ANEXO III

Aeropuerto Internacional Rosario "Islas Malvinas"

SAAR

"ESPECIFICACIONES TÉCNICAS PARA LA PROVISIÓN DE CONTROLES DE ACCESO"

AEROPUERTO INTERNACIONAL ROSARIO ISLAS MALVINAS

Elaboró	Revisó	Controló	Aprobó
Anal.Sist. Uriel Ripani Jefe Departamento TI - AIR	Anal.Sist. Uriel Ripani Jefe Departamento TI - AIR		

Especificaciones Técnicas para un Sistema de Gestión Centralizada de Control de Accesos (SGCAC)

SECCIÓN I: REQUISITOS GENERALES Y ALCANCE

1. Objeto del Suministro

El presente documento tiene por objeto establecer las especificaciones técnicas mínimas para el diseño, suministro, instalación, prueba, puesta en marcha y mantenimiento de un Sistema de Gestión Centralizada de Control de Accesos (SGCAC) para 92 accesos del Aeropuerto Internacional Rosario. El sistema debe ser una solución llave en mano que proporcione gestión de seguridad centralizada, control integrado y monitoreo remoto para la totalidad del sitio.

1.2. Conformidad y Modularidad

El SGCAC debe ser de arquitectura abierta, basado en Servidor. El diseño debe ser modular, ofreciendo la flexibilidad de agregar o eliminar componentes y/o funciones controladas a medida que cambien los requisitos operativos o se expanda el sistema. El sistema debe ser diseñado para permitir cambios organizacionales y procedimentales previsibles, y la adición de unidades de hardware adicionales debe ser posible sin modificar la configuración existente de hardware, software o red.

1.3. Capacidad Operacional y Escalabilidad

El sistema propuesto deberá ser un sistema multi-tarea y multi-usuario. El sistema debe ser escalable para soportar, como mínimo, las siguientes capacidades:

- Número de tarjetahabientes activos: **50.000**
- Número de lectores: **1.000**

- Número de grupos de acceso: **255**
- Número de estaciones de trabajo operando concurrentemente: **80**

1.4. Interfaz de Usuario y Localización

El software de aplicación del SGCAC (AS) debe ser robusto, confiable y de fácil uso, requiriendo una capacitación mínima para el operador. El AS debe ofrecer descripciones y mensajes en español, además de soportar otros idiomas como inglés, alemán, francés, etc. El sistema deberá proporcionar una Interfaz Gráfica de Usuario (GUI) con visor de mapas (Map Viewer) para el monitoreo y control.

1.5. Norma EN60839

Tanto el SGCAC como el hardware de operación del sistema (Controladoras y fuentes de alimentación) deben conformar la norma EN60839 para sistemas de acceso.

SECCIÓN II: ARQUITECTURA Y COMUNICACIONES DEL SISTEMA

2.1. Topología General del Sistema

La figura 1 muestra la topología general del sistema.

2.2. Estructura del Servidor y Requisitos de Sistema Operativo

El sistema operativo del servidor del SGCAC debe ser robusto y seguro, soportando las versiones más recientes como Windows Server 2022 o 2025. El software cliente (estación de trabajo del operador) debe ser compatible con

sistemas operativos de escritorio modernos como Windows 11 Professional y Enterprise.

