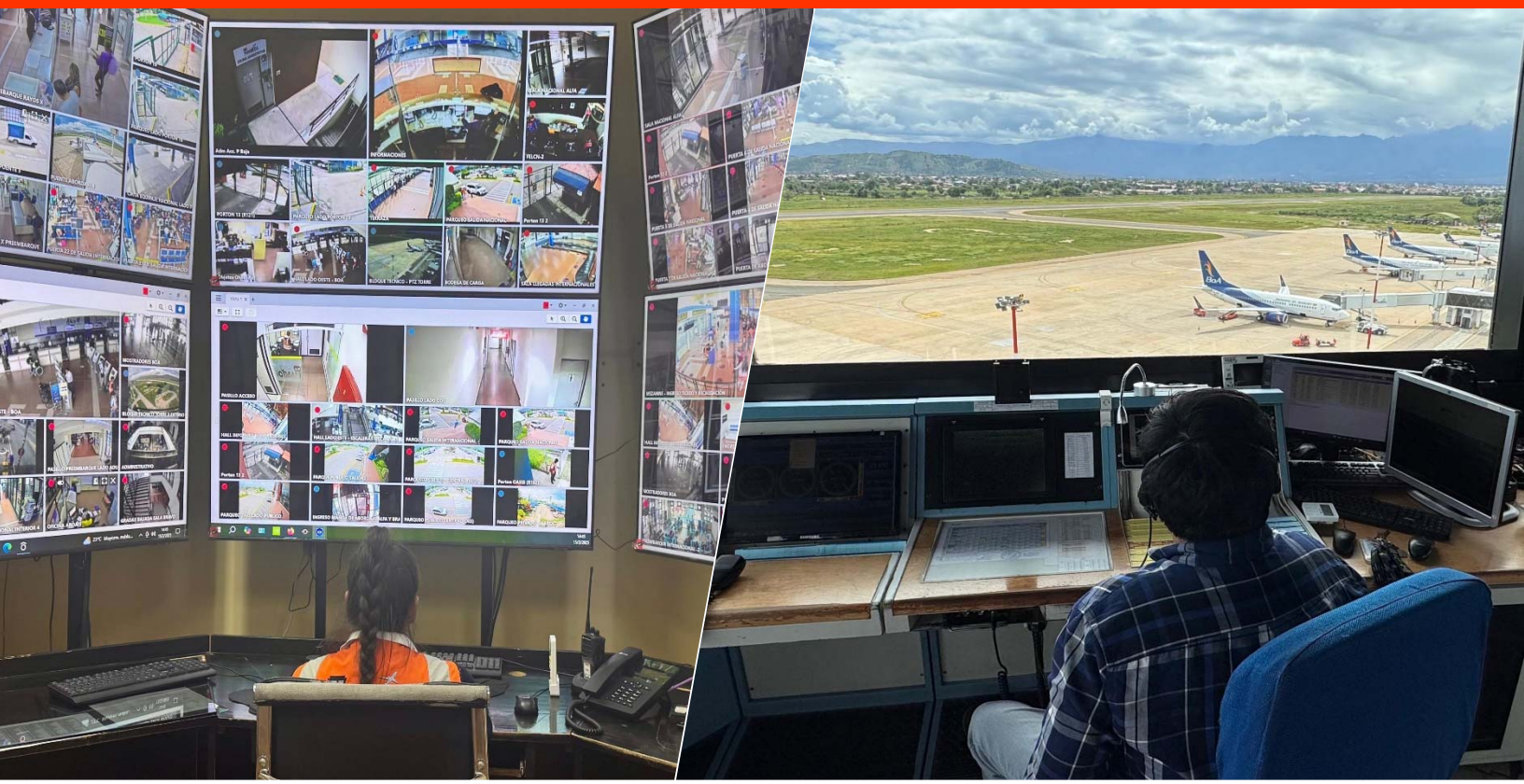
DGAC
DIRECCIÓN GENERAL DE AERONÁUTICA CIVIL

Documento AVSEC – CIB

CIBERSEGURIDAD

Enmienda 1, aprobada mediante R.A. N° 658 de 31/12/2024



Dirección General de Aeronáutica Civil

ESTADO PLURINACIONAL DE BOLIVIA

COPIA LEGALIZADA
ARCHIVO CENTRAL - DGAC

DGAC

RESOLUCIÓN ADMINISTRATIVA Nº 658
La Paz, 31 DIC 2024

VISTOS:

El Informe Técnico Jurídico DGAC-54391/2024 DTA-2992/2024 de 12 de diciembre de 2024, emitido por la Unidad AVSEC de la Dirección de Transporte Aéreo y la Unidad de Análisis Jurídico de la Dirección Jurídica referido al Informe Técnico para la Aprobación con Resolución Administrativa de la Enmienda Nro. 1 de los Documentos AVSEC OPS, IFS, PAX y CGO.

CONSIDERANDO:

Que el numeral 11 del Artículo 316 de la Constitución Política del Estado establece como una de las funciones del Estado en la economía la de regular la actividad aeronáutica en el espacio aéreo del país.

Que el inciso f) del Artículo 9 de la Ley N° 2902 de 29 de octubre de 2004, de la Aeronáutica Civil de Bolivia, refiere que la Autoridad Aeronáutica Civil es la Máxima Autoridad Técnica Operativa del sector aeronáutico civil nacional, ejercida dentro de un organismo autárquico, conforme a las atribuciones y obligaciones fijadas por Ley y normas reglamentarias, teniendo a su cargo la aplicación de la Ley de la Aeronáutica Civil de Bolivia y sus reglamentos, así como de reglamentar, fiscalizar, inspeccionar y controlar las actividades aéreas e investigar los incidentes y accidentes aeronáuticos.

Que en fecha 2 de diciembre de 2005, se aprobó el Decreto Supremo N° 28478, Marco Institucional de la Dirección General de Aeronáutica Civil, cuyo Artículo 2 establece que esta Entidad, es un órgano autárquico de derecho público, con personalidad jurídica y patrimonio propio, con jurisdicción nacional, tiene autonomía de gestión administrativa, legal y económica para el cumplimiento de su misión institucional.

Que el Artículo 8 del citado Decreto Supremo, señala que la Dirección General de Aeronáutica Civil tiene las siguientes funciones enunciativas y no limitativas: "5. Formular, aprobar y ejecutar las normas técnico-operativas, administrativas, comerciales y legales dentro del ámbito de su competencia".

Que de conformidad con el numeral 5) del Artículo 14, del citado Decreto Supremo, es atribución del Director Ejecutivo de la Dirección General de Aeronáutica Civil, emitir Resoluciones Administrativas sobre asuntos de su competencia, asimismo el numeral 8) del mismo artículo entre otras, describe: 8. Aprobar los Manuales y Procedimientos Técnico-Operativos y Comerciales.

DIRECTOR EJECUTIVO V°B° Ing. MSc. Jose Ivan Figueroa Terceros D.G.A.C.

CONSIDERANDO:

Que a través del Informe Técnico Jurídico DGAC-54391/2024 DTA-2992/2024 de 12 de diciembre de 2024, emitido por la Unidad AVSEC de la Dirección de Transporte Aéreo y la Unidad de Análisis Jurídico de la Dirección Jurídica referido al Informe Técnico para la Aprobación con Resolución Administrativa de la Enmienda Nro. 1 de los Documentos AVSEC OPS, IFS, PAX y CGO, señala que: *"En el marco de la preparación del Estado Plurinacional de Bolivia para la auditoria USAP-CMA, programada para la gestión 2025 y de acuerdo al Plan de trabajo AVSEC/USAP 2024, la Unidad AVSEC, dependiente de la Dirección de Transporte Aéreo, ha identificado la necesidad de revisar y consolidar documentos de orientación AVSEC, que tengan por objetivo proporcionar directrices claras para la implementación de medidas de seguridad en la aviación civil a nivel aeropuerto, cruciales para asegurar la integridad de las operaciones aéreas y la protección de los pasajeros. --- Los documentos de orientación vigentes, datan de la gestión 2023, estos no cuentan con aprobación por Resolución Administrativa. La elaboración y revisión de la primera enmienda de estos documentos se fundamenta en lo establecido en la Reglamentación Aeronáutica Boliviana (RAB), las orientaciones contenidas en el Documento 8973 - Manual de Seguridad de la Aviación, y las preguntas de protocolo del CE-5 de la USAP-CMA. Estos marcos normativos son esenciales para garantizar que Bolivia cumpla con los estándares internacionales de Seguridad de la Aviación".*

DIRECTOR JURIDICO V°B° Abg. Javier Mollinedo Ledezma DGAC

JEFE UNID. DE ANÁLISIS JURIDICO V°B° Abg. Julio Cesar Beyer Pacheco D.G.A.C.

