Departamento
de Controle do Espaço Aéreo
Department of Airspace Control

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DEL COMANDO AERONÁUTICO

Objetivo

Presentar la Política de Seguridad de la Información de COMAER y sus reflejos en la implementación de SWIM en Brasil

Roteiro

Directrices
Infraestructuras Críticas
Defensa Cibernética
Seguridad Física Y Ambiental
Controles De Acceso
Gestión De Uso De Recursos Operativos Y De Comunicación
Procesos
Ciberseguridad Vinculada a SWIM

Directrices

Un sistema de información enfocado en el uso de TI, para operar adecuadamente y brindar Seguridad de la Información, disponible en formato digital, necesita ambientes controlados y protegidos contra desastres naturales (incendios, terremotos e inundaciones), fallas estructurales (interrupción de suministro eléctrico, sobrecargas y otros), sabotaje, fraude, acceso no autorizado (hackers, espionaje industrial, venta de información confidencial)

Directrices

La Seguridad de la Información en COMAER comprende un conjunto de objetivos, lineamientos, reglamentos técnicos y de gestión, y otros controles destinados a garantizar la confidencialidad, disponibilidad, integridad, irreversibilidad y autenticidad de la información a lo largo de su ciclo de vida, disponible o en tránsito en un entorno digital o físico

Directrices

La Seguridad de la Información, además de basar las acciones para adecuarse a la privacidad de los datos, comprenderá también la Ciberseguridad, la Ciberdefensa, la seguridad física y la protección de los datos y activos de información, tal y como establece la Política Nacional de Seguridad de la Información y prevé la Gobernanza de la seguridad de la información

Directrices

El éxito de las acciones en materia de Seguridad de la Información está directamente asociado a la formación científico-tecnológica del capital humano involucrado, la concientización del público interno, la calidad de las soluciones adoptadas y la protección de la información contra amenazas internas y externas

Infraestructuras Críticas

Todos los activos de información producidos o procesados en el Sistema de Tecnología de la Información Aeronáutica (STI) y otros activos considerados críticos en el Sistema deben estar claramente identificados, inventariados y sujetos a procedimientos de seguridad y análisis de riesgo continuo

INFRAESTRUCTURAS CRÍTICAS

La seguridad física y operativa debe conocerse y monitorearse para garantizar la prestación de estos servicios esenciales, y la seguridad efectiva comienza con una comprensión clara de todos los tipos y niveles de riesgo que enfrenta una organización

DEFENSA CIBERNÉTICA

La Ciberdefensa es el conjunto de acciones ofensivas, defensivas y exploratorias, realizadas en el Ciberespacio, con el propósito de proteger los sistemas de información de interés para la Defensa Nacional

DEFESA CIBERNÉTICA

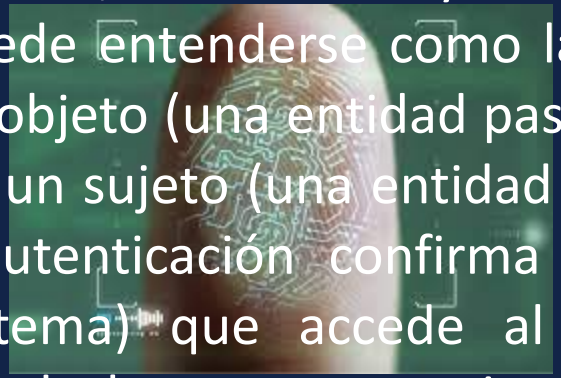
El futuro Centro de Ciberdefensa Aeronáutica (CDCAER), como Órgano Central del futuro Sistema de Ciberdefensa (SISDCAER), deberá ejercer responsabilidades de Seguridad de la Información, Comunicaciones y Ciberseguridad, en conjunto con el Órgano Central del Sistema Tecnológico. (STI) y el Servicio de Telecomunicaciones del Comando de la Fuerza Aérea (STCA)

SEGURIDAD FÍSICA Y AMBIENTAL

La implementación de controles de seguridad y protección contra amenazas físicas y ambientales brindará más que solo protección de la información. Estos controles contribuyen a la protección de activos que representan valor para la organización, requiriendo atención y dedicación de la administración con el cuidado con la seguridad de los equipos que contienen estos activos de información, instalados en lugares definidos como áreas seguras

