ANEXO II

REGLAMENTO GENERAL DE SISTEMAS DE CIRCUITO CERRADO DE TELEVISIÓN (PÚBLICO)

I. OBJETO Y GENERALIDADES

1. El presente Reglamento tiene por objeto establecer las reglas generales para el funcionamiento y los diferentes usos de los Sistemas de Circuito Cerrado de Televisión (en adelante, “Sistema de CCTV”) en los aeropuertos integrantes del Sistema Nacional de Aeropuertos (SNA), conforme a lo establecido por la Ley N° 26.102 de Seguridad Aeroportuaria, por la Ley N° 25.326 de Protección de Datos Personales y demás normativa vigente.
2. La POLICÍA DE SEGURIDAD AEROPORTUARIA (PSA) es la autoridad de aplicación de las pautas contenidas en el presente Reglamento.
3. A los fines de la presente reglamentación, se entiende por Sistema de CCTV al conjunto de dispositivos de cámaras/videocámaras y/u otros tipos de dispositivos electrónicos, digitales, térmicos, ópticos o electro-ópticos que permiten captar y enviar imágenes hacia puestos de visualización, control o tratamiento de datos, con el objetivo de observar o registrar lo que sucede en un sector o instalación definidos.
4. Cuando se instala con propósitos integrales de control, el Sistema de CCTV comprende también a dispositivos de monitoreo, almacenamiento, procesamiento, análisis, extracción de información y aplicación de herramientas tecnológicas complementarias a la seguridad, y a los recintos físicos donde reporte el Sistema; a su vez, comprende a los procedimientos aplicados para la operación y la administración del Sistema.

II. ALCANCE Y FINALIDAD

5. El alcance del presente Reglamento se extiende a:

5.1. Los Sistemas de CCTV instalados en los aeropuertos con fines de seguridad y control aeroportuario (en adelante “Sistemas de CCTV de Seguridad”), y toda imagen registrada por los mismos.

5.2. Los Sistemas de CCTV instalados por personas humanas o jurídicas, públicas o privadas, permisionarios, explotadores de aeronaves, Organismos públicos,

empresas prestadoras de servicios y comercios en el ámbito aeroportuario que, independientemente de su finalidad o ubicación, puedan resultar de interés para la seguridad aeroportuaria (en adelante “Sistemas de CCTV de Terceros”), y toda imagen registrada por los mismos.

5.3. Los sistemas, tecnologías y dispositivos que puedan complementar a los Sistemas de CCTV.

6. Los Sistemas de CCTV de Seguridad tienen por finalidad:

6.1. Detectar conductas o actividades que puedan constituir delitos o infracciones, a través de la vigilancia permanente mediante imágenes de seguridad.

6.2. Monitorear y comunicar cualquier evento inusual o sospechoso que pudiera constituir un delito o una infracción en jurisdicción de la PSA, identificado en las imágenes de seguridad captadas.

6.3. Almacenar imágenes a los fines de las labores propias de seguridad ejercidas por la PSA.

6.4. Contribuir a la seguridad aeroportuaria mediante el control de las operaciones del aeropuerto.

7. El marco técnico de referencia para el despliegue de cámaras de Sistemas de CCTV de Seguridad se establece en las “PAUTAS PARA EL DESPLIEGUE DE SISTEMAS DE CCTV DE SEGURIDAD (RESERVADO)” que se adjunta al presente como APÉNDICE A.

8. Las reglas particulares para el uso de los Sistemas de CCTV de seguridad se establecen en el “REGLAMENTO PARTICULAR DE OPERACIONES POLICIALES CON SISTEMAS DE CCTV DE SEGURIDAD Y TECNOLOGÍAS COMPLEMENTARIAS (RESERVADO)” que se adjunta al presente como APÉNDICE B.

9. Todo Sistema de CCTV instalado en el ámbito aeroportuario se considera contribuyente a la seguridad aeroportuaria.

10. Todo Sistema de CCTV considerado como “de Seguridad” se encuentra regulado y fiscalizado por esta PSA en cuanto a su diseño, integración, control operativo y al uso y control de acceso a las imágenes. El establecimiento de la condición de “Sistema de CCTV de Seguridad” puede alcanzar a la totalidad del sistema del que

se trate, o a determinadas cámaras, componentes, equipamiento o procedimientos de operación del mismo.

11. Todo Sistema de CCTV que no se adecúe a las regulaciones establecidas por esta PSA queda bajo exclusiva responsabilidad de su propietario o responsable operativo, siendo éstos pasibles de las consecuencias civiles o penales que su instalación y uso indebido conlleven.

12. Se excluyen de las regulaciones contenidas en el presente las imágenes ocasionales captadas por el público usuario y las imágenes eventuales captadas por organismos o empresas que hayan obtenido la correspondiente autorización para la filmación de actividades con fines comerciales o institucionales, siempre que no registren hechos delictivos o vulneren la seguridad aeroportuaria.

13. **(RESERVADO)**

III. USUARIOS DE SISTEMAS DE CCTV DE SEGURIDAD

14. Quienes cumplen funciones o prestan servicios en el ámbito jurisdiccional de aplicación de este Reglamento pueden ser incorporados como usuarios de los Sistemas de CCTV de Seguridad, siempre que obtengan en cada caso en particular la autorización correspondiente de acuerdo a lo establecido en este Reglamento.

15. La Dirección Ejecutiva del Centro de Análisis, Comando y Control de la Seguridad Aeroportuaria (CEAC) es la instancia encargada de evaluar, autorizar, denegar, modificar, renovar y revocar las solicitudes de usuarios de Sistemas de CCTV de Seguridad. Las UOSP y las Unidades Regionales de Seguridad Aeroportuaria (URSA), deberán remitir las solicitudes incorporando informes técnicos contribuyentes a una mejor evaluación.

    15.1. Las solicitudes deben ser presentadas ante la UOSP, acompañando la “Solicitud de Usuario del Sistema de CCTV de Seguridad” y la “Declaración Jurada de Compromiso de Confidencialidad - CCTV” firmadas ante la UOSP por todas las personas que soliciten un usuario (ANEXOS ALFA y BRAVO del presente).

    15.2. La incorporación de usuarios al Sistema de CCTV de Seguridad está

sujeta a la evaluación de la pertinencia, la razonabilidad y la finalidad pretendida de la solicitud, considerando:

15.2.1. Las políticas, estrategias, directivas y disposiciones que dicte la PSA en el cumplimiento de sus funciones.

15.2.2. La protección de las garantías de los datos personales, de la intimidad y de la privacidad de las personas.

15.2.3. El cumplimiento de medidas de seguridad del lugar donde se efectúa la visualización de las imágenes, del equipamiento por medio del cual se visualizan, almacenan y transmiten las imágenes, y de las medidas de seguridad propias de las imágenes transmitidas.

15.3. **(RESERVADO)**

16. Los explotadores de aeropuertos y concesionarios pueden acceder a imágenes captadas por dispositivos que formen parte del Sistema de CCTV de Seguridad para sus propios propósitos, incluso aquellos no relacionados a la seguridad (tales como el control operativo de distintos sectores de un aeropuerto), de acuerdo a las pautas establecidas en el “REGLAMENTO PARA LA GESTIÓN CONJUNTA DE SISTEMAS DE CCTV DE SEGURIDAD CON EXPLOTADORES DE AEROPUERTOS O CONCESIONARIOS” que se adjunta al presente como APÉNDICE C.

17. **(RESERVADO)**

18. La autorización de acceso otorgada a un usuario es personal e intransferible. La violación de esta premisa será causal de inicio de las acciones legales y administrativas que correspondan.

19. Los usuarios de Sistemas de CCTV de Seguridad tienen las siguientes responsabilidades:

19.1. Mantener bajo resguardo los datos de permiso de acceso restringido (usuario, contraseña y otros datos del permiso) a los Sistemas de CCTV de Seguridad, no divulgarlos, ni transferirlos, ni permitir que sean accesibles a otros usuarios o terceras personas.

19.2. Dar aviso fehaciente a la UOSP correspondiente ante cualquier modificación producida por cese o cambio del personal que posea un

usuario. Esta responsabilidad es compartida por el propio usuario y por la persona jurídica, pública o privada, para la cual presta servicios.

19.3. El buen uso y conservación de los recursos materiales y técnicos que le fueran asignados.

20. Los usuarios de Sistemas de CCTV de Seguridad tienen las siguientes obligaciones:

20.1. Ante la observación de una situación que pueda presumirse como un delito o riesgo para la seguridad, dar aviso inmediato al personal policial de la UOSP.

20.2. Informar anomalías en el funcionamiento de los Sistemas de CCTV de Seguridad.

20.3. Mantener la confidencialidad sobre las imágenes a las que accedan.

21. La habilitación de usuarios para el acceso a las imágenes de los Sistemas de CCTV de Seguridad en forma remota deberá evaluarse en términos individuales, restrictivos, y basados en necesidad y pertinencia debidamente justificados por el solicitante.

21.1. Las solicitudes de acceso remoto deberán especificar medidas de seguridad de las imágenes que garanticen su transmisión segura, su integridad y su trazabilidad.

IV. SISTEMAS DE CCTV DE TERCEROS

22. Las solicitudes de habilitación de Sistemas de CCTV de Terceros deben ser presentadas ante la UOSP, conforme el “REGLAMENTO PARA LA HABILITACIÓN DE SISTEMAS DE CCTV DE TERCEROS” que se adjunta al presente como APÉNDICE D.

23. Los Sistemas de CCTV de Terceros son de exclusiva responsabilidad de sus propietarios, independientemente de la habilitación otorgada por la PSA.

24. Se propiciará la integración al Sistema de CCTV de Seguridad de aquellos otros sistemas que registren sectores de los aeropuertos que sean de circulación común.

24.1. **(RESERVADO)**

24.2. **(RESERVADO)**

25. Ningún dispositivo de captación de imágenes de terceros puede obstaculizar, vulnerar o superponerse con el Sistema de CCTV de Seguridad.

26. La PSA se reserva la potestad de desinstalar o impedir la visualización, de manera total o parcial, de cualquier dispositivo de captación de imágenes cuando:

26.1. Se establezca que el mismo es contribuyente a la seguridad aeroportuaria, resulte de interés contar con su visualización en tiempo real, y su propietario o responsable se oponga a efectuar su integración al Sistema de CCTV de Seguridad del aeropuerto.

26.2. Su ubicación y orientación vulnere la seguridad aeroportuaria.

26.3. El dispositivo resulte desproporcionado a la función que su propietario realiza en el aeropuerto.

26.4. El propietario o responsable, o los operadores del dispositivo de captación no estén facultados para observar las actividades realizadas por otros Organismos, empresas, explotadores o permisionarios.

26.5. Cualquier otra razón, condición o circunstancia que no haya sido expresamente autorizada por la PSA.

IV. REGISTROS DE LOS SISTEMAS DE CCTV

27. Cada UOSP debe crear y mantener actualizado el registro de Sistemas de CCTV instalados en el aeropuerto de su ámbito jurisdiccional.

