Plantilla de la lista de verificación de la política de gestión de la ciberseguridad del tránsito aéreo

Introducción

El presente documento es una lista de verificación que tiene como objetivo una autoevaluación de todos los requisitos sobre la implementación de ciberseguridad explicados en la Plantilla de la política de gestión de la ciberseguridad.

El documento no es un requisito obligatorio para la implementación, pero contiene información relevante que apoya el desarrolla de su propio Manual de política de ciberseguridad.

Enfoque

Este documento cubre toda la estructura funcional de la aviación de todas las partes interesadas como son las autoridades de aviación civil, Proveedores de Servicios de Navegación Aérea y toda entidad u organización que es parte de un sistema estatal de aviación, para asegurar la implementación de procedimientos y prácticas de ciberseguridad en todos los servicios bajo la vigilancia del Estados, como son:

- ✓ Dependencias de servicios de tránsito aéreo (Torre de control de aeródromo o control de aeródromo –TWR, servicio de control de aproximación – APP, y Centro de control de área - ACC)
- ✓ Datos e infraestructura de Comunicación, navegación y vigilancia (CNS)
- ✓ Sistemas de información digital (información aeronáutica, información meteorológica y otra de apoyo a la información para la toma de decisiones)
- ✓ Sistemas para interoperabilidad de la aviación
- ✓ Otras de acuerdo con los servicios y operaciones del Estado

Este documento aplica a todas las locaciones e instalaciones del sistema de aviación que alberguen:

- ✓ Información requerida por los servicios de Gestión del tránsito aéreo (ATM).
- ✓ Infraestructura de tecnologías de la información (TI) en la que confían los servicios ATM
- ✓ Tecnología operacional (TO) y sistemas industriales interconectados y sistemas controlados automatizados (IACS)
- ✓ Servicios ampliados y asociación e interconexiones de sistemas de información relacionados
- ✓ Todo el personal de la aviación y organizaciones externas que tengan acceso a la información de navegación aérea, servicios e instalaciones

In cooperation with

Plantilla de la lista de verificación de la política de gestión de la ciberseguridad del tránsito aéreo

Estado:
Punto de Contacto (s): Por favor integre nombre, posición en la Organización, correo electrónico y número telefónico.

Lista de verificación

1. Documentación de seguridad ATM

-> PLANTILLA DE LA POLÍTICA DE CIBERSEGURIDAD ATM, CAPÍTULO 6

		Sí	% en progreso	No
1.1	¿Ha establecido una política de seguridad de información para su organización?			
1.2	¿Ha establecido ISMS para su organización?			
1.3	Su documentación ATM está: • Implementada • Con mantenimiento • Basada con un enfoque de gestión del riesgo			
	¿Ha identificado y delimitado su infraestructura (como "TI", "TO" y "IACS") para que su seguridad pueda ser gestionada apropiada y proporcionalmente?			

Infraestructura TI	Infraestructura TO y IACS

Anexe otras hojas si es necesario, para listar toda la infraestructura TI, TO y IACS

Plantilla de la lista de verificación de la política de gestión de la ciberseguridad del tránsito aéreo

2. Gestión del riesgo -> PLANTILLA DE LA POLÍTICA DE CIBERSEGURIDAD ATM, CAPÍTULO 7				
		Sí	**% en progreso**	**No**
2.1	¿Se aborda la seguridad en todas las fases del ciclo de vida del sistema?			
2.2	¿Tiene implementado un procedimiento (metodología) de gestión del riesgo definido y repetible?			
2.3	Los riesgos de seguridad son: • Rastreados • Monitoreados • Revisados con regularidad			
2.4	¿Ha tomado pasos para procesar la gestión de vulnerabilidades en los sistemas?			
2.5	¿Ha identificado todos los activos ATM (datos, sistemas, personal) y establecido procedimientos de control para éstos?			
2.6	¿Ha empoderado al personal adecuado para tomar decisiones de tratamiento sobre riesgos de seguridad?			
2.7	¿Tiene procesos definidos sobre gestión de la información de seguridad? (que atienden todas las actividades de seguridad)			
2.8	¿Ha establecido medidas técnicas y operacionales de seguridad (políticas y procedimientos)? La intención de esto es reducir el riesgo a un nivel aceptable a pesar del error humano, accidente o incidente, impacto de un desastre natural y otros.			

