Pregunta 10: ¿Qué protocolos de seguridad, privacidad y confidencialidad serán utilizados a efectos de mantener la privacidad de la información recopilada desde su captura hasta su procesamiento?

La fuerza de seguridad respeta la confidencialidad y el personal deberá mantener estricta reserva, confidencialidad y sigilo respecto de toda información, ya sea por planes, desarrollos, proyectos y/o trabajos realizados o a realizarse, de los que tome conocimiento durante su desempeño laboral, como así también respecto de su tarea específica, y de aquellas que le sean requeridas por autoridad competente.

El personal tampoco difundirá ni divulgará, la información que obtenga al realizar su trabajo, bajo ningún concepto, a terceros ajenos al ámbito del lugar de su tarea habitual, a excepción del aviso de emergencia que corresponda conforme el protocolo de actuación del área.

Como manifestamos anteriormente respecto a las prohibiciones, el personal conoce perfectamente que está terminantemente prohibido sustraer información de cualquier soporte y por cualquier método para ser utilizada con otros fines distintos a los propios del área, dada la naturaleza y el carácter de relevancia y exclusividad que denota la misma para el Centro de Monitoreo Urbano.

Además, se estipuló en la normativa vigente que en el caso de incumplimiento de la declaración jurada de confidencialidad será pasible de las sanciones dispuestas en la reglamentación correspondiente (Ley Nº 5.688 y Decreto 53/17); como así también la aplicación de la normativa vigente que correspondiere al caso.

Al respecto, los operadores que visualizan las cámaras que poseen reconocimiento facial, tienen suscrito una “Declaración Jurada de Confidencialidad” conociendo la normativa vigente respecto a la video vigilancia, los convenios celebrados y prohibiciones al respecto.

La declaración jurada de confidencialidad dispone que compromete a guardar secreto aún después del retiro o baja de la institución en todo cuanto se relacione con los asuntos del

servicio que, por su naturaleza, o en virtud de disposiciones especiales, impongan esa conducta, salvo requerimiento judicial (Ley Nº 5688/16, artículo 109, Punto 10 – Personal Policial – y artículo 255, Punto 7 – Personal Civil –).

Pregunta 13: ¿Qué técnica de borrado es utilizada? ¿Cómo se audita y de qué manera se asegura que las imágenes son efectivamente eliminadas?

En el caso de las imágenes que no generan coincidencias con los rostros contenidos en la base de los buscados, se realiza una liberación forzosa de la memoria sin producirse registro de la imagen en el sistema. En específico, se efectúa el proceso denominado "dispose", cuyo objeto se remite a la liberación forzosa de la memoria.

Por añadidura, el sistema posee óptimas barreras de seguridad informática y física, ya que se encuentra alojado en su la sede ministerial, el cual cumple con las mayores restricciones de acceso. Asimismo, el sistema se encuentra aislado de todas las redes del Ministerio y, por añadidura, la actualización de la información en dicho sistema se realiza mediante un protocolo, el cual mantiene la base de datos -de donde se obtiene la información de prófugos- aislada física y lógicamente del sistema de reconocimiento facial de prófugos.

Cabe destacar que la empresa proveedora del servicio aloja los servidores que brindan la infraestructura necesaria en la sala cofre de este Ministerio y los mismo se encuentran aislados en una red de datos privada. Es menester destacar que la empresa nombrada cuenta a su vez con certificación ISO 27001, la cual implica procesos constantes de auditoría externa por un organismo internacional.

Pregunta 44: ¿En qué tipo de aparatos reciben las alertas generadas por el sistema los agentes de la Policía? ¿En qué momentos los agentes destruyen aquellos archivos que le fueron enviados a esos aparatos? ¿Qué sistema o protocolo de seguridad se sigue para la protección de esos datos generados y transmitidos? y ¿Cómo se audita su correcta destrucción?

Como se mencionara precedentemente, los dispositivos utilizados son Smartphone con tecnología 4G; sistema operativo Android de la marca Samsung -en sus diferentes modelos-, están interconectados a la red del MJYS a través de un APN provista por la firma Telefónica de Argentina S.A. Estos equipos tienen instalado el sistema MDA y Airwatch, lo que hace que el mismo no tenga ningún tipo de conexión hacia otras redes de datos que no sea lo provisto por este Ministerio. Una vez procesadas las alertas positivas, estas se eliminan del equipo de forma automática

Las alertas emitidas no son almacenadas en los dispositivos móviles. Las mismas se guardan en el servidor central y son consultadas de manera remota por los teléfonos institucionales (POC) y/o empujada desde el servidor central a estos dispositivos.

