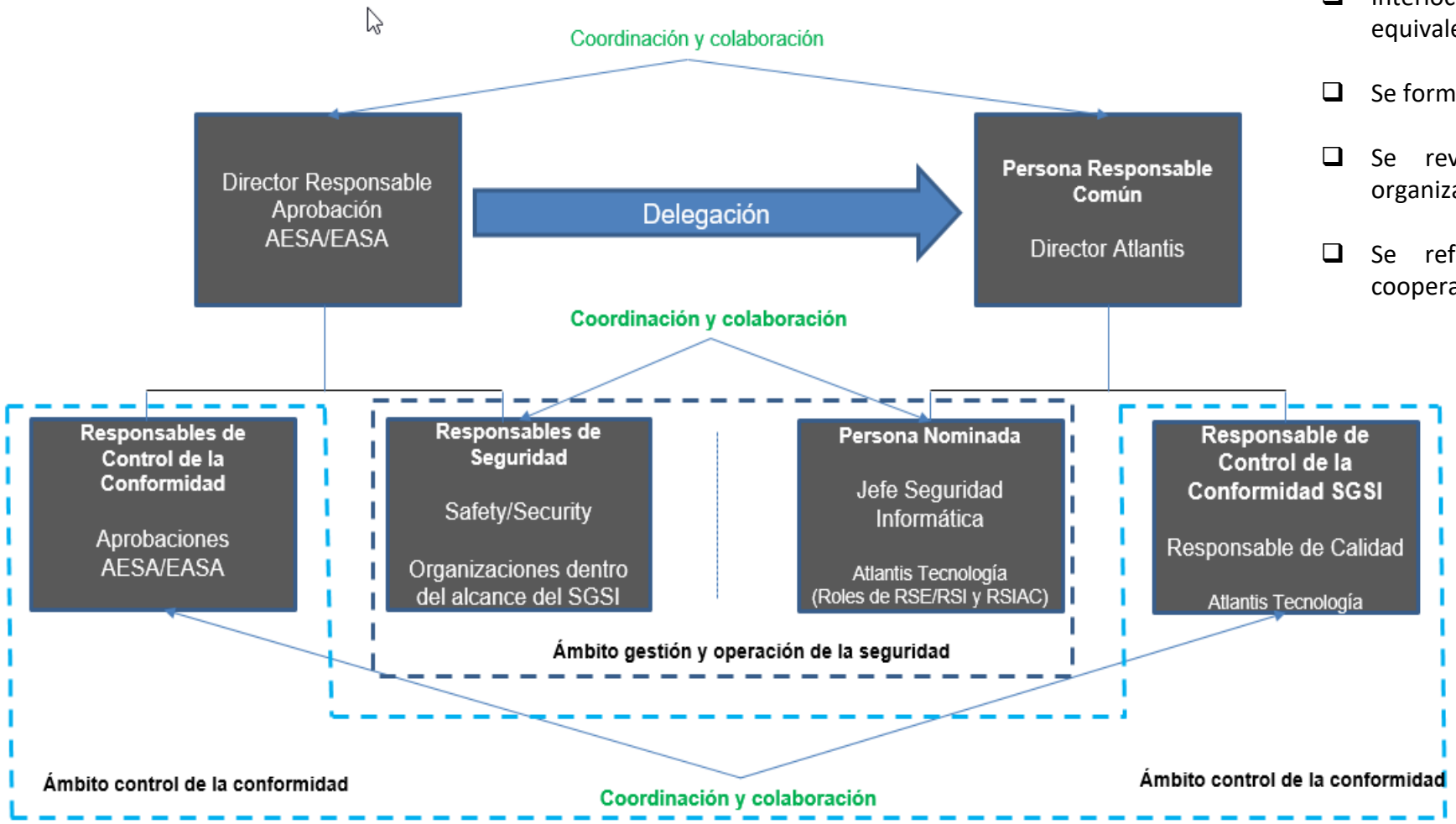
Permitió identificar **retos** y poner en común **conclusiones y lecciones aprendidas**.

