CIRCULAR OBLIGATORIA

CO SA 17.18/24

QUE ESTABLECE LOS REQUISITOS MÍNIMOS DE CIBERSEGURIDAD QUE DEBERÁN IMPLEMENTAR LAS PERSONAS CONCESIONARIAS, ASIGNATARIAS Y PERMISIONARIAS DEL TRANSPORTE AÉREO, AERÓDROMOS CIVILES, Y PRESTADORES DE SERVICIOS AEROPORTUARIOS Y COMPLEMENTARIOS PARA PREVENIR ACTOS DE INTERFERENCIA ILÍCITA PERPETRADOS MEDIANTE MEDIOS DE ATAQUE REMOTOS, CIBERNÉTICOS, INFORMÁTICOS Y/O TECNOLÓGICOS.

09 de febrero 2024

CIRCULAR OBLIGATORIA

Que establece los requisitos mínimos de ciberseguridad que deberán implementar los concesionarios y permisionarios del transporte aéreo, aeródromos civiles, y prestadores de servicios aeroportuarios y complementarios para prevenir actos de interferencia ilícita perpetrados mediante medios de ataque remotos, cibernéticos, informáticos y/o tecnológicos.

1. OBJETIVO

La presente Circular Obligatoria, tiene como objetivo principal establecer y estandarizar los requisitos mínimos de ciberseguridad que deberán implementar las personas concesionarias, asignatarias y permisionarias del transporte aéreo, aeródromos civiles, y prestadores de servicios aeroportuarios y complementarios para prevenir actos de interferencia ilícita perpetrados mediante medios de ataque remotos, cibernéticos, informáticos y/o tecnológicos.

2. FUNDAMENTO LEGAL

La presente Circular Obligatoria, es emitida con fundamento en los artículos 1, 17, 18, 26 y 36 fracciones IV, V, y XXVII de la Ley Orgánica de la Administración Pública Federal; 2, fracciones I, XVIII, XXXII y XXXIII, 6 Bis, fracciones III, XVIII, XLV, XLVI y LI, 17, 33, 34, 78 Octies, 78 Decies y 78 Undecies de la Ley de Aviación Civil; 2, fracción VII Ter; 6 Bis, fracciones, III, XII, XIII, XIV y XXI y 73 BIS de la Ley de Aeropuertos; 44, 46, 47 y 109 fracción IX del Reglamento de la Ley de Aviación Civil; 151 y 152 fracción XI del Reglamento de la Ley de Aeropuertos; 1°, 10, fracciones V y XXIV y 37 del Reglamento Interior de la Secretaría de Comunicaciones y Transportes; 1, 2, 3 y 4 del Decreto por el que se crea el órgano administrativo desconcentrado de la Secretaría de Comunicaciones y Transportes, denominado Agencia Federal de Aviación Civil, publicado en el Diario Oficial de la Federación el 16 de octubre de 2019, y la Circular de Asesoramiento CO DET-1.01/24 "Que establece los Lineamientos para la Elaboración y Publicación de Disposiciones Técnico Administrativas, Circulares de Asesoramiento y Cartas de Política a Cargo de la Agencia Federal de Aviación Civil", se emite la presente Circular Obligatoria.

3. APLICABILIDAD

La presente Circular Obligatoria aplica a las personas concesionarias, asignatarias y permisionarias de aeródromos civiles, personas concesionarias, asignatarias y permisionarias de transporte aéreo, a los prestadores de servicios aeroportuarios, complementarios y comerciales, así como a toda persona moral y/o física que intercambia información remota, tecnológica, o informática que pudiera afectar la Seguridad de la Aviación Civil en los Estados Unidos Mexicanos.

4. DEFINICIONES Y ABREVIATURAS

I. **ABORDO DE LA AERONAVE.** La ubicación, presencia o colocación en cabina de pilotos (cabina de vuelo), cabina de pasajeros, así como sus cocinas, baños, alacenas, guardarropas, dormitorios y demás compartimentos que se encuentren en el interior de la aeronave en que tenga acceso el pasajero, tripulación de vuelo, tripulación de sobrecargos o personal de servicio en el interior de la aeronave.

II. **ACTO DE INTERFERENCIA ILÍCITA.** Actos, o tentativas, destinados a comprometer la seguridad de la aviación civil incluyendo, de forma enunciativa más no limitativa, lo siguiente:

a. Apoderamiento ilícito de aeronaves;
b. Destrucción de una aeronave en servicio;
c. Toma de rehenes a bordo de aeronaves o en los aeródromos;
d. Intrusión por la fuerza a bordo de una aeronave, en un aeropuerto o en el recinto de una instalación aeronáutica;
e. Introducción, a bordo de una aeronave o en un aeropuerto, de armas, artefactos o sustancias peligrosas, sin la autorización correspondiente;
f. El uso de una aeronave en servicio que cause la muerte, lesiones corporales graves o daños graves a los bienes muebles o al medio ambiente;
g. Comunicación de información falsa que comprometa la seguridad de una aeronave en vuelo, o en tierra, o la seguridad de las personas pasajeras, tripulación, personal de tierra y público en un aeropuerto o en el recinto de una instalación de aviación civil.

III. **ACTUACIÓN HUMANA.** Aptitudes y limitaciones humanas que inciden en la seguridad operacional, la protección y en la eficiencia de las operaciones aeronáuticas de la aviación civil.

IV. **ADMINISTRADORA AEROPORTUARIA.** Persona física designada por la persona concesionaria,

V. **AERÓDROMO CIVIL.** Área definida de tierra o agua adecuada para el despegue, aterrizaje, acuatizaje o movimiento de aeronaves, con instalaciones o servicios mínimos para garantizar la seguridad de su operación. Los aeródromos civiles se clasifican en aeródromos de servicio al público y aeródromos de servicio particular.

VI. **AEROPUERTO.** Aeródromo civil de servicio público con instalaciones y servicios adecuados para la recepción y despacho de aeronaves, personas pasajeras, carga y correo del servicio de transporte aéreo regular y no regular, así como de servicios aéreos a terceros y operaciones de aeronaves para uso particular.

Los aeródromos civiles que tengan el carácter de aeropuerto únicamente pueden prestar servicio a las aeronaves de transporte aéreo regular.

VII. **ALERTA DE BOMBA.** Estado de alerta implantado por la autoridad aeroportuaria para poner en marcha un plan de intervención destinado a contrarrestar las posibles

consecuencias de una amenaza comunicada, anónima o de otro tipo, o el descubrimiento de un artefacto o de un objeto sospechoso en una aeronave, en un aeropuerto o en una instalación de aviación civil.

VIII. **AMENAZA DE BOMBA.** Es la comunicación por cualquier medio, de información falsa o verdadera de que se ha colocado un artefacto explosivo que compromete la seguridad de una aeronave en vuelo, en tierra o la seguridad de los pasajeros, la tripulación, el personal de tierra y el público en un aeródromo civil o en el recinto de una instalación de aviación civil.

IX. **CIBERATAQUE**. Actos o tentativas a comprometer las bases de datos, software, hardware, comunicaciones, así como soportes lógicos y físicos de los sistemas críticos de información utilizados en las operaciones, que pueden abarcar, de manera enunciativa más no limitativa, los sistemas utilizados para:

a) Control del acceso y vigilancia de alarmas;
b) Control de salidas;
c) Cotejo del equipaje con los pasajeros;
d) Inspección o detección de explosivos, mediante sistemas parte de una red o autónomos;
e) Bases de datos sobre operadores de servicio de pasajeros y de carga aérea, agentes acreditados y expedidores reconocidos de carga;
f) Gestión del tránsito aéreo;
g) Tratamiento de datos personales;
h) Reservas de los explotadores y presentación de los pasajeros;
i) Vigilancia mediante televisión en circuito cerrado;
j) Mando, control y despacho en materia de seguridad;
k) Servicios aeroportuarios y complementarios.