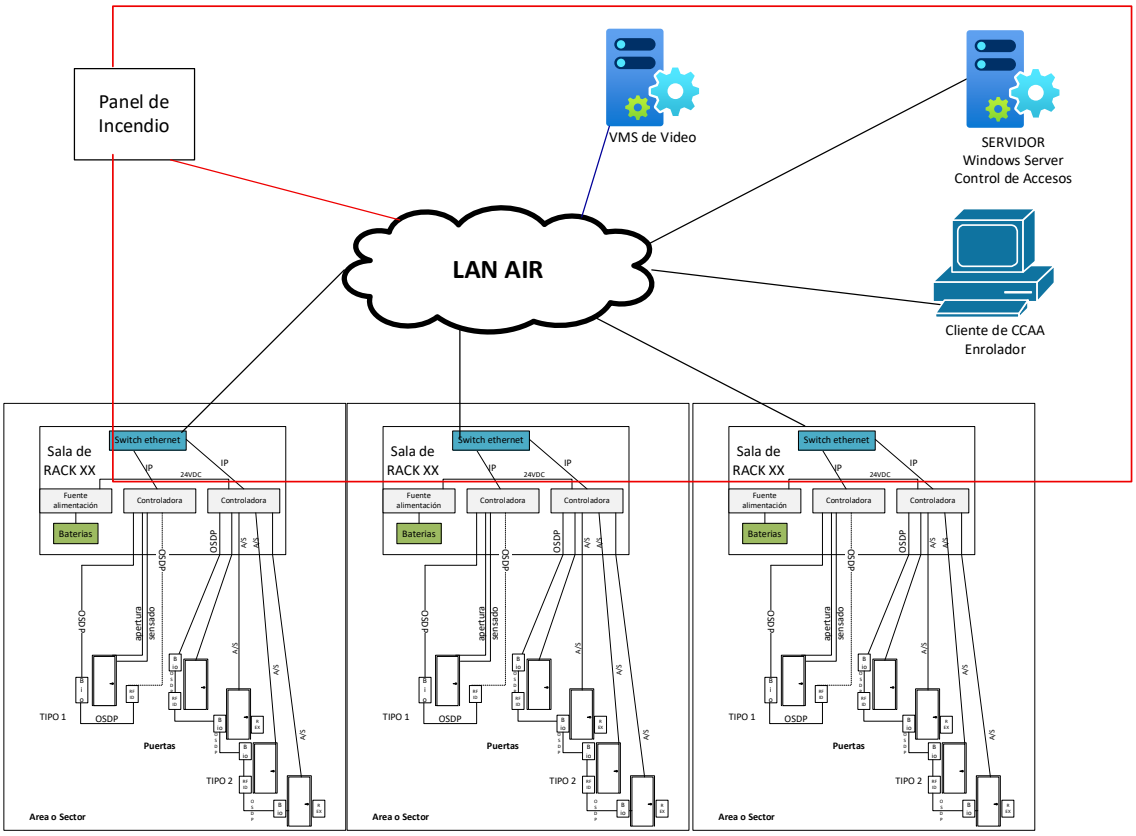

Figura 1: Topología solicitada

2.3. Bases de Datos y Rendimiento

El SGCAC debe utilizar una arquitectura que separe el almacenamiento de la información crítica de la gestión de eventos, buscando optimizar el rendimiento y reducir la carga de la base de datos principal.

Base de Datos Principal (SQL)

El sistema debe utilizar un servidor de base de datos SQL moderno para el almacenamiento de datos transaccionales, de configuración y de usuarios.

Almacenamiento de Eventos (No SQL)

Elaboró	Revisó	Controló	Aprobó
Anal.Sist. Uriel Ripani Jefe Departamento TI - AIR	Anal.Sist. Uriel Ripani Jefe Departamento TI - AIR		

Los datos de eventos del sistema (como eventos de acceso o bloqueos de SSO) no deben almacenarse en el servidor SQL. En su lugar, deben ser gestionados por un motor de búsqueda e indexación basado en archivos incluido en el sistema.

Beneficio de Rendimiento

Esta separación debe lograr un rendimiento mejorado en la recuperación de eventos (hasta 10 veces más rápido) y una reducción en el espacio de almacenamiento.

Registro de Eventos

El número máximo de eventos registrados debe estar limitado por el espacio en disco duro disponible del servidor en lugar de las limitaciones de la base de datos SQL. Por defecto, los eventos del sistema (incluyendo los eventos de auditoría y entrada) deben tener un tiempo de retención configurable (por defecto 30 días), que puede ser ajustado para gestionar el tamaño de los archivos de backup.

Diseñador de Credenciales

En el producto se incluye la personalización de tarjetas, que permite diseñar acreditaciones, realizar adquisiciones de imágenes con cámara USB y utilizar las impresoras de tarjetas más comunes del mercado.

2.4. Seguridad en la Comunicación y Autenticación

La seguridad de las comunicaciones debe ser reforzada en múltiples niveles:

Cifrado de Cliente-Servidor

La protección de la conexión entre el cliente y el servidor debe ser mejorada. El sistema debe garantizar que los programas que utilicen interfaces de desarrollo

de software (SDK) antiguos no puedan conectarse al servidor, forzando el uso de la última versión del SDK para la conectividad.

Single Sign-On (SSO)

El sistema debe soportar la integración con proveedores de identidad externos (IdP), permitiendo que los usuarios de estos IdPs se autentiquen como operadores dentro del SGCAC.

Debe permitir la asignación de perfiles a estos operadores mediante Mapeo de Perfiles Basado en Roles (gestión externa) o asignación manual tras la primera autenticación.

