Organización de Aviación Civil Internacional
Oficina Regional Sudamericana
Décimo Séptima Reunión de Autoridades de Aviación Civil de la Región Sudamericana (RAAC/17)
(Santiago, Chile, 10 al 14 de abril de 2023)

Cuestión 1A del Orden del Día: **Situación regional y sus prioridades**

EVALUAR DOCUMENTO TÉCNICO DE CIBERSEGURIDAD PARA LA AVIACIÓN CIVIL

(Nota presentada por Chile)

RESUMEN

La presente nota tiene como objetivo presentar a la RAAC/17, una propuesta de un documento técnico que contemple los fundamentos generales de ciberseguridad en base a los cuales deben ser diseñadas, instaladas y operadas de manera segura las redes y sistemas utilizados para la prestación de servicios aeronáuticos regulados, que sirva de guía para que los Estados SAM puedan establecer un marco regulatorio sobre esta materia.

Referencias:

- Estrategia de ciberseguridad de la aviación
- Plan de acción de ciberseguridad
- Norma ISO 27001:2022
- Norma ISO 27002:2022
- Norma ISO 27035-1:2016

Objetivos Estratégicos de la OACI:	*Seguridad de la Aviación y Facilitación*

1. Introducción

1.1 La tendencia actual en la gestión del sistema aeronáutico nacional e internacional, se está dirigiendo de manera rápida a cambios e integración producto de la transformación digital y el aumento de necesidad de un mayor intercambio de información, la creación de una conciencia común, con un amplio espectro de partes interesadas en la aviación sin duda puede mejorar la eficiencia de las operaciones y aumenta la productividad, pero es aquí también donde se abre el potencial para propiciar un ataque cibernético.

1.2 Atendiendo a que las vulnerabilidades están creciendo debido a que los sistemas actuales y de próxima generación, requieren más intercambio de información al usar la tecnología disponible comercialmente, tales como redes compartidas e infraestructuras informáticas, arquitecturas y operaciones centradas en redes, y que a diferencia del pasado, el intercambio de información en el futuro no se limitará a las comunicaciones punto a punto, ya que también utilizará la arquitectura de sistemas abiertos y el flujo de información basado en Internet. Que los sistemas de control de las distintas áreas de operación han experimentado una tendencia hacia un mayor uso de las tecnologías existentes, una creciente

interoperabilidad entre los sistemas y el uso de la automatización para mejorar la productividad, donde la identificación de amenazas son una pieza clave en el tratamiento de riesgo que se debe desarrollar para cada una de estas. Los servicios fijos aeronáuticos por sus siglas en ingles AFS, establecen una serie de amenazas identificadas, tales como: inundación de información, interceptación pasiva de información, interceptación activa de información, modificación de la configuración o los datos del sistema, destrucción de la configuración de los sistemas, ataques de interrupción o denegación de servicio.

2. Discusión

2.1 Se invita a los Estados a discutir la creación de un documento técnico que funcione como base para incluir en los programas nacionales de seguridad de la aviación civil (NCASP) y otros programas nacionales pertinentes, disposiciones apropiadas para proteger los mencionados sistemas críticos, incluidos sus soportes físicos y lógicos, contra ciberataques e interferencia.

3. Acción sugerida

3.1 Se invita a la RAAC/17 a:

a) Tomar conocimiento de esta nota de estudio y Apéndice A; y
b) analizar, comentar, la propuesta presentada en el Apéndice A.

- - - - -

APÉNDICE A

DOCUMENTO TÉCNICO DE CIBERSEGURIDAD PARA LA AVIACIÓN

Titulo I. Disposiciones Generales

1. Objeto

La presente norma técnica tiene por objeto establecer un marco regulatorio que comprenda los fundamentos generales de ciberseguridad en base a los cuales deben ser diseñadas, instaladas y operadas de manera segura las redes y sistemas utilizados para la prestación de servicios aeronáuticos regulados. Lo anterior, habida consideración al resguardo y a la resiliencia de las redes, sistemas y su continuidad operacional, confidencialidad, integridad y disponibilidad de la información.

La presente norma cubre aspectos de gestión de riesgo en materias de ciberseguridad en el ámbito de los servicios aeronáuticos regulados por la Ley, identificando tanto el análisis de impacto operacional como los riesgos y controles mitigantes; además del ciclo de vida de una ciberincidencia, considerando tanto la prevención, detección, análisis, notificación, contención, erradicación, recuperación y documentación a su respecto.

De igual manera, este busca establecer lineamientos para los reportes sobre ciberincidencias que los operadores y empresas de servicios aeronáuticos deben enviar a la autoridad competente, sea directamente o a través del órgano que ésta indique, con el objeto de coordinar las acciones orientadas a mitigar sus efectos e impactos y contribuir a una oportuna normalización y estabilización de los servicios afectados.

2. **Definiciones**

Para los efectos de aplicación de esta norma técnica, los términos que a continuación se señalan tendrán el significado que se indica:

- ✓ Autenticación:

Proceso utilizado en los mecanismos de control de acceso con el objetivo de verificar la identidad de un usuario, dispositivo o sistema mediante la comprobación de credenciales de acceso.

- ✓ Ciberespacio:

Dominio global y dinámico dentro del entorno de la información que corresponde al ambiente compuesto por las infraestructuras tecnológicas, los componentes lógicos de la información, los datos (almacenados, procesados o transmitidos) que abarcan los dominios físico, virtual y cognitivo y las interacciones sociales que se verifican en su interior.

Las infraestructuras tecnológicas corresponden a los equipos materiales empleados para la transmisión de las comunicaciones, tales como enlaces, enrutadores, conmutadores,

estaciones, sistemas radiantes, nodos, conductores, entre otros. Los componentes lógicos de la información, en tanto, son los diferentes softwares que permiten el funcionamiento, administración y uso de la red.

- ✓ Ciberincidencia o ciberincidente:

Todo evento que comprometa la disponibilidad, autenticidad, integridad o confidencialidad de los sistemas o datos informáticos almacenados, transmitidos o procesados, o los servicios correspondientes ofrecidos por los sistemas de información y su infraestructura, que puedan afectar al normal funcionamiento de los mismos.