Que asimismo el Informe Técnico Jurídico DGAC-54391/2024 DTA-2992/2024 de 12 de diciembre de 2024, concluye: *"En el marco del Plan de Trabajo AVSEC/USAP 2025, se enmendaron y revisaron los Documentos AVSEC, de acuerdo con lo establecido en la Reglamentación Aeronáutica*

PROF. III EN ANÁLISIS JURIDICO V°B° Abg. Pablo Daril Soza Arteaga DGAC

ESTADO PLURINACIONAL DE BOLIVIA

DGAC

Boliviana (RAB), el Documento 8973 - Manual de seguridad de la aviación y las preguntas de protocolo del CE-5 de la USAP-CMA. --- La Enmienda Nro. 1 de los Documentos AVSEC, incorpora la estructura de los documentos generados por la Unidad AVSEC (Programas Nacionales y Manuales); su contenido esta validado respecto al cumplimiento de las preguntas de protocolo del CE-5 de la USAP-CMA, en su versión 2022, y está acorde a las orientaciones del documento 8973 – Manual de seguridad de la aviación. --- Los documentos AVSEC fueron revisados y validados por parte de Personal AVSEC, el Jefe de Unidad AVSEC, y el Director de Transporte Aéreo. Este proceso fue esencial para validar tanto la estructura como el contenido de los documentos y, en consecuencia, poner a consideración de su Autoridad la aprobación del documento mediante Resolución Administrativa. --- La Dirección Ejecutiva de la DGAC, es la instancia de aprobación de documentos en el ámbito de su competencia, de acuerdo al D.S. 28478. --- En mérito al análisis y en virtud a la normativa antes citada corresponde a través de Resolución Administrativa la aprobación de LA ENMIENDA NRO. 1 DE LOS DOCUMENTOS AVSEC – OPS (OPERACIONES AEROPORTUARIAS), – IFS (SEGURIDAD DE LA AERONAVE Y EN VUELO), – PAX (SEGURIDAD DE LOS PASAJEROS Y EL EQUIPAJE) – CGO (SEGURIDAD DE LA CARGA, LOS SUMINISTROS DE A BORDO Y CORREO) y CIB (CIBERSEGURIDAD)." y recomienda: *"Elaborar el Proyecto de Resolución Administrativa de aprobación de la enmienda Nro.1 de los Documentos AVSEC. Se adjunta un ejemplar de los documentos. --- Firmar la Resolución Administrativa que apruebe la enmienda Nro.1 de los Documentos AVSEC – OPS (OPERACIONES AEROPORTUARIAS), – IFS (SEGURIDAD DE LA AERONAVE Y EN VUELO), – PAX (SEGURIDAD DE LOS PASAJEROS Y EL EQUIPAJE) – CGO (SEGURIDAD DE LA CARGA, LOS SUMINISTROS DE A BORDO Y CORREO) y CIB (CIBERSEGURIDAD). --- Posterior a la Emisión de la Resolución Administrativa por la Dirección Ejecutiva, remitir el documento original a la Unidad AVSEC de la Dirección de Transporte Aéreo para su registro, control, difusión e implementación".*

CONSIDERANDO:

Que mediante Resolución Suprema N° 27883, de 31 de octubre de 2022, ha sido designado como Director Ejecutivo Interino de la Dirección General de Aeronáutica Civil DGAC, el Ing. José Ivan Fernando García Terceros.

Que el numeral 5 del Artículo 14 del Decreto Supremo N° 28478, establece como atribución del Director Ejecutivo de la Dirección General de Aeronáutica Civil, la emisión de Resoluciones Administrativas sobre asuntos de su competencia;

POR TANTO:

EL DIRECTOR EJECUTIVO INTERINO DE LA DIRECCIÓN GENERAL DE AERONÁUTICA CIVIL DGAC, EN USO DE LAS ATRIBUCIONES CONFERIDAS POR LEY;

RESUELVE:

PRIMERO.- APROBAR la Enmienda Nro. 1 de los Documentos AVSEC – OPS (OPERACIONES AEROPORTUARIAS), – IFS (SEGURIDAD DE LA AERONAVE Y EN VUELO), – PAX (SEGURIDAD DE LOS PASAJEROS Y EL EQUIPAJE) – CGO (SEGURIDAD DE LA CARGA, LOS SUMINISTROS DE A BORDO Y CORREO) y CIB (CIBERSEGURIDAD).

SEGUNDO.- REMITIR el documento original a la Unidad AVSEC de la Dirección de Transporte Aéreo para su registro, control difusión e implementación.

TERCERO.- La Unidad de Seguridad de la Aviación Civil (AVSEC) de la Dirección de Transporte Aéreo, queda encargada de realizar todos los trámites necesarios para el cumplimiento de la presente Resolución Administrativa.

Regístrese, comuníquese y archívese.

JEFE UNID. DE ANÁLISIS JURÍDICO V°B° Abg. Julio Cesar Beyer Pacheco D.G.A.C.

Abg. Javier C. Limojosa Ledezma
DIRECTOR JURÍDICO
Dirección General de Aeronáutica Civil

Ing. MSc. Jose Ivan F. Garcia Terceros
DIRECTOR EJECUTIVO a.i
Dirección General de Aeronáutica Civil

JIFGT/JCHL/jcbp/pdsa
Cc. Archivo
Cc. DJ

PROF. III EN ANÁLISIS JURÍDICO V°B° Abg. Pablo Daniel Soza Arteaga D.G.A.C.

Tabla de registro de enmiendas

Enmienda	Origen	Temas	Fecha Aprobación
01	1ra versión del documento aprobada por Resolución Administrativa	Todos	31/12/2024
-	-	-	-
-	-	-	-
-	-	-	-
-	-	-	-

Lista de páginas efectivas

Página	Fecha	Enmienda
1	31/12/2024	Original
2	31/12/2024	Original
3	31/12/2024	Original
4	31/12/2024	Original
5	31/12/2024	Original
6	31/12/2024	Original
7	31/12/2024	Original
8	31/12/2024	Original
9	31/12/2024	Original
10	31/12/2024	Original
11	31/12/2024	Original
12	31/12/2024	Original
13	31/12/2024	Original
14	31/12/2024	Original
15	31/12/2024	Original
16	31/12/2024	Original
17	31/12/2024	Original
18	31/12/2024	Original
19	31/12/2024	Original
20	31/12/2024	Original
21	31/12/2024	Original
22	31/12/2024	Original

Contenido

CAPÍTULO 1. INFORMACIÓN GENERAL

1.1. INTRODUCCIÓN

La ciberseguridad es un componente esencial para garantizar la Seguridad de la Aviación Civil en las operaciones aéreas y la protección de la información crítica. En un mundo cada vez más interconectado, los sistemas de tecnologías de la información y la comunicación (TIC) son fundamentales para el funcionamiento eficaz de aeropuertos, control de tráfico aéreo, gestión de vuelos y operaciones de mantenimiento. No obstante, esta interconexión también expone a la aviación civil a una variedad de amenazas cibernéticas que pueden comprometer la integridad y disponibilidad de estos sistemas, así como la seguridad de los pasajeros y la tripulación.

Además de los riesgos cibernéticos, la aviación civil debe enfrentarse a actos de interferencia ilícita, que incluyen desde amenazas terroristas hasta actividades delictivas que pueden poner en peligro la seguridad de las aeronaves y los aeropuertos. La protección contra estas amenazas requiere una colaboración estrecha entre la Autoridad de Aviación Civil, el Explotador de Aeropuertos y Explotadores de Aeronaves. La implementación de medidas adecuadas de ciberseguridad y la defensa contra actos de interferencia ilícita son esenciales para mantener la confianza del público en la seguridad del transporte aéreo.

La naturaleza dinámica de las amenazas en el ámbito de la aviación civil exige un enfoque proactivo y adaptable en la gestión de la ciberseguridad. Esto implica no solo la identificación y protección de los sistemas críticos, sino también la capacidad de detectar y responder rápidamente a los incidentes de seguridad. La formación continua del personal, la realización de simulacros de respuesta a incidentes y el establecimiento de protocolos de comunicación claros son componentes vitales para enfrentar los desafíos que presenta la ciberseguridad en la aviación.

1.2. OBJETIVO

El objetivo del Documento AVSEC – CIB es proporcionar una orientación clara y concisa, que complemente lo establecido en la Reglamentación Aeronáutica Boliviana, sobre las mejores prácticas en ciberseguridad específicamente diseñadas para la Seguridad de la Aviación Civil. A través de la identificación de sistemas críticos, la implementación de medidas de protección, el establecimiento de un sistema de monitoreo continuo y la preparación para la respuesta a ciberataques, se busca fortalecer la resiliencia del sector ante las amenazas emergentes

1.3. ALCANCE

El Documento AVSEC - CIB establece los procedimientos, lineamientos y criterios relacionados a la aplicación de las medidas de ciberseguridad a nivel aeropuerto, desprendidas de la Reglamentación Aeronáutica Boliviana 107 y 108, estas comprenden lo siguiente:

a) La identificación de sistemas de tecnologías de la información y la comunicación críticos.

b) La protección de sistemas de tecnologías de la información y la comunicación críticos.

c) La detección de ciberataques mediante el establecimiento de un sistema de monitoreo continuo de la seguridad de la información.

d) La respuesta a ciberataques.

e) Un plan de comunicaciones para situaciones de crisis.

f) Análisis posterior a los eventos.