X. **CIBERSEGURIDAD.** Conjunto de tecnologías, controles, medidas, procesos y prácticas diseñados para proteger la confidencialidad, integridad, disponibilidad y protección general de sistemas, redes, programas, dispositivos, información y datos contra ataques o daños y acceso, uso y/o explotación no autorizados.

XI. **COMITÉ LOCAL DE SEGURIDAD AEROPORTUARIA.** Un comité en cada aeropuerto que preste servicios a la aviación civil para ayudar a la autoridad aeroportuaria a coordinar la aplicación de controles y procedimientos de seguridad, tal como se especifique en el Programa Local de Seguridad Aeroportuaria.

XII. **COORDINADOR DE SEGURIDAD DEL AEROPUERTO (CSA).** Es la persona designada por el administrador aeroportuario, que cuenta con la capacitación y adiestramiento sobre el Programa de Seguridad del Aeródromo y la normatividad en materia de seguridad de la aviación civil Cada aeropuerto deberá contar durante su horario de operaciones con un Coordinador de Seguridad del Aeropuerto.

XIII. **COORDINADOR DE SEGURIDAD EN TIERRA (CST).** Es la persona designada por el concesionario o permisionario de transporte aéreo que cuenta con la capacitación y el adiestramiento sobre el Programa de Seguridad de la Aerolínea y de su

normatividad. Cada concesionario o permisionario de transporte aéreo, deberá contar durante el horario de operación de sus vuelos, con un Coordinador de Seguridad en Tierra en cada terminal aérea donde preste servicio.

XIV. **COORDINADOR DE SEGURIDAD EN VUELO (CSV).** El concesionario, asignatario o permisionario de transporte aéreo, deberá capacitar a sus comandantes de aeronaves, acerca de los procedimientos, métodos y medidas de seguridad en aeropuertos, para coordinar acciones en caso de presentarse actos de interferencia ilícita.

XV. **CONCESIONARIO, ASIGNATARIO O PERMISIONARIO DEL TRANSPORTE AÉREO (OPERADOR O EXPLOTADOR).** Persona física o moral que previo cumplimiento de los requisitos legales ha obtenido una concesión o permiso para la prestación de Servicios de Transporte Aéreo, en cualquiera de sus modalidades, y en general la operación y explotación de aeronaves.

XVI. **CONCESIONARIO O PERMISIONARIO AEROPORTUARIO.** Sociedad mercantil constituida conforme a las leyes mexicanas quien obtiene una concesión por parte de la Secretaría de Comunicaciones y Transportes para la administración, operación, explotación y, en su caso, construcción en los Aeropuertos Nacionales.

XVII. **CONTRASEÑA SEGURA**. Método de autenticación que utiliza información secreta para controlar, ya sea denegando o permitiendo el acceso hacia algún recurso que es considerado como Restringido. Las contraseñas seguras son el recurso principal de la seguridad digital, que cumplen con criterios de longitud, complejidad y uso con responsabilidad.

XVIII. **CONTROL DE SEGURIDAD.** Medios diseñados por los cuales se previene que se introduzcan armas, explosivos, artículos peligrosos, sustancias o productos prohibidos, u otros artefactos susceptibles de ser utilizados para cometer actos de interferencia ilícita.

XIX. **DATOS PERSONALES.** Cualquier información concerniente a una persona física identificada o identificable.

XX. **ENTIDAD REGULADA.** Concesionarios o permisionarios de transporte aéreo, concesionarios o permisionarios de aeródromos, operadores de aeropuertos, arrendatarios de aeropuertos y empresas públicas o privadas que proporcionan servicios aeroportuarios o complementarios de seguridad y vigilancia, que deben cumplir con la normativa aeronáutica aplicable en materia de capacitación de seguridad de la aviación civil, de acuerdo con lo establecido en el Programa Nacional de Seguridad Aeroportuaria.

XXI. **EQUIPO DE SEGURIDAD.** Elementos materiales y humanos de carácter especializado que se utilizan, individualmente o como parte de un sistema, en la prevención o detección de actividades delictivas por actos de interferencia ilícita en contra de la Aviación Civil, sus instalaciones y servicios.

XXII. **ESTUDIO DE SEGURIDAD.** Evaluación de las necesidades en materia de seguridad, incluyendo la identificación de los puntos vulnerables que podrían aprovecharse para cometer un acto de interferencia ilícita, y la recomendación de medidas correctivas.

XXIII. **EXPLOTADOR AÉREO.** Persona, organismo o empresa que se dedica, o propone dedicarse, a la explotación de aeronaves.

XXIV. **IMPREVISIBILIDAD.** La aplicación de medidas de seguridad con frecuencias irregulares, en distintos lugares y/o utilizando medios variados, de acuerdo con un marco definido, con el objetivo de aumentar su efecto disuasivo y su eficacia.

XXV. **INSPECCIÓN.** Aplicación de medios técnicos u otras medidas para identificar y/o detectar armas, explosivos u otros artefactos peligrosos que puedan ser utilizados para cometer un acto de interferencia ilícita.

XXVI. **INSPECCIÓN DE SEGURIDAD.** Examen de la aplicación de los requisitos pertinentes del programa nacional de seguridad de la aviación civil por un explotador aéreo, un aeródromo u otro organismo encargado de la seguridad de la aviación.

XXVII. **INSTALACIONES ESTRATÉGICAS.** Se consideran instalaciones estratégicas, a los espacios, inmuebles, construcciones, muebles, equipo y demás bienes, destinados al funcionamiento, mantenimiento y operación de las actividades consideradas como estratégicas por la Constitución Política de los Estados Unidos Mexicanos, así como de aquellas que tiendan a mantener la integridad, estabilidad y permanencia del Estado Mexicano, en términos de la Ley de Seguridad Nacional.

XXVIII. **INSTRUCCIÓN.** Proceso por el cual se proveen conocimientos teóricos y prácticos para contribuir al desarrollo de competencias de un individuo para desempeñar una función en materia de seguridad de la aviación civil.

XXIX. **INSTRUCTOR.** Persona facultada por la Autoridad Aeronáutica, para llevar a cabo actividades de docencia relacionadas con la actividad aeronáutica.

XXX. **JEFE DE SEGURIDAD DEL AEROPUERTO (JSA).** Persona empleada y designada por el Administrador Aeroportuario para implementar, coordinar, supervisar y mantener actualizadas las medidas de seguridad de la aviación civil de su responsabilidad en el Aeropuerto, y otras contenidas en el Programa de Seguridad de la instalación aeroportuaria.

XXXI. **JEFE DE SEGURIDAD DEL CONCESIONARIO O PERMISIONARIO DEL TRANSPORTE AÉREO (JSTA).** Persona empleada y designada por el Concesionario o permisionario del transporte aéreo para implementar, coordinar, supervisar y mantener actualizadas las medidas de seguridad de la aviación civil, instrucción y otras contenidas en el Programa de seguridad del concesionario o permisionario del transporte aéreo autorizado por la autoridad aeronáutica.