- ✓ Ciberseguridad:

Conjunto de acciones posibles para la prevención, mitigación, investigación y manejo de las amenazas e incidentes sobre los activos de información, datos y servicios, así como para la reducción de los efectos de los mismos y del daño causado antes, durante y después de su ocurrencia.

- ✓ Ciberataque:

Cualquier incidente cibernético, provocado deliberadamente y que afecte a un sistema informático.

- ✓ Confidencialidad:

Principio de seguridad que requiere que los datos deberían únicamente ser accedidos por el personal autorizado a tal efecto.

- ✓ Disponibilidad:

Capacidad de ser accesible y estar listo para su uso a demanda de una entidad autorizada.

- ✓ Integridad:

Principio de seguridad que certifica que los datos y elementos de configuración sólo son modificados por personal y actividades autorizadas. La Integridad considera todas las posibles causas de modificación, incluyendo fallos software y hardware, eventos medioambientales e intervención humana.

- ✓ Centro Coordinador de Respuestas ante Incidentes de Seguridad Informática:

Centros conformados por especialistas capacitados para coordinar respuesta ante incidentes de ciberseguridad, en forma rápida y efectiva.

- ✓ Gestión de incidentes:

Procedimientos para la detección, análisis, manejo, contención y resolución de una incidencia de ciberseguridad y responder ante ésta.

- ✓ Incidente:

Evento inesperado o no deseado con consecuencias en detrimento de la seguridad de las redes y sistemas de información aeronáuticos.

- ✓ Infraestructura crítica Aeronáutica de información:

Las instalaciones, redes, servicios y equipos físicos y de tecnología de la información cuya afectación, degradación, denegación, interrupción o destrucción pueden tener una repercusión importante en la seguridad operacional o el bienestar económico de los ciudadanos o en el eficaz funcionamiento del Estado.

- ✓ Neutralidad tecnológica:

Principio regulatorio conforme el cual las normas técnicas destinadas a limitar las externalidades negativas de una actividad deben describir el resultado que se logrará, pero otorgando a los regulados libertad para adoptar la tecnología más apropiada para lograr el resultado, asimismo, implica aplicar unos mismos principios reguladores indistintamente de qué tecnología es utilizada y que la regulación no sea usada como un medio para impulsar el mercado hacia una estructura particular que el regulador considera óptima.

- ✓ No repudio:

Servicio de seguridad que provee al emisor y receptor de los datos de una prueba del origen y destino de los mismos, que puede usarse ante intentos del emisor o receptor de negar su remisión.

- ✓ Resiliencia:

Capacidad de los sistemas o redes para seguir operando pese a estar sometidos a un incidente o ciberataque, aunque sea en un estado degradado, debilitado o segmentado. Así como, incluye la capacidad de restaurar con presteza sus funciones esenciales después de un incidente o ataque de modo de recuperarse con presteza de una interrupción, por lo general con un efecto reconocible mínimo.

- ✓ Riesgo:

Toda circunstancia o hecho razonablemente identificable que tenga un posible efecto adverso en la seguridad de las redes y sistemas de información de telecomunicaciones. Se puede cuantificar como la probabilidad de materialización de una amenaza que produzca un impacto en términos de operatividad, de integridad física de personas o material o de imagen corporativa.

Cualquier otro término no definido en esta norma técnica tendrá el significado que se le atribuya en la respectiva normativa sectorial de Aeronáutica

3. Ámbito de aplicación

Esta norma tiene su alcance en:

- ✓ Explotadores de Terminales Aéreos.
- ✓ Explotador del Terminal Aéreo de Carga.
- ✓ Explotadores de Aeronaves.
- ✓ Empresas de Servicios, que operan en Aeródromos y Aeropuertos.
- ✓ Prestadores de servicios Aeronáuticos

4. Declaración de relevancia

El entorno operacional de la aviación civil cambia rápida y significativamente con la introducción de nuevas tecnologías avanzadas y sistemas de comunicación que pasan de procedimientos manuales a procedimientos, comunicaciones y archivo automatizados más eficaces, con miras a reforzar la seguridad y la facilitación.

Los explotadores aeronáuticos, incluidos los explotadores de aeronaves y aeropuertos, los proveedores de servicios de tránsito aéreo y otros, deberían determinar los soportes lógicos y físicos de los sistemas críticos de información utilizados en sus operaciones, que pueden abarcar, entre otros, los sistemas siguientes utilizados para:

- control del acceso y vigilancia de alarmas;
- control de salidas;
- cotejo del equipaje con los pasajeros;
- inspección o detección de explosivos, mediante sistemas parte de una red o autónomos;
- bases de datos sobre agentes acreditados y expedidores reconocidos;
- gestión del tránsito aéreo;
- reservas de los explotadores y presentación de los pasajeros;
- vigilancia mediante televisión en circuito cerrado; y
- mando, control y despacho en materia de seguridad.

Constituyen puntos vulnerables posibles el uso de los mencionados sistemas, el mayor número de conexiones o enlaces entre los sistemas terrestres y las aeronaves, así como el uso de soportes lógicos y físicos adquiridos en el comercio, La seguridad de los pasajeros, la tripulación y el personal de tierra se pondría en peligro en caso de interferencia con dichos sistemas. Además, la información personal sobre pasajeros y empleados debería protegerse contra acceso y uso no autorizados.

Artículo 5°. Obligaciones generales de Ciberseguridad
El objetivo de la presente norma sectorial, es incluir en los programas nacionales de seguridad de la aviación civil (NCASP) y otros programas nacionales pertinentes, disposiciones apropiadas para proteger los mencionados sistemas críticos, incluidos sus soportes físicos y lógicos, contra ciberataques e interferencia.