Principales **hitos**:

1. **Estructura organizativa**: CRP, persona(s) nominada(s).
2. Adecuación del **alcance**.
3. Adecuación del **análisis de riesgos**
4. Modificación de la **gestión de cambios del SGSI** (ya implantada al ser requisito de la ISO/IEC 27001:2022)
5. Revisión y **adaptación de documentación** (procesos, procedimientos, …)
6. **Manual del SGSI**

Contexto: **Múltiples organizaciones**/aprobaciones con un **único SGSI. Dos autoridades: AESA y EASA** (DOA).

Estructura organizativa: CRP, persona(s) nominada(s)



- ❑ No se modifica la organización. La estructura ya existía.
- ❑ Interlocución, coordinación y colaboración entre niveles equivalentes de las organizaciones.
- ❑ Se formaliza la delegación entre DR y CRP.
- ❑ Se revisan y actualizan los contratos entre las organizaciones.
- ❑ Se refuerzan los mecanismos de coordinación y cooperación.

Adecuación del **alcance**.

1. Se modifica el alcance del SGSI (2024) y se incluyen en el certificado las empresas con aprobaciones.
2. Se identifican los activos que afectan a SAFETY (y a cada aprobación) al realizar el AR.
3. Se mejora la documentación.

SW-AIMS

FUENTES DE INFORMACIÓN

- [ ] [A-145] Parte 145
- [x] [A-AOC] AOC -Operador Aéreo
- [x] [A-ATO] ATO - Organización de Entrenamiento Aprobada
- [x] [A-CAMO] CAMO - Gestión de la aeronavegabilidad
- [ ] [A-DOA] DOA - Aprobación de Organización de Diseño
- [ ] [A-POA] POA - Aprobación de Organización de Producción
- [x] [C-OT] Operaciones Tierra/Handling
- [x] [C-OV] Operaciones de Vuelo
- [ ] [E-ATC] Aeronautical Training Canarias
- [ ] [E-AD] ADM Tech
- [ ] [E-ATAVIS] Atavis
- [x] [E-AH] Atlantica de Handling
- [ ] [E-AC] Atlantis Cargo
- [ ] [E-AT] Atlantis Tecnología y Sistemas
- [x] [E-NT] Binter Airlines
- [x] [E-BT] Binter Technic
- [x] [E-CA] Canair
- [x] [E-PM] Canaryfly
- [ ] [E-GA] GAIC
- [x] [E-IS] ISA
- [x] [E-NY] NAYSA
- [ ] [E-SA] SATI
- [x] [CAR-SAFETY] Puede afectar a la seguridad operacional (SAFETY)
- [ ] [CAR-SECURITY] Puede afectar a la seguridad aeroportuaria (SECURITY)
- [ ] [CAR-AGR] Agrupación
- [ ] [CAR-PROSEG] Problema de Seguridad

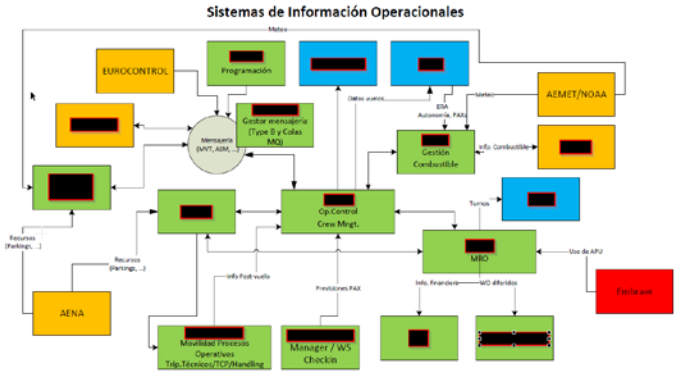
Fecha 07/11/2025	ATS-SG.SI-PRO.IANR-REG20251107 Registro de Activos por Fuente

Fuente de Información de Activos: Etiquetas utilizadas para describir características específicas de los activos, tales como su certificación, empresa respons
Referencia: Definición de Fuente según ATS-SG.SI-PRO.IANR-MAN Manual de Análisis de Riesgos