XXXII. **MALWARE**. Software que está diseñado para generar daño en el entorno de funcionamiento habitual, realizando acciones en un sistema informático de forma intencional y sin el conocimiento del usuario.

XXXIII. **OPERADORES DE AEROPUERTOS.** Figuras que no cuentan con una concesión o permiso para explotación de un aeropuerto, pero son responsables de su operación, tales como Aeropuertos y Servicios Auxiliares, Aeropuertos Estatales, entre otros.

XXXIV. **PERSONAL DE SEGURIDAD.** Aquellas personas responsables de aplicar las siguientes medidas de seguridad:

a) Control del acceso
b) Vigilancia y patrulla
c) Seguridad de las aeronaves
d) Seguridad en vuelo, como la aplicada por la tripulación de cabina y de vuelo
e) Inspección de pasajeros y equipaje de mano
f) Inspección del equipaje de bodega, carga y correo
g) Inspección de vehículos
h) Procedimientos relativos a suministros para servicio de a bordo y suministros de concesionarios y permisionarios de aeródromos civiles y de transporte aéreo
i) Instrucción y/o capacitación en seguridad de la aviación
j) Aplicación de medidas de control de la calidad
k) Gestión de la seguridad de la aviación.

XXXV. **PERSONAL QUE NO ES DE SEGURIDAD.**

a) Todo personal al que se otorgue acceso a zonas de seguridad restringidas

b) Todo personal empleado por un concesionario o permisionario de transporte aéreo, de aeródromos civiles, agente expedidor, agente de carga, servicio postal o proveedor de control de tránsito aéreo que desempeñe funciones relacionadas con las operaciones de la aviación civil y pueda como tal participar en la aplicación de medidas de seguridad.

XXXVI. **PLAN DE CONTINGENCIA.** Documento que contiene los procedimientos tendientes a minimizar los efectos sobre las personas, equipos e instalaciones, cuando ocurre un acto de interferencia ilícita que afecte o ponga en peligro las operaciones aeronáuticas o el funcionamiento de los servicios relacionados con estas.

XXXVII. **PLAN DE SEGURIDAD.** Documento que contiene las disposiciones y métodos para prevenir todo acto de interferencia ilícita contra la seguridad de las personas y mercancías del transporte aéreo, así como regular el desplazamiento de personas y vehículos dentro del recinto aeroportuario.

XXXVIII. **PROGRAMA LOCAL DE SEGURIDAD AEROPORTUARIA.** Medidas, disposiciones, métodos y procedimientos, preventivos y de contingencia, destinados a prevenir

actos de interferencia ilícita contra la aviación y los métodos para hacer frente a dichos actos.

XXXIX. **PROGRAMA DE SEGURIDAD DE LA AVIACIÓN CIVIL DEL ESTADO MEXICANO (antes PNSAC).** Medidas generales adoptadas para proteger a la infraestructura aeroportuaria y a la aviación civil en contra de su posible utilización para actividades delictivas y/o de actos de interferencia ilícita.

El que elabore el Comité Nacional de Seguridad de Aviación Civil integrado por las personas representantes de las secretarías de la Defensa Nacional, de Marina, de Infraestructura, Comunicaciones y Transportes y apruebe la persona titular de la Secretaría de Infraestructura, Comunicaciones y Transportes.

XL. **PRUEBA DE SEGURIDAD.** Ensayo, secreto o no, de una medida de seguridad de la aviación en la que se simula un intento de cometer un acto de interferencia ilícita.

XLI. **PUNTO VITAL DEL AERÓDROMO.** Instalaciones o áreas esenciales para la operación normal que en caso de ser dañadas o destruidas impedirían el buen funcionamiento de este o la suspensión parcial o total de sus actividades.

XLII. **PUNTO VULNERABLE.** Toda instalación en el aeropuerto o conectada con el mismo que, en caso de ser dañada o destruida, perjudicaría seriamente el funcionamiento normal de un aeropuerto.

XLIII. **SABOTAJE.** Acto u omisión deliberada para destruir maliciosa o injustificadamente un bien, poniendo en peligro la aviación civil y sus instalaciones y servicios, o que resulte en un acto de interferencia ilícita.

XLIV. **SECRETARÍA.** La Secretaría de Infraestructura, Comunicaciones y Transportes.

XLV. **SEGURIDAD DE LA AVIACIÓN.** Protección de la aviación civil contra los actos de interferencia ilícita mediante una combinación de medidas y recursos humanos y materiales.

XLVI. **SEGURIDAD NACIONAL.** Las acciones destinadas de manera inmediata y directa a mantener la integridad, estabilidad y permanencia del Estado mexicano que conllevan a:

a) Proteger al país frente a riesgos y amenazas.
b) Preservar la soberanía, independencia, territorio y la unidad de la federación.
c) Mantener el orden constitucional y fortalecer las instituciones democráticas de gobierno.
d) Defender al país frente a otros Estados o sujetos de derecho internacional.
e) Preservar el régimen democrático fundado en el desarrollo social, económico y político.

XLVII. SEGURIDAD PÚBLICA. Una cualidad de los espacios públicos y privados, que se caracteriza por la inexistencia de amenazas que socaven o supriman los bienes y derechos de las personas y en la que existen condiciones propicias para la convivencia pacífica y el desarrollo individual y colectivo de la sociedad.

5. ANTECEDENTES

El Anexo 17 al Convenio sobre Aviación Civil Internacional, Seguridad de la Aviación, así como el Manual de Seguridad de la Organización de la Aviación Civil y el Programa Nacional de Seguridad de la Aviación Civil, establecen que los Estados Contratantes deberán implementar medidas que mitiguen la amenaza de actos de interferencia ilícita perpetrados por ataques cibernéticos o informáticos.

6. DESCRIPCION.

La presente circular obligatoria establece los requisitos mínimos de ciberseguridad que deberán implementar las personas concesionarias, asignatarias y permisionarias del transporte aéreo, aeródromos civiles, y prestadores de servicios aeroportuarios y complementarios para prevenir actos de interferencia ilícita perpetrados mediante medios de ataque remotos, cibernéticos, informáticos y/o tecnológicos".

7. DISPOSICIONES GENERALES.

Las entidades reguladas están obligadas a cumplir las disposiciones referidas en la presente Circular obligatoria deberán observar los parámetros que se indican a continuación como los aspectos preventivos, de detección y de reacción ante posibles ciberataques:

7.1. Inventario de Software autorizado y no autorizado:

Las entidades reguladas a que se refiere el numeral 3, de la presente Circular Obligatoria, deberán:

7.1.1. Formular un inventario de todos los activos de información donde se identifiquen los datos, la información y los sistemas, sensibles o críticos para la institución. Se debe proteger y restringir el acceso a dicho inventario solo al personal autorizado.

7.1.2. Implementar como política de red perimetral en firewalls el cierre de todos los puertos por defecto y la apertura de los servicios únicamente con autorización del administrador de la red.

7.1.3. Establecer reglas de filtrados de contenido mediante proxys en la red interna.

7.1.4. Inhabilitar por defecto la función Wake on LAN para evitar que los equipos se enciendan remotamente.

7.1.5. Contar con políticas que impidan el acceso a páginas web, documentos, archivos multimedia y otros contenidos no autorizados.