A. Protección de Sistemas Críticos de Información

La protección material de los sistemas críticos de información de la DGAC debe iniciarse en la etapa de diseño o lo antes posible para asegurarse de que sean lo más resilientes posible a ciberataques. Esto puede lograrse aplicando un método de niveles múltiples, lo que supone, entre otras cosas:

- controles administrativos, tales como:

- ✓ normas, políticas y procedimientos de seguridad;
- ✓ contratación, selección e instrucción apropiadas del personal, particularmente las personas con derechos a título de administradores, incluidas verificaciones de antecedentes;
- ✓ evaluación de amenazas y riesgos para determinar la vulnerabilidad de un sistema y la probabilidad de un ataque;
- ✓ control de calidad, incluidas inspecciones y pruebas; y
- ✓ seguridad de la cadena de suministro de soportes físicos y lógicos;

- controles virtuales o lógicos, tales como:

  - ✓ cortafuegos;
  - ✓ cifrado de datos;
  - ✓ sistema de detección de intrusión en las redes; y
  - ✓ sistemas antivirus.

- controles materiales, tales como:

  - ✓ asegurarse de que los soportes físicos del sistema, particularmente los servidores, estén debidamente protegidos y situados en áreas con acceso controlado;
  - ✓ implantar sistemas de autentificación, tales como métodos de registro biométrico o contraseñas, que permiten limitar el acceso al sistema exclusivamente a personas autorizadas;
  - ✓ limitar el número de personas con acceso autorizado;
  - ✓ exigir más de una persona para las aprobaciones dentro de los sistemas, por ejemplo, producir permisos de identificación de aeropuerto sólo si los autorizan dos personas;
  - ✓ vigilar y controlar el acceso a los sistemas de manera permanente;
  - ✓ utilizar sistemas de contingencia remotos en caso de pérdida del sistema principal; y
  - ✓ mantener registros de actividades que pueden servir para auditorías y evaluaciones y proporcionar alertas en caso de actividades fuera de los parámetros operacionales normales.

La protección de los sistemas críticos de TIC aeronáuticas, incluidos sus soportes físicos y lógicos y sus datos, deberían incluirse en los procedimientos de evaluación de amenazas establecidos.

La DGAC exigirá que los explotadores evalúen la vulnerabilidad de sus sistemas de TIC aeronáuticas, establezcan medidas para hacer frente a posibles ciberataques y verificar la aplicación de tales medidas como parte de sus actividades regulares de vigilancia del cumplimiento, tales como inspecciones y auditorías.

B. Medidas de seguridad para la infraestructura

- Seguridad mediante el diseño

  - ✓ La DGAC asegurará de que los explotadores incluyan medidas de seguridad en el diseño, implantación y operación de nuevos sistemas de tecnología de la información y las comunicaciones aeronáuticas, incluida la eliminación de soportes físicos y lógicos. En las modificaciones a los sistemas existentes, en la medida de lo posible, se deben aplicar estas medidas. Así, si esto se aplica desde las primeras etapas, serán más apropiados el diseño y la construcción de instalaciones de explotadores de aeropuertos y aeronaves, tales como mostradores de presentación y embarque o de venta de billetes, puestos de inspección y centros de carga y logística para suministros aeroportuarios.
  - ✓ En las especificaciones relativas a nuevos sistemas de TIC aeronáuticas y su adquisición deben figurar disposiciones de seguridad. Los proveedores deben proporcionar información sobre la manera en que se protege la información y la operación del sistema, incluidos arreglos para apoyo y mantenimiento continuos, sea en el mismo lugar o a distancia. Debe programarse y administrarse mantenimiento preventivo; si el apoyo y el mantenimiento son objeto de contratación externa, debe limitarse el número de personas a las que se permita el acceso a los soportes lógicos y físicos del sistema. Asimismo, las vías para los cables deben diseñarse de modo que los sistemas críticos de información aeronáutica no puedan ser infiltrados fácilmente.

- Separación entre redes

  - ✓ La DGAC asegurará de que las redes utilizadas para sistemas críticos de TIC aeronáuticas estén separadas de las redes accesibles al público.
  - ✓ Los soportes lógicos y físicos de un sistema moderno de comunicación e información aeronáuticas no pueden funcionar sin los cables necesarios y la conexión a otra red de sistemas operacionales para facilitar la transmisión e intercambio de datos. Por dicho motivo, deben examinarse los sistemas para asegurarse de que no resulten comprometidos los objetivos de seguridad al quedar expuestos a redes de comunicaciones no controladas o de acceso libre; además, deben establecerse políticas y prácticas apropiadas para reducir a un mínimo las conexiones necesarias. Esta práctica recibe a menudo el nombre de “reforzamiento”.

- ✓ Las conexiones a redes deben efectuarse en condiciones controladas en que se conozcan el tipo de información y la frecuencia o método de intercambio de datos entre el sistema y la red. Debe establecerse un sistema de gestión eficaz para dichas interfaces a fin de asegurarse de que todas las conexiones a un sistema sean objeto de documentación, examen y actualización, según corresponda, y se cuente, de ser necesario, con protección adecuada contra virus y programas maliciosos ("malware").
- ✓ Debe considerarse un método de varios niveles para la gestión de soportes lógicos. Un número limitado de personas debe tener derechos a título de administradores de un sistema crítico de TIC aeronáuticas. El acceso al sistema debería basarse en el principio de necesidad legítima. Así, algunas personas podrían recibir únicamente derechos que se limiten a la lectura, mientras que otras podrían recibir autorización para tener acceso únicamente a las partes del sistema que se relacionen con sus tareas concretas.