El Documento AVSEC - CIB está dirigido a las siguientes entidades (que desempeñan funciones de Seguridad de la Aviación Civil):

a) Explotador de Aeropuerto.

b) Explotador de Aeronaves.

c) Proveedor de Servicios de Aprovisionamiento de a Bordo.

d) Proveedor de Servicios de Tránsito Aéreo.

e) Proveedor de Servicios de Seguridad.

1.4. MARCO LEGISLATIVO

La DGAC, es la Máxima Autoridad Aeronáutica Civil del Estado Plurinacional de Bolivia, acorde a las atribuciones conferidas por la legislación del Estado:

a) Ley No. 2902 – Ley de Aeronáutica Civil.- En su artículo Nro. 9 inciso establece que la Autoridad Aeronáutica Civil es la máxima autoridad técnica operativa del sector aeronáutico civil nacional, ejercida dentro un organismo autárquico, conforme a las atribuciones y obligaciones fijadas por Ley y normas reglamentarias, teniendo a su cargo la aplicación de la Ley de la Aeronáutica Civil de Bolivia y sus reglamentos, así como de reglamentar, fiscalizar, inspeccionar y controlar las actividades aéreas e investigar los incidentes y accidentes aeronáuticos.

b) Ley No. 165 – Ley General de Transporte.- Establece la responsabilidad de la Seguridad de la Aviación Civil del Estado Plurinacional de Bolivia, en el marco de la reglamentación sectorial correspondiente.

c) Ley 428 – Ley de articulo único que modifica el artículo Nro. 140 (Seguridad de la Aviación) de la Ley No. 165 – Ley General de Transporte.- Establece que la Seguridad de la Aviación Civil del Estado Plurinacional de Bolivia, está a cargo y bajo responsabilidad de la Dirección General de Aeronáutica Civil.

1.5. AUTORIDAD PARA ELABORAR, APLICAR Y MANTENER EL DOCUMENTO AVSEC - CIB

En el Decreto Supremo No. 28478 - Marco Institucional de la DGAC, en su artículo 22, numeral 9, se atribuye la responsabilidad a la DTA para elaborar y aplicar, la reglamentación, programas y procedimientos asignados mediante el PNSAC, los Anexos al Convenio sobre Aviación Civil Internacional, y Acuerdos Internacionales en la materia.

1.6. BASE NORMATIVA

a) Programa Nacional de Seguridad de la Aviación Civil (PNSAC)

b) RAB 107 - Reglamento sobre Seguridad de la Aviación - Explotador de Aeropuerto y Proveedor de Servicios de Tránsito Aéreo

c) RAB 108 - Reglamento sobre Seguridad de la Aviación - Explotador de Aeronaves y Empresas de Aprovisionamiento de a Bordo

d) RAB 109 - Reglamento sobre Seguridad de la Aviación – Seguridad de la Carga y Correo.

1.7. DISTRIBUCIÓN

La distribución del Documento AVSEC - CIB se realizará a través de su publicación en la página web de la DGAC y en el Núcleo AVSEC, en formato digital protegido.

1.8. DEFINICIONES Y ACRÓNIMOS

En el presente Documento AVSEC – CIB se aplican las definiciones y acrónimos establecidos en los Programas Nacionales y la Reglamentación Aeronáutica Boliviana

1.9. ENMIENDA

La aprobación de una enmienda del Documento AVSEC - CIB se oficializará mediante Resolución Administrativa de la DGAC para lo cual su tramitación se ajustará al siguiente procedimiento:

Inicio: La Unidad AVSEC elabora la enmienda del Documento AVSEC - CIB, siendo revisada por el Jefe de Unidad AVSEC y Director de Transporte Aéreo.

Coordinación: Se coordinará con las partes interesadas y se sostendrá una reunión de validación con el personal de la Unidad AVSEC, para la socialización de las modificaciones realizadas en el documento.

Informe para aprobación: De no existir observaciones, la Unidad AVSEC presentará el Informe al Director Ejecutivo de la DGAC, vía el Jefe de Unidad y el Director de Transporte Aéreo, recomendando la aprobación de la enmienda del Documento AVSEC, mediante Resolución Administrativa. Se adjuntará la propuesta de enmienda.

Aprobación: El Director Ejecutivo instruye a la Dirección Jurídica la elaboración del proyecto de Resolución Administrativa para aprobación de la enmienda del documento. En la misma también se resolverá que el nuevo Documento AVSEC - CIB sea remitido a la Unidad AVSEC de la DTA para su control y difusión.

CAPÍTULO 2. IDENTIFICACIÓN DE SISTEMAS DE TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN CRÍTICOS

2.1. INVENTARIO EXHAUSTIVO DE SISTEMAS

La elaboración de un **inventario exhaustivo de sistemas** es un proceso fundamental para la identificación de los sistemas de tecnologías de la información y la comunicación (TIC) críticos en la aviación civil. Este inventario implica la recopilación detallada de todos los sistemas, aplicaciones y equipos utilizados en las operaciones aéreas, así como su clasificación en función de su importancia para la seguridad de la aviación en las operaciones. Un inventario bien estructurado no solo identifica los recursos tecnológicos, sino que también permite a las organizaciones evaluar sus vulnerabilidades y establecer las medidas de protección adecuadas.

En el contexto de la gestión aeroportuaria, el Explotador de Aeropuertos y el Proveedor de Servicio de Tránsito Aéreo utilizan una variedad de sistemas y equipos que son esenciales para la operación segura y eficiente de las instalaciones. Algunos ejemplos de estos sistemas incluyen:

a) Sistemas de Gestión de Aeropuertos: Estas plataformas integran diversas funciones, como la gestión de vuelos, la programación de aterrizajes y despegues, así como la coordinación de recursos en tierra. El Explotador de Aeropuertos utiliza estos sistemas para optimizar las operaciones y garantizar que las aeronaves sean atendidas de manera segura y oportuna.

b) Sistemas de Control de Tráfico Aéreo: Aunque estos sistemas son operados principalmente por controladores de tráfico aéreo, el Explotador de Aeropuerto también deben estar al tanto de su funcionamiento y de su integración con las operaciones en tierra. Estos sistemas son cruciales para la gestión del espacio aéreo y para garantizar que las aeronaves se mantengan en rutas seguras.

c) Sistemas de Información para Pasajeros: Estos sistemas proporcionan información en tiempo real sobre vuelos, puertas de embarque y horarios, tanto en pantallas dentro del aeropuerto como a través de aplicaciones móviles. Son fundamentales para mantener a los pasajeros informados y facilitar su experiencia en el aeropuerto.

d) Sistemas de Seguridad y Vigilancia: Incluyen cámaras de vigilancia, sistemas de control de acceso y detección de metales. Estos sistemas son esenciales para la seguridad del aeropuerto y ayudan a prevenir actos de interferencia ilícita.

Por otro lado, los Explotadores de Aeronaves y las Empresas de Aprovisionamiento de a Bordo también utilizan una serie de sistemas y equipos críticos para garantizar la seguridad y eficacia de las operaciones de vuelo. Algunos ejemplos son:

a) Sistemas de Gestión de Aeronaves: Estas plataformas permiten a los explotadores gestionar el mantenimiento, la programación de vuelos y la logística de las aeronaves. Los AMS son vitales para garantizar que las aeronaves estén en condiciones óptimas para volar.

b) Sistemas de Navegación y Comunicaciones: Incluyen equipos de navegación que utilizan GPS y sistemas de comunicación por radio que permiten la comunicación entre la aeronave y el control de tráfico aéreo. Estos sistemas son esenciales para la seguridad de los vuelos y para mantener la comunicación durante el trayecto.

c) Sistemas de Monitoreo de Vuelo: Estas herramientas permiten a los explotadores rastrear en tiempo real el estado de sus aeronaves, así como la información sobre el rendimiento de los motores y

otros sistemas críticos. El acceso a datos precisos y en tiempo real es fundamental para la toma de decisiones informadas durante el vuelo.

d) Sistemas de Gestión de Pasajeros y Carga: Los Explotadores de Aeronaves utilizan software especializado para gestionar la información de los pasajeros, el embarque, la carga y el equipaje. Estos sistemas ayudan a optimizar la experiencia del pasajero y a garantizar que la carga se maneje de manera segura.

La creación de este inventario detallado debe llevarse a cabo de manera sistemática, utilizando herramientas de documentación que permitan registrar no solo los sistemas y equipos, sino también su ubicación, características técnicas, responsables de su gestión y cualquier interdependencia con otros sistemas. Este enfoque asegura que todas las áreas del aeropuerto y las operaciones de las aerolíneas estén debidamente contempladas, lo que resulta esencial para el desarrollo de una estrategia integral de ciberseguridad que abarque toda la organización. Además, permite la identificación de posibles puntos de vulnerabilidad y facilita la implementación de medidas de seguridad adecuadas para mitigar riesgos.