7.1.6. Establecer un control de software autorizado en cada equipo de la organización de acuerdo con lo siguiente:

Inventario y control de activos software			
Tipo de activo	**Función de Seguridad**	**Control**	**Descripción**
Aplicaciones	Identificar	Mantener un inventario de software autorizado.	Mantenga una lista actualizada de todo el software autorizado que es requerido en la organización para todos los fines y sistemas de negocio.
Aplicaciones	Identificar	Asegurar que el software tenga soporte del fabricante.	Asegure que en el inventario de software autorizado de la organización se incluya únicamente software (aplicaciones o sistemas operativos) que actualmente cuente con soporte. El software que no cuenta con soporte debe ser marcado como no soportado en el sistema de inventario.
Aplicaciones	Identificar	Utilizar herramientas de inventario de software.	Utilice herramientas de inventario de software en toda la organización para automatizar la documentación de todo el software en los sistemas de negocio.
Aplicaciones	Identificar	Rastrear información del inventario de software.	El sistema de inventario de software debe obtener el nombre, la versión, el autor y la fecha de instalación de todo el software, incluidos los sistemas operativos autorizados por la organización.
Aplicaciones	Identificar	Integrar los inventarios de activos de hardware y software.	El sistema de inventario de software debe estar vinculado al inventario de activos de hardware para que todos los dispositivos y el software asociado sean rastreados desde una sola ubicación.

7.1.7. Las entidades reguladas deben de contar con la implementación de firewall, antivirus, sistemas de detección y respuesta de puntos finales (EDR), sistemas de detección de intrusiones (IDS) y sistemas de prevención de intrusiones (IPS) basados en *host*, junto con listas blancas y negras de aplicaciones.

7.1.8. Mantener actualizados todos los programas, considerando aplicaciones, paquetería de oficina, navegadores web y sistemas operativos.

7.1.9. Respaldar periódicamente los archivos del equipo de cómputo, en medios de almacenamiento electrónicos y externos; o bien en la nube.

7.1.10. Usar contraseñas seguras, que sean diferentes para todos los dispositivos, considerando las siguientes recomendaciones:

a) Utilizar contraseña con una longitud mínima de 10 caracteres.

b) Incluir números aleatorios combinados a lo largo de la contraseña.
c) Utilizar mayúsculas y minúsculas combinadas a lo largo de la contraseña.
d) Inserta caracteres especiales, como puede ser el símbolo asterisco (*), guion bajo (_), ampersand (&), porcentaje (%), por referir algunos.
e) Cambiar las contraseñas periódicamente.
f) No compartir contraseñas ni credenciales de acceso a equipos, aplicativos y sistemas.
g) Evitar utilizar la misma contraseña para todos los archivos, servicios y dispositivos.
h) No escribir las contraseñas en libretas o papeles de fácil acceso para personas no autorizadas.
i) No mantenerlas las contraseñas visibles.

7.1.11. Asegurarse que los usuarios no resguarden sus credenciales de acceso y contraseñas en los lugares de trabajo.

7.1.12. Encriptar equipos y medios de almacenamiento que contengan información crítica para la operación y/o datos personales.

7.2. Inventario de dispositivos autorizados y no autorizados:

7.2.1. Las entidades reguladas deben gestionar activamente todo dispositivo hardware en la red (inventario, seguimiento y corrección), de tal manera que solo los dispositivos autorizados obtengan acceso y que los dispositivos no autorizados y no gestionados sean detectados y se prevenga que obtengan acceso, de conformidad con lo siguiente:

Inventario y control de activos hardware			
Tipo de activo	**Función de Seguridad**	**Control**	**Descripción**
Equipos	Identificar	Utilizar una herramienta de descubrimiento activo.	Utilice una herramienta de descubrimiento activo a fin de: • Escanear de manera periódica mediante el uso de protocolos DNS, ICMP y SNMP o cualquier otro protocolo que surja con motivo de los avances tecnológicos, a efecto de identificar nuevos dispositivos y cambios en la topología de red. • El monitoreo proactivo de software y sus actualizaciones en los dispositivos para garantizar la seguridad, mediante el uso de protocolos como SNMP o cualquier otro protocolo que surja con motivo de los avances tecnológicos, para recopilar información sobre el inventario de

Inventario y control de activos hardware			
Tipo de activo	**Función de Seguridad**	**Control**	**Descripción**
			software. • Realizar auditorías al software y hardware que comprenden el inventario de activos de TI.
Equipos	Identificar	Utilizar una herramienta de descubrimiento pasivo de activos.	Utilice una herramienta de descubrimiento pasivo a fin de: • Identificar dispositivos no autorizados o no gestionados. • Monitorear el uso de software y el tráfico de aplicaciones. • Recopilar datos sobre la actividad de los dispositivos y de los usuarios. • Identificar dispositivos conectados a la red de la organización y actualizar automáticamente el inventario de activos.
Equipos	Identificar	Utilizar DHCP Logging para actualizar el inventario de activos.	Utilice un sistema de logging de DHCP (Dynamic Host Configuration Protocol) en todos los servidores DHCP o herramientas de gestión de direcciones IPs para actualizar el inventario de activos hardware de la organización.
Equipos	Identificar	Mantener un inventario de activos detallado.	Mantenga un inventario actualizado de todos los activos tecnológicos capaces de almacenar y/o procesar información. El inventario debe incluir todos los activos de hardware, estén o no conectados a la red de la organización.
Equipos	Identificar	Mantener la información del inventario de activos.	Asegúrese que el inventario de activos de hardware registre, como mínimo, las direcciones de red, nombre, propósito, responsable, departamento de cada activo, así como también si el activo de hardware ha sido aprobado o no para ser conectado a la red.
Equipos	Responder	Gestionar los activos no autorizados.	Asegúrese de que los activos no autorizados se eliminen de la red y/o se pongan en cuarentena.

Inventario y control de activos hardware			
Tipo de activo	**Función de Seguridad**	**Control**	**Descripción**
Equipos	Proteger	Implementar control de acceso a nivel de puerto.	Implemente control de acceso a nivel de puertos según el estándar 802.1x para limitar y controlar qué equipo puede autenticarse en la red. El sistema de autenticación debe estar vinculado a los datos de inventario de activos hardware para asegurar que sólo los equipos autorizados se pueden conectar a la red.
Equipos	Proteger	Utilizar certificados clientes para autenticar activos hardware.	Utilice certificados clientes para autenticar los activos de hardware que se conectan a la red de confianza de la organización.

7.2.2. Se deberán establecer políticas para el uso de red privada virtual (VPN). Cada máquina que usa una dirección IP debe incluirse en el inventario de activos de una organización.

7.3. Gestión continua de vulnerabilidades:

7.3.1. Las entidades reguladas deberán evaluar y tomar medidas continuamente sobre vulnerabilidades, y minimizar la ventana de oportunidad para los ataques, de conformidad con lo siguiente:

Gestión continua de vulnerabilidades			
Tipo de activo	**Función de Seguridad**	**Control**	**Descripción**
Aplicaciones	Detectar	Ejecutar herramientas de escaneo automatizados de vulnerabilidades.	Utilice una herramienta actualizada de escaneo de vulnerabilidades para escanear automáticamente todos los sistemas en la red de forma semanal o más frecuente para identificar todas las vulnerabilidades potenciales en los sistemas de la organización.
Aplicaciones	Detectar	Realizar análisis de vulnerabilidades autenticados.	Realice escaneos de vulnerabilidades autenticados con agentes que se ejecutan localmente en cada sistema o con escáneres remotos que están configurados con derechos elevados en el sistema que se audita.
Aplicaciones	Proteger	Proteger las cuentas	Utilice una cuenta dedicada al escaneo de vulnerabilidades autenticado, la cual