- Acceso remoto
  - ✓ Se deberá asegurar de que sólo se permita el acceso remoto a sistemas críticos de TIC aeronáuticas en condiciones establecidas de antemano y seguras y de que los proveedores no tengan acceso no autorizado, una vez adquiridos o instalados dichos sistemas.
  - ✓ En la mayoría de los casos, el acceso remoto al sistema se exigirá que los proveedores tengan un medio apropiado para ello. Los explotadores deben asegurar de que están enterados de la vía de dicho acceso y de que están concientes del método y las condiciones de entrada.
  - ✓ Sólo el personal autorizado debe llevar a cabo el mantenimiento de los sistemas en los días y las horas establecidos de antemano y aprobados. Los explotadores deberían solicitar a los proveedores que limiten el número de personas autorizadas para proporcionar apoyo y mantenimiento del sistema. Dichas personas deberían ser objeto de verificación de antecedentes, incluidos los antecedentes penales en la medida en que lo permitan las leyes.
  - ✓ La DGAC podrá añadir a las medidas mencionadas una auditoría apropiada y un sistema de notificación de excepciones que genere un informe automático siempre que tenga lugar una actividad anormal en el sistema, tales como el acceso fuera de las horas normales de trabajo. Se examinarán regularmente los registros de auditoría para determinar el acceso excepcional y examinar sus circunstancias.

- ✓ La DGAC y los explotadores deberían solicitar un certificado de los proveedores en que se indique que no existe acceso por puertas traseras y garantizando la integridad del sistema. Esto sería útil en el caso de que sea necesario recurrir a enjuiciamiento.

C. Seguridad de la cadena de suministro para soportes físicos y lógicos

- Los sistemas de TIC aeronáuticas deben actualizarse periódicamente debido a los cambios en los requisitos operacionales o la modernización de soportes lógicos y a menudo exigen que se modifiquen los soportes lógicos o físicos.

- Se debe contar con medidas para asegurar de que se recurra únicamente a proveedores reconocidos y legítimos para adquirir soportes físicos y lógicos para los sistemas de TIC aeronáuticas. En la medida de lo posible, debe aplicarse el concepto de seguridad de la cadena de suministro. El objetivo de esta medida consiste en asegurar que la integridad de los soportes lógicos y físicos se proteja contra interferencia no autorizada en la totalidad de la cadena de suministro. Debe exigirse que los proveedores informen sobre sus propias medidas de seguridad no sólo en la etapa de instalación, sino también durante toda la vida útil del sistema.

D. Registros de incidentes de ciberataques

La comprensión de la amenaza y de los posibles métodos de ataque constituyen un elemento esencial en la elaboración de medidas de seguridad apropiadas para proteger los sistemas de TIC aeronáuticas contra ciberataques. Se deben adoptar diversas medidas para que esto sea eficaz, lo que abarca, entre otras cosas, lo siguiente:

- elaborar e implantar una plantilla para notificar incidentes de ciberataques. Esto facilitará la recopilación y análisis de información, incluida la evaluación de la amenaza, y la implantación de contramedidas apropiadas;
- establecer un sistema de alerta para facilitar la comunicación con los explotadores y otras parte interesadas; y
- establecer disposiciones para exigir que los explotadores implanten un régimen de notificación en sus organizaciones y lo incluyan en sus programas de seguridad.

E. Consideraciones de Ciberseguridad en la operación aeroportuaria

- Sistema de control de salidas

  - ✓ Los proveedores deberán garantizar la redundancia, sistemas de respaldo o protocolos de contingencia ante la falla del sistema de control de salida.
  - ✓ Los proveedores deben disponer de medios estándar para mitigar los ataques de denegación de servicio y proteger sus redes de intrusiones.

- Sistema de visualización de información de vuelo
  - ✓ Se debe impedir el acceso físico a los sistemas de visualización de información de vuelo a agentes no autorizados.
  - ✓ Las copias de seguridad físicas, anuncios o el despliegue de personal para dirigir a los pasajeros deben ser consideradas ante la falla de este sistema.

- Base de datos operacional del aeropuerto
  - ✓ Se debe garantizar la seguridad del control de acceso a la base de datos operacional, sólo se requerirá intervención humana cuando exista un mal funcionamiento de la misma.

- Sistema de manejo de equipaje

  - ✓ Estos sistemas instalados en diferentes terminales deberán estar segregados / separados
  - ✓ Se debe considerar la posibilidad de utilizar algunos elementos de forma aislada del sistema completo para restaurar el servicio parcialmente ante situaciones de contingencia (por ejemplo, operación manual de cintas transportadoras sin automatización completa / dirección del equipaje).

- Escáner de búsqueda en área principal
  - ✓ Se debe garantizar los controles de seguridad física, de software y de red del equipo de escaneo.
  - ✓ Si las máquinas se administran de forma remota, el grado de conectividad deberá ser aislado de otras redes y monitoreado de manera permanente.
  - ✓ Se deben implementar sistemas de detección en caso de fallas importantes y generalizadas del equipo.
  - ✓ Se debe garantizar la separación lógica o física de la infraestructura comercial / operativa en los entornos de mayor riesgo.

- ✓ Se deben implementar procedimientos de verificación del personal y prácticas y de seguridad para proteger el acceso a los equipos.
- ✓ Se debe establecer un procedimiento de actualización de la base de datos de este equipamiento.

- Sistema de control de acceso físico

  - ✓ Se deben implementar procedimientos de revisión de todo el personal con acceso a la zona de operaciones y controles de seguridad en el acceso a las áreas restringidas
  - ✓ Se deben implementar procedimientos para patrullas de seguridad y controles del perímetro físico, de manera permanente.

- Sistema de integración de edificios

  - ✓ Para la integración de los distintos edificios al interior de un aeropuerto, se deben implementar defensas de red robustas, protección perimetral, detección de intrusos, entre otros.

- Radar de movimiento terrestre

  - ✓ Se deben implementar controles de seguridad física para impedir la interrupción de las operaciones de la aeronave.

- Sistema de control y monitoreo de iluminación

  - ✓ Se deben implementar controles de seguridad física para impedir que las operaciones de las aeronaves se vean gravemente afectadas en determinados momentos del día.

5. Obligaciones de reportar ciberincidencias

A. **clasificación de incidentes**

	Clase de Incidente	**Tipo de Incidente**	**Descripción**
1	Contenido Abusivo	Pornografía Infantil – Sexual – Violencia	Pornografía infantil, glorificación de la violencia, otros.
		Spam	"Correo masivo no solicitado", lo que significa que el destinatario no ha otorgado permiso verificable para que el mensaje sea enviado y además el mensaje es enviado como parte de un grupo masivo de mensajes, todos teniendo un contenido similar.
		Difamación	Desacreditación o discriminación de alguien.
2	Código Malicioso	Malware, Virus, Gusanos, Troyanos, spyware, Dialer, rootkit	Software que se incluye o inserta intencionalmente en un sistema con propósito dañino. Normalmente, se necesita una interacción del usuario para activar el código.