28. **(RESERVADO)**

V. RESTRICCIONES A LA UTILIZACIÓN DE SISTEMAS DE CCTV

29. La captación, almacenamiento, transmisión, difusión y eliminación de imágenes y datos generados por Sistemas de CCTV en los términos establecidos en el presente Reglamento deben realizarse conforme a lo establecido por la Ley N° 25.326 de Protección de Datos Personales y demás normativa vigente.

30. El acceso a la información obtenida mediante el uso del Sistema de CCTV es restrictivo a los usuarios debidamente autorizados. Se prohíbe la cesión, copia o divulgación de las imágenes de seguridad, excepto en los supuestos previstos en la normativa vigente.

VI. SUPUESTOS NO CONTEMPLADOS E INNOVACIONES TÉCNICAS

31. Cualquier proyección de Sistema de CCTV, sea o no de seguridad, o sistema, tecnología o dispositivo complementario que incorpore algún aspecto técnico, procedimental o de uso distinto o no contemplado en la presente reglamentación, será motivo de una evaluación particular quedando supeditada su ejecución a la aprobación por parte de esta PSA con las condiciones que se establezcan.
    31.1. **(RESERVADO)**
32. Las innovaciones tecnológicas que requieran de una nueva reglamentación serán incorporadas a la presente como Anexos del APÉNDICE E.

ANEXO ALFA

SOLICITUD DE USUARIO DEL SISTEMA DE CCTV DE SEGURIDAD

Por la presente, quien suscribe……..en mi carácter de…….de……según la documentación que acompaña la presente, solicito la incorporación como Usuario del Sistema de CCTV de la POLICÍA DE SEGURIDAD AEROPORTUARIA instalado en el Aeropuerto……, Localidad de……., Provincia de……, en los términos y condiciones del “REGLAMENTO GENERAL DEL SISTEMA DE CIRCUITO CERRADO DE TELEVISIÓN” del Registro de la POLICÍA DE SEGURIDAD AEROPORTUARIA.

En tal sentido, solicito acceso a la visualización de las siguientes cámaras:

Cámara denominada:…… Ubicada en:…….

Cámara denominada:…… Ubicada en:…….

Cámara denominada:…… Ubicada en:…….

Cámara denominada:…… Ubicada en:…….

Cámara denominada:…… Ubicada en:…….

Fundamento la solicitud en:

……
……
……
……

Informo que las cámaras serán visualizadas en la oficina/recinto ubicado en……, el cual posee las medidas de seguridad que a continuación se detallan para impedir accesos indebidos:…… y serán monitoreadas por el personal que a continuación se detalla:

Nombre completo…….....D.N.I. N°:…....……..
Nacionalidad…….....Fecha de nacimiento…...…….....

Nombre completo…….....D.N.I. N°:…...……
Nacionalidad…….....…….....…Fecha de nacimiento…….....

Nombre completo…….....D.N.I. N°:.....…….
Nacionalidad…….....Fecha de nacimiento……..…...…

Informo los datos de contacto de la oficina/recinto desde donde se accederá al sistema:

Teléfono/s (de atención permanente 24/7):…….....……..

Correo electrónico:…….....

Acompaño a la presente la correspondiente DECLARACIÓN JURADA DE COMPROMISO DE CONFIDENCIALIDAD - CCTV de cada una de las personas con acceso a la visualización de las cámaras solicitadas y a la información producida por ellas, y copia del Documento Nacional de Identidad o del Permiso Personal Aeroportuario de cada uno, según corresponda.

Finalmente, declaro conocer y aceptar los términos del “REGLAMENTO GENERAL DE SISTEMAS DE CIRCUITO CERRADO DE TELEVISIÓN”, obligándome a cumplir y hacer cumplir en todos sus términos y condiciones, bajo apercibimiento de ser excluido del sistema con las responsabilidades penales y civiles que pudieran corresponder.

En…….....…., a los..…..... días del mes de…….....……. de 20…...

Firma:

Aclaración:

ANEXO BRAVO

DECLARACIÓN JURADA DE COMPROMISO DE CONFIDENCIALIDAD - CCTV

Por la presente, quien suscribe…….., D.N.I. N°…….., de nacionalidad ……., fecha de nacimiento……....., y en virtud de las funciones que debo cumplir como empleado de.....……, empresa/Organismo (tachar lo que no corresponda) que desarrolla labores en el Aeropuerto……..……..…….....…., Localidad de ….……....…, Provincia de ……, tomo conocimiento del “Reglamento General de Sistemas de Circuito Cerrado de Televisión” y de las obligaciones y prohibiciones que de allí se desprenden en materia de captación y almacenamiento de imágenes.

Asimismo, tomo conocimiento de que los datos personales a los que acceda en el marco del desarrollo de las labores mediante el empleo de Sistemas de CCTV que me sean asignadas, se encuentran protegidos por la Ley Nº 25.326.

En consecuencia, me comprometo a guardar la máxima reserva y secreto sobre la información a la que acceda en virtud de mis funciones; a utilizar los datos de carácter personal a los que tenga acceso, única y exclusivamente para cumplir con mis obligaciones; a observar y adoptar las medidas de seguridad que sean necesarias para asegurar la confidencialidad e integridad de la información; a no ceder en ningún caso a terceras personas no autorizadas información generada o almacenada a través del Sistema de CCTV al que tenga acceso, y a informar inmediatamente a la PSA acerca de hechos que pudieran ser constitutivos, preparatorios o posteriores a actos ilícitos o vulneratorios de la seguridad aeroportuaria, o constitutivos de infracciones o faltas administrativas relacionadas con la seguridad aeroportuaria, identificados en las imágenes de seguridad captadas.

En.....……, a los.....… días del mes de…….....……. de 20…...

Firma:

Aclaración:

ANEXO CHARLIE

GLOSARIO

Los conceptos y definiciones establecidos en el presente Glosario serán de aplicación general en todo lo relacionado con los Sistemas de CCTV en el ámbito jurisdiccional de aplicación de la seguridad aeroportuaria. A los fines del presente, se entiende por:

1. **(RESERVADO)**
2. **Almacenamiento de imágenes**: archivo generado en los equipos de grabación por las imágenes, desde el instante de captura de la imagen hasta su eliminación por parte del propio sistema, salvo que se efectúe su resguardo.
3. **(RESERVADO)**
4. **Archivo, registro, base o banco de imágenes**: conjunto organizado de imágenes que sean objeto de tratamiento o procesamiento, electrónico o no, cualquiera fuere la modalidad de su obtención, almacenamiento, grabación, acceso y reproducción.
5. **Cámara**: dispositivo, fijo o móvil (Domo o PTZ), que permite la captura de imágenes, con o sin sonido.
6. **(RESERVADO)**
7. **(RESERVADO)**
8. **(RESERVADO)**
9. **D.O.R.I.**: Conjunto de herramientas video-analíticas de Detección, Observación, Reconocimiento e Identificación.
10. **(RESERVADO)**
11. **(RESERVADO)**
12. **Imagen**: representación formada por la convergencia de los rayos luminosos que atraviesan una lente o aparato óptico, y que puede ser proyectada en una pantalla.

13. **Imagen de seguridad**: imagen utilizada con fines de seguridad o que produzcan información útil y pertinente al conocimiento estratégico o táctico sobre procedimientos policiales o hechos vulneratorios de la seguridad, y la investigación de ilícitos.

14. **(RESERVADO)**

15. **ONVIF** (*Open Network Video Interface Fórum*): el Protocolo ONVIF permite visualizar cámaras en red desde una estación de trabajo, compatibilizando con dispositivos de seguridad de diferentes fabricantes que usen otros estándares de comunicación.

16. **(RESERVADO)**

17. **Responsable de archivo, registro, base o banco de imágenes**: persona humana o jurídica, pública o privada, que es titular de un archivo, registro, base o banco de imágenes.

18. **Seguridad electrónica**: área de especialidad que utiliza herramientas tecnológicas comprendiendo, entre otros, a los sistemas de vigilancia electrónica y sus video-analíticos, de control de acceso, de detección de intrusión perimetral, de identificación biométrica y de alarmas. La seguridad electrónica es complementaria de los Sistemas de CCTV de Seguridad.

19. **(RESERVADO)**

20. **(RESERVADO)**

21. **Usuario de Sistema de CCTV de Seguridad**: persona humana poseedora de la autorización correspondiente y con un perfil de usuario otorgado por la UOSP para el acceso y utilización de los Sistemas de CCTV de Seguridad.

22. **(RESERVADO)**

23. **(RESERVADO)**

24. **(RESERVADO)**

25. **(RESERVADO)**

26. **(RESERVADO)**

27. **(RESERVADO)**

28. **(RESERVADO)**

APÉNDICE A

PAUTAS PARA EL DESPLIEGUE DE SISTEMAS DE CCTV DE SEGURIDAD (RESERVADO)

APÉNDICE B

REGLAMENTO PARTICULAR DE OPERACIONES POLICIALES CON SISTEMAS DE CCTV DE SEGURIDAD Y TECNOLOGÍAS COMPLEMENTARIAS (RESERVADO)

APÉNDICE C

REGLAMENTO PARA LA GESTIÓN CONJUNTA DE SISTEMAS DE CCTV DE SEGURIDAD CON EXPLOTADORES DE AEROPUERTOS O CONCESIONARIOS

I. OBJETO Y GENERALIDADES

1. El presente Reglamento tiene por objeto establecer las pautas para la gestión conjunta (proyección, adquisición, instalación, ampliación, actualización, operación y mantenimiento) de los Sistemas de CCTV de Seguridad y sistemas complementarios entre esta PSA y los explotadores de aeropuertos o concesionarios.

2. El explotador del aeropuerto o concesionario tiene a su cargo la adquisición, el mantenimiento, la reparación, la ampliación, la actualización y la modernización tecnológica de los Sistemas de CCTV de Seguridad, como así también el mantenimiento general del espacio donde estén instalados o se operen los sistemas. Sin perjuicio de ello, la PSA se reserva la potestad de implementar Sistemas de CCTV de Seguridad cuando lo considere conveniente.
   2.1. Los Sistemas de CCTV de Seguridad se definen como “críticos” en los términos del REGLAMENTO DE SEGURIDAD DE LA AVIACIÓN - RSA - N° 22 “CIBERAMENAZAS A LA SEGURIDAD DE LA AVIACIÓN CIVIL”.
   2.2. La información producida por los Sistemas de CCTV de Seguridad y los sistemas complementarios se gestionarán conforme la “POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE LA POLICÍA DE SEGURIDAD AEROPORTUARIA” aprobada por Disposición PSA N° 532 del 10 de mayo de 2023 o la que en el futuro la reemplace.
3. La autoridad sobre los Sistemas de CCTV de Seguridad gestionados en los términos del presente Reglamento es exclusiva de la PSA.
4. El acceso a la información producida por los Sistemas de CCTV de Seguridad será restrictivo. Se prohíbe la cesión, copia o divulgación de las imágenes, salvo en los supuestos previstos en el presente.
5. El explotador del aeropuerto o concesionario cederá a la UOSP responsable de la jurisdicción:
   5.1. El control operativo de los Sistemas de CCTV de Seguridad del aeropuerto.