Gestión continua de vulnerabilidades			
Tipo de activo	**Función de Seguridad**	**Control**	**Descripción**
		dedicadas a auditorías.	no debe ser utilizada para otras tareas administrativas y que debe ser vinculada a máquinas específicas en direcciones IPs específicas.
Aplicaciones	Proteger	Implementar herramientas de gestión automatizada de parches del sistema operativo.	Implemente herramientas de actualización de software automatizadas para garantizar que los sistemas operativos cuenten con las actualizaciones de seguridad más recientes provistas por el proveedor del software.
Aplicaciones	Proteger	Implementar herramientas de gestión automatizada de parches de software.	Implemente herramientas de actualización de software automatizadas para garantizar que el software de terceros en todos los sistemas cuente con las actualizaciones de seguridad más recientes provistas por el proveedor del software.
Aplicaciones	Responder	Comparar escaneos de vulnerabilidades consecutivos.	Compare regularmente los resultados de escaneos de vulnerabilidades consecutivas para verificar que las vulnerabilidades se hayan remediado de manera oportuna.
Aplicaciones	Responder	Utilizar un proceso de calificación de riesgo.	Utilice un proceso de calificación de riesgo para priorizar la corrección de vulnerabilidades descubiertas.

7.3.2. Las herramientas avanzadas de análisis de vulnerabilidades deberán ser configuradas con credenciales de usuario para iniciar sesión en los sistemas escaneados y realizar escaneos más exhaustivos de lo que se puede lograr sin las credenciales de inicio de sesión

7.3.3. La frecuencia de los escaneos deberá aumentarse a medida que aumenta la diversidad de los sistemas de una organización, de modo a tener en cuenta los ciclos de parches variables de cada proveedor.

7.4. Uso controlado de privilegios administrativos:

7.4.1. Conforme a esta circular obligatoria, las entidades reguladas deberán de contar con procesos y herramientas utilizados para rastrear, controlar, prevenir y corregir el uso, la asignación y la configuración de privilegios administrativos en computadoras, redes y aplicaciones.

7.4.2. De manera enunciativa mas no limitativa los controles deberán considerar lo siguiente:

Uso controlado de privilegios administrativos			
Tipo de activo	**Función de Seguridad**	**Control**	**Descripción**
Usuarios	Detectar	Mantener un inventario de cuentas administrativas.	Use herramientas automatizadas para inventariar todas las cuentas administrativas, incluidas las cuentas de dominio y locales, para garantizar que solo las personas autorizadas tengan privilegios elevados.
Usuarios	Proteger	Cambiar contraseñas por defecto.	Antes de implementar cualquier activo nuevo, cambie todas las contraseñas por defecto para que tengan valores consistentes con las cuentas de nivel administrativo.
Usuarios	Proteger	Asegurar el uso de cuentas administrativas dedicadas.	Asegúrese de que todos los usuarios con acceso a la cuenta administrativa utilicen una cuenta dedicada o secundaria para actividades elevadas. Esta cuenta solo se debe usar para actividades administrativas y no para la navegación por Internet, correo electrónico o actividades similares.
Usuarios	Proteger	Usar contraseñas únicas.	Cuando no está soportada la autenticación multifactor (como el administrador local, root o cuentas de servicio), las cuentas usarán contraseñas que son únicas de ese sistema.

Uso controlado de privilegios administrativos			
Tipo de activo	**Función de Seguridad**	**Control**	**Descripción**
Usuarios	Proteger	Usar autenticación multifactor para todo acceso administrativo.	Utilice autenticación de multifactor y canales encriptados para todos los accesos de cuentas administrativas.
Usuarios	Proteger	Usar máquinas dedicadas para toda tarea administrativa.	Asegúrese de que los administradores utilicen una máquina dedicada para todas las tareas administrativas o tareas que requieren acceso

Uso controlado de privilegios administrativos			
Tipo de activo	**Función de Seguridad**	**Control**	**Descripción**
			administrativo. Esta máquina debe estar en un segmento de red diferente al principal de la organización y no se le permitirá el acceso a Internet. Esta máquina no se usará para leer correos electrónicos, manipular documentos o navegar en Internet.
Usuarios	Proteger	Limitar el acceso a herramientas de scripts.	Limite el acceso a las herramientas de scripting (como Microsoft PowerShell y Python) solo a usuarios administrativos o de desarrollo que necesiten acceder a esas funcionalidades.
Usuarios	Detectar	Registrar y alertar cambios de miembros en grupos administrativos.	Configure los sistemas para que generen una entrada de registro y una alerta cuando se agregue o elimine una cuenta a cualquier grupo que tenga asignados privilegios administrativos.
Usuarios	Detectar	Registrar y alertar los inicios de sesión fallidos a cuentas administrativas.	Configure los sistemas para generar una entrada de registro y una alerta de inicios de sesión fallidos en una cuenta administrativa.

7.5. Configuración segura para hardware y software en dispositivos móviles, computadoras portátiles, estaciones de trabajo y servidores:

7.5.1. Se deberá establecer, implementar y gestionar activamente (rastrear, informar, corregir) la configuración de seguridad de dispositivos móviles, computadoras portátiles, servidores y estaciones de trabajo utilizando una rigurosa gestión de configuraciones y un proceso de control de cambios para evitar que los atacantes exploten servicios y configuraciones vulnerables.

7.5.2. De manera enunciativa mas no limitativa los controles deberán considerar lo siguiente:

Control: Configuración segura para hardware y software en dispositivos móviles, computadoras portátiles, estaciones de trabajo y servidores			
Tipo de activo	**Función de Seguridad**	**Control**	**Descripción**
Aplicaciones	Proteger	Establecer configuraciones seguras.	Mantenga estándares de configuración de seguridad estándar documentados para todos los sistemas operativos y software autorizados.
Aplicaciones	Proteger	Mantener imágenes seguras.	Mantenga imágenes o plantillas seguras para todos los sistemas de la organización según los estándares de configuración aprobados por la organización. Cualquier implementación de sistema nuevo o sistema existente que se vea comprometido se debe volver a reconstruirlo con una de esas imágenes o plantillas.
Aplicaciones	Proteger	Almacenar las imágenes maestras de forma segura.	Almacene las imágenes maestras y las plantillas en servidores configurados de forma segura, validados con herramientas de monitoreo de integridad, para garantizar que solo sean posibles los cambios autorizados en las imágenes.
Aplicaciones	Proteger	Implementar herramientas de gestión de configuración de sistema.	Implemente las herramientas de gestión de configuración de sistema que automáticamente fuercen y vuelvan a implementar los parámetros de configuración en los sistemas a intervalos regulares programados.

7.6. Protección de correo electrónico y navegador web:

7.6.1. Las entidades reguladas deberán de gestionar la protección de os navegadores web y los clientes de correo electrónico a fin de mitigar los puntos de entrada y ataque.