Separación de API para Acceso Móvil (Mobile Access API Splitting)

Para fortalecer la seguridad de TI, la interfaz de programación de aplicaciones (API) para credenciales virtuales y gestión de visitantes debe dividirse en dos canales:

- **Canal Frontal (Front-channel/Registro):** Comunicación con dispositivos móviles. Este canal debe configurarse para ser accesible desde fuera, con un puerto separado (ej. 5700 por defecto) para permitir reglas de firewall específicas para el tráfico móvil.
- **Canal Trasero (Back-channel/Administrativo):** Comunicación con la Gestión de Credenciales y la Gestión de Visitantes. Este canal debe configurarse como seguro y restringido, permitiendo la comunicación solo con la máquina del servidor SGCAC (ej. 5701 por defecto).

2.5. Tolerancia a Fallos

El sistema debe estar diseñado para que las fallas locales no impliquen la falla de todo el sistema. Los controladores de acceso local deberán continuar operando incluso si falla la conexión de red con el software de gestión.

SECCIÓN III: ESPECIFICACIONES DE HARDWARE DE CONTROL DE ACCESO

3.1. Requisitos Generales del Controlador

El hardware de control de acceso (Controladores de Acceso Local – LAC o Controladores de Acceso Maestro – MAC) debe ser de diseño modular y soportar la instalación en racks de 19" o rieles.

3.2. Conectividad y Protocolos

El controlador debe estar equipado con interfaces comunes, como Ethernet y RS-485, para la conexión al SGCAC.

- El hardware de control de acceso deberá admitir la conectividad de hasta un máximo de **8 lectores** de interfaz serial que operen sobre tecnología de bus RS485.
- La comunicación entre el controlador y los lectores debe utilizar el protocolo de comunicación seguro **OSDP** "Open Supervised Device Protocol" (Protocolo Abierto de Dispositivos Supervisados) basado en la interfaz serial (RS485) para garantizar la integridad de los datos y la supervisión de la conexión.

3.3. Funcionalidad Autónoma (Off-line)

Los controladores de acceso y todos los dispositivos conectados a ellos deben continuar operando y controlando el acceso en modo fuera de línea (off-line) si la red de comunicación o la gestión central falla.

- La memoria del controlador debe almacenar una base de datos con una capacidad mínima de **50.000 tarjetahabientes**.
- El hardware de control debe incluir una tarjeta de memoria **Compact Flash (CF)** para almacenar datos de tarjetahabientes y eventos de

acceso. Esta tarjeta CF debe estar formateada con un sistema de archivos FAT estándar para permitir la lectura de datos mediante un lector de tarjetas estándar en caso de fallo del hardware.

- El controlador de acceso no debe perder una sola transacción, ni siquiera la última, en caso de fallo de alimentación.
- El controlador deberá estar alimentado por una Fuente Cargador de baterías, y esta fuente deberá ser supervisada por el Sistema (por lo tanto de la misma marca que el controlador), reportando status de las baterías y temperatura.
- Se deberá equipar cada fuente con **2 baterías VRLA de PbCa, de 12V 9Ah**.

3.4. Conectividad Segura del Host

La comunicación entre el servidor central (Host) y los controladores de acceso (AMC/MAC) deberá realizarse exclusivamente a través de la red IP/Ethernet.
Con la implementación del soporte de seguridad avanzado (DTLS), el controlador ya no deberá soportar conexiones RS485 o RS232 entre el Host (servidor) y el controlador de acceso (AMC). Esta conexión debe ser puramente IP para asegurar el cifrado de extremo a extremo.

SECCIÓN IV: ESPECIFICACIONES DE LECTORES Y BIOMETRÍA

4.1. Requisitos Físicos del Lector Biométrico

Los lectores biométricos deben ser de diseño robusto y estar sellados en una carcasa resistente a la intemperie (policarbonato o similar) para soportar ambientes hostiles para uso tanto en interiores como en exteriores, proporcionando un alto grado de resistencia al vandalismo.

Elaboró	Revisó	Controló	Aprobó
Anal.Sist. Uriel Ripani Jefe Departamento TI - AIR	Anal.Sist. Uriel Ripani Jefe Departamento TI - AIR		

Especificaciones técnicas:

- 1:10,000 user identification in 1 second
- 30,000 templates, 250,000 IDs in authorized user list, 1 million logs
- Fake finger detection, duress finger, timed anti-pass back
- IP65 rated and vandal resistant (IK08)
- Prox, iCLASS or MIFARE DESFire

4.2. Autenticación y Modos de Operación

El lector biométrico debe proporcionar autenticación de doble factor, combinando una tarjeta de proximidad/tarjeta inteligente sin contacto y la biometría de huella dactilar (FP).