2.2. EVALUACIÓN DE LA CRITICIDAD DE LOS SISTEMAS

La evaluación de la criticidad de los sistemas utilizados por el Explotador de Aeropuertos, los Explotadores de Aeronaves, Empresas de Aprovisionamiento de a Bordo, Proveedor de Servicio de Tránsito Aéreo, etc. es un proceso esencial para garantizar la seguridad de la aviación en las operaciones aéreas. Esta evaluación no solo ayuda a identificar los sistemas más vulnerables, sino que también permite priorizar las inversiones en ciberseguridad y establecer protocolos de respuesta adecuados.

a) Análisis de Impacto en las Operaciones: Los sistemas utilizados por estas entidades son interdependientes y críticos para el funcionamiento diario. Por lo tanto, es fundamental realizar un análisis de impacto que considere:

- Sistemas de Gestión de Aeropuertos: Estos sistemas son responsables de la coordinación de todas las actividades en el aeropuerto, desde la programación de vuelos hasta la gestión de recursos y servicios. Un fallo en estos sistemas podría resultar en retrasos significativos, pérdida de equipaje y, en casos extremos, comprometer la seguridad de los pasajeros y la tripulación.

- Sistemas de Control de Tráfico Aéreo: Los explotadores de aeronaves dependen de estos sistemas para recibir instrucciones y actualizaciones sobre el estado del tráfico aéreo. La interrupción de estos sistemas podría llevar a situaciones de riesgo, como colisiones en el aire o en la pista.

b) Clasificación de Riesgos: La clasificación de riesgos es un componente clave en la evaluación de la criticidad. Este proceso implica:

- Identificación de Amenazas: Evaluar las amenazas potenciales que podrían afectar a los sistemas, como ataques cibernéticos, fallos técnicos o desastres naturales. Por ejemplo, un ataque de ransomware que comprometa el sistema de gestión de vuelos podría paralizar las operaciones del aeropuerto.

- Evaluación de Vulnerabilidades: Analizar las debilidades en los sistemas actuales que podrían ser explotadas por atacantes. Esto incluye la revisión de configuraciones de seguridad, la falta de actualizaciones de software y la capacitación insuficiente del personal.

- Determinación del Impacto: Asignar un nivel de impacto a cada sistema en función de las consecuencias de un posible compromiso. Los sistemas que afectan directamente la seguridad de los vuelos y la gestión de emergencias deben clasificarse como de alta criticidad.

La evaluación de la criticidad de los sistemas utilizados por el Explotador de Aeropuertos y los Explotadores de Aeronaves es un proceso integral que permite identificar y priorizar los riesgos asociados a la ciberseguridad.

2.3. IDENTIFICACIÓN DE DEPENDENCIAS

En el contexto de la Seguridad de la Aviación Civil, la identificación de dependencias entre los sistemas utilizados por el explotadores y proveedores de servicios es fundamental para protegerse contra actos de interferencia ilícita. Estos actos pueden incluir desde el acceso no autorizado a sistemas críticos hasta amenazas físicas que puedan comprometer la seguridad de las operaciones aéreas. Comprender estas dependencias permite anticipar y mitigar riesgos que podrían afectar la integridad y la seguridad de la aviación.

a) Interacción de Sistemas Críticos: Los sistemas utilizados por estas entidades son interdependientes y deben trabajar en conjunto para garantizar la seguridad. Ejemplos de estas interacciones incluyen:

- Sistemas de Control de Acceso: El Explotador de Aeropuertos utiliza sistemas de control de acceso para gestionar quién puede ingresar a áreas restringidas, como las pistas y las zonas de embarque. Estos sistemas dependen de información precisa y actualizada sobre el estado de los vuelos, que es proporcionada por los sistemas de gestión de vuelos de los explotadores de aeronaves. Si el sistema de control de acceso falla o se ve comprometido, puede permitir el acceso no autorizado a áreas sensibles, poniendo en riesgo la seguridad del aeropuerto y de las aeronaves.

- Sistemas de Vigilancia y Monitoreo: Las cámaras de seguridad y otros sistemas de vigilancia son esenciales para detectar actividades sospechosas en el aeropuerto. Estos sistemas dependen de la información que proporcionan el Explotador de Aeropuertos sobre la programación de vuelos y las operaciones en curso. Si hay un fallo en la comunicación de esta información, puede dar lugar a una vigilancia inadecuada y a la posibilidad de que se lleven a cabo actos ilícitos sin ser detectados.

b) Dependencias en la Comunicación y Coordinación: La Seguridad de la Aviación Civil requiere una comunicación efectiva y una coordinación entre las entidades. Las dependencias en este ámbito incluyen:

- Sistemas de Alerta y Respuesta a Incidentes: En caso de un acto de interferencia ilícita, como un intento de secuestro o un ataque terrorista, es vital que exista un sistema de alerta que notifique a las autoridades pertinentes de inmediato. Los explotadores de aeronaves deben tener acceso a información en tiempo real sobre cualquier amenaza potencial, lo que les permite tomar decisiones rápidas y efectivas. Cualquier interrupción en la comunicación entre los sistemas de alerta y los explotadores puede retrasar la respuesta y aumentar el riesgo para la seguridad.

- Protocolos de Emergencia: La coordinación entre el Explotador de Aeropuertos y los Explotadores de Aeronaves es esencial para llevar a cabo procedimientos de emergencia en caso de un incidente de seguridad. Esto incluye desde la evacuación de pasajeros hasta el manejo de situaciones en las que se detecta un objeto sospechoso. Si la información sobre la situación de seguridad no es compartida de manera oportuna y efectiva, se pueden producir confusiones que pongan en peligro a los pasajeros y al personal.

c) Dependencias en la Protección Física y Tecnológica: La defensa contra actos de interferencia ilícita también implica la protección de los sistemas tecnológicos que soportan las operaciones en el aeropuerto:

- Sistemas de Gestión de Seguridad: Estos sistemas permite al Explotador de Aeropuertos gestionar y coordinar todos los aspectos de la seguridad de las instalaciones, incluyendo la protección contra amenazas internas y externas. La efectividad de estos sistemas depende de la información proporcionada por los Explotadores de Aeronaves sobre amenazas potenciales, como pasajeros conflictivos o comportamientos sospechosos. Un fallo en la comunicación o en los sistemas de gestión puede resultar en una respuesta inadecuada a una amenaza.

- Integración de Tecnologías de Seguridad: La integración de tecnologías avanzadas, como el reconocimiento facial y la biometría, es cada vez más común en los aeropuertos. Estas tecnologías dependen de sistemas de información que proporcionan datos sobre los pasajeros y su historial. Cualquier interrupción en la integridad de estos sistemas puede comprometer la capacidad de identificar y prevenir actos de interferencia ilícita.

d) Evaluación del Impacto en la Seguridad: La identificación de dependencias también debe incluir una evaluación del impacto que podría tener la interrupción de un sistema crítico en la seguridad general de la aviación civil. Por ejemplo:

- Fallo en los Sistemas de Control de Acceso: Si el sistema de control de acceso se compromete, no solo podría facilitar la entrada de individuos no autorizados, sino que también podría poner en riesgo la integridad de la aeronave y de los pasajeros. Esto podría resultar en un ataque físico o en un acto de sabotaje.

- Interrupción de Sistemas de Comunicación: Si los sistemas de comunicación entre el Explotador de Aeropuertos y los explotadores de aeronaves sufren un fallo, puede haber una falta de información sobre amenazas potenciales, lo que podría resultar en una respuesta inadecuada ante un acto de interferencia ilícita

La identificación de dependencias en los sistemas utilizados por las entidades es vital para fortalecer la Seguridad de la Aviación Civil y protegerse contra actos de interferencia ilícita. Al comprender cómo estos sistemas interactúan y dependen unos de otros, las organizaciones pueden anticipar y mitigar riesgos, lo que contribuye a un entorno de aviación más seguro y confiable. Este enfoque proactivo en la identificación y gestión de dependencias no solo protege a los pasajeros y al personal, sino que también refuerza la confianza del público en la seguridad de la aviación.

2.4. INVOLUCRAMIENTO DE PARTES INTERESADAS

El involucramiento de diversas partes interesadas es fundamental para garantizar la Seguridad de la Aviación Civil, en la protección contra actos de interferencia ilícita. La colaboración entre diferentes grupos garantiza que se aborden todos los aspectos de la seguridad y que se implementen medidas efectivas para prevenir y responder a amenazas potenciales. A continuación, se detalla cómo cada parte interesada contribuye a este objetivo.

a) Explotador de Aeropuertos: El Explotador de Aeropuertos es responsable de la operación y gestión de las instalaciones aeroportuarias y tienen un papel clave en la implementación de medidas de seguridad. Su involucramiento incluye:

- Desarrollo de Políticas de Seguridad: Participan en la creación de políticas y procedimientos para la seguridad aeroportuaria, asegurando que se alineen con la reglamentación nacional, internacional y las mejores prácticas en la protección contra actos de interferencia ilícita.

- Gestión de Sistemas de Seguridad Física: Son responsables de la implementación y supervisión de sistemas de seguridad, como controles de acceso, vigilancia y patrullaje. Esto incluye la evaluación de tecnologías avanzadas, como el reconocimiento facial y la detección de intrusos, para mejorar la seguridad de las instalaciones.