Codigo activo	Nombre Activo	Under	A-145	A-AOC	A-ATO	A-CAMO	A-DOA	A-POA
INFO	Información							
INFO-MRO	Información de mantenimiento	INFO						
INFO-MRO-TecPiezas	Información técnica de piezas	INFO-MRO	X				X	X
INFO-MRO-TecAeronaves	Información técnica de aeronaves	INFO-MRO	X	X	X	X	X	X
INFO-MRO-MtoPiezasAeronaves	Información mantenimiento de piezas aeronaves	INFO-MRO	X	X		X		
INFO-MRO-RegAeronaves	Registros de aeronaves	INFO-MRO	X	X		X		
INFO-MRO-BoletinesFabricante	Boletines de fabricantes (SB)	INFO-MRO	X	X		X		X
INFO-MRO-ICA	Instructions for Continuing Airworthiness	INFO-MRO	X	X		X	X	X
INFO-MRO-DIRAERO	Directivas de aeronavegabilidad	INFO-MRO	X	X		X		
INFO-MRO-TOOL	Información de herramientas	INFO-MRO	X					X
INFO-MRO-PRO	Documentación de procesos, procedimientos y prácticas recomendadas MRO	INFO-MRO	X					
INFO-MRO-REGTEC	Registro técnico de mantenimientos	INFO-MRO	X					
INFO-MRO-CRS	Certificado de Aptitud para el Servicio (CRS)	INFO-MRO	X			X		
INFO-AIR	Información aeronaves y vuelo	INFO						
INFO-AIR-PBN	Información sobre Procedimientos de Vuelo Basados en Prestaciones (PBN)	INFO-AIR			X	X		
INFO-AIR-PlanesVuelo	Planes de vuelos	INFO-AIR		X				
INFO-AIR-Meteo	Información meteorológica	INFO-AIR		X				
INFO-AIR-SistAvion	Datos de los sistemas a bordo	INFO-AIR	X	X		X		
INFO-AIR-Rutas	Información de rutas y destinos	INFO-AIR		X				

dispone de un sistema de gestión de seguridad de la información conforme con la Norma UNE-EN ISO/IEC 27001:2023

para las actividades: Los sistemas de información que sustentan los servicios gestionados de Datacenter y los servicios de diseño, gestión, despliegue y mantenimiento de infraestructuras de tecnologías de la información, redes y telecomunicaciones, ciberseguridad, computación en la nube, desarrollo de software, mantenimiento de aplicaciones, soporte, atención y asesoramiento a usuarios.
Los servicios de información que soportan servicios esenciales prestados por la organización o por sus clientes y los servicios que puedan repercutir sobre la seguridad aérea y aeroportuaria, incluyendo los de mantenimiento de aeronaves, gestión del mantenimiento de la aeronavegabilidad (CAMO), operadores aéreos, los de organizaciones de producción y organizaciones de diseño de aeronaves, piezas y componentes y los de organizaciones de instrucción reconocidas (ATO).
Todo ello de acuerdo a la declaración de aplicabilidad vigente en la fecha de la emisión del certificado.