La información de las alertas no reside en la memoria permanente del dispositivo móvil, es por ello que dicho evento no requiere un proceso de auditoría a tal fin.

Pregunta 45: ¿A través de qué sistema les llegan las alertas generada a los Policías? ¿Qué información les es remitida?

Mediante la aplicación móvil UltraIP VMS – Face ID, la cual permite a los usuarios (interventores asignados a estas tareas) tener disponible la información remitida desde la central de alertas en tiempo real. Dicha comunicación, se realiza por medio del protocolo HTTPS y Signal R.

Esta aplicación muestra a los usuarios las alertas de identificación con la siguiente información por cada una de ellas:

- Nombre de la cámara (Fuente: sistema de gestión e identificación UltraIP).
- Fecha y hora (sistema de gestión e identificación UltraIP).
- Imagen de la persona en el momento de la identificación (sistema de gestión e identificación UltraIP).
- Imagen de la persona enrolada (Fuente: base de datos RENAPER)

- Nombre y DNI (Fuente: base de datos pública CONARC)
- Detalle del motivo del pedido de captura (Fuente: base de datos pública CONARC)
- Juzgado interventor (Fuente: base de datos pública CONARC)

47) ¿cuántos agentes reciben esta información?

En lo que respecta a la pregunta en cuestión, tal como fuera informado oportunamente cabe poner de resalto que únicamente los agentes destinados a los puntos donde se encuentra instalado el SRFP tienen acceso al sistema de alerta y no la totalidad de la fuerza.

En cuanto al número, éste es variable dependiendo de múltiples factores tenidos en cuenta al momento del despliegue territorial. Se trata en definitiva de información dinámica variando en forma constante.

52) ¿Cuántas de las personas detenidas o demoradas, con causa en el levantamiento de una alerta por el Sistema de Reconocimiento Facial, no estaban siendo buscadas por un "delito grave"? Se remite a la definición de "delito grave" utilizada en el anexo de la resolución Resolución 1068 - E/2016.

El Ministerio de Justicia y Seguridad efectúa consulta sobre la base de datos pública del CONARC.

El sistema no permite realizar un filtrado particular acorde lo solicitado en el presente cuestionario.

Asimismo, se debe tener presente que la información general que pueda aportarnos el Sistema de Reconocimiento Facial de Prófugos, va ir fluctuando desde la puesta en marcha del mismo.

Respecto a la interpretación de los delitos graves, este órgano no es competente para conceptuar o definir los mismos.

Por su parte la Resolución 1068 – E/2016 y su Anexo respectivo, procede a crear el sistema los más buscados, de acuerdo a los delitos graves previstos en el Código Penal Argentino de la Nación.

En virtud de lo anterior, se enuncia que, desde abril de 2019 (periodo en que se implementó el Sistema de Reconocimiento Facial de Prófugos), 2.048 personas fueron identificadas y puestas a disposición de la Justicia, entre quienes eran buscados por delitos contra la propiedad, contra las personas, contra la libertad, contra la ley de estupefacientes y contra la integridad sexual, contra la fe pública, entre otros, englobando figuras típicas como el homicidio doloso, el abuso sexual y la estafa.

53) Por el contrario, ¿Cuántas personas han sido detenidas con causa en el levantamiento de una alerta por el Sistema de Reconocimiento Facial de Prófugos, que estaban siendo buscadas por haber cometido un "delito grave"?

Remítase al punto 52).

Pregunta 58: Para el caso de que la empresa [DANAIDE S.A., a quien se adjudicó directamente el contrato administrativo tendiente a desarrollar el SRFP] entre en concurso, quiebra o cualquier otra forma reglamentaria dc liquidación, o esta sufra algún contratiempo ya sea técnico o administrativo, ¿Se ha previsto algún tipo de control de crisis para proteger los datos de los ciudadanos?