- Entrenamiento y Concientización: Deben asegurar que el personal del aeropuerto reciba capacitación adecuada sobre los protocolos de seguridad y cómo reconocer comportamientos sospechosos. Esto es crucial para detectar y prevenir actos de interferencia ilícita antes de que ocurran.

b) Explotadores de Aeronaves: Los explotadores de aeronaves, incluidos pilotos, tripulaciones y personal de mantenimiento, también juegan un papel fundamental en la seguridad de la aviación. Su participación incluye:

- Comunicación de Amenazas: Deben estar capacitados para informar cualquier comportamiento sospechoso observado durante las operaciones, ya sea en tierra o en vuelo, a las autoridades pertinentes. Esta comunicación es esencial para la detección temprana de posibles actos de interferencia ilícita.

- Implementación de Protocolos de Seguridad: Los explotadores deben seguir estrictamente los procedimientos de seguridad establecidos, incluyendo los protocolos de verificación de pasajeros y carga. Esto ayuda a garantizar que no se introduzcan elementos peligrosos en las aeronaves.

- Coordinación con Administradores de Aeropuertos: Es esencial que los Explotadores de Aeronaves trabajen conjuntamente con el Explotador de Aeropuertos para asegurar que se implementen las medidas de seguridad adecuadas y que haya una respuesta coordinada ante incidentes de seguridad.

c) Dirección General de Aeronáutica Civil: La DGAC, es responsable de establecer normativas y fiscalizar su cumplimiento. Su involucramiento incluye:

- Establecimiento de Estándares de Seguridad: La autoridad desarrolla y actualiza estándares de seguridad que el Explotador de Aeropuertos y Explotadores de Aeronaves deben seguir para protegerse contra actos de interferencia ilícita.

- Actividades de Fiscalización: Realizan actividades de fiscalización periódicas para evaluar la efectividad de las medidas de seguridad en los aeropuertos y en las aeronaves, proporcionando recomendaciones para mejorar la protección.

El involucramiento de las diversas partes interesadas es fundamental para garantizar una evaluación exhaustiva de la criticidad de los sistemas utilizados en la aviación civil. Al aprovechar los conocimientos y perspectivas de cada grupo, se puede obtener una visión integral de los riesgos y dependencias, lo que permite desarrollar estrategias de ciberseguridad más efectivas y adaptadas a las necesidades específicas de la industria aeronáutica.

CAPÍTULO 3. PROTECCIÓN DE SISTEMAS DE TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN CRÍTICOS

La protección de los sistemas de tecnologías de la información y la comunicación (TIC) críticos es fundamental para salvaguardar la Seguridad de la Aviación Civil. Un enfoque integral de protección no solo implica medidas técnicas, sino también políticas, procedimientos y prácticas de capacitación. A continuación, se detallan las estrategias y medidas que pueden implementarse para proteger estos sistemas vitales.

3.1. SEGURIDAD PERIMETRAL

La seguridad perimetral es la primera línea de defensa para proteger los sistemas TIC contra accesos no autorizados y ataques cibernéticos.

a) Firewalls: Los firewalls son dispositivos de seguridad que controlan el tráfico de red permitiendo o bloqueando conexiones según reglas predefinidas. Los firewalls de próxima generación (NGFW) van más allá de las capacidades de filtrado de puertos y protocolos; ofrecen funciones avanzadas como inspección profunda de paquetes, detección de intrusiones y filtrado de contenido. Es vital que estos firewalls se configuren adecuadamente para responder a las amenazas específicas del entorno de aviación, asegurando que se bloqueen los accesos no autorizados y que se monitoricen las actividades sospechosas.

b) Sistemas de Detección y Prevención de Intrusiones (IDS/IPS): Un IDS monitoriza el tráfico de la red en busca de patrones que indiquen actividades maliciosas. Por otro lado, un IPS no solo detecta estas actividades, sino que también puede tomar medidas para bloquear ataques en tiempo real. La implementación de ambos sistemas proporciona una defensa en profundidad, permitiendo a los administradores de seguridad recibir alertas sobre posibles incidentes y responder de manera adecuada antes de que se produzca un daño significativo.

c) Segmentación de Redes: La segmentación de redes implica dividir la red de la organización en varios segmentos o zonas de seguridad. Esto limita el acceso a sistemas críticos y datos sensibles, asegurando que, incluso si un atacante logra infiltrarse en un segmento, no pueda moverse fácilmente a otros sistemas críticos. Por ejemplo, los sistemas de control de tráfico aéreo pueden estar en un segmento separado de los sistemas de gestión de pasajeros, lo que ayuda a contener cualquier intrusión.

3.2. CONTROLES DE ACCESO

Los controles de acceso son esenciales para garantizar que solo los usuarios autorizados puedan acceder a sistemas críticos y datos sensibles.

a) Autenticación Multifactor (MFA): La MFA agrega una capa adicional de seguridad al requerir que los usuarios proporcionen dos o más formas de verificación antes de acceder a los sistemas. Esto puede incluir algo que saben (una contraseña), algo que tienen (un token o teléfono móvil) y algo que son (biometría como huellas digitales). La implementación de MFA reduce significativamente el riesgo de accesos no autorizados.

b) Control de Acceso Basado en Roles (RBAC): Este enfoque limita el acceso a información y sistemas según el rol del usuario dentro de la organización. Al definir roles específicos y asignar permisos de acceso basados en esos roles, se minimiza el riesgo de que empleados no autorizados accedan a datos sensibles o realicen acciones inapropiadas.

c) Revisión Periódica de Permisos: Realizar auditorías regulares de los permisos de acceso es esencial para garantizar que los empleados tengan acceso solo a la información necesaria para realizar sus funciones. Esto implica revocar permisos que ya no sean pertinentes, especialmente cuando un empleado cambia de función o deja la organización.

3.3. CIFRADO DE DATOS

El cifrado de datos es una medida crítica para proteger la información sensible, tanto en tránsito como en reposo.

a) Cifrado en Tránsito: El cifrado en tránsito implica proteger los datos mientras se transfieren entre diferentes sistemas, dispositivos o redes. Esto se puede lograr utilizando protocolos seguros como TLS (Transport Layer Security) o HTTPS (Hypertext Transfer Protocol Secure). Al cifrar los datos en tránsito, se evita que sean interceptados y leídos por atacantes durante su transmisión, lo que es particularmente importante en comunicaciones entre aeronaves y centros de control.

b) Cifrado en Reposo: El cifrado en reposo se refiere a la protección de los datos almacenados en servidores, bases de datos o dispositivos de almacenamiento. Esto asegura que, incluso si un atacante logra acceder al sistema, no podrá leer la información sin la clave de cifrado. Las organizaciones deben utilizar algoritmos de cifrado robustos y gestionar las claves de manera segura para proteger la información crítica.

c) Gestión de Claves: La gestión de claves es un componente esencial del cifrado. Las claves de cifrado deben almacenarse de manera segura y sus accesos deben ser restringidos solo al personal autorizado. La rotación regular de claves, el uso de hardware seguro para el almacenamiento de claves y la auditoría de su uso son prácticas recomendadas que ayudan a mantener la seguridad de los datos cifrados.

3.4. ACTUALIZACIONES Y PARCHES

Mantener los sistemas actualizados es una de las estrategias más efectivas para protegerse contra vulnerabilidades conocidas.

a) Política de Gestión de Parches: La creación de una política de gestión de parches que defina cómo y cuándo se aplicarán actualizaciones de software es crucial. Esta política debe incluir la identificación de sistemas críticos que requieren atención inmediata y la programación de parches regulares para otros sistemas. Las actualizaciones deben aplicarse tan pronto como sea posible, especialmente en respuesta a la divulgación de nuevas vulnerabilidades.

b) Monitoreo de Vulnerabilidades: Utilizar herramientas de escaneo de vulnerabilidades permite a las organizaciones identificar debilidades en el software y hardware utilizados. Esto incluye evaluar configuraciones inseguras, software desactualizado y otros problemas que requieren atención. Las auditorías de seguridad regulares también deben realizarse para identificar y remediar vulnerabilidades.

3.5. RESILIENCIA OPERATIVA

La resiliencia operativa garantiza que la organización pueda continuar funcionando incluso en caso de un incidente de ciberseguridad.

a) Redundancia de Sistemas: La implementación de sistemas redundantes permite que, en caso de fallo de un sistema crítico, haya otros en funcionamiento que puedan tomar el relevo. Esto es crucial para minimizar el tiempo de inactividad y asegurar la continuidad de las operaciones. Por ejemplo, los sistemas de control de tráfico aéreo pueden tener sistemas de respaldo que se activen automáticamente en caso de un fallo.

b) Pruebas de Recuperación ante Desastres: Las pruebas de recuperación ante desastres son esenciales para garantizar que los procedimientos de respuesta estén actualizados y que el personal esté preparado para actuar en caso de un incidente. Esto incluye simulaciones de recuperación de datos y la restauración de sistemas críticos para evaluar la eficacia de los planes y la capacitación del personal.