El lector biométrico, junto con la tarjeta, deberá soportar los siguientes modos de operación:

- Modo de Verificación **1:1**
- Modo de Identificación **1:N**

4.3. Especificaciones de Captura Biométrica (Huella Dactilar)

Para la identificación de huella dactilar, se requiere que el lector biométrico:

- Utilice técnicas de verificación capacitiva para el reconocimiento de dedo vivo y resistencia de la piel humana.
- La imagen de la huella dactilar capturada debe tener una resolución mínima de **500 ppp**.
- Se permitirá asignar hasta un máximo de **10 plantillas** de huella dactilar a un solo usuario.
- Las plantillas biométricas deben almacenarse en la base de datos centralizada del SGCAC o en la memoria del lector.
- Es un requisito fundamental para la privacidad de los datos que las imágenes reales de las huellas dactilares capturadas **no se almacenen**.

4.4. Integración de la Inscripción Biométrica

El enrolamiento de plantillas biométricas (como huellas dactilares o imágenes de venas de la palma) debe estar completamente integrado en la Interfaz de Usuario del SGCAC sin la necesidad de software de terceros. El mismo lector biométrico utilizado para el control de acceso debe poder utilizarse también como estación de enrolamiento.

4.5. Requisito de Protocolo Seguro para Lectores Periféricos (OSDP-SC)

La comunicación de baja capa entre los controladores de acceso y los dispositivos lectores (incluyendo los biométricos) a través de la interfaz serial (RS485) debe soportar un protocolo de comunicación supervisado y seguro de dispositivo periférico (Open Supervised Device Protocol - OSDP), incluyendo el Canal Seguro (Secure Channel).

SECCIÓN V: REQUISITOS DE SOFTWARE DE GESTIÓN DE ACCESO

5.1. Gestión de Tarjetahabientes

El software debe permitir la inscripción de credenciales electrónicas (tarjetas, fobs) a través de lectores de control de acceso conectados al controlador (LAC) o mediante lectores USB.

- Una persona puede tener asignadas hasta **cinco tarjetas** a la vez.
- Se deben soportar hasta **tres tipos de códigos PIN** para cada tarjetahabiente (PIN de Verificación, PIN de Identificación, PIN de Armado), con una longitud configurable de 4 a 8 dígitos.

5.2. Funciones de Seguridad Avanzada

El software deberá incluir las siguientes funcionalidades de seguridad:

Gestión de Nivel de Amenaza

Debe ser posible pre-configurar al menos **15 niveles de amenaza** diferentes para activación instantánea en caso de emergencia.

Doble o Múltiple Acceso Autorizado

Posibilidad de requerir que dos o más tarjetahabientes autorizados presenten sus credenciales consecutivamente para permitir el acceso.

Alarma de Código de Coacción (Duress Code)

Se debe generar una alarma si un tarjetahabiente introduce su PIN en orden inverso, o de alguna otra manera predefinida.

Revisión Aleatoria (Random Screening)

La funcionalidad de revisión aleatoria debe estar disponible para seleccionar personas al azar para controles de seguridad adicionales. El sistema debe bloquear automáticamente al tarjetahabiente seleccionado hasta que el guardia reinicie manualmente el bloqueo en el software de control de acceso.

5.3. Gestión de Credenciales Virtuales y Visitantes

El SGCAC debe ofrecer módulos integrados para:

Gestión de Credenciales Virtuales (Acceso Móvil)

Solución para permitir el uso de credenciales virtuales seguras a través de smartphones.

Gestión de Visitantes

Software de gestión de visitantes que optimiza el proceso de registro para operadores y visitantes, el cual se sincroniza de forma optimizada con el SGCAC central para garantizar la precisión de los datos.

Integración de Gestión de Llaves

El sistema debe integrarse con sistemas de gestión de armarios de llaves externos, incluyendo la capacidad de soportar la comunicación y la transferencia de datos de tarjetas cifrados para múltiples formatos.

5.4. Integración de Subsistemas

El SGCAC debe ser capaz de integrarse con otros subsistemas de seguridad:

Integración de Video

El sistema debe integrarse con un mínimo de **2 sistemas diferentes** de gestión de video (VMS) para proporcionar funciones como:

- Verificación de video en vivo (comparación de imagen de la base de datos con la transmisión en vivo de la cámara durante el acceso).
- Seguimiento Forense de Personas (búsqueda rápida de videos grabados asociados a las acciones de entrada de una persona).

Integración Biometría

El sistema deberá soportar la identificación y verificación biométrica, incluyendo el reconocimiento de huellas dactilares y el reconocimiento facial de diferentes proveedores.

Integración de Intrusión

El SGCAC debe ser capaz de integrarse con paneles de detección de intrusión (IDS), soportando hasta **50 paneles** para comando y control. La gestión de usuarios (hasta 2000 usuarios de panel) debe centralizarse en el SGCAC. La

comunicación entre el SGCAC y los paneles de intrusión debe realizarse a través de una Interfaz de Programación de Aplicaciones (API) específica.