Los datos de los ciudadanos se encuentran protegidos dado que los sistemas y la base de datos correspondiente se encuentran alojados y administrados en servidores propios del Ministerio de Justicia y Seguridad de la Ciudad Autónoma de Buenos Aires. Los mismo se hallan físicamente en instalaciones ministeriales y son gestionados por personal de la Subsecretaría de Tecnología e Informática. En el caso de generarse una crisis, el personal de este Ministerio procederá a la ejecución del protocolo de contingencia el cual procede, en primera instancia, a restringir los accesos físicos a los servidores.

Por añadidura, el sistema posee óptimas barreras de seguridad informática y física, ya que se encuentra alojado en su la sede ministerial, el cual cumple con las mayores restricciones de acceso. Asimismo, el sistema se encuentra aislado de todas las redes del

Ministerio y, por añadidura, la actualización de la información en dicho sistema se realiza mediante un protocolo, el cual mantiene la base de datos -de donde se obtiene la información de prófugos- aislada física y lógicamente del sistema de reconocimiento facial de prófugos.

61) ¿Qué método de detección de rostros se utilizó? En caso de utilizar redes neuronales, ¿qué modelo/arquitectura se utilizó y cuál fue el set de datos que se utilizó para entrenar el modelo?

En relación a los patrones de identificación que hacen al funcionamiento del sistema, se hace saber que corresponde al código fuente, sobre el cual el GCABA no es dueño, y el desarrollador no revela. El objeto de la contratación se remite a la implementación de un servicio, no a la adquisición del software. El mismo incluye 300 licencias de uso, de operación simultánea y rotativa, conteniendo la arquitectura técnica, mantenimiento preventivo y correctivo del software y la arquitectura técnica asociada. Al no ser el propietario de la solución informática, el GCABA no tiene acceso a los recursos que se vieron involucrados en su programación.

62) ¿Qué datasets fueron utilizados para ese entrenamiento?

De igual modo que ante la consulta 61), se destaca que esta información corresponde al desarrollo del producto y es un detalle que posee el copyright de la licencia del mismo, por lo cual no se posee acceso a esta información.

Pregunta 67: ¿Se ha hecho una auditoría del software por un tercero independiente?

La Universidad Nacional de La Plata, entidad pública autárquica y autónoma, se encuentra realizando un proceso de auditoría sobre el software. Los ejes del análisis son la seguridad de las comunicaciones y la información generada.

Por otra parte, la empresa proveedora del Sistema, en la actualidad se encuentra certificada conforme ISO 27001, la cual se trata de una norma internacional que permite

el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan. Así también se encuentra certificada conforme ISO 9001 la cual se trata de una norma de estándar internacional que se centra en la eficacia de los Sistemas de Gestión de la Calidad.

Por su parte, el Centro de Monitoreo Urbano (CMU), quien gestiona operativamente el Sistema, se encuentra certificado en ISO 9001.

De manera complementaria, el tratamiento de la información que se genera a través del SRFP se enmarca en lo dispuesto en la Ley de Seguridad Pública de la Ciudad de Buenos Aires (Ley N° 5.688) y en los regímenes nacionales y locales específicos, sujeto al régimen de penalidades en vigencia.

Asimismo, como corolario del principio de transparencia en el ejercicio de las funciones públicas y dando intervención a un órgano constitucional de control de ejercicio de las funciones de las autoridades administrativas incluidas las fuerzas de seguridad local, la misma resolución creadora del SRFP invitó a la Defensoría del Pueblo de la Ciudad Autónoma de Buenos Aires a auditar su funcionamiento.

Para ello, la Secretaría de Justicia y Seguridad y la Defensoría del Pueblo de la Ciudad Autónoma de Buenos Aires han suscripto un Convenio Marco de Colaboración con el objeto de salvaguardar los derechos fundamentales de todas las personas, en particular la intimidad y expectativa de privacidad en la vía pública. Todo ello con el único objetivo de generar la confianza pública suficiente respecto del uso correcto de este sistema y su aplicación respetuosa respecto a los derechos individuales de los ciudadanos.

De esta manera se aprobó un Protocolo de Actuación para el cual el Ministerio de Justicia y Seguridad de la Ciudad facilita a la Defensoría el acceso a los ámbitos institucionales correspondientes sea en la sede de la Policía de la Ciudad a través de entrevistas a actores claves, visita al CMU y compulsa de documentación. Estos trabajos podrán ser publicados ya sea de manera individual o conjunta por cualquiera de las partes. Todo ello, se viene

llevando adelante, producto de lo cual los resultados fueron progresivamente mejorando optimizándose.