Plantilla de la lista de verificación de la política de gestión de la ciberseguridad del tránsito aéreo

		Sí	% en progreso	No
2.9	¿Ha identificado interfaces para asegurar tratamiento del riesgo de seguridad sobre la seguridad ATM eficientes y coordinadas?			
2.10	¿Ha establecido un proceso de gestión del riesgo que cubra riesgos de seguridad de la información ATM con una revisión y un monitoreo periódicos?			

3. Gobernanza de la seguridad y organización

-> PLANTILLA DE LA POLÍTICA DE CIBERSEGURIDAD ATM, CAPÍTULO 8

		Sí	% en progreso	No
3.1	¿Ha establecido una autoridad apropiada para la gestión de la seguridad ATM a nivel de dependencia (Unidad)?			
3.2	¿Ha establecido roles y responsabilidades dentro de la gestión del riesgo de seguridad ATM?			
3.3	¿Ha implementado procesos definidos para inteligencia (información) y monitoreo de la amenaza?			
3.4	¿Ha implementado procesos definidos para la gestión de incidentes y crisis?			

4. Recursos humanos (Medidas de seguridad durante todas las fases de empleo)

-> PLANTILLA DE LA POLÍTICA DE CIBERSEGURIDAD ATM, CAPÍTULO 9

		Sí	% en progreso	No
4.1	Antes del empleo: ¿utiliza medidas tales como revisión de antecedentes de acuerdo con las regulaciones locales?			
4.2	Durante el empleo: ¿desarrolla una cultura de la seguridad a través de capacitación regular y conciencia situacional?			

Plantilla de la lista de verificación de la política de gestión de la ciberseguridad del tránsito aéreo

		Sí	% en progreso	No
4.3	¿Después de la contratación: ¿se protege asegurando el proceso de eliminación de accesos y recordando al personal los compromisos de no divulgación (cuando lo permite la ley)?			
4.4	¿Tiene procedimientos para asignar y limitar el acceso del personal de acuerdo con sus responsabilidades?			

5. Gestión de activos

-> PLANTILLA DE LA POLÍTICA DE CIBERSEGURIDAD ATM, CAPÍTULO 10

		Sí	% en progreso	No
5.1	¿Tiene un inventario de activos ATM y los mantiene actualizados?			
5.2	¿El inventario incluye evaluación de la criticidad (sobre seguridad operacional y operatividad) de cada activo?			
5.3	¿Ha considerado acceso lógico y físico y se ha asegurado de que hay consistencia entre ellos?			
5.4	¿Se han considerado y clasificado todos los datos ATM y han sido protegidos a un nivel adecuado?			
5.5	¿Tiene procedimientos para asegurar que todos los datos ATM serán protegidos durante su almacenaje, procesamiento e intercambio, en línea con perfil de confidencialidad?			

6. Control de acceso

-> PLANTILLA DE LA POLÍTICA DE CIBERSEGURIDAD ATM, CAPÍTULO 11

		Sí	% en progreso	No
6.1	¿El acceso a todos los activos ATM es a través de un proceso de verificación adecuado para evitar riesgos			

	inaceptables?			
6.2	¿Tiene controles para cubrir los accesos de los sistemas físicos y lógicos?			
7. Seguridad física y del entorno de los componentes CNS/ATM -> PLANTILLA DE LA POLÍTICA DE CIBERSEGURIDAD ATM, CAPÍTULO 12				
		Sí	**% en progreso**	**No**
7.1	¿Se ha asegurado que la seguridad física ATM salvaguarda TI, TO, IACS y la infraestructura CNS/ATM contra interferencia ilícita y acceso no autorizado?			
7.2	¿Se ha asegurado que la seguridad física ATM identifica zonas que alberguen activos CNS/ATM de acuerdo con su criticidad (desde la perspectiva de seguridad operacional y operatividad)?			
7.3	¿Ha implementado medidas de seguridad física ATM para proteger todos los servicios y operaciones CNS/ATM de interferencia intencional o ilícita?			
7.4	¿Ha implementado seguridad física ATM para proteger flujos de información entrante y saliente entre zonas de almacenaje y centros de datos?			
8. Seguridad de las operaciones -> PLANTILLA DE LA POLÍTICA DE CIBERSEGURIDAD ATM, CAPÍTULO 13				
		Sí	**% en progreso**	**No**
8.1	¿Ha establecido zonas confiables?			
8.2	¿Ha establecido procedimientos para asegurar la coordinación sobre ciberseguridad ATM de las operaciones de seguridad, monitoreo y mejora continua del procesamiento de información?			
8.3	¿Se ha asegurado que las Operaciones de ciberseguridad ATM incluyan TI, TO, IACS e			