5.2. La administración de altas, bajas y modificaciones de usuarios y perfiles de acceso a los programas informáticos mediante los cuales se operan los Sistemas de CCTV de Seguridad.

5.3. Los permisos necesarios para fiscalizar a los Sistemas de CCTV de Seguridad y a las redes informáticas que los soportan.

5.4. La autoridad sobre la gestión y uso de la información producida por los Sistemas de CCTV de Seguridad.

6. El explotador del aeropuerto o concesionario brindará a la PSA la asistencia técnica necesaria para la utilización de Sistemas de CCTV de Seguridad.

7. La proyección de nuevos Sistemas de CCTV de Seguridad, ampliación y/o modernización de los existentes debe basarse en la coordinación entre el concesionario o el explotador y la PSA, considerando las “PAUTAS PARA EL DESPLIEGUE DE SISTEMAS DE CCTV DE SEGURIDAD”, la evaluación particular de las condiciones de seguridad del aeropuerto y las necesidades de control de la gestión aeroportuaria.

8. En el proceso de adquisición, modernización, actualización o ampliación de un Sistema de CCTV de Seguridad, el explotador del aeropuerto o concesionario debe proveer la capacitación gratuita al personal que la PSA designe como requisito para la contratación del servicio.

9. El explotador del aeropuerto o concesionario debe cumplir las instrucciones, directivas y órdenes dictadas por la PSA en cuanto al uso de los Sistemas de CCTV de Seguridad, así como lo relativo a las modalidades de visualización y el acceso a las imágenes almacenadas.

II. INSTALACIÓN Y USO DE LOS SISTEMAS DE CCTV DE SEGURIDAD

10. La evaluación de toda proyección de Sistemas de CCTV de Seguridad se efectúa atendiendo la particularidad del proyecto, conforme los supuestos indicados a continuación:

10.1. La proyección de un Sistema de CCTV de Seguridad nuevo o la ampliación o modernización de un sistema ya existente mediante la

incorporación de más de DIEZ (10) cámaras y su equipamiento asociado será tramitada conforme las reglas del RSA N° 33 “PROCEDIMIENTO DE EVALUACIÓN, APROBACIÓN Y FISCALIZACIÓN DE LA SEGURIDAD AEROPORTUARIA EN OBRAS DE INFRAESTRUCTURA”.

10.2. Las ampliaciones o modernizaciones de Sistemas de CCTV de Seguridad existentes que prevean la incorporación de hasta DIEZ (10) cámaras y su equipamiento asociado será tramitada al nivel local mediante la presentación ante la UOSP de una solicitud de autorización acompañada de la documentación técnica correspondiente y la fundamentación del uso pretendido de las nuevas cámaras.

10.3. Cuando las ampliaciones o modernizaciones de Sistemas de CCTV de Seguridad existentes se realicen en atención a un requerimiento o solicitud de esta PSA no será necesario que el explotador o concesionario presente una solicitud, debiendo en este caso informar únicamente las características técnicas de la ampliación proyectada.

11. La existencia de Sistemas de CCTV de Seguridad debe ser informada por el concesionario o explotador en su página web oficial.

12. El uso de Sistemas de CCTV de Seguridad se regirá por los siguientes objetivos:

12.1. Prevenir, conjurar, constatar y/o investigar delitos y contravenciones, e identificar a sus autores.

12.2. Prevenir y/o verificar eventuales incidentes relativos a lesiones a las personas o daños a los bienes públicos y privados.

12.3. Asegurar la protección de los edificios, instalaciones y espacios públicos y aeronáuticos, así como sus accesos.

12.4. Permitir un relevamiento de los distintos sectores del aeropuerto a fin de optimizar las prestaciones de los servicios a los pasajeros.

12.5. Contribuir a la gestión operativa del aeropuerto.

13. En ningún caso los Sistemas de CCTV de Seguridad regidos por el presente Reglamento podrán captar sonidos.

14. La PSA tiene prioridad para el uso de los comandos de movimientos de las cámaras del tipo PAN TILT ZOOM (PTZ), o que posean algún tipo de movimiento, debiendo coordinar con el explotador o concesionario el modo en que éstos podrán visualizar esas cámaras cuando se encuentren autorizados.

15. Se prohíbe divulgar información de los Sistemas de CCTV de Seguridad sin autorización expresa de la PSA.

III. VISUALIZACIÓN Y ACCESO A LAS IMÁGENES DE SEGURIDAD

16. La PSA puede otorgar al explotador del aeropuerto o concesionario acceso a la visualización de aquellas imágenes en tiempo real o datos que sean de su incumbencia, siempre que no afecten la seguridad aeroportuaria y sean requeridas formalmente y de manera fundada.

17. El explotador del aeropuerto o concesionario puede solicitar la visualización en forma permanente de cámaras que correspondan a la gestión operativa del aeropuerto, conforme las siguientes condiciones:

    17.1. Se otorgará la visualización permanente cuando se cumplan las siguientes condiciones:

        17.1.1. No se trate de cámaras que registran la aplicación de controles de seguridad en puestos fijos.

        17.1.2. Se trate de cámaras que captan las instalaciones correspondientes a los Organismos o dependencias estatales y el solicitante cuente con la autorización expresa de la autoridad correspondiente.

        17.1.3. Las estaciones de monitoreo cuenten con un aviso de confidencialidad que deba ser aceptado por el operador al momento de identificarse para ingresar al sistema. La PSA facilitará al explotador o concesionario el texto que deberá incorporar al sistema para cumplir con el presente requisito.

    17.2. La solicitud se efectúa mediante nota acompañando la “Solicitud de Usuario del Sistema de CCTV de Seguridad” y la “Declaración Jurada de Compromiso de Confidencialidad - CCTV” –ANEXOS ALFA y

BRAVO, respectivamente del “REGLAMENTO GENERAL DE SISTEMAS DE CIRCUITO CERRADO DE TELEVISIÓN”–, completado y firmado por la autoridad que el explotador del aeropuerto o concesionario designe a tal fin.

17.3. Cuando el sistema permita el uso de información analítica, se podrá otorgar acceso a esa información a los fines de utilizarla en la gestión operativa del aeropuerto, siempre que ello no comprometa la seguridad aeroportuaria, bajo las siguientes condiciones:

17.3.1. Las imágenes generadas pueden ser interrumpidas por la PSA ante un evento u operativo que así lo requiera, siendo repuestas al explotador del aeropuerto una vez finalizado el mismo. No se interrumpirá la provisión de la información analítica cuando pueda ser separada de la imagen.

17.3.2. El acceso a la información analítica será otorgado a usuarios que operen el sistema y a cuentas lógicas de usuarios de servicios que interactúen con otros sistemas o con algoritmos para hacer uso de dichas analíticas mediante API (interfaz de programación de aplicaciones) o servicios a través de internet (*Web services*).

17.3.3. El administrador de la plataforma de video deberá otorgar privilegios para poder desarrollar algoritmos que puedan hacer uso de las analíticas, tanto de las cámaras como de los sistemas NVR, para analizar automáticamente y en tiempo real las imágenes captadas y evaluar la información de un vídeo de acuerdo a patrones específicos prestablecidos. Las imágenes analizadas no podrán ser vistas por los usuarios, quienes tendrán acceso sólo a los datos esperados por el procesamiento que realicen los algoritmos, sin dejar registro de las imágenes.

17.3.4. Se podrá solicitar la información analítica del conjunto de las cámaras instaladas en todas las zonas del aeropuerto alcanzadas por el Sistema de CCTV de Seguridad, siempre que se informe y justifique el uso de las imágenes, ponderando la

gestión operativa del aeropuerto, sin afectar la seguridad aeroportuaria.

17.3.5. Se prohíbe al explotador del aeropuerto o concesionario utilizar información analítica producida sobre imágenes de procedimientos policiales.

18. Las solicitudes de imágenes en tiempo real desde ubicaciones remotas serán evaluadas en forma individual, conforme a solicitudes específicas debidamente justificadas en la necesidad y en la pertinencia.

18.1. Las solicitudes deberán especificar medidas de seguridad de las imágenes que garanticen su transmisión segura, su integridad y su trazabilidad.

19. El concesionario o explotador podrá solicitar la visualización de un hecho ocurrido o una copia de las imágenes, en cuyo caso:

19.1.1. El explotador del aeropuerto o concesionario podrá designar hasta DOS (2) responsables que tendrán acceso a la visualización de imágenes de archivo.

19.1.2. El Jefe de UOSP y el Administrador del aeropuerto elaborarán y aprobarán un procedimiento local para la visualización de imágenes de archivo.

19.1.3. La visualización se realizará en las instalaciones bajo control de la UOSP de jurisdicción, ante la presencia de un Oficial de la PSA y siempre que no interfiera con operaciones policiales que se estén produciendo en ese momento.

19.2. El concesionario o explotador podrá solicitar mediante nota con fecha y número de registro dirigida al Jefe de UOSP las imágenes de un hecho de interés, identificando el día, la hora o el rango horario aproximado, el sector del aeropuerto, una descripción y su interés en los mismos, y de ser posible, la identificación de las cámaras que registraron el hecho.

19.2.1. En caso de que opere alguna causal para restringir la solicitud, se realizará un resguardo de las imágenes por un plazo no mayor a NOVENTA (90) días corridos, y se informará al solicitante que las imágenes sólo se entregarán contra presentación de nota u oficio de autoridad competente, judicial o

fiscal, o representante letrado debidamente autorizado a requerirla.

19.2.2. En caso de que las imágenes captadas registren hechos judicializados o judicializables, se denegará la solicitud y se informará que dichas imágenes deben ser solicitadas a la autoridad judicial competente. Preventivamente las imágenes serán resguardadas.

19.2.3. En caso de que no opere ninguna causal para requerir autorización de otra índole, el COC confeccionará la respuesta a la solicitud, junto con las imágenes extraídas, elevándola a la División de Operaciones Policiales para su revisión y posterior elevación a la Jefatura de UOSP, instancia que procederá a la entrega al solicitante, quien deberá firmar de conformidad la recepción de las mismas. La respuesta deberá contener una descripción que permita identificar las imágenes que se entregan.

19.2.4. El personal del COC podrá efectuar recortes espaciales y temporales sobre las secuencias de imágenes registradas cuando ello posibilite satisfacer la solicitud sin vulnerar la seguridad aeroportuaria, de lo cual deberá dejar debida constancia en la elevación de respuesta a la solicitud.

20. Se prohíbe la entrega de imágenes sin autorización de la Jefatura de UOSP u otra autoridad competente.

20.1. Ante una controversia en cuanto a la pertinencia de obtener las imágenes, se resguardarán las imágenes y se elevará la solicitud para su resolución por una instancia superior a la Jefatura de UOSP.