Pregunta 76: Asimismo, se han detectado ciertas expresiones en el llamado "Pliego de Especificaciones Técnicas del Servicio de Análisis Integral de Video" obscuras y poco claras que a continuación señalaremos y sobre las cuales solicitamos cierta información: Con respecto al Punto 1. (Objeto): "[…] Dicho servicio tendrá como objetivo el análisis integral en tiempo real sobre imágenes de video en vivo para la detección facial de personas buscadas basada en bases de datos de imágenes de rostros y de análisis integral de video para la detección de diferentes patrones de comportamiento y cambios de condiciones ambientales. El servicio será prestado sobre todas las cámaras de video vigilancia que técnicamente lo permitan, como así también a las imágenes almacenadas en los sistemas de resguardo de imágenes, al momento de la presentación de su oferta […]" "[…] Las imágenes captadas que generen algún tipo de alerta como toda la información vinculada a la misma, deberán ser guardada de forma encriptada para futuros análisis […]" "[…] Contar con una base de datos fotográfica de hasta cien mil (100.000) rostros para su posterior identificación formando una lista negra de personas buscadas […]"(EI destacado es nuestro).

En virtud de promover una mejor comprensión de las características técnicas enunciadas en el pliego técnico de referencia, es meritorio advertir que el objeto de la presente licitación pública corresponde a tres (3) sistemas divergentes -Sistema Forense, Sistema Predictivo y Sistema de Reconocimiento Facial de Prófugos- de análisis de imágenes de video y gestión de alertas sobre los registros fílmicos en tiempo real y el análisis de imágenes almacenadas.

a. ¿Qué se quiso decir con "detección de diferentes patrones de comportamiento"?

El proceso de licitación tuvo por objeto contar con una herramienta tecnológica para la identificación de distintos eventos relacionados con el análisis inteligente de imágenes de video en tiempo real. Se entiende por patrón de comportamiento, a una pluralidad de reglas que pueden ser configuradas en el sistema a fin de poder identificar ciertas conductas y/o indicadores

anómalos en una escena. El sistema predictivo de referencia nuclea los siguientes patrones de comportamiento de análisis de imágenes, a saber:

- Objetivo moviéndose en un área de interés predefinida durante un tiempo determinado.
- Objetivo cruzando una línea predeterminada en un sentido determinado o en ambos.
- Vehículo detenido en un área de interés predefinida por un período de tiempo predefinido.
- Concentración de un número de personas, a ser definido por el operador, en un área de interés predefinida, durante un período de tiempo definido.
- Objeto abandonado en una zona de interés. Dicha zona y el tiempo de permanencia del objeto deberá ser definida por los operadores del sistema.

b. ¿Qué se quiso decir con "cambios de condiciones ambientales"?

Se pretendió que el software pueda soportar los cambios de entorno de la escena (cambios de iluminación, emplazamiento de dispositivo, condiciones climáticas, entre otros), y, de esta forma, garantizar el correcto funcionamiento del análisis de video.

c. ¿Cuál es la cantidad de cámaras instaladas en la vía pública pertenecientes al gobierno de la Ciudad Autónoma de buenos Aires y de la Policía de la Ciudad?

Al 21 de enero del 2022, El Ministerio de Justicia y Seguridad de la Ciudad Autónoma de Buenos Aires posee 11.784 dispositivos de video entre el parque propio de este organismo y dispositivos integrados con otras agencias de gobierno. Es relevante destacar que el Ministerio se encuentra en un proceso de instalación de cámaras progresivo.

d. ¿Qué cantidad de esas cámaras permiten utilizar el software de reconocimiento facial?

El SRFP permite la aplicación del software sobre la totalidad de dispositivos que poseen tecnología 4K, pertenecientes al Sistema de Videovigilancia del Ministerio de Justicia y Seguridad de la Ciudad

Autónoma de Buenos Aires. El mismo incluye 300 licencias de uso, de operación simultánea y rotativa.

e. ¿Qué tipo de encriptación se utiliza para el almacenamiento de esas imágenes que generen alertas?

Se utiliza el estándar de encriptación AES con clave de 256 bits para el almacenamiento de los eventos.

f. ¿En qué consisten esos "futuros análisis" que se mencionan?