3.6. CAPACITACIÓN DEL PERSONAL

El personal es a menudo el eslabón más débil en la cadena de seguridad. Por lo tanto, la capacitación y la concienciación son fundamentales.

a) Programas de Concienciación en Ciberseguridad: Desarrollar e implementar programas de capacitación continua para todos los empleados es esencial. Estos programas deben enfocarse en las mejores prácticas de ciberseguridad, la identificación de amenazas y la respuesta a incidentes. Esto puede incluir talleres, seminarios y sesiones de capacitación en línea, adaptados a las necesidades específicas de cada puesto dentro de la organización.

b) Simulacros de Phishing: Realizar simulacros de ataques de phishing ayuda a educar a los empleados sobre cómo reconocer y manejar correos electrónicos y enlaces sospechosos. Al enfrentarse a situaciones simuladas, los empleados se vuelven más conscientes y menos propensos a caer en trampas de ingeniería social. La retroalimentación posterior a estos simulacros es fundamental para mejorar el conocimiento y la preparación del personal.

3.7. AUDITORÍAS Y CUMPLIMIENTO

Las auditorías de seguridad son esenciales para evaluar la efectividad de las medidas de seguridad implementadas.

a) Auditorías de Seguridad: Llevar a cabo auditorías de seguridad periódicas permite evaluar el estado de la organización. Estas auditorías deben incluir pruebas de penetración y evaluaciones de vulnerabilidad, así como revisiones de políticas y procedimientos. La implicación de auditores externos puede aportar una visión objetiva y aportar mejores prácticas del sector.

b) Cumplimiento Normativo: Asegurarse de que todas las prácticas de ciberseguridad cumplan con las regulaciones y estándares de la industria es esencial. Esto incluye seguir las directrices de la Organización de Aviación Civil Internacional (OACI), así como las normativas locales de protección de datos. La falta de cumplimiento puede resultar en sanciones y daños a la reputación de la organización

3.8. GESTIÓN DE RIESGOS

La gestión de riesgos es un componente crítico de la ciberseguridad que permite a las organizaciones identificar, analizar y mitigar riesgos.

a) Evaluación de Riesgos: Realizar evaluaciones de riesgo periódicas es esencial para identificar las amenazas y vulnerabilidades que pueden afectar a los sistemas TIC. Esto incluye analizar el impacto potencial y la probabilidad de ocurrencia de diferentes tipos de amenazas. Herramientas de análisis de riesgos pueden ayudar a priorizar los riesgos y asignar recursos para abordarlos.

b) Planificación de Mitigación: Desarrollar planes de mitigación específicos para abordar los riesgos identificados. Esto implica establecer estrategias para reducir la probabilidad de que un ataque ocurra y para minimizar su impacto en caso de que se produzca. La planificación de mitigación debe ser un proceso dinámico que se ajuste a medida que cambian las amenazas y el entorno operativo.

La protección de los sistemas de tecnologías de la información y la comunicación críticos es un elemento esencial para garantizar la seguridad de la aviación civil. Al implementar medidas robustas de seguridad perimetral, controles de acceso, cifrado de datos, actualizaciones regulares, resiliencia operativa, capacitación del personal y auditorías de cumplimiento, las organizaciones pueden reducir significativamente el riesgo de ciberataques y proteger la integridad de sus operaciones. Este enfoque proactivo y multifacético es crucial para mantener la confianza en la seguridad de la aviación y salvaguardar tanto a los pasajeros como a la infraestructura esencial.

CAPÍTULO 4. DETECCIÓN DE CIBERATAQUES MEDIANTE UN SISTEMA DE MONITOREO CONTINUO DE LA SEGURIDAD DE LA INFORMACIÓN (ISCM)

La detección temprana de ciberataques es fundamental para mitigar su impacto en la Seguridad de la Aviación Civil. Un Sistema de Monitoreo Continuo de la Seguridad de la Información (ISCM) permite a las organizaciones monitorear, detectar y responder a amenazas cibernéticas en tiempo real. Este sistema se basa en la recopilación y análisis de datos de seguridad, lo que proporciona una visión integral del estado de la seguridad de la información.

4.1. COMPONENTES CLAVE DEL ISCM

a) Monitoreo en Tiempo Real: La implementación de herramientas de monitoreo que analicen el tráfico de red y la actividad de los sistemas críticos es esencial. Esto incluye el uso de sistemas de gestión de eventos e información de seguridad (SIEM), que recopilan y correlacionan datos de diferentes fuentes para identificar patrones de comportamiento anómalos que puedan indicar un ataque.

b) Análisis de Logs: Los registros de eventos (logs) son una fuente valiosa de información para la detección de ciberataques. El análisis regular de estos registros permite identificar accesos no autorizados, intentos de intrusión y otras actividades sospechosas. Las organizaciones deben establecer políticas para la retención y análisis de logs, asegurando que se revisen de manera sistemática.

c) Alertas Automatizadas: Configurar sistemas de alertas que notifiquen al equipo de seguridad sobre incidentes potenciales es crucial. Estas alertas deben ser personalizables y basadas en umbrales específicos que reflejen el contexto operativo de la organización. La capacidad de recibir alertas en tiempo real permite una respuesta rápida y efectiva ante incidentes.

d) Inteligencia de Amenazas: Integrar información sobre amenazas emergentes y vulnerabilidades conocidas es fundamental para mejorar la detección. Esto puede incluir el uso de feeds de inteligencia de amenazas que proporcionen datos sobre nuevas tácticas, técnicas y procedimientos (TTP) utilizados por los atacantes. La inteligencia de amenazas ayuda a ajustar las defensas y a priorizar las respuestas.

e) Análisis de Comportamiento: Implementar tecnologías de análisis de comportamiento puede ayudar a identificar actividades inusuales que podrían indicar un ataque. Esto incluye el uso de algoritmos de aprendizaje automático que analizan patrones de uso normal y detectan desviaciones que podrían ser indicativas de un compromiso.

4.2. PROCESO DE IMPLEMENTACIÓN DEL ISCM

a) Evaluación de Necesidades: Antes de implementar un ISCM, es esencial realizar una evaluación de las necesidades de seguridad de la organización. Esto incluye identificar los sistemas críticos, las amenazas potenciales y los recursos disponibles para la implementación.

b) Selección de Herramientas: Elegir las herramientas adecuadas para el monitoreo y análisis es crucial. Las soluciones deben ser escalables y capaces de integrarse con los sistemas existentes. Es importante considerar tanto las capacidades técnicas como la facilidad de uso y la capacidad de personalización.

c) Desarrollo de Políticas y Procedimientos: Establecer políticas claras sobre el uso del ISCM, incluyendo la gestión de incidentes, la respuesta a alertas y la escalación de problemas. Estas políticas deben ser comunicadas a todo el personal involucrado en la seguridad de la información.

d) Capacitación del Personal: Proporcionar capacitación adecuada al personal sobre el uso del ISCM y la interpretación de alertas es fundamental. El personal debe estar familiarizado con los procedimientos de respuesta a incidentes y cómo utilizar las herramientas de monitoreo de manera efectiva.

e) Pruebas y Ajustes: Una vez implementado, el ISCM debe ser probado regularmente para evaluar su efectividad. Esto incluye simulaciones de incidentes y revisiones de los procedimientos de respuesta. Los ajustes deben realizarse en función de los resultados de estas pruebas y de la evolución del panorama de amenazas.

4.3. BENEFICIOS DEL ISCM EN LA SEGURIDAD DE LA AVIACIÓN CIVIL

a) Detección Temprana: La capacidad de detectar ciberataques en sus primeras etapas permite a las organizaciones responder rápidamente, minimizando el impacto en la Seguridad de la Aviación Civil en las operaciones.

b) Mejora Continua: Un ISCM proporciona datos valiosos que pueden utilizarse para mejorar continuamente las políticas y procedimientos de seguridad. La retroalimentación obtenida a través del monitoreo y análisis ayuda a identificar áreas de mejora.

c) Cumplimiento Normativo: La implementación de un ISCM puede ayudar a las organizaciones a cumplir con las regulaciones y estándares de seguridad de la información, lo que es especialmente importante en la industria de la aviación, donde la Seguridad de la Aviación Civil es primordial.

d) Confianza del Público: Al demostrar un compromiso con la ciberseguridad y la capacidad de responder a incidentes, las organizaciones pueden aumentar la confianza de los pasajeros y otras partes interesadas en la Seguridad de la Aviación Civil de sus operaciones.

La implementación de un Sistema de Monitoreo Continuo de la Seguridad de la Información (ISCM) es esencial para la detección proactiva de ciberataques en la aviación civil. Al establecer un enfoque integral que incluya monitoreo en tiempo real, análisis de logs, alertas automatizadas, inteligencia de amenazas y análisis de comportamiento, las organizaciones pueden fortalecer su postura de seguridad y responder de manera efectiva a las amenazas cibernéticas. La inversión en un ISCM no solo protege los sistemas críticos, sino que también contribuye a la resiliencia y confianza en la seguridad de la aviación.