5.5. Visor de Mapas y Alarmas

El sistema debe contener un visor de mapas para la presentación gráfica de las instalaciones mediante planos de planta.

- En los mapas, los dispositivos (controladores, lectores, entradas/salidas) deben posicionarse como iconos dinámicos que muestren la ubicación y el estado real del dispositivo.
- En caso de alarma, el mapa se centrará automáticamente en la ubicación de la alarma.
- El software deberá registrar de forma segura todos los eventos y acciones del operador en los archivos de registro de alarmas/eventos para evitar manipulaciones. Los eventos comunes a registrar incluyen, pero no se limitan a: Tarjeta desconocida, Tarjeta no autorizada, Alarma de coacción, Puerta abierta por tiempo excesivo, y Tamper del lector/controlador.

5.6. Reportes y Documentación

Módulo Avanzado de Reportes

Se requiere un módulo dedicado a la Gestión de Reportes diseñado para optimizar la creación y personalización de reportes (incluidos los de tiempo y asistencia). Este módulo debe soportar la marca corporativa consistente, ser multi-idioma y contar con medidas de seguridad.

5.7. Tarjetas para Usuarios

Se deberán proveer una cantidad de **3000 tarjetas de proximidad RFID, Mifare 13,5MHz**.

Elaboró	Revisó	Controló	Aprobó
Anal.Sist. Uriel Ripani Jefe Departamento TI - AIR	Anal.Sist. Uriel Ripani Jefe Departamento TI - AIR		

Todos los productos deberán certificar **UL, CE**.

SECCIÓN VI: EQUIPAMIENTO COMPLEMENTARIO

6.1. Impresora de Tarjetas

HID FARGO modelo de referencia.

6.2. PC de Administración

Especificaciones MÍNIMAS de PC clientes:

- CPU Intel Core i7-8700 @ 3,2 GHz (6 cores, 12 logical)
- RAM 8 GB (2667 MHz)
- Disco de instalación: SSD
- Sistema operativo Microsoft Windows 11
- GPU Intel UHD Graphics 630 (4GB GPU memory)

6.3. Servidor

Especificaciones MÍNIMAS del Servidor:

- CPU Intel Xeon E-2144G @ 3,6GHz (4 cores, 8 logical)
- RAM 32 GB (2667 MHz)
- Disco de sistema NVMe
    - Velocidad de escritura: 1440MB/s
    - Velocidad de lectura: 2250MB/s
- Disco de instalación: SSD
    - Velocidad de escritura: 1000MB/s
    - Velocidad de lectura: 100MB/s
- Sistema operativo Microsoft Server 2022/2025 Standard Edition

SECCIÓN VII: HARDWARE DE SEGURIDAD FÍSICA

7.1. Cerraduras para Rack Server

Para los controles de acceso de rack servers se deberán cambiar cerraduras de los racks existentes Schneider Easy Server, tanto de las puertas delanteras como de las traseras, por cerraduras con lector incorporado de RFID compatibles con monitoreo de puertas. Tipo **ASSA ABLOY modelo KS210**.

No se permitirán el uso de retenciones magnéticas que alteren la geometría y estructuras de los racks, debilitándolos o sacrificando unidades operativas de rack.

7.2. Brazos Empuje para Puertas

Deberán de uso profesional de alto tránsito con apertura de 90° mínimo con traba, para puertas de 60 a 80kgs. Modelo de referencia **ASSA ABLOY**.

7.3. Retenciones Magnéticas

Las retenciones magnéticas se deberán instalar con sus respectivos accesorios según el tipo de puerta, y de deberán tener una capacidad de **280kg**, y contar con sensor de apertura por contacto seco integrado a la retención.

SECCIÓN VIII: INTEGRACIÓN CON SISTEMAS DE EMERGENCIA

8.0. Integración

Se deberá proveer de un sistema basado en hardware, que comandado por la central de incendios permita la liberación de puertas por zonas, sin que esto genere un corte de energía en la alimentación de las controladoras y el evento debe quedar registrado en la base de datos del sistema.

Elaboró	Revisó	Controló	Aprobó
Anal.Sist. Uriel Ripani Jefe Departamento TI - AIR	Anal.Sist. Uriel Ripani Jefe Departamento TI - AIR		

La cantidad de zonas o subsectores se estima en una cantidad de **10**.

Deberá permitir también la instalación de pulsadores tipo golpe de puño con retención o rompa el vidrio con llaves para objetivos de evacuación por cualquier otro motivo.