Contar con el historial de eventos permite brindar la información necesaria, en caso de que sea requerida, como sustento de procesos judiciales o con fines estadísticos/operativos y auditables.

g. ¿Durante cuánto tiempo se guardarán dichas imágenes?

Las imágenes se guardan solo en casos de alerta positiva durante Sesenta (60) días corridos de acuerdo a lo estipulado en el artículo 484 de la Ley Nº 5.688/16 (B.O. Nº 5030 de fecha 21/12/2016) y Decreto reglamentario Nº 312-MJYSGC/18 (B.O. N° 5464 de fecha 25/9/2018).

h. ¿Dónde se encuentran físicamente los servidores donde se almacena la información del registro resultante entre la inclusión de la base de datos de la CONARC con la del RENAPER, y la información de la estructura facial del rostro capturado por las cámaras instaladas en la vía pública de la Ciudad?

Se encuentra ubicada en la sede central del Ministerio de Justicia y Seguridad de la Ciudad de Buenos Aires, en la correspondiente sala cofre.

i. ¿Qué protocolos de seguridad son utilizados para el almacenamiento de la información del registro resultante entre la base de datos de la CONARC y el RENAPER, y lo grabado por las cámaras instaladas en la vía pública de la Ciudad?

La información del evento puede ser, únicamente, accedida por medio del sistema centralizado de gestión de video UltraIP (plataforma de visualización de imágenes) mediante un usuario autorizado con los niveles de permisos acorde a las tareas que se requiera realizar. Cabe destacar que, el sistema registra la totalidad de las acciones de los usuarios, lo cual garantiza la trazabilidad y el seguimiento de las actividades realizadas por cada uno de los usuarios del sistema. A su vez,

este se encuentra encriptado como se mencionó anteriormente. Asimismo, el lugar de almacenamiento de la información se encuentra en servidores dentro de la sala cofre del Ministerio de Justicia y Seguridad de CABA, que cuenta con sistemas de seguridad electrónica (control de acceso biométrico, video vigilancia, mecanismos de extinción de incendios, entre otros).

j. ¿Quién realiza esta llamada "lista negra"?

El Sistema de Reconocimiento Facial de Prófugos opera con los registros que están incorporados en la base de datos del CONARC (Consulta Nacional de Rebeldías y Capturas) y, de forma excepcional, se integra también con los requerimientos judiciales específicos que deviene del poder judicial. Lo antes mencionado, genera la "lista negra" con la cual opera el Sistema de Reconocimiento Facial de Prófugos.

k. ¿Cómo y que procedimiento se utiliza para la confección de la llamada "lista negra"?

La confección se realiza diariamente por medio de un software desarrollado por la Subsecretaría de Tecnología e Informática de este Ministerio, el cual realiza la actualización de la información (altas y bajas de registro de prófugos) verificando las novedades publicadas en la CONARC (Consulta Nacional de Rebeldías y Capturas). A su vez, este proceso cuenta con una verificación de datos previo a su incorporación.

l. ¿Cuántas personas hay en esta lista?

Los registros están contenidos en la CONARC (Consulta Nacional de Rebeldías y Capturas) y la cantidad de los mismos varia en conformidad a la altas y bajas diarias de registros de prófugos que realiza el Ministerio de Justicia y Derechos Humanos de la Nación.

m. ¿Cuál es el criterio que se sigue para ingresar y/ egresar de esta lista?

Los ingresos y egresos dependen de las actualizaciones de la CONARC (Consulta Nacional de Rebeldías y Capturas) y/o requerimientos judiciales.

n. ¿Quién tiene permiso para modificar esta lista? ¿Qué parámetros o requisitos pide el sistema a efectos de modificar la lista?

Los registros de prófugos son actualizados por la CONARC (Consulta Nacional de Rebeldías y Capturas) de manera diaria. Estas actualizaciones impactan automáticamente con un software de este Ministerio el cual refleja dichas actualizaciones en la lista en cuestión.