CAPÍTULO 5. RESPUESTA A CIBERATAQUES

La respuesta a ciberataques es un componente crítico de la ciberseguridad en la aviación civil. Dado el potencial impacto de un ataque cibernético en la seguridad de los vuelos, la integridad de los datos y la confianza del público, es esencial contar con un plan de respuesta bien estructurado y efectivo. Este plan debe ser capaz de abordar incidentes de manera rápida y eficiente, minimizando el daño y restaurando las operaciones normales lo más pronto posible.

5.1. PREPARACIÓN PARA LA RESPUESTA

La preparación es la clave para una respuesta efectiva a ciberataques. Esto implica establecer un equipo de respuesta a incidentes (IRT) que esté capacitado y listo para actuar en caso de un ataque.

a) Formación del Equipo de Respuesta: El equipo debe incluir personal de diversas áreas, como IT, seguridad, operaciones y comunicaciones. Cada miembro debe tener roles y responsabilidades claramente definidos. La capacitación regular en ciberseguridad y simulacros de incidentes son esenciales para mantener al equipo preparado.

b) Desarrollo de un Plan de Respuesta a Incidentes: Este plan debe detallar los procedimientos a seguir en caso de un ciberataque. Debe incluir protocolos para la detección, contención, erradicación, recuperación y comunicación. La claridad en los procedimientos ayuda a reducir la confusión y a acelerar la respuesta.

5.2. DETECCIÓN E IDENTIFICACIÓN

La detección temprana de un ciberataque es crucial para mitigar su impacto. Esto se logra mediante el uso de herramientas de monitoreo y análisis.

a) Monitoreo Continuo: Implementar un Sistema de Monitoreo Continuo de la Seguridad de la Información (ISCM) permite detectar anomalías en el tráfico de red y en el comportamiento de los sistemas. Las alertas automatizadas pueden notificar al equipo de seguridad sobre actividades sospechosas.

b) Análisis de Incidentes: Una vez que se detecta un posible ataque, es fundamental realizar un análisis inicial para determinar la naturaleza y el alcance del incidente. Esto incluye identificar qué sistemas están comprometidos y qué datos pueden haber sido afectados.

5.3. CONTENCIÓN

La contención es el proceso de limitar el impacto del ataque y evitar que se propague a otros sistemas.

a) Aislamiento de Sistemas Afectados: Una vez identificado el sistema comprometido, debe ser aislado de la red para evitar que el ataque se extienda. Esto puede implicar desconectar el sistema de la red o desactivar ciertos servicios.

b) Implementación de Medidas de Contención: Dependiendo del tipo de ataque, pueden ser necesarias medidas específicas de contención. Por ejemplo, en un ataque de ransomware, puede ser necesario bloquear el acceso a archivos críticos o deshabilitar cuentas de usuario comprometidas.

5.4. ERRADICACIÓN

Una vez que el ataque ha sido contenido, el siguiente paso es erradicar la amenaza de los sistemas afectados.

a) Eliminación de Malware: Utilizar herramientas de seguridad para eliminar cualquier malware o software malicioso que haya sido instalado durante el ataque. Esto puede incluir la ejecución de análisis completos del sistema y la eliminación de archivos sospechosos.

b) Restauración de Sistemas: Después de eliminar la amenaza, es importante restaurar los sistemas a su estado normal. Esto puede implicar la restauración de datos desde copias de seguridad y la reinstalación de software afectado.

5.5. RECUPERACIÓN

La recuperación implica restaurar las operaciones normales y asegurar que los sistemas estén funcionando de manera segura.

a) Verificación de la Integridad de los Sistemas: Antes de volver a poner en línea los sistemas afectados, es crucial verificar que estén libres de amenazas y que funcionen correctamente. Esto puede incluir pruebas de funcionalidad y revisiones de seguridad.

b) Monitoreo Post-Incidente: Después de la recuperación, se debe continuar monitoreando los sistemas para detectar cualquier actividad inusual que pueda indicar que el ataque no ha sido completamente erradicado.

5.6. COMUNICACIÓN

La comunicación efectiva durante y después de un ciberataque es esencial para mantener la confianza de las partes interesadas.

a) Comunicación Interna: Mantener informados a todos los empleados sobre la situación y las acciones que se están tomando. Esto ayuda a reducir la incertidumbre y a asegurar que todos estén alineados en la respuesta.

b) Comunicación Externa: Informar a las partes interesadas externas, como reguladores, clientes y medios de comunicación, sobre el incidente. La transparencia es clave para mantener la confianza del público. Se deben preparar mensajes claros que expliquen la situación y las medidas adoptadas para abordar el incidente.

5.7. ANÁLISIS POST-INCIDENTE

Después de que se ha gestionado un ciberataque, es fundamental realizar un análisis exhaustivo para aprender de la experiencia.

a) Revisión del Incidente: Evaluar cómo se gestionó el ataque, qué medidas fueron efectivas y qué áreas necesitan mejora. Esto incluye revisar el tiempo de respuesta, la efectividad de la contención y la recuperación.

b) Identificación de Vulnerabilidades: Determinar qué brechas de seguridad permitieron que el ataque tuviera éxito. Esto puede incluir la revisión de políticas de seguridad, configuraciones de sistemas y prácticas de capacitación del personal.

c) Actualización de Protocolos: Basado en el análisis post-incidente, actualizar el plan de respuesta a incidentes y las políticas de seguridad. Esto asegura que la organización esté mejor preparada para futuros ataques.

d) Capacitación Continua: Utilizar las lecciones aprendidas para reforzar la capacitación del personal y mejorar la preparación general de la organización frente a ciberataques.

La respuesta a ciberataques en la aviación civil es un proceso complejo que requiere una preparación meticulosa, una detección rápida y una gestión efectiva de incidentes. Al establecer un plan de respuesta bien estructurado y capacitar al personal adecuadamente, las organizaciones pueden minimizar el impacto de los ciberataques y garantizar la Seguridad de la Aviación Civil en las operaciones. La comunicación clara y el análisis post-incidente son esenciales para aprender de cada experiencia y fortalecer la postura de seguridad en el futuro.

CAPÍTULO 6. PLAN DE COMUNICACIONES PARA SITUACIONES DE CRISIS

En el contexto de la ciberseguridad en la aviación civil, un plan de comunicaciones efectivo para situaciones de crisis es fundamental para gestionar la información y mantener la confianza de todas las partes interesadas. La forma en que una organización comunica un ciberataque puede influir en la percepción pública, la reputación de la empresa y la efectividad de la respuesta al incidente. Un plan de comunicaciones bien estructurado debe abordar tanto la comunicación interna como la externa, garantizando que la información fluya de manera oportuna y precisa.

6.1. DEFINICIÓN DE ROLES Y RESPONSABILIDADES

La claridad en los roles y responsabilidades es esencial para una comunicación eficaz durante una crisis.

a) Equipo de Gestión de Crisis: Designar un equipo de gestión de crisis que sea responsable de la coordinación de la comunicación durante un ciberataque. Este equipo debe incluir miembros de alta dirección, comunicaciones, relaciones públicas y seguridad de la información.

b) Portavoz Oficial: Nombrar un portavoz oficial que se encargue de comunicar información a los medios de comunicación y otras partes interesadas. Este portavoz debe estar bien informado sobre el incidente y capacitado para manejar preguntas difíciles.

c) Red de Contacto Interna: Crear una red de contacto interna que incluya a los líderes de cada departamento. Estos líderes deben ser responsables de comunicar información relevante a sus equipos y asegurar que todos estén alineados en el mensaje.

6.2. PROTOCOLOS DE COMUNICACIÓN

Los protocolos claros son necesarios para guiar la comunicación antes, durante y después de un ciberataque.

a) Evaluación Inicial del Incidente: Establecer un protocolo para evaluar el incidente y determinar la naturaleza y el alcance del ataque. Esto incluye la recopilación de hechos y la verificación de la información antes de comunicarla.

b) Mensajes Clave: Desarrollar mensajes clave que se utilizarán durante la crisis. Estos mensajes deben ser claros, concisos y adaptados a diferentes audiencias (empleados, medios de comunicación, reguladores, etc.). Ejemplos de mensajes clave pueden incluir:

- Confirmación de que se ha detectado un incidente.
- Aseguramiento de que se están tomando medidas para mitigar el impacto.
- Información sobre cómo se están protegiendo los datos de los clientes y empleados.

6.3. COMUNICACIÓN INTERNA

La comunicación interna es crucial para mantener la moral y la confianza del personal durante una crisis.

a) Notificación a Empleados: Establecer un sistema para informar a todos los empleados sobre el incidente. Esto puede incluir correos electrónicos, reuniones virtuales o mensajes a través de plataformas de comunicación interna. La comunicación debe ser honesta y directa, proporcionando detalles sobre lo que se sabe del incidente y las medidas que se están tomando.

b) Actualizaciones Regulares: Proporcionar actualizaciones regulares a los empleados sobre el progreso de la respuesta al incidente. Esto ayuda a mantener a todos informados y minimiza la propagación de rumores. Las actualizaciones deben ser programadas y comunicadas de manera consistente.

c) Canales de Retroalimentación: Crear canales para que los empleados puedan hacer preguntas y expresar preocupaciones. Esto puede incluir reuniones de preguntas y respuestas, correos electrónicos directos al equipo de gestión de crisis o foros internos donde se puedan discutir inquietudes.