3	Recopilación de Información	Scanning	Ataques que envían solicitudes a un sistema para descubrir puntos débiles. Se incluye también algún tipo de proceso de prueba para reunir información sobre hosts, servicios y cuentas. Ejemplos: fingerd, consultas DNS, ICMP, SMTP (EXPN, RCPT, …), escaneo de puertos.
		Sniffing	Observar y registrar el tráfico de la red (escuchas telefónicas o redes de datos).
		Ingeniería Social	Recopilación de información de un ser humano de una manera no técnica (por ejemplo, mentiras, trucos, sobornos o amenazas).
4	Intentos de Intrusión	Intentos de acceso	Múltiples intentos de inicio de sesión (adivinar / descifrar contraseñas, fuerza bruta).
		Explotación de vulnerabilidades conocidas	Un intento de comprometer un sistema o interrumpir cualquier servicio explotando vulnerabilidades conocidas que ya cuentan con su clasificación estandarizada CVE (por ejemplo, el búfer desbordamiento, puerta trasera, secuencias de comandos cruzadas, etc.).
		Nueva Firma de Ataque	Un intento de usar un exploit desconocido.
5	Intrusión	Compromiso de Cuenta Privilegiada	Un compromiso exitoso de un sistema o aplicación (servicio). Esto puede han sido causado de forma remota por una vulnerabilidad conocida o nueva, pero también por un acceso local no autorizado. También incluye ser parte de una botnet.
		Compromiso de Cuenta sin privilegios	
		Compromiso de Aplicación, Bot	
6	Disponibilidad	Ataque de denegación de servicio (DoS / DDoS)	Con este tipo de ataque, un sistema es bombardeado con tantos paquetes que las operaciones se retrasan o el sistema falla. Algunos ejemplos DoS son ICMP e inundaciones SYN, ataques de teardrop y bombardeos de mail's. DDoS a menudo se basa en ataques DoS que se originan en botnets, pero también existen otros escenarios como Ataques de amplificación DNS. Sin embargo, la disponibilidad también puede verse afectada por acciones locales (destrucción, interrupción del suministro de energía, etc.), fallas espontáneas o error humano, sin mala intención o negligencia.
		Sabotaje	
		Intercepción de información	
7	Información de seguridad de contenidos	Acceso no autorizado a la información	Además de un abuso local de datos y sistemas, la seguridad de la información puede ser en peligro por una cuenta exitosa o compromiso de la aplicación. Además, son posibles los ataques que interceptan y acceden a información durante la transmisión (escuchas telefónicas, spoofing o secuestro). El error humano / de configuración / software también puede ser la causa.
		Modificación no autorizada de la información	
8	Fraude	Phishing	Enmascarado como otra entidad para persuadir al usuario a revelar una credencial privada.
		Derechos de Autor	Ofrecer o instalar copias de software comercial sin licencia u otros materiales protegidos por derechos de autor (Warez).
		Uso no autorizado de recursos	Usar recursos para fines no autorizados, incluida la obtención de beneficios empresas (por ejemplo, el uso del correo electrónico para participar en cartas de cadena de ganancias ilegales) o esquemas piramidales).

		Falsificación de registros o identidad	Tipo de ataques en los que una entidad asume ilegítimamente la identidad de otro para beneficiarse de ello.
9	Vulnerable	Sistemas y/o softwares Abiertos	Sistemas “Open Resolvers”, impresoras abiertas a todo el mundo, vulnerabilidades aparentes detectadas con nessus u otros aplicativos, firmas de virus no actualizadas, etc.
10	Otros	Todos los incidentes que no encajan en alguna de las otras categorías dadas	Si la cantidad de incidentes en esta categoría aumenta, es un indicador de que el esquema de clasificación debe ser revisado.
11	Test	Para pruebas	Producto de pruebas de seguridad controladas e informadas.

B. Nivel de peligrosidad

El Nivel de peligrosidad determina la potencial amenaza que supondría la materialización de un incidente en las redes y sistemas del operador, así como para la calidad o continuidad de servicios prestados. Este indicador se fundamenta en las características intrínsecas a la tipología de amenaza.

Conforme sus características, las amenazas serán clasificadas con los siguientes niveles de peligrosidad: Crítico, Muy Alto, Alto, Medio y Bajo. El nivel asignado se determinará según se indica en la tabla a continuación:

Ilustración 2. Niveles de peligrosidad del ciberincidente

CRITERIOS DE DETERMINACIÓN DEL NIVEL DE PELIGROSIDAD		
Nivel	**Clasificación**	**Tipo de incidente**
CRÍTICO	Otros	**APT**
MUY ALTO	Código dañino	**Distribución de malware**
		Configuración de malware
	Intrusión	**Robo**
	Disponibilidad	**Sabotaje**
		Interrupciones

ALTO	Contenido abusivo	**Pornografía infantil, contenido sexual o violento inadecuado**
	Código dañino	**Sistema infectado**
		Servidor C&C (Mando y Control)
	Intrusión	**Compromiso de aplicaciones**
		Compromiso de cuentas con privilegios
	Intento de intrusión	**Ataque desconocido**
	Disponibilidad	**DoS (Denegación de servicio)**
		DDoS (Denegación distribuida de servicio)
	Compromiso de la información	**Acceso no autorizado a información**
		Modificación no autorizada de información
		Pérdida de datos
	Fraude	**Phishing**
MEDIO	Contenido abusivo	Discurso de odio
	Obtención de información	Ingeniería social
	Intento de intrusión	Explotación de vulnerabilidades conocidas
		Intento de acceso con vulneración de credenciales
	Intrusión	Compromiso de cuentas sin privilegios
	Disponibilidad	Mala configuración
	Fraude	Uso no autorizado de recursos
		Derechos de autor
		Suplantación
	Vulnerable	Criptografía débil
		Amplificador DDoS
		Servicios con acceso potencial no deseado
		Revelación de información