V.15. Pregunta 77: En el mismo pliego se ha hecho una serie de manifestaciones genéricas que, dado el efecto que la interpretación que las mismas tendrían en los derechos fundamentales de las personas, hacen de suma importancia que se aclare. Así, se ha establecido los siguientes requisitos: `[…] Ante eventos repetitivos, el sistema deberá enmascarar automáticamente dichos eventos a modo de optimizar la visualización de operadores y proveer de información de notificaciones eficientemente […]´ `[…] El sistema deberá considerar áreas de enmascaramiento tanto dentro como fuera de la zona de detección para así evitar falsos positivos. […]´ `[…] El sistema deberá tener una historia de los eventos con toda la información necesaria para su comprensión: imagen y posibilidad de reproducción de la grabación alrededor del tiempo en que el evento ocurrió […]´ `[…] El sistema deberá tener la capacidad de purga periódica de datos acumulados, considerando su antigüedad. […]´ `[…] El sistema deberá considerar dos (2) niveles

de permisos: Uno limitado a la visualización de datos y otro con disponibilidad para todas operaciones. […]´ `[…] El sistema no deberá superar la detección de falsos positivos en un 15% del total de los eventos detectados […]´ `[…]. Persona que cruza una línea […]´ `[…] Persona moviéndose en un área: ante la detección de una persona en una zona estéril definida previamente […]´ `[…] Hacinamiento: alerta por la detección de una cierta cantidad de personas detectadas durante una cierta cantidad de tiempo. […]´ ` […] Acercamiento entre personas: alerta ante la detección de un cruce de línea de una segunda persona en un tiempo menor al

definido en la regla. […]´ `[…] Merodeo: alerta por personas residiendo en una zona durante un tiempo mínimo definido y comportándose de una manera sospechosa que respalde la credibilidad de que su objetivo es una actividad delictiva […]´ `[…] Ocupación: alerta ante la detección de un límite de personas definidas para un área. […]´ ` […] El sistema deberá permitir configurar una tolerancia sobre las búsquedas, permitiendo y aceptando posibles falsos positivos para la obtención de información […]´ `[…] A su vez, deberá permitir la detección de la emoción del rostro (feliz, sorprendido, neutral, triste, miedo, enojo y disgusto). […]´ `[…] Deberá permitir la indexación masiva de dalos de video, registrando la información de todas las personas que aparecen, permitiendo una búsqueda dinámica y veloz de las personas de interés. […]´…

En virtud de promover una mejor comprensión de las características técnicas enunciadas en el pliego técnico de referencia, es meritorio advertir que el objeto de la presente licitación pública corresponde a tres (3) sistemas divergentes -Sistema Forense, Sistema Predictivo y Sistema de Reconocimiento Facial de Prófugos- de análisis de imágenes de video y gestión de alertas sobre los registros fílmicos en tiempo real y el análisis de imágenes almacenadas.

a. ¿Qué se considera como un "evento repetitivo" y qué criterios se utilizan para definirlo?

Se considerarán eventos repetitivos aquellos donde un mismo indicador identificable se reitera repetidamente. El sistema garantiza la no reiteración de estas alertas a fin de poder optimizar la gestión y operación del evento, evitando que el operador reciba una pluralidad de alertas sobre el mismo hecho.

b. ¿En qué consiste un "Área de Enmascaramiento" y como puede su consideración evitar "falsos positivos"?

El área de enmascaramiento es una zona que se puede definir en la escena, la cual permanece excluida del análisis de video. Mediante este proceso se evitan zonas de la escena que afecten la identificación debido a diferencia de contrastes, contraluces, destellos o cualquier otra condición que afecte el análisis de video.

c. ¿A qué se refiere con "zonas de detección"? ¿Cuáles son estas zonas?

La zona de detección es un área que puede ser definida con el objetivo de acotar la escena de análisis a una porción del área total visualizada.

d. ¿A qué se refiere con historia de los eventos? ¿Qué información se almacena? ¿Dónde es almacenada esta información? ¿Quién tiene acceso a esa información y por cuánto tiempo?

La historia de eventos se refiere a la historia de identificaciones que realiza el sistema, las cuales son guardadas con su propio "*time stamp*", dispositivo de captura, tipo de alerta, reglas identificadas, intersecciones, franja horaria de detección del evento, entre otros. Esta información se guarda en un repositorio de datos del Ministerio de Justicia y Seguridad de la Ciudad Autónoma de Buenos Aires. Sólo tienen acceso a esta información los usuarios autorizados del sistema con los privilegios suficientes para acceder a la misma.

e. ¿Qué información se considera como "purgable"? ¿Dónde se almacena esa información? ¿Cuáles los plazos máximos y mínimos que se consideran a efectos de realizar esa purga?