21. Si el personal designado por el explotador del aeropuerto o concesionario observa situaciones que puedan presumirse como un delito o riesgo para la seguridad aeroportuaria o para la seguridad de la aviación civil, deberá dar aviso inmediato al personal policial.

22. Los recintos y las terminales de visualización que se encuentren bajo el control del explotador del aeropuerto o concesionario deberán poseer las siguientes medidas mínimas de seguridad:

22.1. Los gabinetes de las terminales de visualización deberán garantizar que no pueda efectuarse una extracción de imágenes o el sabotaje al sistema en su integridad y funcionamiento.

22.2. El acceso del personal al recinto de visualización deberá estar expresamente autorizado por el responsable designado por parte del explotador o concesionario. Podrá solicitarse acceso al recinto de visualización para los siguientes supuestos:

22.2.1. Personal que posea usuario y acceso seguro al sistema.

22.2.2. Personal que designe el explotador del aeropuerto o concesionario y que no posea usuario y acceso seguro al sistema, pero que por sus responsabilidades deba acceder al recinto de monitoreo.

22.2.3. Personal que no pertenezca al explotador del aeropuerto o concesionario y que eventualmente deba ingresar al recinto de monitoreo por razones fundadas.

22.3. Los recintos donde se realicen tareas de visualización deberán contar con control de acceso biométrico, con tarjeta de proximidad tipo MIFARE o cualquier otra tecnología que asegure el control de acceso.

22.4. Se prohíbe el ingreso al recinto de visualización con cámaras fotográficas, filmadoras o cualquier otro dispositivo capaz de captar imágenes del sistema o del recinto, a excepción de los teléfonos celulares del personal, los cuales deberán ser declarados ante la UOSP. El responsable del explotador del aeropuerto o concesionario deberá supervisar dichos dispositivos no sean utilizados indebidamente para captar imágenes generadas por Sistemas de CCTV de Seguridad.

22.5. El explotador del aeropuerto o concesionario podrá, eventualmente, solicitar mediante nota una excepción a la prohibición indicada en el numeral anterior para realizar un registro fílmico del recinto de visualización con fines institucionales, la cual será evaluada y autorizada por la UOSP, instancia que fiscalizará la implementación de las medidas de seguridad necesarias para impedir que se registren imágenes del sistema.

22.6. Las imágenes que se proyecten en los monitores de visualización deberán contar con una marca de agua en la que se observe la denominación del explotador del aeropuerto o concesionario, la identificación del aeropuerto, la identificación de la/s cámara/s, la fecha y la hora, y la identificación del usuario que se encuentra utilizando el monitor.

23. La PSA podrá ingresar a los recintos de visualización de imágenes del concesionario o explotador del aeropuerto sin necesidad de autorización previa.

IV. GESTIÓN DE SISTEMAS COMPLEMENTARIOS

24. La implementación por parte de explotadores de aeropuertos o concesionarios de sistemas tecnológicos utilizados para diversos propósitos de control operativo de los aeropuertos y que resulten complementarios a los Sistemas de CCTV de Seguridad serán evaluados en forma particular por la PSA a través de las mismas Instancias indicadas en el numeral 31.1 (RESERVADO) del “REGLAMENTO GENERAL DE SISTEMAS DE CIRCUITO CERRADO DE TELEVISIÓN”.
25. Independientemente del propósito por el cual se propicia la implementación de un sistema complementario, si el dispositivo de captación de información produce una imagen el sistema será considerado parte del Sistema de CCTV de Seguridad.
    25.1. En estos casos, podrá evaluarse y eventualmente autorizarse el acceso por parte del personal del explotador del aeropuerto o concesionario a imágenes grabadas siempre que las mismas se limiten al tiempo mínimo necesario para cumplir con el propósito del sistema complementario; transcurrido ese tiempo, las imágenes deben quedar a resguardo en las unidades de almacenamiento del Sistema de CCTV de Seguridad.
26. En ningún caso los sistemas complementarios podrán interferir con los Sistemas de CCTV de Seguridad.
27. En caso de que el sistema complementario utilice imágenes del Sistema de CCTV de Seguridad para realizar su propósito y, para ello, se disponga de un servidor o soporte distinto del alojado en el propio Sistema de CCTV de Seguridad, deberá garantizarse que el servidor o soporte del sistema complementario no realice

extracciones de imágenes sin autorización ni las conserve durante más tiempo que el autorizado.

28. Toda implementación de un sistema complementario debe contemplar la provisión a la PSA de una herramienta que permita suspender la provisión de imágenes al explotador del aeropuerto o concesionario, manteniéndolas habilitabas para la PSA.

APÉNDICE D

REGLAMENTO PARA LA HABILITACIÓN DE SISTEMAS DE CCTV DE TERCEROS (PÚBLICO)

I. OBJETO

1. El presente Reglamento tiene por objeto establecer las pautas para la habilitación de Sistemas CCTV solicitada por parte de personas humanas o jurídicas, públicas o privadas (“Tercero” o “Terceros”, según se consigne).

    1.1. Las reglas contenidas en el presente aplican a los Sistemas de CCTV instalados o a instalarse en locaciones físicas inmuebles.

    1.2. Los Sistemas de CCTV proyectados a instalarse en vehículos terrestres que no permanezcan en el aeropuerto o en aeronaves serán objeto de evaluaciones particulares a cargo del Centro de Análisis Comando y Control de la Seguridad Aeroportuaria (CEAC), sin perjuicio de lo indicado en el numeral 2.

    1.3. El presente Reglamento no será de aplicación para aquellos Sistemas de CCTV instalados por explotadores de aeropuertos o concesionarios con fines de seguridad. No obstante, se aplicará a sus Sistemas de CCTV instalados para captación de imágenes en el interior de sus espacios propios.

2. Todo Sistema de CCTV de Tercero que se instale en el ámbito aeroportuario y no solicite su habilitación ante la PSA quedará sujeto a las consecuencias civiles, penales o administrativas que pudieran corresponder por el uso indebido del sistema, pudiendo la PSA obturar o retirar cámaras ubicadas en lugares no habilitados cuando corresponda por razones de seguridad.

3. Para la habilitación de un Sistema de CCTV de Tercero deberá considerarse su finalidad, su razonabilidad y su proporcionalidad, a efectos de armonizar el interés particular del solicitante con el interés público.

4. Por principio general, un Sistema de CCTV de Tercero se considera contribuyente a la seguridad aeroportuaria. Los Jefes de las Unidades Regionales de Seguridad Aeroportuaria (URSA) podrán habilitar un sistema que no reúna todos los requisitos técnicos establecidos en el presente en tanto no atente contra la seguridad aeroportuaria.

5. **(RESERVADO)**

II. ASPECTOS GENERALES PARA LA HABILITACIÓN

6. El Sistema de CCTV de Tercero será administrado por la persona humana o jurídica, pública o privada, que haya solicitado para tal fin la habilitación a esta PSA.

    6.1. Cuando el sistema sea instalado con fines de seguridad deberá contratarse para su operación a una empresa prestadora del servicio de seguridad privada en el ámbito aeroportuario.

7. Cuando el Sistema de CCTV de Tercero se proponga para implementar medidas de seguridad en cumplimiento de la normativa vigente aplicable deberá ser operado exclusivamente por personal de una empresa prestadora del servicio de seguridad privada en el ámbito aeroportuario.

8. Todas las personas que accedan al Sistema de CCTV de Tercero habilitado por la PSA deberán firmar la “Declaración Jurada de Compromiso de Confidencialidad – CCTV de Terceros”, incorporada al presente Reglamento como ANEXO ALFA.

9. El responsable del Sistema de CCTV de Tercero habilitado deberá adoptar las medidas que sean necesarias para impedir el acceso no autorizado a las imágenes.

10. Cuando el Sistema de CCTV de Tercero se instale en la parte pública de un aeropuerto, su propietario deberá dar cumplimiento a lo dispuesto en los numerales 5 y 6 del ANEXO a la Resolución MS N° 283/12, por la que se aprobó el “PROTOCOLO GENERAL DE FUNCIONAMIENTO DE VIDEOCÁMARAS EN ESPACIOS PÚBLICOS”.

11. La habilitación tendrá vigencia mientras permanezcan inalteradas las características técnicas del Sistema de CCTV de Tercero, así como la cantidad, ubicación y orientación de las cámaras que lo componen.

12. Cuando el Sistema de CCTV de Tercero cuya habilitación se solicita contemple cámaras que capten imágenes por fuera de los espacios físicos propios del solicitante y su perímetro físico o virtual, la evaluación de la UOSP y de la URSA deberá considerar particularmente si tales cámaras resultan de interés para la

seguridad aeroportuaria y, además, aplicar las prescripciones establecidas en los numerales 26.1, 26.2, 26.3, 26.4 y 26.5 del “REGLAMENTO GENERAL DE SISTEMAS DE CIRCUITO CERRADO DE TELEVISIÓN”.

12.1. Se considera “espacio propio” a aquel al cual accede el personal dependiente del propietario del Sistema de CCTV de Tercero, personas ajenas pero debidamente autorizadas por el mismo propietario y clientes en el caso de locales comerciales, independientemente de las características físicas del espacio (cerrado, abierto, semi-cubierto, etc.).

12.2. Se considera “espacio no propio” a aquel por el cual puede transitar una persona que es ajena al propietario o responsable del sistema de CCTV de Tercero sin necesidad de autorización de éste.

13. En el supuesto indicado en el numeral 12 del presente, la PSA podrá requerir total o parcialmente las condiciones indicadas a continuación, según la evaluación particular:

13.1. La integración obligatoria al Sistema de CCTV de Seguridad del aeropuerto.

13.2. Cuando se trate de cámaras móviles tipo domo, que el control de movimientos sea compartido, debiendo ceder a la PSA la prioridad en el movimiento ante su requerimiento.

13.3. Que el sistema de grabación y almacenamiento disponga de medidas de seguridad físicas o procedimentales para que la extracción de imágenes se realice únicamente a instancias de la PSA.

13.4. Que las imágenes generadas por el sistema posean identificación de origen y trazabilidad con marca de agua, cuando ello sea requerido por la PSA en la evaluación de la solicitud de habilitación.

13.5. Que se garantice la imposibilidad de extraer imágenes de esas cámaras sin la correspondiente autorización de la PSA.

14. El responsable del Sistema de CCTV de Tercero habilitado deberá garantizar la seguridad y confidencialidad de las imágenes, de modo de evitar su adulteración,

pérdida, cesión o tratamiento no autorizado, y detectar desviaciones de información intencionales o accidentales.

15. La adulteración, destrucción o alteración de imágenes que estén relacionadas con hechos que formen parte de una investigación en curso podrán ser motivo de denuncia penal.

16. La cesión o difusión de imágenes a personas no autorizadas, así como la sustracción, alteración o pérdida de imágenes captadas del “espacio no propio” del propietario del Sistema de CCTV de Tercero deberá ser comunicada a la PSA de manera inmediata apenas conocida la situación.