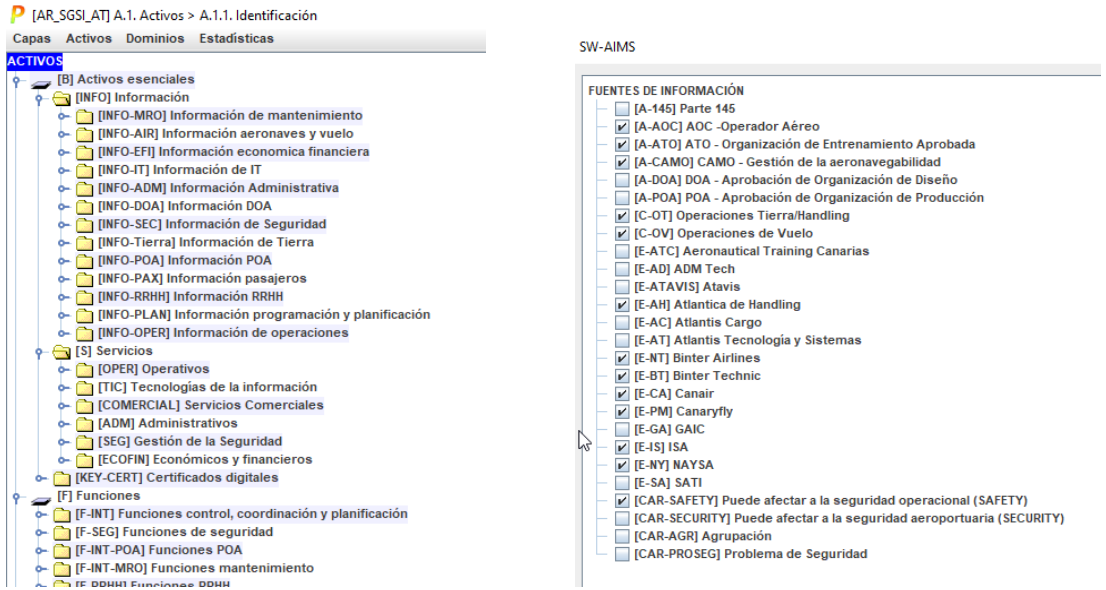
Binter

Adecuación del **análisis de riesgos**

- Metodología para el AR de seguridad de la información: **MAGERIT**

MAGERIT – versión 3.0
Metodología de Análisis y Gestión
de Riesgos de los Sistemas de Información

- Herramienta utilizada: **PILAR**
- Manual para realizar el análisis de riesgos utilizando PILAR en evolución y mejora continua.
- Uso de la funcionalidad denominada “Fuentes de información” de PILAR para “etiquetar los activos.
- Realimentación entre “Safety assessment” – “Information security assessment”



ICAO – DOC 10204 – Manual on Aviation Information Security

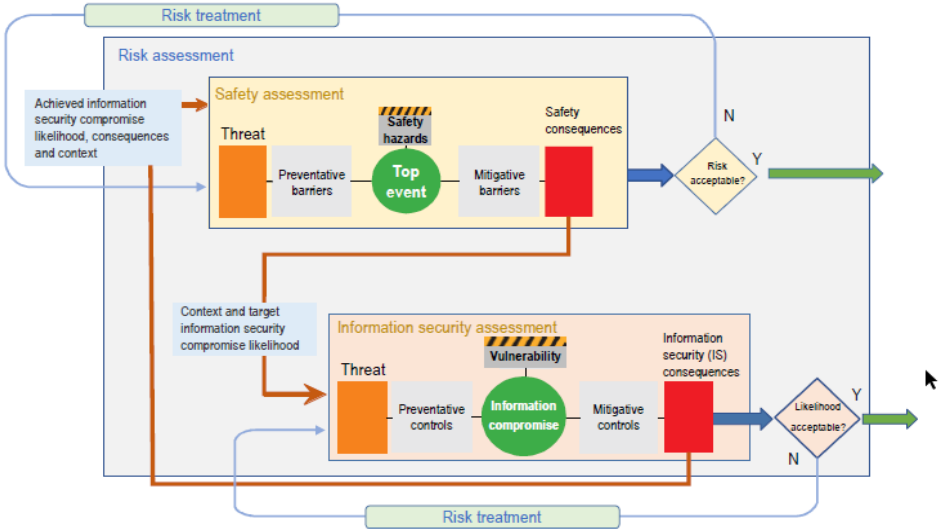


Figure 2-1. Information security risk assessment in the context of safety consequences

Binter

Revisión y **adaptación de documentación** (procesos, procedimientos, …) dentro del proceso de implantación de Part-IS y de la mejora continua.

Se revisaron múltiples documentos, entre otros:

- ❑ Política de Seguridad de la Información.
- ❑ Alcance y contexto del SGSI.
- ❑ Documento de roles y responsabilidades en seguridad de la información.
- ❑ Gestión de cambios del SGSI.
- ❑ Proceso de mejora continua.
- ❑ Gestión de incidentes de seguridad de la información.
- ❑ Gestión de vulnerabilidades.
- ❑ Proceso de seguimiento y evaluación.
- ❑ Manual del Análisis de Riesgos.