Se consideran purgables los eventos de identificación que realiza el sistema que no resulta en alerta positiva. Las imágenes se guardan solo en casos de alerta positiva durante Sesenta (60) días corridos de acuerdo a lo estipulado en el artículo 484 de la Ley Nº 5.688/16 (B.O. Nº 5030 de fecha 21/12/2016) y Decreto reglamentario Nº 312-MJYSGC/18 (B.O. N° 5464 de fecha 25/9/2018).

f. ¿Cuántos usuarios con los dos distintos permisos existen? ¿Qué cantidad de usuarios están limitados a la visualización de los datos? ¿Cuántos usuarios existen con total disponibilidad para todas las operaciones? ¿Quién otorga estos permisos? ¿De qué manera y con qué criterio se otorgan esos permisos?

Los usuarios que poseen los dos tipos de permisos son 10 (diez); 4 (cuatro) administradores correspondientes al área técnica del Centro de Monitoreo Urbano y 6 (seis) asignados a la operación.

Los usuarios que poseen permisos para visualización de los datos son 10 (diez), estos son operadores de la sala del Centro de Monitoreo Urbano. No existen usuarios que posean sólo disponibilidad a las operaciones sin la visualización de los datos correspondientes.

Los permisos son otorgados por el comisario a cargo del Centro de Monitoreo Urbano, conforme a criterios operativos de la Policía de la Ciudad.

g. ¿Cuáles son la totalidad de las operaciones?

Se refiere a las distintas acciones que puede realizar un usuario dentro la plataforma de gestión de video UltraIP de la Policía de la Ciudad; como ser operación, visualización, gestión de imágenes y/o administrador del sistema. Cabe destacar, que el borrado de imágenes o eventos de forma manual se encuentra imposibilitada por el sistema.

h. ¿Qué criterio se utilizó a efectos de considerar que un 15% de falsos positivos era un porcentaje aceptable?

Este porcentaje se definió en base a un promedio de error en las detecciones de Sistemas con características análogas. Sin embargo, en virtud de lo expuesto, cabe destacar que, desde los últimos ajustes en la configuración del sistema que se efectuaron en septiembre de 2019.

i. ¿Quién determina las líneas virtuales mencionadas, y dónde se encuentran dichas líneas?

Estas configuraciones las determina un analista según la escena que se visualiza y el análisis delictual que se requiera. Para ello, el analista define una línea imaginaria sobre el campo visual del dispositivo de video a fin de detectar comportamientos anómalos para la seguridad pública. *Véase respuesta 76 (a).*

j. ¿A qué se refiere con "zona estéril"?

Una "zona estéril" es un área donde no debería detentarse circulación de personas, vehículos y/u objetos.

k. ¿Cuál es la cantidad (mínima) de personas y durante cuánto tiempo (mínimo) es necesario para que este se considere Como hacinamiento?

Ambos parámetros -cantidad de personas y tiempo- son configurables y gestionables por el analista conforme a la necesidad operativa policial. Esta regla permite mensurar el aforo en un área determinada y si el mismo se mantiene durante el tiempo que se haya prefijado en el sistema.

l. ¿En qué condiciones puede suceder un cruce de línea que implique un "acercamiento entre personas"? ¿Cuál es la utilidad práctica de esta categoría?

Estando configurado y seteado el sistema, atendiendo a la escena bajo análisis, el tiempo entre dos alertas por cruce de línea (en el mismo sentido) puede determinar cuan cerca se hallan dos objetos/sujetos consecutivos. Si se conoce estadísticamente el flujo de objetos en la escena, puede determinarse o preverse, saturaciones o prever posibles hechos delictivos.

m. ¿Cuánta es la cantidad mínima de personas necesarias para que se dé un caso de "merodeo"?

La mínima cantidad de personas sería una (1). Entendemos por "merodeo" el comportamiento de una persona que este vagando en una zona o "vigilando" algún objeto o lugar, una sola persona es suficiente para poner en sobre alerta a quien corresponda, evitando por ejemplo casos de vandalismo.

n. ¿Qué se considera como "comportándose de una manera sospechosa"? ¿Cuáles son las actividades puntuales que el sistema está entrenado para reconocer? ¿Cómo se puede prever una actividad delictiva cuando se da este supuesto?