III. CONSIDERACIONES TÉCNICAS PARA LA HABILITACIÓN

17. El cumplimiento total o parcial de las especificaciones técnicas indicadas en el presente apartado deberá ser evaluado por la autoridad competente, considerando para cada caso lo indicado en el numeral 4 del presente Reglamento.

18. Los Sistemas de CCTV de Terceros a instalarse deberán ser de tecnología IP (Protocolo de Internet) y su sistema de administración y almacenamiento de imágenes deberán ser de tecnología NVR (Grabador de Video en Red), debiendo todos sus componentes poseer estándar ONVIF (Foro Abierto de Interfaces de Video en Red) en su versión más actualizada disponible.

19. Las imágenes en tiempo real deberán cumplir las siguientes características:

    19.1. Calidad igual o superior a UN (1) megapixel (1Mpx).

    19.2. Velocidad de reproducción igual o superior a VEINTICUATRO (24) cuadros por segundo.

    19.3. Formato de compresión de video H.264 o superior.

20. Los Sistemas de CCTV de Terceros de más de DIEZ (10) cámaras deberán poseer una capacidad de almacenamiento de datos suficiente para grabar en forma continua las VEINTICUATRO (24) horas, los SIETE (7) días de la semana por un tiempo igual o superior a los TREINTA (30) días corridos desde el momento de su captación.

20.1. El tiempo de almacenamiento podrá reducirse cuando el sistema contemple algoritmos analíticos que permitan la activación de la grabación ante movimientos, en cuyo caso la grabación deberá garantizar el registro completo de cualquier movimiento que se produzca dentro del espacio que capte la cámara.

21. El sistema de grabación y almacenamiento de datos podrá ser físico o remoto.

22.1. En caso de sistema físico, el mismo deberá estar ubicado físicamente en un lugar que cuente con medidas de seguridad físicas o electrónicas o procedimentales que sean proporcionales al riesgo que evalúen la UOSP y la URSA como parte del trámite de habilitación.

22.2. En caso de proponer la contratación de un servicio de almacenamiento remoto, la evaluación de la habilitación deberá considerar los requisitos técnicos establecidos en el numeral 9 de las "ESPECIFICACIONES TÉCNICAS PARA SISTEMAS DE CCTV DE SEGURIDAD" (Apéndice E), particularmente si el sistema contempla cámaras por fuera del espacio propio del solicitante.

IV. TRÁMITE DE HABILITACIÓN

23. El trámite de habilitación de un Sistema de CCTV de Tercero comenzará con la presentación de una Nota dirigida a la UOSP correspondiente al aeropuerto en el cual se pretende instalar el mismo.

24. La Nota deberá consignar la siguiente información:

24.1. Identificación del solicitante:

24.1.1. En el caso de personas humanas, deberá consignarse nombre/s y apellido/s, nacionalidad, tipo y número de documento de identidad, domicilio fiscal, teléfono y correo electrónico.

24.1.2. En el caso de personas jurídicas, deberá consignarse razón social, Clave Única de Identificación Tributaria (CUIT), domicilio fiscal, datos del responsable del Sistema de CCTV (con los mismos datos exigidos a las personas humanas), adjuntando

poder o autorización para representar a la razón social ante la PSA.

24.2. Actividad que desarrolla en el aeropuerto.

24.3. Aeropuerto en el que se instalará el sistema.

24.4. Razón o motivo para la instalación del sistema.

24.5. Planimetría detallando:

24.5.1. Cantidad, ubicación y orientación de los dispositivos a instalar.

24.5.2. Tipo de cámara/videocámaras (fijas, móviles, IP, etc.).

24.5.3. Zona de cobertura de dichas cámaras/videocámaras.

Ubicación del equipo de grabación y sala de monitoreo (de corresponder).

24.6. Especificaciones técnicas sobre el sistema de procesamiento y almacenamiento de la información, indicando marca, modelo, tiempo de guardado de las imágenes, calidad y formato en que se grabarán, lugar donde se monitorean o graban (si el mismo se encuentra dentro o fuera del aeropuerto y si se pretende contar con más de una sala de monitoreo).

24.7. Nómina del personal a cargo de la operatoria en cualquiera de sus fases, etapas y partes del procesamiento y o tratamiento de imágenes, informando:

24.7.1. Nombre/s y apellido/s, nacionalidad, tipo y número de documento de identidad, domicilio real, teléfono y correo electrónico.

24.7.2. Número de Permiso Personal Aeroportuario de Seguridad por cada persona declarada, o en su defecto, constancia de haber iniciado el trámite correspondiente.

24.8. De corresponder, razón social de la empresa de seguridad privada que realizará la operación o monitoreo del Sistema de CCTV, informando:

24.8.1. Nómina del personal a cargo de la operatoria en cualquiera de sus fases, etapas y partes del procesamiento y o tratamiento de imágenes, informando los mismos datos

personales que los requeridos en el numeral 24.7 del presente Reglamento.

24.8.2. Nómina del personal que supervisará las tareas, responsable jerárquico superior o del gerenciamiento del sistema, informando los mismos datos personales que los requeridos en el numeral 24.7 del presente Reglamento.

24.9. Se deberá adjuntar una “Declaración Jurada de Compromiso de Confidencialidad – CCTV de Terceros” (incorporada al presente Reglamento como ANEXO ALFA), rubricada por cada una de las personas que tengan o pudieran tener acceso al Sistema de CCTV.

24.9.1. Cuando el sistema proyectado supere las DIEZ (10) cámaras, la firma de la “Declaración Jurada de Compromiso de Confidencialidad – CCTV de Terceros” del responsable a cargo del sistema deberá estar certificada ante escribano público, mientras que las de los operadores podrán ser certificadas ante la UOSP correspondiente.

24.9.2. Cuando el sistema cuya habilitación se solicita no supere las DIEZ (10) cámaras, la certificación de la totalidad de las firmas podrá hacerse ante la UOSP correspondiente.

24.10. En cuanto al proveedor del sistema: razón social, nómina del personal que intervendrá en la instalación, período en el que trabajarán en la instalación y constancia de trámite de Permiso Personal Aeroportuario de Seguridad.

24.11. Certificado de inscripción de la base de datos en el Registro Nacional de Bases de Datos, dependiente de la Dirección Nacional de Protección de Datos Personales.

24.12. Nota de presentación firmada. En los casos de personas jurídicas, la nota deberá acompañarse del poder que acredite la potestad del firmante.

25. Presentada la solicitud de habilitación, la UOSP deberá:

25.1. Verificar la documentación presentada.

25.2. Remitir las actuaciones a la URSA, junto con un informe de evaluación de la solicitud.

25.3. Obtenida la respuesta por parte de la URSA, con el otorgamiento o el rechazo de la habilitación solicitada, notificar al solicitante.

26. Recibidas las actuaciones originadas por la UOSP, la URSA evaluará la solicitud pudiendo:

26.1. Otorgar o rechazar la habilitación, fundamentando la decisión adoptada.

26.2. Requerir información adicional que resulte necesaria para realizar la evaluación.

27. Toda modificación de las características y especificaciones del Sistema de CCTV de Tercero habilitado o del personal a cargo de la operación, supervisión o gerenciamiento del sistema en cualquiera de sus fases, etapas y partes del procesamiento de la información, deberá ser informada fehacientemente a la UOSP correspondiente, acompañando la documentación relativa a la modificación que se propicia, dentro de los DIEZ (10) días hábiles de efectuada la modificación.

27.1. El solicitante podrá continuar operando el sistema con una habilitación provisoria otorgada por la UOSP de asiento.

27.2. La UOSP deberá evaluar si la modificación amerita un nuevo trámite de habilitación o si puede mantenerse la otorgada.

27.3. **(RESERVADO)**

28. Toda persona humana o jurídica, pública o privada, que posea un Sistema de CCTV de Tercero habilitado por la PSA, y requiera dejarlo fuera de servicio temporal o definitivamente, deberá informar previamente tal circunstancia a la UOSP correspondiente.

29. Los gastos que demande el cumplimiento de los requisitos aquí establecidos, así como los originados por la habilitación, instalación (incluyendo la integración al Sistema de CCTV de Seguridad del aeropuerto, cuando corresponda), operación o actualización del Sistema de CCTV de Tercero, correrán por cuenta del solicitante.

V. OBLIGACIONES RELATIVAS A LA SEGURIDAD AEROPORTUARIA

30. Si de la observación en tiempo real o en tiempo pasado de imágenes se toma conocimiento de la comisión de hechos que pudieran ser constitutivos, preparatorios o posteriores a actos ilícitos o vulneratorios de la seguridad, los operadores del sistema o el responsable tienen la obligación de informar inmediatamente a la PSA, aplicándose en cada caso las siguientes medidas:

    30.1. Las imágenes registradas se deberán poner a disposición de la PSA con la mayor inmediatez posible y, en todo caso, en el plazo máximo de DOCE (12) horas desde su almacenamiento. De no poder cumplirse este requerimiento por circunstancias de fuerza mayor (las que serán debidamente justificadas), se relatarán verbalmente los hechos observados ante la PSA, debiendo dejarse constancia escrita del relato recibido en sede policial mediante una denuncia o una declaración testimonial, pudiéndose ampliar el plazo para la entrega de las grabaciones.

31. La omisión de informar a la PSA acerca de hechos que pudieran ser constitutivos, preparatorios o posteriores a actos ilícitos o vulneratorios de la seguridad podrá ser motivo de denuncia penal, sin perjuicio de las sanciones administrativas que puedan corresponder.

32. El uso indebido del Sistema de CCTV de Tercero habilitado, así como cualquier otro incumplimiento al presente Reglamento será pasible de las sanciones administrativas, civiles o penales que correspondan.

    32.1. De manera preventiva, la PSA podrá desinstalar y/o impedir la visualización, de manera total o parcial, de cualquier dispositivo de captación de imágenes o cualquier otro componente del sistema, incluyendo la clausura del recinto donde se realiza la visualización o a donde reportan las imágenes.

VI. LIBROS DE REGISTROS

33. Los propietarios o responsables de Sistemas de CCTV de Terceros que cuenten con más de DIEZ (10) dispositivos de captación de imágenes deben llevar los siguientes registros rubricados y foliados por la UOSP de la jurisdicción:

33.1. Libro de Registro de Inspecciones PSA, en el que se dejará constancia de:

33.1.1. Fecha en que se realiza la inspección.

33.1.2. Detalle de la documentación, libros, material y personal inspeccionados.

33.1.3. Observaciones formuladas, si las hubiere.

33.1.4. Identificación de los funcionarios actuantes de la PSA y del personal del prestador de servicios de seguridad privada que hubiesen intervenido en la misma.

33.1.5. Intimación al responsable del sistema a formular el descargo pertinente en caso de encontrarse irregularidades, dejándose constancia de ello.