		Sistema vulnerable
BAJO	Contenido abusivo	Spam
	Obtención de información	Escaneo de redes (scanning)
		Análisis de paquetes (sniffing)

A. Nivel de impacto

Los criterios empleados para la determinación del nivel de impacto asociado a un ciberincidente atienden los parámetros que se indican a continuación, sin un orden de prelación o importancia predeterminado:

- ✓ Impacto en la Seguridad Nacional o en la Seguridad Ciudadana.
- ✓ Efectos en la prestación de un servicio de telecomunicaciones o en una infraestructura crítica.
- ✓ Tipología de la información o sistemas afectados.
- ✓ Grado de afectación a las instalaciones de la organización.
- ✓ Posible interrupción en la prestación del servicio normal de la organización.
- ✓ Tiempo y costes propios y ajenos hasta la recuperación del normal funcionamiento de las instalaciones.
- ✓ Pérdidas económicas.
- ✓ Extensión geográfica afectada.
- ✓ Daños reputacionales asociados.

Los posibles niveles de impacto de una ciberincidencia son Crítico, Muy Alto, Alto, Medio, Bajo o Sin Impacto. El nivel de impacto correspondiente se asignará usando como referencia la siguiente tabla:

NIVEL DE IMPACTO DE LOS CIBERINCIDENCIA	
Nivel	**Descripción**
	Afecta apreciablemente a la Seguridad Nacional.
	Afecta a la seguridad ciudadana, con potencial peligro para la vida de las personas.
	Afecta a una Infraestructura Crítica.

CRÍTICO	Afecta a sistemas clasificados SECRETO.
	Afecta a más del 90% de los sistemas de la organización.
	Interrupción en la prestación del servicio superior a 24 horas y superior al 50% de los usuarios.
	El ciberincidente precisa para resolverse más de 100 Jornadas-Persona.
	Impacto económico superior al 0,1% del P.I.B. actual.
	Extensión geográfica supranacional.
	Daños reputacionales muy elevados y cobertura continua en medios de comunicación internacionales.
MUY ALTO	Afecta a la seguridad ciudadana con potencial peligro para bienes materiales.
	Afecta apreciablemente a actividades oficiales o misiones en el extranjero.
	Afecta a un servicio esencial.
	Afecta a sistemas clasificados RESERVADO.
	Afecta a más del 75% de los sistemas de la organización.
	Interrupción en la prestación del servicio superior a 8 horas y superior al 35% de los usuarios.
	El ciberincidente precisa para resolverse entre 30 y 100 Jornadas-Persona.
	Impacto económico entre el 0,07% y el 0,1% del P.I.B. actual.
	Extensión geográfica superior a 4 CC.AA. o 1 T.I.S.
	Daños reputacionales a la imagen del país
	Daños reputacionales elevados y cobertura continua en medios de comunicación nacionales.
ALTO	Afecta a más del 50% de los sistemas de la organización.
	Interrupción en la prestación del servicio superior a 1 hora y superior al 10% de usuarios.
	El ciberincidente precisa para resolverse entre 5 y 30 Jornadas–Persona.

6. Artículo 8°. Contenidos de los Reportes

Los sujetos obligados por la presente norma, deberán reportar en tiempo y forma toda aquella información relativa a la ciberincidencia que sea exigible. Sin embargo, en el reporte inicial solamente deberá proporcionar la información que tenga en su conocimiento en ese momento, debiendo completarla en los reportes que envíe con posterioridad.

Los reportes de ciberincidencias deberán contener, a lo menos, los siguientes campos de
información:

- ✓ Resumen ejecutivo de la ciberincidencia.
- ✓ Identificación del operador relevante.
- ✓ Encargado de ciberseguridad en funciones.
- ✓ Fecha y hora precisas de ocurrencia de la ciberincidencia.
- ✓ Fecha y hora precisas de detección de la ciberincidencia.
- ✓ Descripción detallada de lo sucedido.
- ✓ Recursos tecnológicos afectados.
- ✓ Origen o causa identificable de la ciberincidencia.
- ✓ Taxonomía, clasificación o tipo de ciberincidencia.
- ✓ Nivel de peligrosidad.
- ✓ Nivel de impacto.
- ✓ Impacto transfronterizo, si corresponde.
- ✓ Indicadores de compromiso: indicadores de compromiso de nivel IP, indicadores de compromiso de nivel de dominios y subdominios, indicadores de compromiso de correos, indicadores de compromiso a nivel MD5, entre otros similares.
- ✓ Plan de acción y medidas de resolución y mitigación.
- ✓ Afectados actuales y potenciales.
- ✓ Medios necesarios para la resolución calculados en horas hombre (HH) / persona.
- ✓ Impacto económico estimado, si procede y es conocido.
- ✓ Extensión geográfica, si se conoce.
- ✓ Daños reputacionales, aun cuando sean eventuales.
- ✓ Las bitácoras generadas de forma automática por los sistemas.
- ✓ Antecedentes que se adjuntan, si procede.

En el caso particular de ciberincidencias que afecten o puedan afectar infraestructuras críticas, el reporte deberá indicar los motivos por los que un reporte no contiene toda la información pertinente, la que deberá ser enviada tan pronto como sea obtenida.

Para ciberincidentes que afecten a infraestructuras críticas o impacten sectores estratégicos, el operador deberá contratar un análisis independiente forense, indicando las medidas tomadas para su correcta mitigación y solución.

7. Artículo 9°. Oportunidad de los reportes

Los operadores que se vean afectados por una ciberincidencia deberán generar un reporte obligatorio, el cual deberá ser remitido en tiempo y forma, considerando un reporte inicial, reportes intermedios y un reporte final.

El reporte inicial es una comunicación consistente en poner en conocimiento y alertar de la existencia de una ciberincidencia.