Manual del SGSI

Entradas: punto de partida del SGSI + requisitos de la norma (fundamentales las Easy Access Rules) + feedback y aprendizaje + manuales SG de las organizaciones dentro del alcance + piloto AESA + workshop/webminar/... autoridades.

Desarrollo: sucesivos borradores y feedback desde seguridad operacional, seguridad aeroportuaria, calidad y control de conformidad.

Apoyo importante: aprendizaje y el feedback recibido durante el proyecto piloto con AESA, los múltiples webinar y conferencias organizadas por AESA y EASA y las guías publicadas como la DSA-SG-P01-GU04 Guía del Manual del Sistema de Gestión de Seguridad de la Información.

Estructura: tras la publicación de la guía DSA-SG-P01-GU04 la modificamos para adaptarla a la misma en lo posible. La necesidad de considerar otras normas añadió complejidad.

Resultado: primera versión del manual (creemos que con un amplio margen de mejora todavía).

El manual no solamente pretende dar respuesta a los requisitos de Part-IS. Por la propia naturaleza del SGSI hemos **considerado** también los **requisitos** de la ISO **27001 y del resto de normativas** que nos resultan de aplicación.

Revisión control de conformidad

Finalidad: verificar que el sistema de gestión de seguridad de la información implementado cumple los requisitos de los **niveles "Present & Suitable"** (según "Guidelines Part-IS oversight approach - Guidelines for Competent Authorities for the conduct of oversight activities of organisations implementing Part-IS").

Revisión basada en la norma y en la tabla 2 de la guía ("Elements to be assessed for "Present" and "Suitable" levels (including readiness to start operating the ISMS").

Revisión inicial realizada por la responsable de control de conformidad del SGSI (Atlantis).

Pre-AUDITORÍA INTERNA DE CALIDAD realizada por el equipo de calidad y control de conformidad de ADMtech (POA, DOA).

Estado actual

Presentada documentación ante AESA (POA) y EASA (DOA).

Solicitud presentada ante AESA:

- ❑ Solicitud de cambio.
- ❑ POE
- ❑ Manual SGSI.
- ❑ Documentación referenciada en el manual del SGSI.
- ❑ Procedimiento gestión de cambios del SGSI.
- ❑ Evaluación inicial de control de la conformidad.

Actualmente en espera de respuesta.

Binter

Conclusiones

Volamos por ti

Nuestras conclusiones:

- La **buena disposición de la autoridad** (AESA y EASA), su cercanía y sus aportaciones en forma de guías, webminar y conferencias han facilitado el proceso.

- La guía **Part-IS TF G-03** "Part-IS oversight approach - Guidelines for Competent Authorities for the conduct of oversight activities of organisations implementing Part-IS" supuso un aportación crucial que aclaró muchas dudas. El planteamiento de **los niveles P/S/O/E facilita y clarifica el proceso de implantación**.

- Es necesario, y la norma lo ha previsto, **considerar** la existencia de **organizaciones complejas** con múltiples entidades/empresas que comparten estructuras organizativas, políticas, procesos y procedimientos de seguridad de la información e infraestructuras tecnológicas y que cuentan con una **gestión única y homogénea de la seguridad de la información**.

- **Es esencial tener una visión unificada de la seguridad de la información** (y en general de la seguridad).

- Es **fundamental** que se aplican **criterios de aprobación, inspección y auditoría homogéneos**.

- Hay que buscar un **fórmula** que asegure que se realiza la **adecuada supervisión de la parte IS** sin penalizar a las organizaciones complejas que comparten **un SGSI común.**

- Sugerimos se **valore una supervisión única del sistema de gestión de la seguridad de la información** que aplique una visión holística y global, que contemple todas las aprobaciones y que considere también los requisitos de AVSEC (SA-16).

Binter

bintercanarias.com