33.2. Libro de Registro de Imágenes Resguardadas y Entregadas, en el que se dejará constancia de:

33.2.1. Número de orden, fecha, soporte electrónico y lugar de almacenamiento en el que se realiza el resguardo.

33.2.2. Fecha, hora y breve descripción del hecho sobre el que se resguardaron imágenes.

33.2.3. Registro del documento mediante el que se solicitó dicha información (fecha, Organismo solicitante –PSA, Poder Judicial, Ministerio Público u otra autoridad competente–, número de nota, memorando, oficio, actuación, etc.).

33.2.4. Fecha, firma y aclaración de la persona que recibió dicha información.

34. Los libros de registro deberán conservarse por un plazo mínimo de CINCO (5) años y deberán ser exhibidos a la PSA cuando ésta así lo requiera.

35. La sustracción o pérdida de alguno de los libros deberá ser denunciada a la PSA en el término perentorio de VEINTICUATRO (24) horas de sucedido el hecho.

ANEXO ALFA

DECLARACIÓN JURADA DE COMPROMISO DE CONFIDENCIALIDAD - CCTV de Terceros

Por la presente, quien suscribe, ……., DNI N°……., de nacionalidad ……., y en virtud de las funciones que debo cumplir como empleado de ……, empresa/Organismo (*tachar lo que no corresponda*) que desarrolla labores en el Aeropuerto……..……..……, Localidad de ….……, Provincia de……, tomo conocimiento del "REGLAMENTO PARA LA HABILITACIÓN DE SISTEMAS DE CCTV DE TERCEROS" y de las obligaciones y prohibiciones que de allí se desprenden.

Asimismo, tomo conocimiento de que los datos personales a los que acceda en el marco del desarrollo de las labores mediante el empleo de Sistemas de CCTV que me sean asignadas se encuentran protegidos por la Ley Nº 25.326.

En consecuencia, me comprometo a guardar la máxima reserva y secreto sobre cualquier tipo de información a la que acceda en virtud de mis funciones; a utilizar los datos de carácter personal a los que tenga acceso, única y exclusivamente para cumplir con mis obligaciones; a observar y adoptar las medidas de seguridad que sean necesarias para asegurar la confidencialidad e integridad de la información; a no ceder en ningún caso a terceras personas no autorizadas información generada o almacenada a través del Sistema de CCTV al que tenga acceso, y a informar inmediatamente a la PSA acerca de hechos que pudieran ser constitutivos, preparatorios o posteriores a actos ilícitos o vulneratorios de la seguridad aeroportuaria, o constitutivos de infracciones o faltas administrativas relacionadas con la seguridad aeroportuaria, identificados en las imágenes de seguridad captadas.

En……..…, a los...….. días del mes de…….. de 20…...

Firma:
Aclaración:

APÉNDICE E

ESPECIFICACIONES TÉCNICAS PARA SISTEMAS DE CCTV DE SEGURIDAD

I. OBJETO

1. El presente documento tiene por objeto establecer las especificaciones técnicas para la proyección, planificación, incorporación e implementación de Sistemas de CCTV de Seguridad en el Sistema Nacional de Aeropuertos (SNA), así como también los lineamientos técnicos respecto a las medidas de seguridad para la protección de los componentes del sistema y de la información producida por los mismos.

II. ASPECTOS TÉCNICOS GENERALES DE SISTEMAS DE CCTV DE SEGURIDAD

2. Los Sistemas de CCTV de Seguridad deberán ser digitales, basados en tecnología IP y bajo Protocolo ONVIF (en la versión más actual disponible al momento de implementar el sistema).
3. Cuando por razones técnicas o materiales no sea posible alcanzar los estándares técnicos establecidos en el presente, se podrá considerar si otros estándares pueden ser adecuados (de manera parcial o integral) a las características específicas del aeropuerto (sus partes y sectores) donde se proyecte la implementación. A tal efecto, deberá evaluarse la implementación en función de los objetivos específicos de seguridad, las hipótesis delictivas y el nivel de riesgo vigente.
4. El tiempo estándar de almacenamiento de imágenes se establece en TREINTA Y CINCO (35) días. La PSA podrá autorizar el resguardo de imágenes por un tiempo menor al establecido cuando resulte suficiente y adecuado para la seguridad aeroportuaria de aeropuertos cuya complejidad o nivel de riesgo lo permitan.
5. La calidad de imagen deberá ser de VEINTICINCO (25) cuadros por segundo o superior y con una compresión H.265 o superior.
6. Los Sistemas de CCTV de Seguridad deberán incorporar algoritmos analíticos proporcionales a las hipótesis de seguridad propias de cada aeropuerto, lo que resultará de la evaluación casuística de cada proyecto de implementación.

7. Las cámaras dotadas de lentes especiales pueden suplir en cantidad a las cámaras con lentes comunes.

    7.1. Se evaluará en cada caso en particular si los tipos de lentes seleccionados satisfacen las necesidades en términos de seguridad.

        7.1.1. En virtud de las diferentes opciones tecnológicas de lentes de cámaras disponibles al momento de la proyección se deberán establecer las más adecuadas según sea el requerimiento de uso y las características del sector a monitorear (por ejemplo, Mini Domo Interior IP, Bulled Exterior IP, Domo Exterior C/PTZ IP, Lente Gran Angular, Ojo de Pez, Infrarrojas, Térmicas, u otro dispositivo de captación de imagen que pudiera existir en el mercado).

    7.2. Independientemente del tipo de cámara que se proyecte instalar, deberán evaluarse sin excepción en cada uso y requerimiento al momento de la instalación los siguientes factores principales:

        7.2.1. Distancia entre la cámara de seguridad y el área que se desea cubrir. Debe considerarse que cuanto mayor sea la distancia focal de la lente, menor será el ángulo de visión y mayor será la distancia de monitoreo.

        7.2.2. Ancho de superficie del campo visual a cubrir.

        7.2.3. Tamaño del sensor de la cámara a instalar.

        7.2.4. Campo de visión (evaluación del lente según la distancia focal).

8. El equipamiento de los Sistemas de CCTV de Seguridad instalados en los COC o en otras instalaciones donde reporten imágenes del sistema, deberá contar con medidas de seguridad aprobadas por la UOSP del aeropuerto. Los distintos recintos que conformen un COC deberán disponer de un único acceso que posea control, ya sea por medio de un sistema de cerradura, acceso con clave, tarjeta de acceso, o cualquier mecanismo eléctrico, electrónico o mecánico que proporcione la seguridad necesaria; el mismo requisito aplica para cualquier otro recinto donde reporten imágenes de Sistemas de CCTV de Seguridad.

9. Almacenamiento remoto: podrá evaluarse la factibilidad de contratar un servicio de almacenamiento remoto para los Sistemas de CCTV de Seguridad, en tanto cumplan las siguientes condiciones:

9.1. Cuando se trate de las imágenes generadas por el sistema, independientemente de su formato o de la modalidad de almacenamiento, la persona humana o jurídica que provea el servicio de almacenamiento remoto deberá poseer dentro del territorio de la REPÚBLICA ARGENTINA:

9.1.1. El domicilio fiscal.

9.1.2. El domicilio real o domicilio legal, según corresponda a una persona humana o jurídica.

9.1.3. Las oficinas e instalaciones desde donde se presta el servicio contratado.

9.1.4. El personal contratado para prestar el servicio.

9.1.5. Los servidores de almacenamiento, los sistemas de back-ups, los sistemas de resguardo y todo otro equipamiento que se utilice para la prestación del servicio contratado.

9.2. La conexión entre el Sistema de CCTV de Seguridad instalado en el aeropuerto y la unidad de almacenamiento remoto deber realizarse mediante una red privada.

9.3. La instalación, configuración, administración, mantenimiento, adición de la capacidad de almacenamiento o cualquier otro procedimiento que involucre la logística u operatividad de la nube, será responsabilidad del proveedor y deberá ser previamente autorizada por la PSA.

9.4. El proveedor del almacenamiento remoto deberá garantizar la integridad de la información almacenada y, particularmente, de las imágenes, tal cual fueron producidas por el Sistema de CCTV de Seguridad, incluyendo las demarcaciones incorporadas a la imagen para su trazabilidad (marca de agua, fechado, números de cámaras, etc.).

9.5. Control administrativo: El proveedor del almacenamiento remoto deberá garantizar el acceso irrestrictico a la visualización, chequeo o descarga de la información, datos, archivos, gráficos, imágenes, videos, registros de procedimientos policiales, o cualquier documentación alojada. Asimismo,

deberá garantizar el control de asignación de distintos perfiles de acceso determinados por el responsable de administración del sistema.

9.6. Cumplimiento normativo: El proveedor de almacenamiento remoto deberá garantizar por escrito el cumplimiento de las regulaciones de privacidad vigentes que enmarquen a la información, datos, archivos, gráficos, imágenes, videos, registros de procedimientos policiales, o cualquier documentación ya sea escrita o gráfica, almacenada bajo su responsabilidad.

9.7. La PSA se reserva el derecho a decidir y administrar la jerarquía y el estatus de la información almacenada remotamente.

10. En la proyección de despliegue de cámaras, deberán considerarse también las características climáticas de la región donde se emplaza el aeropuerto, los accidentes del terreno, las particularidades de la infraestructura y los obstáculos visuales (naturales y artificiales).

11. Los parámetros podrán adaptarse de acuerdo a futuros escenarios y avances tecnológicos en materia de seguridad electrónica, procurando mantener o mejorar el nivel de cobertura adecuada de los objetivos.

12. Los registros fílmicos deberán disponer de la capacidad de ser compartidos entre diferentes operadores activos del sistema.

12.1. Se deberá disponer de los medios técnicos que posibiliten el manejo en simultaneo de múltiples monitores, los cuales permitan ampliar el patrullaje virtual, ponderando necesidades específicas, con el fin de dar prioridad a aquellos sectores considerados críticos o de mayor relevancia que ameriten la proyección de imágenes en más de UN (1) monitor en tiempo real.

12.2. El equipamiento deberá contar con la alternativa de sincronismo de escenas en reproducción de videos, con ajuste de calidad de visualización, acercamiento y captura de imagen.

13. Características Técnicas de las Grabadoras de Video Digital (DVR):

13.1. Deberá poseer como mínimo OCHO (8) canales analógicos.

13.2. Deberá ser compatible con la compresión de video H.265 o superior.

13.3. Admitir entradas de video HDCVI / AVH / TVI / CVBS / IP.

13.4. Deberá disponer de un mínimo de CUATRO (4) entradas de cámaras IP y cada canal de hasta SEIS (6) megapixeles.

13.5. Deberá soportar las resoluciones de pantalla 1920x1080, 1280x1024 y 1280x720, las cuales permitan apreciar de forma óptima los detalles en la visualización de imágenes.