7.6.2. De manera enunciativa mas no limitativa los controles deberán considerar lo siguiente:

Protección de correo electrónico y navegador web			
Tipo de activo	**Función de Seguridad**	**Control**	**Descripción**
Aplicaciones	Proteger	Asegurar el uso de navegadores y clientes de correo electrónico que cuenten con soporte.	Asegúrese de que solo los navegadores web y los clientes de correo electrónico que cuenten con soporte completo puedan ejecutarse en la organización, idealmente solo con la última versión de los navegadores y clientes de correo electrónico proporcionados por el proveedor.
Aplicaciones	Proteger	Deshabilitar plugins innecesarios de navegadores o clientes de correo electrónico.	Desinstalar o deshabilitar cualquier plugin o aplicación add-on para navegador o cliente de correo electrónico no autorizados.
Aplicaciones	Proteger	Limitar el uso de lenguajes de scripting en navegadores web y clientes de correo electrónico.	Asegúrese de que solo los lenguajes de scripting autorizados puedan ejecutarse en los navegadores web y clientes de correo electrónico.
Red	Proteger	Mantener y aplicar filtros de URL basados en red.	Aplique los filtros de URL basados en red que limitan la capacidad de un sistema para conectarse a sitios web no aprobados por la organización. Este filtrado se aplicará para cada uno de los sistemas de la organización, ya sea que se encuentren físicamente en las instalaciones de una organización o no.
Red	Proteger	Utilizar servicios de filtrado DNS.	Utilice servicios de filtrado de DNS para ayudar a bloquear el acceso a dominios maliciosos conocidos.
Red	Proteger	Implementar DMARC y habilitar verificación del lado del receptor.	Para reducir la posibilidad de correos electrónicos falsificados o modificados de dominios válidos, implemente y verifique la política de Autenticación, Reporte y Conformidad de mensajes basada en dominio (Domain-based Message Authentication, Reporting and Conformance - DMARC), comenzando por implementar los

Protección de correo electrónico y navegador web			
Tipo de activo	**Función de Seguridad**	**Control**	**Descripción**
			estándares Sender Policy Framework (SPF) y DomainKeys Identified Mail (DKIM).
Red	Proteger	Bloquear tipos de archivos innecesarios.	Bloquee todos los archivos adjuntos de correo electrónico que ingresen a la pasarela de correo electrónico de la organización si los tipos de archivos son innecesarios para los fines de negocio de la organización.
Red	Proteger	Utilizar técnicas de sandbox para todos los adjuntos de correo electrónico.	Utilice técnicas de sandboxing para analizar y bloquear los archivos adjuntos de correo electrónico que tengan un comportamiento malicioso.

7.7. Defensa contra malware:

7.7.1. Las entidades reguladas deberán de controlar la instalación, propagación y ejecución de código malicioso en múltiples puntos de la organización, al mismo tiempo que optimizar el uso de automatización para permitir la actualización rápida de la defensa, la recopilación de datos y la acción correctiva.

7.7.2. De manera enunciativa mas no limitativa, los controles deberán considerar lo siguiente:

Defensa contra malware			
Tipo de activo	**Función Seguridad**	**Control**	**Descripción**
Equipos	Proteger	Utilizar software antimalware de gestión centralizada.	Utilice software antimalware gestionado centralmente para monitorear y defender continuamente cada una de las estaciones de trabajo y servidores de la organización.
Equipos	Proteger	Asegurar que el software antimalware y las firmas estén	Asegúrese de que el software antimalware de la organización actualice su motor de exploración y la base de datos de firmas periódicamente.

Defensa contra malware			
Tipo de activo	**Función Seguridad**	**Control**	**Descripción**
		actualizadas.	
Equipos	Proteger	Habilitar características anti-explotación de sistemas operativos / implementar tecnologías anti explotación.	Habilite las características anti-explotación como la Prevención de ejecución de datos (Data Execution Prevention - DEP) o Address Space Layout Randomization (ASLR) que están disponibles en los sistemas operativos o implemente los kits de herramientas adecuados que pueden configurarse para aplicar protección a un conjunto más amplio de aplicaciones y ejecutables.
Equipos	Detectar	Configurar escaneo anti-malware de dispositivos removibles.	Configure los dispositivos para que automáticamente realicen un análisis anti-malware de los medios extraíbles cuando se inserten o se conecten.
Equipos	Proteger	Configurar equipos para no auto-ejecutar contenido.	Configure los equipos para no ejecutar automáticamente el contenido de medios extraíbles.
Equipos	Detectar	Centralizar los registros antimalware.	Envíe todos los eventos de detección de malware a las herramientas de administración antimalware de la organización y a los servidores de registro de eventos para análisis y alertas.

7.8. Control de acceso inalámbrico

7.8.1. Las entidades reguladas tendrán procesos y herramientas utilizados para rastrear/controlar/prevenir/corregir el uso seguro de las redes inalámbricas (WLAN), puntos de acceso y sistemas de clientes inalámbricos.

7.8.2. De manera enunciativa mas no limitativa los controles deberán considerar lo siguiente:

Control de acceso inalámbrico			
Tipo de activo	**Función Seguridad**	**Control**	**Descripción**
Red	Identificar	Mantener un inventario de puntos de acceso inalámbrico autorizados.	Mantenga un inventario de los puntos de acceso inalámbrico autorizados conectados a la red cableada.
Red	Detectar	Detectar puntos de acceso inalámbricos conectados a la red cableada.	Configure las herramientas de exploración de vulnerabilidades de red para detectar y alertar sobre puntos de acceso inalámbrico no autorizados conectados a la red cableada.
Red	Detectar	Usar un sistema de detección de intrusión inalámbrica.	Use un sistema inalámbrico de detección de intrusos (WIDS) para detectar y alertar sobre puntos de acceso inalámbrico no autorizados conectados a la red.
Equipos	Proteger	Deshabilitar el acceso inalámbrico en dispositivos si no se requiere.	Deshabilite el acceso inalámbrico en dispositivos que no tienen un propósito de negocio para el acceso inalámbrico.
Equipos	Proteger	Inhabilitar las capacidades de red inalámbrica punto a punto en clientes inalámbricos.	Inhabilite las capacidades de redes inalámbricas punto a punto (adhoc) en clientes inalámbricos.
Red	Proteger	Usar estándar de cifrado avanzado (AES) para cifrar datos inalámbricos.	Aproveche el estándar de cifrado avanzado (Advanced Encryption Standard - AES) para cifrar datos inalámbricos en tránsito.
Red	Proteger	Usar protocolos de autenticación inalámbrica que requieran autenticación	Asegúrese de que las redes inalámbricas utilicen protocolos de autenticación como Protocolo de autenticación extensible / Seguridad de capa de transporte (Extensible Authentication Protocol-Transport Layer Security - EAP / TLS), que requiere autenticación mutua de múltiples

Control de acceso inalámbrico			
Tipo de activo	**Función Seguridad**	**Control**	**Descripción**
		mutua multi-factor.	factores.
Equipos	Proteger	Deshabilitar el acceso periférico inalámbrico de dispositivos.	Deshabilite el acceso periférico inalámbrico de dispositivos (como Bluetooth y NFC), a menos que dicho acceso sea necesario para fines de negocio.
Red	Proteger	Crear una red inalámbrica separada para dispositivos personales y no confiables.	Cree una red inalámbrica separada para dispositivos personales o que no sean de confianza. El acceso de la empresa desde esta red debe tratarse como no confiable y debe filtrarse y auditarse en consecuencia.
Red	Proteger	Segmentar la red en subredes.	Contar con segmentación de red en subredes para cada departamento de la empresa. El acceso a cada una de estas subredes debe de basarse en el tipo de actividad que se realiza, de forma enunciativa más no limitativa: 1) área administrativa, 2) área de TI, 3) área de marketing, etc.

7.9. Monitoreo y control de cuentas:

7.9.1. Las entidades reguladas deberán establecer monitoreos en el ciclo de vida de las cuentas del sistema y de aplicaciones (su creación, uso, latencia, eliminación) con el fin de minimizar las oportunidades para que los atacantes las aprovechen.