Los reportes intermedios actualizan los datos disponibles en ese momento en relación a la ciberincidencia comunicada. Se efectuarán tantos reportes intermedios como se consideren necesarios a partir de la hora en que se generó el reporte inicial inmediato.

El reporte final amplía y confirma los datos definitivos en relación a la ciberincidencia reportada a partir del día en que se generó el reporte inicial inmediato.

El envío del reporte se realizará siempre que sea posible por escrito usando los medios indicados por DGAC para ello o, en caso de no estar disponibles, mediante correo electrónico, o en su defecto, por el medio más idóneo que se encuentre disponible.

Oportunidad de reportes obligatorios			
Nivel de peligrosidad	Reporte inicial	Reporte intermedio	Reporte final
Critico	Inmediato	3/ 6/ 12/ 24/ 48 horas	Máximo 10 días
Muy alto	Inmediato	48 / 72 horas	Máximo 20 días
alto	Inmediato	Sin plazo	Máximo 30 días

Los reportes deberán enviarse en forma oportuna y sucesiva conforme el desarrollo de la ciberincidencia, incorporando toda la información que sea pertinente y reportando cada cambio sustancial a medida que suceda. Además, el operador deberá aplicar las medidas de seguridad durante el proceso de transmisión de los reportes de incidencias.

Deberá mantenerse registro de la evolución de la ciberincidencia conforme su desarrollo y, en caso de que puedan afectar o se afecten infraestructuras críticas, el registro debe extenderse hasta que se hubiere cerrado, es decir, su completa resolución.

8. Tratamiento de los reportes

Los reportes de ciberincidencias serán tratados como documentación confidencial por los organismos del Estado que tomen conocimiento de ellos. En particular, en aquellos datos que pudiera exponer antecedentes técnicos propios del operador, que pongan en riesgo la ciberseguridad del operador, así como la información de clientes en conformidad a la legislación sobre protección de la vida privada.

9. Información a terceros e intercambio de información

En caso de reportar y/o alertar a terceros para prevenir, gestionar o resolver una ciberincidencia, el operador relevante podrá solicitar la asistencia del CSIRT de referencia u otro órgano designado por la autoridad competente para dichos efectos, si procediese. En caso de requerir apoyo de Equipos de Respuesta en el extranjero, el operador deberá velar por la privacidad y el debido resguardo de los datos involucrados.

Por su parte, la DGAC, el centro de coordinación de respuesta ante incidentes, o el órgano designado por DGAC para dichos fines, actuará en conformidad a las indicaciones que figuren en los reportes respecto del alcance que puede tener la difusión de la información que contiene conforme el estándar Traffic Light Protocol o TLP. En caso de estimarse que es necesario difundir la información a terceros más allá del

alcance de la designación TLP indicada por el autor del reporte, se requerirá autorización de la fuente original. En general, no se revelarán cualesquiera sean los datos que pudieran exponer antecedentes técnicos propios del operador, que pongan en riesgo la ciberseguridad del operador, así como cualquier información de sus usuarios, conforme lo dispuesto en ley sobre protección de la vida privada.
En caso de que se decida informar directamente al público o terceros, la publicación estará orientada a la entrega de información sobre las ciberincidencias, posibles causas, medidas de mitigación, recomendaciones de seguridad, alternativas de acciones a seguir, zonas geográficas o sistemas afectados y cualquier otra información de importancia para la correcta y oportuna información del público en general, sin que esto signifique afectaciones a la reputación de los involucrados.

Asimismo, conforme las atribuciones conferidas por la legislación aplicable, la DGAC adoptará medidas y efectuará gestiones orientadas a promover el intercambio de información en materias de seguridad física y de ciberseguridad de redes y sistemas de información entre actores públicos y privados, con el fin de que se adopten las medidas pertinentes en estas materias.

Título VI, Resolución de Ciberincidentes

10. Obligación de resolución de ciberincidentes

Una vez detectada una ciberincidencia que afecte a una red o sistema utilizado para la prestación de servicios de Aeronáuticos, el respectivo operador deberá efectuar de manera oportuna todas las gestiones que sean necesarias para su resolución y restaurar la normal provisión de los servicios afectados, con arreglo a su plan de gestión de riesgos y, en todos los casos, dando primera prioridad a aquellas medidas que permitan evitar o, en su defecto, minimizar el impacto a los usuarios finales.

En caso de que el operador afectado lo considere necesario para la resolución de una ciberincidencia, podrá solicitar cooperación a la DGAC u otras entidades competentes en materia de ciberseguridad, tales como el CSIRT de referencia señalado por DGAC u otros equipos de respuesta ante incidentes informáticos.

Los operadores deberán proporcionar la información adicional que les sea requerida para analizar la naturaleza, causas y efectos de los incidentes notificados, así como para elaborar estadísticas y reunir los datos necesarios para elaborar informes de resultados. La información adicional proporcionada será tratada con reserva y no será usada para fin alguno que sea distinto de los autorizados.

Asimismo, sin perjuicio de las medidas inmediatas conducentes a la mitigación de los efectos y al restablecimiento de los servicios afectados por una ciberincidencia, los operadores deberán subsanar, en la medida que sea técnicamente posible, según los respaldos fundados, las vulnerabilidades de sus sistemas que hubieren permitido o facilitado ciberincidencias.

En caso de que un operador detecte que sus redes y sistemas fueron utilizados como medio para la comisión de algún delito informático, el operador deberá formular las denuncias ante los órganos competentes, ejercer las acciones judiciales pertinentes e informar a DGAC.

Todo operador será responsable, previo proceso sustanciado de conformidad a la Constitución y las leyes, por las pérdidas o filtración de información que sea producto de su negligencia con respecto a la recepción, tenencia, manipulación, almacenamiento y entrega de la información que se transmite o deposita en custodia en los sistemas del proveedor, para garantizar la certeza, confidencialidad, seguridad y no repudiación de la comunicación.

El operador debe establecer los protocolos de recuperación de la información en caso de pérdida de esta por manipulación, ciberincidentes u otras causas de su responsabilidad.