13.6. Deberán tener una resolución de grabación mínima de MIL OCHENTA (1080) pixeles.

13.7. Deberá poseer UNA (1) entrada y UNA (1) salida de audio RCA.

13.8. Deberá poseer como mínimo UNA (1) salida de video tipo VGA y UNA (1) salida de video tipo HDMI.

13.9. Deberá poseer un puerto RJ-45 con capacidad mínima de transmisión de datos de CIEN (100) megabytes por segundo.

13.10. Deberá ser compatible con las siguientes funciones de red: HTTP, HTTPS, TCP / IP, IPv4 / IPv6, UPnP, RTSP, UDP, SMTP, NTP, DHCP, DNS, Filtro de IP, DDNS, FTP, Servidor de Alarma, P2P, Búsqueda de IP.

13.11. Deberá ser compatible con el Protocolo ONVIF (Open Network Video Interface Fórum).

13.12. El sistema de almacenamiento deberá ser compatible con discos tipo SATA de la mayor cantidad posible de terabytes de capacidad al momento de la puesta en funcionamiento del equipamiento.

13.13. Las dimensiones externas de la unidad DVR deberán ser directamente proporcionales a la proyección del sistema.

13.14. Se deberá incluir la fuente de alimentación (interna o externa) para poder conectarse directamente a la red de 220V/50Hz.

13.15. Se priorizarán grabadoras compatibles con interfaces inteligentes de vigilancia profesional, que permitan la integración de diferentes tipos y modelos de componentes de los Sistemas de CCTV de Seguridad en una sola interface de gestión y mantenimiento de dispositivos.

14. Características Técnicas de las Grabadoras de Video en Red (NVR):

14.1. Deberá poseer como mínimo OCHO (8) puertos tipo “Power Over Ethernet” (POE).

14.2. Deberá ser compatible con la compresión de video H265 o superior.

14.3. Deberá soportar las resoluciones de pantalla 1920x1080, 1280x1024 y 1280x720, las cuales permitan apreciar de forma óptima los detalles en la visualización de imágenes.

14.4. Deberán tener una resolución de grabación mínima de MIL OCHENTA (1080) pixeles.

14.5. Deberá poseer una entrada y una salida de audio RCA.

14.6. Deberá poseer como mínimo UNA (1) salida de video tipo VGA y UNA (1) salida de video tipo HDMI.

14.7. Deberá poseer un puerto RJ-45 con capacidad mínima de transmisión de datos de CIEN (100) megabytes por segundo.

14.8. Deberá ser compatible como mínimo con las siguientes funciones de red: HTTP, HTTPS, TCP / IP, IPv4 / IPv6, UPnP, RTSP, UDP, SMTP, NTP, DHCP, DNS, Filtro de IP, DDNS, FTP, Servidor de Alarma, P2P, Búsqueda de IP.

14.9. Deberá ser compatible con el Protocolo ONVIF (Open Network Video Interface Fórum).

14.10. El sistema de almacenamiento deberá ser compatible con discos tipo SATA de hasta SEIS (6) terabytes de capacidad cada uno.

14.11. Las dimensiones externas de la unidad DVR deberán ser directamente proporcionales a la proyección del sistema.

14.12. Se deberá incluir la fuente de alimentación (interna o externa) para poder conectarse directamente a la red de 220V/50Hz.

14.13. Se priorizarán grabadoras compatibles con interfaces inteligentes de vigilancia profesional, que permitan la integración de diferentes tipos y modelos de componentes de los Sistemas de CCTV de Seguridad en una sola interface de gestión y mantenimiento de dispositivos.

III. HERRAMIENTAS PARA LA OPERACIÓN TÉCNICA

15. Los Sistemas de CCTV de Seguridad deberán:

15.1. Disponer de las herramientas necesarias para realizar tareas del tipo forense o analíticas de posibles eventos que ameriten la intervención

del personal especializado (captura de pantalla, fotograma de rostro/s, con y sin acercamiento, incorporación de textos aclaratorios, extracción de imagen para posterior análisis, etcétera).

15.2. Contar con la posibilidad de generar exportación de videos y o imágenes de múltiples cámaras, de ser necesario en UN (1) solo archivo, con la debida encriptación o su correspondiente sello de agua, evitando así exportaciones en formatos que no garanticen la seguridad del tratamiento, de igual modo contar con la posibilidad de proteger datos mediante un sistema de contraseñas, las cuales deberán ser altamente robustas para los dispositivos, incorporando requisitos específicos de OCHO (8) caracteres alfanuméricos como mínimo, con uso de mayúsculas, minúsculas y caracteres especiales.

15.3. Poseer la capacidad de realizar búsquedas automatizadas según los siguientes parámetros:

15.3.1. Por detección de movimiento (de personas, de animales o por acción de la naturaleza).

15.3.2. Por imágenes, independientemente del tamaño de las mismas.

15.3.3. Por alerta (mediante sistemas de sensores de alarma pasivos).

15.3.4. Por marcadores programables por el/la operador/a.

15.3.5. Por eventos individuales.

15.3.6. Por eventos, independientemente de la cantidad de cámaras de vigilancia, que se encuentren en servicio.

15.3.7. Sin desatender alarmas o sensores.

15.4. Disponer de la opción de marcación por eventos previamente programables, que serán de activación según corresponda:

15.4.1. Manipulación de elementos técnicos para mitigar actos con posibles fines de sabotaje.

15.4.2. Ante la activación de ingresos digitales al sistema, ponderando los objetos que formen parte de una clasificación previamente estipulada, basados en estándares de vulnerabilidad de la seguridad aeroportuaria.

15.4.3. Ante eventos que ameriten ser atendidos según Protocolo ONVIF.

15.4.4. Ante la detección de objetos según clasificación de riesgo.

16. Las activaciones de alarmas simultáneas deberán verse reflejadas en las estaciones de trabajo.
17. La interface del sistema deberá representar la acumulación de avisos de alarmas en curso y el tiempo transcurrido entre su aparición y la intervención del operador de turno.
18. Las analíticas deberán ser propias (nativas) del proveedor del sistema.
19. El software deberá incorporar de manera automática la marca de agua en la imagen, con los datos de identificación del usuario que la está operando y otros datos que serán establecidos en cada proyecto en función de la seguridad.

IV. CENTROS OPERATIVOS DE CONTROL, ESTACIONES DE MONITOREO Y VIDEOWALLS

20. Los Sistemas de CCTV de Seguridad deberán proyectarse en Centros Operativos de Control (COC), bajo responsabilidad de las UOSP de la PSA.
21. En los COC convergerá toda la información de los diferentes componentes del Sistema de CCTV de Seguridad.

    21.1. Dentro del COC deberá delimitarse un espacio donde instalar la infraestructura de hardware necesaria para grabación, procesamiento y proyección de imágenes (racks, servidores, NVR, DVR, y todo otro componente que sirva para la recepción y tratamiento de imágenes). Dependiendo de la envergadura del Sistema de CCTV de Seguridad, el recinto de alojamiento de infraestructura de hardware podrá estar delimitado con tabiquería y accesos seguros o podrá estar dentro del mismo recinto en uno o más racks con medidas de seguridad.

22. Deberá propiciarse que en el COC converjan los sistemas de controles de acceso, alarmas de apertura de puertas, y todo otro sistema de seguridad electrónica contribuyente.

23. El COC estará conformado por:
    23.1. Puestos de monitoreo que se denominarán “Estaciones de Trabajo”.
    23.2. Puestos de supervisión.
    23.3. Sistemas de video-wall compuestos por pantallas tipo LED (o tecnología superior), de no menos de CUARENTA Y DOS (42) pulgadas cada una.
    23.4. Cableado estructurado y energía eléctrica acordes.
    23.5. Recinto aislado para análisis, forensia e investigaciones.
    23.6. Recinto tipo office para descanso de los operadores.
    23.7. Accesos restringidos y controlados electrónicamente.
    23.8. Dependiendo de la envergadura del Sistema de CCTV de Seguridad de cada aeropuerto, se establecerán los requisitos adecuados en cuanto a la cantidad de cada uno de los ítems que conforman el COC.
24. Las estaciones de trabajo se instalarán sobre escritorios ergonómicos de no menos de CIENTO VEINTE (120) centímetros de ancho por SETENTA (70) centímetros de profundidad y SETENTA (70) centímetros de altura.
25. Las sillas de los operadores deberán ser ergonómicas.
26. El COC deberá estar climatizado, protegido contra incendios e iluminado conforme las regulaciones aplicables a seguridad e higiene en el trabajo.
27. Las estaciones de trabajo y de supervisión deberán estar enlazadas en una interface unificada de manera tal que permita compartir toda la información del Sistema de CCTV de Seguridad en tiempo real, con las correspondientes autorizaciones según los niveles de usuario.
28. Cada estación de trabajo y de supervisión estará compuesta por:
    28.1. UNA (1) Unidad Central de Procesamiento (CPU), provista de TRES (3) salidas de video de alto rendimiento que soporte al menos DOS (2) monitores, con un flujo de visualización de hasta SETENTA Y DOS (72) cámaras.
    28.2. Arquitectura X86 de 64 bits.
    28.3. Setup residente en ROM con password de booteo y setup.
    28.4. Con contraseña de encendido por BIOS activable y configurable.
    28.5. Capacidad de booteo remoto a través de la conexión LAN.

28.6. Procesador no inferior al modelo “Core i7” si se oferta la marca “INTEL” o no inferior al modelo “Ryzen 7” si se oferta la marca “AMD”. Sin importar la marca o modelo ofertado, el procesador debe tener una antigüedad de lanzamiento al mercado internacional no mayor a VEINTICUATRO (24) meses.

28.7. VIDEO: Se admite que la unidad de procesamiento (CPU) incorpore el procesador gráfico (GPU) en el mismo chip, siempre que dicho GPU cuente con una controladora de video SVGA/XGA o superior, con soporte de resoluciones no inferiores a 1920x1080 (Full HD), con color de TREINTA Y DOS (32) bits o superior y acceso a no menos de DOSCIENTOS CINCUENTA Y SEIS (256) MB de RAM de video.

28.8. Memoria RAM no inferior a DIECISÉIS (16) GB, DDR4-2665 o superior.

28.9. DOS (2) unidades de discos duros. DISCO DURO PRINCIPAL: Disco duro tipo NVMe M.2 PCIe de no menos de DOSCIENTOS CUARENTA (240) GB, con una velocidad de no menos de MIL TRESCIENTOS CINCUENTA (1350) MB/segundo para lectura y no menos de OCHOCIENTOS CINCUENTA (850) MB/segundo para escritura. DISCO DURO SECUNDARIO: Disco duro magnético de no menos de UN (1) TB, con una velocidad de lectura y de escritura no menor a NOVENTA (90) MB/segundo.