7.9.2. De manera enunciativa mas no limitativa los controles deberán considerar lo siguiente:

Monitoreo y control de cuentas			
Tipo de activo	**Función Seguridad**	**Control**	**Descripción**
Usuarios	Identificar	Mantener un inventario de sistemas de autenticación.	Mantenga un inventario de cada uno de los sistemas de autenticación de la organización, incluidos los ubicados en el sitio o en un proveedor de servicios remoto.

Monitoreo y control de cuentas			
Tipo de activo	**Función Seguridad**	**Control**	**Descripción**
Usuarios	Proteger	Configurar un punto de autenticación centralizado.	Configure el acceso para todas las cuentas a través de la menor cantidad posible de puntos de autenticación centralizados, incluidos los sistemas de red, de seguridad y en la nube.
Usuarios	Proteger	Requerir Autenticación Multifactor.	Requiera autenticación de múltiples factores para todas las cuentas de usuario, en todos los sistemas, ya sea que se administren localmente en la organización o por un proveedor de terceros.
Usuarios	Proteger	Cifrar o hashear todas las credenciales de autenticación.	Utilice técnicas de cifrado o *hash* combinado con *salt* con todas las credenciales de autenticación cuando se almacenan.
Usuarios	Proteger	Cifrar la transmisión de nombres de usuario y credenciales de autenticación.	Asegúrese de que todos los nombres de usuario y las credenciales de autenticación de la cuenta se transmitan a través de redes que utilizan canales cifrados.
Usuarios	Identificar	Mantener un inventario de cuentas.	Mantenga un inventario de todas las cuentas organizadas por sistema de autenticación.
Usuarios	Proteger	Establecer un proceso para revocar el Acceso.	Establezca y siga un proceso automatizado para revocar el acceso a sistemas mediante la desactivación de cuentas inmediatamente después de la terminación o el cambio de responsabilidades de un empleado o contratista. Desactivar estas cuentas, en lugar de eliminar cuentas, permite preservar los registros de auditoría.
Usuarios	Responder	Deshabilitar cualquier cuenta no asociada.	Deshabilite cualquier cuenta que no pueda asociarse con un proceso de negocio o un propietario de la organización.
Usuarios	Responder	Desactivar cuentas inactivas.	Deshabilite automáticamente las cuentas inactivas después de un período de inactividad establecido.
Usuarios	Proteger	Asegurar que todas las cuentas tengan fecha de caducidad.	Asegúrese de que todas las cuentas tengan una fecha de vencimiento monitoreada y forzada.

Monitoreo y control de cuentas			
Tipo de activo	**Función Seguridad**	**Control**	**Descripción**
Usuarios	Proteger	Bloquear sesiones de estaciones de trabajo tras inactividad.	Bloquee automáticamente las sesiones de la estación de trabajo después de un período estándar de inactividad.
Usuarios	Detectar	Monitorear los intentos de acceso a cuentas desactivadas.	Monitoree los intentos de acceso a cuentas desactivadas a través de los registros de auditoría.
Usuarios	Detectar	Alertar sobre desviación de comportamiento de inicio de sesión de cuentas.	Alerte cuando los usuarios se desvían del comportamiento normal de inicio de sesión, como la hora y/o el día, la ubicación de la estación de trabajo y la duración.

7.10. Implementar un programa de concienciación y entrenamiento de seguridad:

7.10.1. Las entidades reguladas deberán establecer programas de concientización y entrenamiento de seguridad informática para evaluar, identificar brechas y remediar a través de políticas, planificación organizacional, capacitación y programas de concienciación.

7.10.2. De manera enunciativa mas no limitativa los controles deberán considerar lo siguiente:

Implementar un programa de concienciación y entrenamiento de seguridad			
Tipo de activo	**Función Seguridad**	**Control**	**Descripción**
N/A	N/A	Realizar un análisis de brecha de habilidades.	Lleve a cabo un análisis de la brecha de habilidades para comprender las habilidades y los comportamientos a los que los miembros de la fuerza de trabajo no se están adhiriendo, usando esta información para construir una hoja de ruta base de educación.
N/A	N/A	Realizar capacitación para llenar la brecha de habilidades.	Realice capacitaciones para abordar el vacío de habilidades identificado para impactar positivamente el comportamiento de seguridad de los miembros de la fuerza laboral.

Implementar un programa de concienciación y entrenamiento de seguridad			
Tipo de activo	**Función Seguridad**	**Control**	**Descripción**
N/A	N/A	Implementar un programa de concienciación de seguridad.	Cree un programa de concientización de seguridad para que todos los miembros de la fuerza laboral lo completen regularmente para asegurarse de que entienden y exhiben los comportamientos y las habilidades necesarias para ayudar a garantizar la seguridad de la organización. El programa de concientización de seguridad de la organización debe comunicarse de manera continua y atractiva.
N/A	N/A	Actualice el contenido de concienciación con frecuencia.	Asegúrese de que el programa de concientización de seguridad de la organización se actualice con frecuencia (al menos una vez al año) para abordar nuevas tecnologías, amenazas, estándares y requisitos de negocio.
N/A	N/A	Entrenar a la fuerza laboral en la autenticación segura.	Capacite a los miembros de la fuerza de trabajo sobre la importancia de habilitar y utilizar la autenticación segura.
N/A	N/A	Capacitar a la fuerza laboral en la identificación de ataques de ingeniería social.	Capacite a los empleados sobre cómo identificar diferentes formas de ataques de ingeniería social, como phishing, fraudes telefónicos y llamadas de suplantación.
N/A	N/A	Capacitar a la fuerza laboral en manejo de datos sensibles.	Capacite a los empleados sobre cómo identificar y almacenar, transferir, archivar y destruir información confidencial de manera adecuada.

7.11. Realizar pruebas de penetración y/o ejercicios de *red teaming*:

Las entidades reguladas deberán realizar pruebas de penetración o ejercicios de *red teaming* de tipo caja negra, caja gris y caja blanca en toda su infraestructura informática para: 1) identificar si un atacante remoto podría penetrar las defensas y medidas de seguridad consideradas en los puntos anteriores; y 2) determinar la confidencialidad, integridad y accesibilidad/disponibilidad de la información privada y los servicios de la compañía.

Las pruebas de penetración o ejercicios de *red teaming* deberán de realizarse semestralmente.

7.12. Evaluación del cumplimiento:

7.12.1. Las entidades reguladas deberán enviar un informe semestral de las medidas implementadas para el cumplimiento de esta circular. En dicho informe se deberá 1) detallar si existió o no algún ataque o tentativa con fines de interferencia ilícita y las características de este y 2) presentar el reporte de prueba de penetración o ejercicio de *red teaming* realizado por la Unidad Verificadora Autorizada.

7.12.2. El informe se deberá de enviar a reporteciberseguridadavsec@afac.gob.mx

7.12.3. Los informes antes referidos serán requisito necesario para que la Agencia Federal de Aviación Civil renueve los permisos, autorizaciones o certificaciones a que haya lugar.

7.12.4. La validación del cumplimiento podrá ejecutarse por personal de oficinas Centrales de la Agencia Federal de Aviación Civil, así como por la Comandancia de Aeropuerto que corresponda y/o, Unidad Verificadora Autorizada.

7.13. Sobre las Unidades Verificadoras Autorizadas y Empresas Facilitadoras:

La Agencia Federal de Aviación Civil, podrá autorizar Unidades Verificadoras y empresas facilitadoras, para vigilar el cumplimiento de la presente Circular Obligatoria.