	infraestructura CNS/ATM en el alcance de seguridad de las operaciones?			
8.4	¿Ha implementado operaciones de ciberseguridad ATM para mantener la efectividad de las medidas de seguridad a través de su ciclo de vida?			
8.5	¿Ha establecido un perímetro de seguridad a través de zonas de ciberseguridad ATM para zonas físicas y lógicas?			
8.6	¿Tiene procedimientos para prevenir la explotación de vulnerabilidades técnicas sobre TI, TO, IACS e infraestructura CNS/ATM			
8.7	¿Tiene controles de seguridad sobre el uso de aparatos móviles del personal para actividades CNS/ATM (por ejemplo, su utilización es prohibida?			
8.8	¿Ha tomado pasos para asegurar que los aparatos móviles del personal no representen un riesgo a la seguridad de las actividades CNS/ATM (por ejemplo, conectar un dispositivo personal al equipo operativo para cargarlo)?			
9. Comunicaciones de seguridad -> PLANTILLA DE LA POLÍTICA DE CIBERSEGURIDAD ATM, CAPÍTULO 14				
		Sí	**% en progreso**	**No**
9.1	¿Ha reunido y mantenido un mapeo actualizado de sus redes e interconexiones?			
9.2	¿Se asegura de que las redes ATM están segregadas lógica y físicamente basadas en su criticidad en cuanto a la seguridad operacional y operatividad?			
9.3	¿Ha tomado pasos para asegurar que las tecnologías inalámbricas y acceso a Internet no constituyen un riesgo inaceptable a la seguridad operacional y la			

Plantilla de la lista de verificación de la política de gestión de la ciberseguridad del tránsito aéreo

	seguridad de la aviación?			
10. Adquisición, desarrollo y mantenimiento de sistemas -> PLANTILLA DE LA POLÍTICA DE CIBERSEGURIDAD ATM, CAPÍTULO 15				
		Sí	**% en progreso**	**No**
10.1	¿La seguridad de la información es una parte integral de su gestión de sistemas de información CNS/ATM durante el ciclo de vida completo?			
10.2	¿Se asegura que los sistemas de información están diseñados con base en los siguientes principios? • Ningún punto de vulnerabilidad único ni común • Uso de reglas de codificación de seguridad definidas y verificadas • Gestión de la vulnerabilidad en software y hardware COTS El uso de normas y recomendaciones industriales apropiadas (por ejemplo, NIST, OWASP, EUROCAE/RTCA, etc.)?			
11. Relaciones con proveedores y socios -> PLANTILLA DE LA POLÍTICA DE CIBERSEGURIDAD ATM, CAPÍTULO 16				
		Sí	**% en progreso**	**No**
11.1	¿Ha evaluado la madurez de la seguridad de los proveedores y socios antes de contratarlos?			
11.2	¿Su proceso de gestión del riesgo también abarca el riesgo de proveedores?			
12. Gestión de incidentes de seguridad -> PLANTILLA DE LA POLÍTICA DE CIBERSEGURIDAD ATM, CAPÍTULO 17				
		Sí	**% en progreso**	**No**

Plantilla de la lista de verificación de la política de gestión de la ciberseguridad del tránsito aéreo

12.1	¿Tiene un procedimiento y listas de comunicación en caso de un incidente de seguridad o identificación de debilidades?			
13. Aspectos de seguridad de la Gestión de la continuidad del negocio -> PLANTILLA DE LA POLÍTICA DE CIBERSEGURIDAD ATM, CAPÍTULO 18				
		Sí	**% en progreso**	**No**
13.1	¿Ha identificado interfaces entre la continuidad de negocio AMT y los procesos de gestión de riesgo?			
13.2	¿Realiza ejercicios de gestión de crisis y pruebas basadas en casos de seguridad ATM?			
14. Protección de datos personales -> PLANTILLA DE LA POLÍTICA DE CIBERSEGURIDAD ATM, CAPÍTULO 19				
		Sí	**% en progreso**	**No**
14.1	¿Ha definido una interface entre DPO y el proceso de seguridad ATM?			
15. Cumplimiento -> PLANTILLA DE LA POLÍTICA DE CIBERSEGURIDAD ATM, CAPÍTULO 20				
		Sí	**% en progreso**	**No**
15.1	¿Realiza auditorias se seguridad de terceras partes de sistemas de información ATM/CNS?			
15.2	¿Los resultados de seguridad disparan actualizaciones de la evaluación del riesgo?			

- FIN -