CONTROLES DE ACCESO

El control de acceso, en Seguridad de la Información, se compone de procesos de autenticación, autorización y auditoría. En este contexto, el control de acceso puede entenderse como la capacidad de permitir o denegar el uso de un objeto (una entidad pasiva, como un sistema o un archivo) por parte de un sujeto (una entidad activa, como un individuo o un proceso). La autenticación confirma la identidad del usuario (persona u otro sistema) que accede al sistema, la autorización determina lo que puede hacer un usuario autenticado y la auditoría informa lo que ha hecho el usuario



GESTIÓN DE USO DE RECURSOS OPERATIVOS Y DE COMUNICACIÓN

En cuanto a las comunicaciones, se recomienda encarecidamente que la responsabilidad operativa de las redes se separe de la operación de los recursos informáticos administrativos. Es decir, la segregación entre redes operativas y administrativas supondrá un aumento de la seguridad de los servicios de red

GESTIÓN DE USO DE RECURSOS OPERATIVOS Y DE COMUNICACIÓN

Ambas redes deben ser monitoreadas mediante firewalls de borde para proteger el perímetro de las redes, posibilitando el control del tráfico de información con redes externas por un Centro de Operaciones de Red (NOC) y la gestión de la seguridad, por un Centro de Operaciones de Seguridad (SOC), para que todo este la infraestructura de protección perimetral es gestionada por un NOC/SOC

PROCESOS

La Política de Seguridad de la Información tiene como objetivo buscar el alineamiento con la evolución de la tecnología y sus riesgos, identificando los factores internos y externos que puedan impactar en el logro de los objetivos de COMAER, debe contar con los siguientes procesos:

- Mapeo de activos de información
- Gestión de Riesgos y Vulnerabilidades
- Gestión de Continuidad y Backup
- Gestión del cambio
- Auditoría y Evaluación de la Conformidad

CIBERSEGURIDAD VINCULADA A SWIM

SWIM opera en infraestructuras técnicas (G/G y A/G) a través de las cuales se intercambiará información ATM utilizando servicios de información. La infraestructura técnica de SWIM consiste en servicios de infraestructura (por ejemplo, servicios de mensajería, servicios de seguridad, etc.). Éstas se basan, en la medida de lo posible, en Tecnologías de la Información y la Comunicación que utilizan conectividad de red IP

CIBERSEGURIDAD VINCULADA A SWIM

Se considera desafiante, en el modelo de intercambio de información actual, diseñar marcos de seguridad y respaldar la creciente necesidad de un intercambio de datos abierto y oportuno entre los sistemas y las partes interesadas con la variedad de sistemas actual, respetando las preocupaciones legítimas de seguridad de todos

CIBERSEGURIDAD VINCULADA A SWIM

El registro SWIM, cuando se trata de información crítica sobre servicios e información, debe contar con mecanismos de seguridad para garantizar:

- Control de acceso basado en roles (RBAC), que considera a los diferentes actores que producen, usan o administran información de registros SWIM

- integridad y confiabilidad de la información disponible

CIBERSEGURIDAD VINCULADA A SWIM

- gestión de riesgos y seguridad, para garantizar la disponibilidad del registro SWIM, la confidencialidad basada en el control de acceso y la integridad de la información gestionada por el registro SWIM

CIBERSEGURIDAD VINCULADA A SWIM

Los siguientes aspectos deben ser considerados como premisas para la adopción del concepto SWIM en la ATM nacional por parte de DECEA:

- establecimiento e implementación de los requisitos necesarios para la provisión de la Red de Telecomunicaciones necesaria para soportar el concepto SWIM, incluyendo aspectos de seguridad

- mapeo de los riesgos de ciberseguridad asociados con SWIM y
- elaboración del modelo de gestión de la ciberseguridad asociado;

CIBERSEGURIDAD VINCULADA A SWIM

Los procedimientos y procesos de respaldo de contingencia deben desarrollarse como parte del estándar global (por ejemplo, falla SWIM, incluida la infraestructura y los servicios SWIM u otros casos de grandes amenazas de seguridad cibernética)

Roteiro

Directrices
Infraestructuras Críticas
Defensa Cibernética
Seguridad Física Y Ambiental
Controles De Acceso
Gestión De Uso De Recursos Operativos Y De Comunicación
Procesos
Ciberseguridad Vinculada a SWIM

Objetivo

Presentar la Política de Seguridad de la Información de COMAER y sus reflejos en la implementación de SWIM en Brasil

GRACIAS

Departamento
de Controle do Espaço Aéreo
Department of Airspace Control

FORÇA AÉREA BRASILEIRA
Asas que protegem o País

WWW.DECEA.GOV.BR