28.10. Interfaz de red tipo Gigabit Ethernet autosensing (10/100/1000BaseT) con conectores tipo RJ-45.

28.11. Interfase de pantalla compatible con combinaciones de DVI, DP o HDMI.

28.12. DOS (2) DVI Conexiones de video digital.

28.13. UNA (1) unidad óptica DVD-RW.

28.14. Gateway (puerta de enlace), debe incluir IDRAC (para futuras actualizaciones).

28.15. La cantidad de monitores por cada estación de trabajo será definida en la instancia de evaluación particular de cada proyecto. Cada monitor deberá tener las siguientes características:

28.15.1. No menos de VEINTIÚN (21) pulgadas medida en diagonal.

28.15.2. Relación de aspecto ampliado (16:9) con resolución de no menos de 1920x1080 pixeles.

28.15.3. Interfaz de conexión HDMI.

28.15.4. Tiempo de respuesta no mayor a CINCO (5) milisegundos.

28.15.5. Brillo no inferior a DOSCIENTOS (200) cd/m².

28.15.6. Relación de contraste no menor de 450:1.

28.15.7. Ángulo de visión no menor a 160° horizontal y 160° vertical.

28.15.8. Alimentación eléctrica a 220V, 50Hz, con enchufe de TRES (3) patas planas (se proveerán los cables correspondientes para la alimentación eléctrica y la interconexión con la unidad central de proceso; la fuente será interna al gabinete).

28.15.9. La calidad del panel deberá cumplir con la norma “ISO-9241-302, 303, 305, 307:2008".

28.16. Al menos CUATRO (4) puertos USB 3.0 o superior. DOS (2) de ellos servirán a los efectos de conexión de periféricos (mouse y teclado) y se ubicarán en la parte posterior del CPU. DOS (2) de ellos servirán para conectar unidades de memoria USB y se ubicarán en la parte delantera del CPU. Deberá configurarse la posibilidad de habilitar y deshabilitar los puertos USB por parte de un usuario con perfil Administrador.

28.17. Unidad de lectura/escritura de DVD-RW. Deberá configurarse la posibilidad de habilitar y deshabilitar la unidad por parte de un usuario administrador.

28.18. UN (1) teclado tipo QWERTY que incluya función numérica.

28.19. UN (1) mouse con sensor de movimiento totalmente óptico, con rueda de scroll (rueda de desplazamiento).

28.20. Cualquier aspecto no contemplado para las estaciones de trabajo deberá basarse en los “Estándares Tecnológicos para la Administración Pública Nacional” (ETAP) de la Oficina Nacional de Tecnologías de Información (ONTI). Asimismo, cuando se produzcan mejoras técnicas y sean adoptadas por la ONTI a través de las ETAP se adoptará el nuevo estándar de manera automática.

29. Video Wall: por intermedio de la tercera salida de la unidad de procesamiento se deberá visualizar la proyección en conjunto de pantallas agrupadas para poder visualizar una o varias imágenes en un área mayor, permitiendo magnificar la visualización del patrullaje virtual.

29.1. Las características del video wall, como también la cantidad de pantallas que lo integran, serán definidas en la instancia de evaluación particular de cada proyecto.

V. SEGURIDAD DE REDES INFORMÁTICAS PARA SISTEMAS DE CCTV DE SEGURIDAD

30. El explotador o concesionario del aeropuerto donde se proyecte un Sistema de CCTV de Seguridad deberá incorporar a la proyección un informe conteniendo:
    30.1. La topología de red por la que circula la información producida por el Sistema de CCTV de Seguridad.
    30.2. Las medidas de seguridad informática aplicadas en dicha red.
31. La PSA evaluará dicho informe a través de la Dirección de Gestión Tecnológica y:
    31.1. lo aprobará, o
    31.2. lo desaprobará, realizando las recomendaciones necesarias para su aprobación, o
    31.3. requerirá la información complementaria que resulte necesaria para realizar la evaluación.
32. El resultado de la evaluación de la Dirección de Gestión Tecnológica será comunicado a la instancia del explotador del aeropuerto o concesionario que corresponda.
33. Toda alta, baja o modificación de los activos de los Sistemas de CCTV de Seguridad deberá ser informada a la Dirección de Gestión Tecnológica para su correspondiente evaluación, conteniendo los siguientes datos:
    33.1. Nombre del dispositivo.
    33.2. Dirección MAC (*MAC Address* en inglés, identificador único de 48 bits).
    33.3. Descripción del dispositivo.

34. Siempre que sea posible, al instalarse un Sistema de CCTV de Seguridad, la Dirección de Gestión Tecnológica deberá tener en cuenta los siguientes parámetros técnicos:

34.1. Se deberá diseñar una infraestructura de red que permita la segmentación física de la misma o una segmentación VLAN, *Virtual Local Area Network* (por su sigla en inglés), tanto como sea posible, lo que permitirá una división en varios segmentos o subredes que actúen como redes pequeñas; la Red VLAN deberá cumplir con la norma 7498-1 *Open Systems Interconnection* (“OSI” por su sigla en inglés) de la Organización Internacional de Estandarización (“ISO”, por su sigla en inglés).

34.2. La VLAN deberá comprender a los dispositivos de captación de imágenes, a las unidades de grabación (DVR, NVR o NDVR, según corresponda), a las estaciones de visualización y a las redes de administración de los Sistemas de CCTV de Seguridad, instalados en el aeropuerto.

34.3. La PSA podrá realizar la instalación de un cortafuego (*Firewall*), con el fin de controlar, monitorear y supervisar el acceso a los servidores y aplicaciones por las que deban pasar las conexiones entrantes y salientes de los Sistemas de CCTV de Seguridad.

34.4. Todos los activos de la VLAN de los Sistemas de CCTV deberán reportar *Network Time Protocol* (NTP), *Simple Network Management Protocol* (SNMP) y SySLOG a donde indique la Dirección de Gestión Tecnológica de la PSA.

34.5. Deberá disponerse un dispositivo específico para el resguardo de la información en caso de contingencias.

34.6. Se deberá contemplar la aplicación de una encriptación, ligera y parcial, o fuerte e integral, en el almacenamiento y en los archivos de los servidores de grabación, según resulte de la evaluación de riesgo.

34.7. Se deberá arbitrar los medios para que solo sean habilitados los puertos utilizados por el servidor VMS, y bloquear todos los demás puertos, incluidos los predeterminados en los sistemas operativos.

34.8. Se deberá verificar que cuando un usuario básico inicia sesión en el servidor de gestión, conforme al Protocolo de Seguridad, y no sea utilizado cualquier protocolo disponible.

34.9. Toda versión del Protocolo de Seguridad, deberá estar actualizado y se deberá dejar sin efecto cualquier versión obsoleta de Certificados de Seguridad TLS/SSL., (Transport Layer Segurity, “Secure Sockets Layer”).

34.10. Arbitrar los medios para bloquear los protocolos no seguros a nivel del sistema operativo (OS), evitando así el uso indebido de protocolos inseguros.

35. La Dirección de Gestión Tecnológica podrá convalidar una red informática para un Sistema de CCTV de Seguridad con características técnicas distintas a las indicadas en el presente, siempre que las mismas garanticen un estándar de seguridad adecuado al nivel de riesgo del aeropuerto.

VI. CAPACITACIÓN

36. Los proveedores de Sistemas de CCTV de Seguridad deberán mantener actualizada la información relativa a los mismos, e informar y proveer a la PSA de todas las herramientas disponibles a su alcance, en materia de capacitación, actualización, funcionamiento, despliegue, operación, optimización y rendimiento del sistema, quedando a su cargo la erogación de cualquier costo, si lo tuviere.
37. Las capacitaciones deberán abarcar mínimamente:
    37.1. La totalidad de los aspectos técnicos.
    37.2. El uso adecuado y proactivo de las herramientas.
    37.3. La resolución de problemas técnicos al nivel de software.
38. Las capacitaciones deberán ser dictadas por personal idóneo y experimentado en el uso y aprovechamiento al máximo del sistema.

39. La duración de las capacitaciones no podrá ser inferior a DIECIOCHO (18) horas reloj divididas en TRES (3) días, para la cantidad de personal que esta PSA disponga en cada implementación, independientemente del personal capacitado que pertenezca a explotadores o concesionarios.
40. El proveedor deberá emitir las certificaciones correspondientes a las capacitaciones dictadas.

VII. ACTUALIZACIONES Y LICENCIAS

41. Toda actualización u homologación disponible para los Sistemas de CCTV de Seguridad deberá ser informada por el proveedor, a los efectos de mantener vigente el sistema de seguridad virtual, sin que ello modifique o altere el normal funcionamiento del video patrullaje.
42. Las licencias deberán ser nativas del sistema, con el fin de evitar posibles vulneraciones y a los efectos de proteger el Sistema de Gestión de Video (VMS).
    42.1. Las licencias deberán ser de opción automática o manual, quedando a criterio del usuario responsable la decisión de la aplicación de la opción más conveniente.
43. Deberá ponerse a disposición de la PSA la cantidad de licencias adecuadas para una operación óptima del sistema, en función de la cantidad de Operadores/as que se determine.
44. El proveedor del sistema deberá garantizar la disponibilidad de licencias adicionales cuando sea necesario incrementar la cantidad de Operadores/as y estaciones de monitoreo/análisis.
45. El proveedor deberá informar a la PSA, todas las acciones posibles de realizar con el Sistema de Gestión de Video (VMS).

VIII. POLÍTICAS COMERCIALES DE LOS PROVEEDORES DE SISTEMAS DE CCTV DE SEGURIDAD

46. Toda empresa oferente que pretenda proveer un Sistema de CCTV de Seguridad en el Sistema Nacional de Aeropuertos (SNA) deberá explicitar en su oferta su política comercial en cuanto a:
    46.1. Capacitación y asistencia técnica (permanente o a demanda).
    46.2. Provisión de licencias.
    46.3. Provisión de actualizaciones y mejoras técnicas.
47. Todo proveedor de un Sistema de CCTV de Seguridad en el SNA deberá garantizar asumir la responsabilidad completa por la totalidad de los aspectos técnicos, contractuales, de mantenimiento, de capacitación, de licencias y actualizaciones, de hardware y de software del sistema ofrecido, no pudiendo derivar responsabilidades en terceros o empresas o personal técnico subcontratados.

República Argentina - Poder Ejecutivo Nacional
AÑO DE LA DEFENSA DE LA VIDA, LA LIBERTAD Y LA PROPIEDAD

Hoja Adicional de Firmas
Informe gráfico

Número: IF-2024-117278160-APN-DCPP#PSA

JOSE MARIA EZEIZA, BUENOS AIRES
Viernes 25 de Octubre de 2024

Referencia: ANEXO II - REGLAMENTO GENERAL DE SISTEMAS DE CIRCUITO CERRADO DE TELEVISIÓN (PÚBLICO) - EX-2023-118079040-APN-DCPP#PSA.

El documento fue importado por el sistema GEDO con un total de 55 pagina/s.

Digitally signed by GESTION DOCUMENTAL ELECTRONICA - GDE
Date: 2024.10.25 17:39:42 -03:00

Carlos Gabriel Marrapodi
Director
Dirección de Control Policial Preventivo
Policía de Seguridad Aeroportuaria

Digitally signed by GESTION DOCUMENTAL ELECTRONICA - GDE
Date: 2024.10.25 17:39:43 -03:00