Se considera “comportamiento sospechoso” se detecta algún comportamiento anómalo para la seguridad pública. Ciertos paramentos de análisis de imágenes, permiten advertir y prevenir posibles acometimientos delictivos. Véase respuesta 76 (a) a fin de extender información en relación a las reglas de configuración que permite el sistema preventivo.

o. ¿En qué consiste el presupuesto de "ocupación"? ¿Cuántas personas se necesitan como mínimo en un área para que se configure la ocupación? ¿Cuáles son los presupuestos fácticos de forma detallada para que se configure la ocupación? ¿Cuáles son aquellas áreas pasibles de ocupación?

Se considera al “presupuesto de ocupación” como la cantidad de personas necesarias para alcanzar una relación definida entre el área observada y el número de individuos dentro de esa área.

Dichos parámetros (área y cantidad de personas) deben ser configuradas dependiendo el tipo de escena y el umbral de densidad de ocupación.

Siempre se debe considerar cada escena en particular, en cada una de ellas el “presupuesto de ocupación” puede diferir. Ej: en un ascensor el presupuesto podría ser de cuatro (4) personas, mientras que, en el hall de entrada del edificio, el presupuesto podría ser de diez (10) personas.

En conformidad con lo antedicho, cualquier área es posible ser ocupada, ya que, como se mencionó, se preestablece el número de personas permitidas en el área en cuestión. Se debe actuar con criterio evaluando siempre la escena.

p. ¿En qué consiste la "tolerancia a los falsos positivos" mencionada?

El sistema permite la configuración de umbrales de confiabilidad para la identificación de prófugos cargados en la base de datos de CONARC (Consulta Nacional de Rebeldías y Capturas), donde la escala permite niveles de confiabilidad en las identificaciones.

q. ¿Con que fin se recolecta la información acerca de la detección de emoción en el rostro de las personas? ¿Por qué se necesita detectar la emoción del rostro de las personas cuando el sistema sería utilizado exclusivamente para la detección de prófugos?

La detección de emociones no ha sido activada en la plataforma. El requerimiento expresado en el pliego técnico de referencia tiene como único objeto mensurar la eficiencia de la capacidad de identificación del sistema.

r. ¿En qué consiste la indexación mencionada? ¿Qué se considera como "persona de interés? ¿Por qué razón se necesitaría registrar aquella información de estas "personas de interés"?"

Cabe advertir que esta referencia técnica corresponde al Sistema Forense, el cual tiene como objetivo la realización de búsquedas de objetos, personas y/o vehículos utilizando imágenes de video almacenadas por los dispositivos de captura del sistema de videovigilancia urbana del Ministerio de Justicia y Seguridad del GCBA, permitiendo realizar filtros relacionados con el color, morfología de elementos, sentido de desplazamiento, rango temporal especifico, entre otros. Esta tecnología tiene por objeto dotar de las herramientas necesarias para la realización de procesos de análisis sobre imágenes de video históricas de forma eficiente y asistida, minimizando los tiempos de búsqueda y optimizando los recursos asignados a tareas de naturaleza forense e investigativa.

G O B I E R N O DE LA C I U D A D DE B U E N O S A I R E S
"2022 - Año del 40° Aniversario de la Guerra de Malvinas. En homenaje a los veteranos y caídos en la defensa de las Islas Malvinas y el Atlántico Sur"

Hoja Adicional de Firmas
Informe gráfico

Número: IF-2022-06075098-GCABA-DGADTI

Buenos Aires, Jueves 3 de Febrero de 2022

Referencia: S/ Respuestas_Tecnicas_SRFP

El documento fue importado por el sistema GEDO con un total de 17 pagina/s.

Digitally signed by Comunicaciones Oficiales
DN: cn=Comunicaciones Oficiales
Date: 2022.02.03 20:08:29 -03'00'

Sisti Andres
Director General
D.G. ACTIVOS DIGITALES TECNOLOGIA E INFORMATICA
MINISTERIO DE JUSTICIA Y SEGURIDAD

Digitally signed by Comunicaciones Oficiales
DN: cn=Comunicaciones Oficiales
Date: 2022.02.03 20:08:30 -03'00'