6.4. COMUNICACIÓN EXTERNA

La comunicación externa es vital para gestionar la percepción pública y la reputación de la organización.

a) Declaración Pública Inicial: Emitir una declaración pública inicial tan pronto como se confirme el incidente. Esta declaración debe confirmar que se ha producido un ataque, describir brevemente la naturaleza del mismo y asegurar a las partes interesadas que se están tomando medidas para abordarlo.

b) Gestión de Medios: Establecer una estrategia de gestión de medios que incluya el monitoreo de la cobertura mediática y la preparación de respuestas a preguntas anticipadas. La estrategia debe incluir la identificación de los medios de comunicación clave y un enfoque proactivo para comunicar actualizaciones.

c) Actualizaciones a las Partes Interesadas: Informar a las partes interesadas externas, como clientes, proveedores y reguladores, sobre el incidente y las acciones que se están tomando. Esto puede incluir correos electrónicos, boletines informativos y publicaciones en redes sociales.

6.5. MENSAJES CLAVE DURANTE LA CRISIS

Desarrollar mensajes clave que aborden las preocupaciones más comunes de las partes interesadas.

a) Compromiso con la Seguridad: Reiterar el compromiso de la organización con la seguridad de la información y la protección de los datos de los clientes. Asegurarse de que las partes interesadas comprendan que la organización está tomando el incidente muy en serio.

b) Acciones Correctivas: Comunicar las acciones específicas que se están tomando para abordar el incidente, como la investigación en curso, la implementación de medidas de contención y la colaboración con expertos en ciberseguridad.

c) Compensación y Apoyo: Si corresponde, informar a los clientes y empleados sobre cualquier compensación o apoyo que se ofrecerá como resultado del incidente. Esto puede incluir servicios de monitoreo de crédito, asistencia para la recuperación de datos o líneas de ayuda.

6.6. EVALUACIÓN POST-CRISIS

Después de que se haya gestionado la crisis, es importante evaluar la efectividad de la comunicación.

a) Análisis de la Respuesta de Comunicación: Revisar cómo se gestionó la comunicación durante la crisis. Identificar qué mensajes fueron efectivos, qué áreas podrían mejorarse y cómo se percibió la comunicación por parte de las partes interesadas.

b) Ajustes a Políticas y Procedimientos: Basado en el análisis, ajustar el plan de comunicaciones para futuras crisis. Esto puede incluir la actualización de mensajes clave, la revisión de protocolos de comunicación y la mejora de la capacitación del personal en gestión de crisis.

c) Lecciones Aprendidas: Documentar las lecciones aprendidas y compartirlas con el equipo de gestión de crisis y el personal relevante. Esto ayudará a fortalecer la capacidad de respuesta de la organización en futuros incidentes.

Un plan de comunicaciones bien estructurado para situaciones de crisis es esencial para gestionar la respuesta a ciberataques que comprometan la Seguridad de la Aviación Civil. Al definir roles claros, establecer protocolos de comunicación y mantener informadas a las partes interesadas, las organizaciones pueden mitigar el impacto de un incidente y mantener la confianza de empleados, clientes y reguladores. La evaluación continua y el aprendizaje de cada experiencia son claves para mejorar la respuesta y la comunicación en futuras crisis.

CAPÍTULO 7. ANÁLISIS POSTERIOR A LOS EVENTOS

El análisis posterior a los eventos es una etapa crucial en la gestión de ciberataques, especialmente en el contexto de la aviación civil, donde la seguridad, la confianza y la continuidad operativa son de suma importancia. Este proceso implica una revisión exhaustiva de los eventos relacionados con el ciberataque, y su objetivo es identificar lecciones aprendidas, evaluar la efectividad de la respuesta y ajustar las estrategias de seguridad para prevenir futuros incidentes.

7.1. REVISIÓN DEL INCIDENTE

La revisión del incidente es el primer paso en el análisis posterior. Este proceso debe ser metódico y documentado.

a) Recopilación de Información: Reunir toda la información relevante sobre el ataque, incluyendo registros de seguridad, alertas de monitoreo, comunicaciones internas y cualquier dato recopilado durante la respuesta. Esto incluye detalles sobre cómo se detectó el ataque, el tiempo de respuesta, las acciones tomadas y la duración del incidente.

b) Línea de Tiempo del Incidente: Crear una línea de tiempo que documente los eventos desde la detección inicial del ataque hasta su contención y recuperación. Esto ayuda a visualizar el flujo del incidente y a identificar puntos críticos donde se podrían haber tomado decisiones diferentes.

7.2. EFECTIVIDAD DE LA RESPUESTA

Evaluar la efectividad de la respuesta al incidente es esencial para entender qué funcionó y qué no.

a) Análisis de la Respuesta: Revisar cada etapa de la respuesta al incidente: detección, contención, erradicación y recuperación. Evaluar los tiempos de respuesta y la eficacia de las acciones tomadas en cada fase. Identificar si se siguieron los protocolos establecidos y si hubo desviaciones que afectaron el resultado.

b) Evaluación del Equipo de Respuesta: Analizar el desempeño del equipo de respuesta a incidentes. Esto incluye revisar la comunicación interna, la toma de decisiones y la colaboración entre diferentes departamentos. Identificar si hubo obstáculos que impidieron una respuesta más ágil y efectiva.

7.3. IDENTIFICACIÓN DE VULNERABILIDADES

El análisis posterior debe centrarse en identificar las vulnerabilidades que permitieron que el ataque tuviera éxito.

a) Análisis de Fallas de Seguridad: Revisar las configuraciones de seguridad de los sistemas afectados y determinar si había vulnerabilidades conocidas que no se habían mitigado. Esto incluye la revisión de políticas de acceso, configuraciones de red y parches de seguridad.

b) Revisión de Recursos y Capacidades: Evaluar si la organización contaba con los recursos adecuados (tecnológicos y humanos) para gestionar el incidente. Esto incluye la revisión de herramientas de detección, capacidades de monitoreo y la formación del personal en ciberseguridad.

7.4. DOCUMENTACIÓN Y REPORTE

La documentación es una parte esencial del análisis posterior, ya que proporciona un registro detallado que puede ser utilizado para futuras referencias y mejoras.

a) Informe Post-Incidente: Elaborar un informe detallado que incluya un resumen del incidente, la respuesta dada, las lecciones aprendidas y las recomendaciones para mejorar la seguridad. Este informe debe ser accesible para los miembros relevantes de la organización y, si es necesario, para las partes interesadas externas.

b) Presentación a la Alta Dirección: Preparar una presentación para la alta dirección que resuma los hallazgos más importantes del análisis posterior. Esta presentación debe destacar las implicaciones para la organización y cualquier acción que se requiera para mejorar la postura de seguridad.

7.5. IMPLEMENTACIÓN DE MEJORA CONTINUA

El objetivo final del análisis posterior es implementar mejoras que refuercen la ciberseguridad de la organización.

a) Actualización de Políticas y Procedimientos: Basado en las lecciones aprendidas, revisar y actualizar las políticas y procedimientos de seguridad. Esto puede incluir cambios en el plan de respuesta a incidentes, ajustes en las prácticas de ciberseguridad y mejoras en la capacitación del personal.

b) Pruebas de Estrategias Mejoradas: Realizar simulacros y ejercicios de respuesta a incidentes que integren las lecciones aprendidas del análisis posterior. Esto ayuda a asegurar que el personal esté familiarizado con los nuevos procedimientos y que la organización esté mejor preparada para futuros incidentes.

c) Monitoreo de Resultados: Establecer métricas para evaluar la efectividad de las mejoras implementadas. Esto puede incluir la reducción del tiempo de respuesta a incidentes, la disminución del número de vulnerabilidades detectadas y la mejora en la formación del personal.

7.6. CULTURA DE CIBERSEGURIDAD

Fomentar una cultura de ciberseguridad es esencial para el éxito a largo plazo de las estrategias de seguridad.

a) Capacitación Continua: Implementar programas de capacitación regular para todos los empleados, centrados en la ciberseguridad y la gestión de incidentes. Asegurarse de que todos comprendan su papel en la protección de la organización contra ciberamenazas.

b) Promoción de la Conciencia de Seguridad: Fomentar una cultura en la que los empleados se sientan cómodos reportando incidentes y preocupaciones de seguridad. Esto puede incluir la creación de canales de comunicación donde los empleados puedan informar sobre actividades sospechosas sin temor a represalias.

El análisis posterior a los eventos es un componente esencial de la gestión de ciberataques en relación a la Seguridad de la Aviación Civil. Al realizar una revisión exhaustiva del incidente, evaluar la efectividad de la respuesta, identificar vulnerabilidades y documentar los hallazgos, las organizaciones pueden aprender de cada experiencia y fortalecer su postura de ciberseguridad. La implementación de mejoras continuas y la promoción de una cultura de ciberseguridad son claves para asegurar un entorno operativo más seguro en el futuro.