11. Resguardo de datos personales y datos sensibles

Deberán omitirse en los reportes de ciberincidencias todo dato o información personal de carácter sensible, así como toda otra información a partir de la cual sea posible inferirlos. Asimismo, en los casos en que la autoridad competente instruya al operador para que envíe a un tercero una copia de un reporte, deberá eliminar todos los datos personales o que permitan deducir la identidad de la persona aludida.

En caso de que a partir del análisis de una ciberincidencia se advierta la ocurrencia de una posible vulneración de datos personales, el órgano designado para dicho fin, deberá remitir los informes pertinentes a la entidad a cargo de la protección de los datos personales competente. Junto con las secciones pertinentes de los reportes, se indicarán los motivos por los que pudo haber existido vulneración de datos personales conforme a la ley Nº 19.628.

En todos los casos, deberán considerarse las regulaciones de utilización de la información del usuario y su metadata, ya sea para beneficio propio del operador o de terceros, sin la expresa autorización del cliente, conforme lo establecido en el artículo 9º de la citada ley Nº19.628, sobre Protección de la Vida Privada y conforme los principios transversales de derechos humanos reconocidos por la comunidad internacional.

Título VII, Reportes obligatorios sobre modificación a las redes y sistemas

12. Reportes periódicos

Los operadores relevantes deberán enviar a DGAC, en forma directa o a través del órgano que ésta designe para dicho fin, reportes periódicos que den cuenta de las modificaciones introducidas en sus redes y sistemas, sean en la capa de software o en elementos de hardware, para dar solución a las vulnerabilidades detectadas en el último período informado. El período de los reportes será trimestral.

Las exigencias de reportes mencionadas anteriormente serán obligatorias semestralmente para los operadores no relevantes.

DGAC, utilizará la información proporcionada en los reportes periódicos únicamente con fines estadísticos y para estudios destinados a la formulación de políticas.

Título VIII, Reportes no obligatorios

13. Reportes no obligatorios

Los proveedores xxxxxxxxx que no sean considerados operadores relevantes podrán enviar reportes de ciberincidencias a DGAC, al CSIRT de referencia o al órgano designado para dichos fines. Asimismo, todo proveedor de servicios de telecomunicaciones podrá reportar sobre ciberincidencias que no alcancen los umbrales de información obligatoria especificados en el artículo 7º. En cualquier caso, todo reporte de ciberincidencia obligará al operador respectivo a proseguir reportando el desarrollo de ésta, si así correspondiere conforme la presente norma técnica, y a gestionar su resolución.

Por su parte, las autoridades competentes podrán ponderar de diversa manera la prioridad con que se gestionen los informes no obligatorios en relación con los obligatorios.

Título IX, Supervisión de seguridad

14. Supervisión de seguridad

Los operadores relevantes deberán mantener permanentemente actualizados los planes de gestión de riesgos de las redes y sistemas de telecomunicaciones que utilizan para la prestación de los servicios autorizados. Dichos planes deberán formularse de forma que permitan anticipar consecuencias derivadas de amenazas tales como ciberataques y ciberincidencias no hostiles, en base a un análisis y evaluación de los riesgos a los cuales se exponen sus redes y sistemas, con el objetivo de evitar o reducir la ocurrencia de tales contingencias y mitigar sus eventuales efectos, indicando acciones inmediatas y medidas progresivas de mejoras, con sus respectivos indicadores, controles y documentación.

Asimismo, los operadores relevantes deberán someter regularmente sus redes y sistemas de telecomunicaciones a pruebas de seguridad, con la frecuencia que corresponda de acuerdo al plan de riesgo aprobado y sancionado por su alta **dirección.** Las pruebas podrán ser efectuadas por los operadores en forma interna, o bien, con asistencia por parte de terceros externos especializados en dichos servicios, con la opción de solicitar la cooperación y asesoría de la autoridad competente en materia de ciberseguridad. En todo caso, deberán efectuarse conforme estándares actualizados, sean nacionales o internacionales, o bien, conforme criterios ampliamente aceptados por la industria de las telecomunicaciones. Deberá dejarse constancia de las pruebas efectuadas, los estándares aplicados, los resultados obtenidos y las medidas adoptadas en consecuencia.

Las pruebas de seguridad y simulacros de ciberseguridad deberán considerar, a lo menos, las siguientes actividades de control y documentación:

- ✓ Actualización de la última versión del Plan de Gestión de Riesgo.
- ✓ Identificación y ordenación de las medidas técnicas para la gestión de riesgo.
- ✓ Elaboración del conjunto de pruebas de seguridad a realizar, identificando la
- ✓ infraestructura física y lógica a utilizar.
- ✓ Descripción detallada de cada prueba o simulación, el procedimiento de ejecución y los medios de evidencia o verificación del cumplimiento satisfactorio de las pruebas.
- ✓ Descripción detallada de las actividades o medidas y procedimientos de restauración para la continuidad operacional y de servicio.
- ✓ Verificación de la consistencia y seguridad del almacenamiento de los logs o registros que evidencien los incidentes de ciberseguridad y otros datos tales como direcciones, puertos, aplicaciones, contenidos, datos transmitidos, mensajes de los sistemas sometidos a pruebas o simulación de ciberataque o incidente de ciberseguridad.
- ✓ Preparar un reporte con el resultado de las pruebas o simulaciones de seguridad, con medios de verificación apropiados.

La DGAC, en forma directa o a través del órgano designado para dicho fin, podrá requerir a los operadores relevantes toda la información acerca de las redes y sistemas que utilizan y que sea necesaria para evaluar su vulnerabilidad, incluyendo su plan de gestión de riesgos, los resultados de las pruebas de seguridad y, en general, todo otro tipo de antecedentes relacionados con políticas de seguridad de sus redes y sistemas.

Título X, Disposiciones finales

15. Fiscalización

16. Sanciones

17. Entrada en vigencia

CONTROL DE CAMBIOS

Fecha	Versión	Creado por	Páginas Modificadas	Descripción