Las Unidades verificadoras y empresas facilitadoras interesadas en obtener la autorización a que se refiere esta sección, deberán demostrar lo siguiente:

I. Contar con al menos 3 años en la auditoría de sistemas informáticos y gestión de la seguridad de la información.

II. Comprobar anualmente que su personal auditor no cuenta con antecedentes penales.

III. Haber celebrado un convenio con la Agencia Federal de Aviación Civil, aceptando las condiciones que esta determine.

IV. Contar con un mínimo de dos auditores de ciberseguridad certificados en al menos una de las siguientes certificaciones:

a) Certified Ethical Hacker (CEH).
b) Certified Ethical Hacker and Security Professional (CEHSP).
c) Offensive Security Ceritified Professional (OSCP).
d) Certified Penetretion Testing Specialist (CPTS).
e) NIST Cibersecurity Framework Lead Implementer.

Lo anterior sin perjuicio de cualquier otra certificación de características superiores que surja con motivo de los avances tecnológicos.

8. VIGILANCIA Y SANCION.

Corresponde a la Secretaría de Infraestructura, Comunicaciones y Transportes por conducto de la Agencia Federal de Aviación Civil, sancionar cualquier incumplimiento a la presente Circular Obligatoria, en términos de lo dispuesto por las Leyes, Reglamentos y demás disposiciones jurídicas aplicables.

9. GRADO DE CONCORDANCIA CON NORMAS Y LINEAMIENTOS INTERNACIONALES Y CON LEYES, REGLAMENTOS Y NORMAS OFICIALES MEXICANAS TOMADAS COMO BASE PARA SU ELABORACION.

La presente Circular Obligatoria está realizada de conformidad con lo establecido en la Ley de Aeropuertos, la Ley de Aviación Civil, que establece que las unidades verificadoras pueden coadyuvar en la verificación del cumplimiento de las obligaciones de los concesionarios y permisionarios de aeródromos civiles y del transporte aéreo nacional e internacional establecidos en los artículos 78 de la Ley de Aeropuertos y 84 de la Ley de Aviación Civil, específicamente en la determinación de las obligaciones de Seguridad de la Aviación Civil y Facilitación, el Programa de Seguridad para la Protección de la Aviación Civil contra los Actos de Interferencia Ilícita, Documento (OACI) 8973; y Anexo 17 "Seguridad", Protección de la Aviación Civil Internacional contra los Actos de Interferencia Ilícita del Convenio de Aviación Civil Internacional de la OACI.

Este último documento forma parte del compromiso que México como Estado miembro de la OACI, debe de cumplir en cuanto a las Normas emitidas por este organismo internacional y que se observan en el artículo 37 del Convenio sobre Aviación Civil Internacional, del que México es un país firmante en términos del artículo 133 de la Constitución Política de los Estados Unidos Mexicanos.

10. BIBLIOGRAFÍA.

Convenio sobre Aviación Civil Internacional 1944.
Anexo 17 al Convenio sobre Aviación Civil Internacional. Seguridad. Protección de la aviación civil internacional contra los actos de interferencia ilícita. Décima Edición, abril 2017. Seguridad.
Doc. 8973 Manual de Seguridad para la Protección de la Aviación Civil.
La Ley de Aviación Civil, (Ultima reforma publicada en el Diario Oficial de la Federación el día 03 de mayo de 2023)
Reglamento de la Ley de Aviación Civil, publicada en el diario oficial de la Federación el día 07 de diciembre de 1998
La Ley de Aeropuertos, (Ultima reforma publicada en el Diario Oficial de la Federación el día 03 de mayo de 2023)
Reglamento de la Ley de Aeropuertos, publicada en el diario oficial de la Federación el día 17 de febrero del 2000Programa Nacional de Seguridad de la Aviación Civil, publicado en el DOF el 12 de junio de 2019.
Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
Ley Federal de Protección de Datos Personales en Posesión de los Particulares.
Recomendación UIT-T X.1205 Aspectos generales de la ciberseguridad, emitida por la Unión Internacional de Telecomunicaciones (ITU por sus siglas en inglés).
CO SA 17.1/10 "Que establece el contenido mínimo para el Manual de Seguridad para la Prevención de Actos de Interferencia Ilícita".

CO SA 17.4/12 R3 "Circular obligatoria que establece los requerimientos y medidas de seguridad para la prevención de actos de interferencia ilícita que deben cumplir los concesionarios y permisionarios de transporte aéreo nacional o internacional que transporten carga, encomiendas exprés y/o correo proveniente de embarcadores, expedidores, consolidadores de carga, agentes aduanales, y/o transportistas."
CO SA 17.5/16 "Lineamientos para establecer el sistema de tarjetas de identificación aeroportuaria para personas y vehículos, en los aeródromos civiles."
CO SA 17.6/16 "Procedimiento para la inspección de pasajeros y equipaje de mano en los aeródromos civiles de servicio al público."
CO SA 17.,7/16 R1 "Que establece los requisitos para la certificación y recertificación de instructores de seguridad de la aviación civil."
CO SA 17.8/16 "Que establece el contenido de los programas de instrucción en materia de seguridad de la aviación civil."
CO SA 17.9/16 "Políticas generales para la inspección de equipaje facturado, de bodega o documentado que se transporta en aeronaves del servicio público en territorio nacional."
CO SA 17.10/16 "Que establece el contenido mínimo del programa local de seguridad aeroportuaria."
CO SA 17.16/19 "Que establece la metodología para evaluación de amenazas y gestión de riesgos en seguridad de la aviación civil."
CO SA 17.17/21 "Circular obligatoria que establece los lineamientos de un sistema de certificación y recertificación en competencia laboral del personal que lleva a cabo los controles de seguridad de la aviación en concesionarios y/o permisionarios de aeropuertos y de transporte aéreo de servicio público"
Bases Técnicas de Seguridad Informática para las Dependencias y Entidades de la Administración Pública Federal de la Coordinación de Estrategia Digital Nacional.
Ciberguía 3.0 emitida por la Secretaría de Seguridad y Protección Ciudadana.

11. VIGENCIA.

La presente Circular de Asesoramiento entra en vigor 30 días después de su firma y se dará a conocer a través de la publicación en el portal de internet de la AFAC y se actualizará conforme su contenido se vea afectado. Asimismo, estará vigente indefinidamente hasta su revisión o cancelación.

A T E N T A M E N T E

EL DIRECTOR GENERAL

GRAL. DIV. P.A. D.E.M.A. RET MIGUEL ENRIQUE VALLIN OSUNA

Ciudad de México a 09 de febrero de 2024

Firma Edgar Osvaldo Ahedo Agraz, Director Ejecutivo de Seguridad Aérea, en suplencia del Titular de la Agencia Federal de Aviación Civil, Órgano Administrativo Desconcentrado de la Secretaría de Infraestructura Comunicaciones y Transportes, con fundamento en lo dispuesto en los artículos 10, fracción X, 11 fracción II, 33, fracción XVI y 44 párrafo segundo del Reglamento Interior de la Secretaría de Infraestructura Comunicaciones y Transportes; así como lo dispuesto en el numeral 8.2. del Manual de la Organización de la Agencia Federal de Aviación Civil, publicado en el Diario Oficial de la Federación el 26 de febrero del 2021 y en términos del oficio 4.1.160 de fecha 8 de febrero de 2024.

Elaboro: JLCR **Reviso:** RGPC **Autorizo:** EOAA